



Matcom Office of Public Safety LLC

PUBLIC ACCOUNTABILITY & TRANSPARENCY
PORTAL

MD Security License: 24PLU-
SGPD4620

24/7 Dispatch: 1-855-715-9911

POLICIES & ACCOUNTABILITY

Public Accountability & Transparency Standard Operating Procedures
(SOP Master Index)

**Effective
Date:**

August 13,
2026

**Approving
Authority:**

Dr. Brian C. Askew,
CEO

**Directives
Count:**

40 Public SOPs +
Charter

**NAICS
Code:**

561612

PUBLIC PORTAL MASTER DIRECTIVE INDEX

Welcome to the Matcom Office of Public Safety LLC Public Accountability & Transparency Standard Operating Procedures Master Index. MATCOM is committed to full operational openness, ethical security governance, and public accountability. To ensure community access and institutional transparency, all 40 public-facing Standard Operating Procedures (SOP-PUB series) are published in full below, categorized into five key operational domains.

i Cross-Category Indexing Note: Certain Standard Operating Procedures (e.g., SOP-PUB-07, SOP-PUB-08, SOP-PUB-16, SOP-PUB-18, SOP-PUB-19, SOP-PUB-20, SOP-PUB-30, and SOP-PUB-39) address multi-faceted topics spanning evidence handling, privacy, records requests, public rights, and administrative oversight. Consequently, these directives appear in multiple functional categories in this index to ensure complete navigational accessibility.

CATEGORY 1 TRANSPARENCY 20 Directives		
Policies governing what MATCOM publishes publicly, open data releases, data accuracy, privacy protections, and public reporting mechanisms.		
DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-01	Public Transparency & Open Data Policy	PUBLIC RELEASE
SOP-PUB-02	Public Calls-for-Service Information Release	PUBLIC RELEASE
SOP-PUB-03	Sensitive Incident & Address Suppression Privacy	PUBLIC RELEASE
SOP-PUB-15	Public Records, Privacy & Confidential Information	PUBLIC RELEASE
SOP-PUB-16	Public Records Request Procedure MPIA	PUBLIC RELEASE
SOP-PUB-17	Transparency Portal Data Correction Procedure	PUBLIC RELEASE
SOP-PUB-18	Public Emergency vs. Non-Emergency Reporting Rights	PUBLIC RELEASE
SOP-PUB-23	Officer/Employee Identification & Public Information	PUBLIC RELEASE
SOP-PUB-24	Public Transparency Dashboard Statistics	PUBLIC RELEASE
SOP-PUB-25	Public Use-of-Force Transparency	PUBLIC RELEASE

DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-26	Public Pursuit & Emergency Vehicle Transparency	PUBLIC RELEASE
SOP-PUB-27	Early Intervention System Public Explanation	PUBLIC RELEASE
SOP-PUB-28	Public Policy & Directive Library	PUBLIC RELEASE
SOP-PUB-29	Website & Public Portal Terms of Use	PUBLIC RELEASE
SOP-PUB-30	Public Portal Privacy Notice & Data Collection Privacy	PUBLIC RELEASE
SOP-PUB-36	Public Communication During Critical Incidents	PUBLIC RELEASE
SOP-PUB-37	Media & Public Information Release	PUBLIC RELEASE
SOP-PUB-38	Transparency Portal Audit & Accountability	PUBLIC RELEASE
SOP-PUB-39	Records Retention for Complaints, Commendations & Evidence Records	PUBLIC RELEASE
SOP-PUB-40	Public Accountability Annual Report	PUBLIC RELEASE

CATEGORY 2 COMPLAINTS & INTERNAL AFFAIRS 16 Directives		
Policies governing how complaints are received, assigned tracking numbers, investigated, classified, and resolved through objective Internal Affairs procedures.		
DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-04	Public Complaint Intake & Acceptance	PUBLIC RELEASE
SOP-PUB-06	Complaint Case Number & Tracking Procedure	PUBLIC RELEASE
SOP-PUB-07	Public Evidence Submission & Supplemental Evidence Evidence	PUBLIC RELEASE
SOP-PUB-08	Evidence Integrity & Chain of Custody Evidence	PUBLIC RELEASE
SOP-PUB-09	Complaint Classification & Referral	PUBLIC RELEASE
SOP-PUB-10	Internal Affairs Investigation Process	PUBLIC RELEASE
SOP-PUB-11	Criminal Misconduct Referral Procedure	PUBLIC RELEASE
SOP-PUB-12	Complaint Findings & Dispositions	PUBLIC RELEASE
SOP-PUB-13	Complaint Response, Notification & Final Letter	PUBLIC RELEASE
SOP-PUB-14	Complaint Review, Approval & Quality Assurance	PUBLIC RELEASE

DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-19	Anonymous & Confidential Complaint Procedure Rights	PUBLIC RELEASE
SOP-PUB-20	Anti-Retaliation & Complainant Protection Rights	PUBLIC RELEASE
SOP-PUB-32	Complaint Withdrawal & Continued Investigation	PUBLIC RELEASE
SOP-PUB-33	External Agency Referral & Jurisdictional Complaints	PUBLIC RELEASE
SOP-PUB-34	Conflict of Interest & Independent Review	PUBLIC RELEASE
SOP-PUB-35	Complaint Investigation Timelines & Delayed Cases	PUBLIC RELEASE

CATEGORY 3 COMMENDATIONS & COMMUNITY RELATIONS 2 Directives		
Formal recognition programs, employee praise intake, and community feedback pathways for non-misconduct concerns or general service inquiries.		
DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-05	Public Commendation & Employee Praise Program	PUBLIC RELEASE
SOP-PUB-22	Community Feedback & Service Concern Resolution	PUBLIC RELEASE

CATEGORY 4

EVIDENCE & RECORDS

6 Directives

Policies governing how digital evidence, photos, audio/video recordings, public records, and portal submissions are securely submitted, preserved, managed, and disclosed.

DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
SOP-PUB-07	Public Evidence Submission & Supplemental Evidence Internal Affairs	PUBLIC RELEASE
SOP-PUB-08	Evidence Integrity & Chain of Custody Internal Affairs	PUBLIC RELEASE
SOP-PUB-16	Public Records Request Procedure Transparency	PUBLIC RELEASE
SOP-PUB-30	Public Portal Privacy Notice & Data Collection Transparency	PUBLIC RELEASE
SOP-PUB-31	Cybersecurity & Fraudulent Submission Protection	PUBLIC RELEASE
SOP-PUB-39	Records Retention for Complaints, Commendations & Evidence Transparency	PUBLIC RELEASE

CATEGORY 5 RIGHTS & ACCESSIBILITY 5 Primary Directives		
Directives guaranteeing citizen rights, anti-retaliation protections, anonymous reporting pathways, disability accommodations, Title VI language assistance, and emergency routing protocols.		
DIRECTIVE CODE	STANDARD OPERATING PROCEDURE TITLE	PUBLIC STATUS
CHARTER	MATCOM Public Bill of Rights Featured Charter	PUBLIC CHARTER
SOP-PUB-18	Public Emergency vs. Non-Emergency Reporting Transparency	PUBLIC RELEASE
SOP-PUB-19	Anonymous & Confidential Complaint Procedure Internal Affairs	PUBLIC RELEASE
SOP-PUB-20	Anti-Retaliation & Complainant Protection Internal Affairs	PUBLIC RELEASE
SOP-PUB-21	Accessibility, Disability Accommodation & Language Access ADA / Title VI	PUBLIC RELEASE

STATUTORY GOVERNING FRAMEWORK
MPIA Compliance: State Gov't Art. § 4-101 et seq.
MD Licensing: COMAR 12.10.01 & 12.10.02
Security Guards Act: Bus. Reg. Title 12 Subtitle 1
Police Accountability: MD Police Accountability Act of 2022

MPCTC Standards: COMAR Title 12 Subtitle 12

Language & Disability Access: Title VI & ADA / Section 504

NOTE: All SOPs listed in this index are classified as PUBLIC and are available for inspection and download on the portal. Security-sensitive operational directives, tactical blueprints, and protective site specifics are exempt from public release pursuant to SOP-PUB-28 and MPIA § 4-351.

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207

Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | 24/7 Dispatch: 1-855-715-9911

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed, Exp. Jan 31, 2028) | NAICS: 561612 | Effective Date: August 13, 2026



MATCOM OFFICE OF PUBLIC SAFETY LLC

MATCOM PUBLIC BILL OF RIGHTS

Your Rights When Interacting with the Matcom Office of Public
Safety

**Effective
Date:** August 13,
2026

**Approving
Authority:**

Dr. Brian C. Askew,
CEO

**MD Security Guard
License:** 24PLU-
SGPD4620

**24/7
Dispatch:** 1-855-715-9911



♦ PREAMBLE & ORGANIZATION COMMITMENT

The Matcom Office of Public Safety LLC is dedicated to maintaining the highest standards of professional integrity, public trust, and constitutional accountability across all protective, security, and public safety operations. We recognize that public trust is earned through transparency, objective self-oversight, unwavering adherence to Maryland

and federal law, and respectful engagement with every member of the community we serve.

This Public Bill of Rights serves as our binding public charter. It guarantees that every individual interacting with MATCOM personnel—whether as a client, visitor, witness, complainant, or member of the general public—possesses clear, enforceable rights to voice concerns, request records, commend exceptional service, and receive impartial, retaliatory-free administrative reviews.

FUNDAMENTAL PUBLIC RIGHTS

1

File a Complaint Without Intimidation or Retaliation

You have the absolute right to report misconduct, voice concerns, or file an administrative complaint regarding the conduct, performance, or service of any MATCOM employee, armed/unarmed security officer, or contractor. MATCOM strictly prohibits any form of retaliation, coercion, harassment, or intimidation against any individual who files a complaint or participates in an investigation.

LEGAL & POLICY AUTHORITY:

MD Police Accountability Act of 2022

COMAR 12.10.01

SOP-PUB-04

SOP-PUB-20

2

Submit a Commendation or Positive Recognition

You have the right to commend exceptional service, professionalism, integrity, or lifesaving actions demonstrated by MATCOM personnel. All public commendations are formally processed, reviewed by executive management, and permanently recorded in the officer's official personnel file as part of our employee recognition program.

LEGAL & POLICY AUTHORITY:

MATCOM Public Recognition Program

SOP-PUB-05



Receive an Official Complaint Case Number

Upon submitting a complaint through the public transparency portal, email, mail, or phone, you are entitled to receive a unique, official Complaint Case Number immediately (or within 1 business day for physical mail). This tracking number guarantees administrative accountability and allows you to track the progress of your inquiry.

LEGAL & POLICY AUTHORITY:

COMAR 12.10.01

SOP-PUB-06



Submit Additional Evidence Using Your Case Number

You have the right to submit supplemental evidence—including photographs, audio/video recordings, documents, medical reports, or witness details—at any point during an active investigation using your assigned Case Number. All electronic media submitted is protected by strict chain-of-custody protocols.

LEGAL & POLICY AUTHORITY:

MD Courts & Jud. Proc. § 10-402

SOP-PUB-07

SOP-PUB-08



Receive Confirmation That Your Submission Was Received

You have the right to prompt, written or electronic verification confirming that MATCOM has successfully received your complaint, commendation, public records request, or supplemental evidence submission. Intake confirmation notices include estimated timelines and assigned contact details.

LEGAL & POLICY AUTHORITY:

SOP-PUB-04

SOP-PUB-06

SOP-PUB-16



Check the Status of Your Complaint Where Permitted

You have the right to check the current operational status of your complaint investigation (e.g., Pending Review, Under Investigation, Executive Review, Final Disposition) through our public portal or by contacting Internal Affairs, within the boundaries of applicable privacy and personnel laws.

LEGAL & POLICY AUTHORITY:

Maryland Public Information Act

SOP-PUB-06

SOP-PUB-13



Request Reasonable Disability or Language Assistance

You have the right to access all MATCOM public accountability services without discrimination or barriers. Free auxiliary aids, disability accommodations (including TTY/relay and accessible web forms), and qualified language translation/interpretation services are provided upon request.

LEGAL & POLICY AUTHORITY:

Title VI Civil Rights Act of 1964

ADA / Section 504

MD Disability Access Laws

SOP-PUB-21



Submit a Complaint Anonymously Where Permitted

You have the right to submit complaints anonymously without disclosing your name or personal contact information. While anonymous complaints are investigated to the fullest extent permitted by available evidence, providing contact details allows investigators to verify facts and provide status updates.

LEGAL & POLICY AUTHORITY:

COMAR 12.10.01

SOP-PUB-19



Have Allegations Reviewed Objectively and Impartially

You are guaranteed an objective, thorough, and unbiased investigation conducted by designated Internal Affairs personnel or independent external reviewers. MATCOM investigators strictly evaluate physical evidence, body camera footage, witness testimony, and official logs free from administrative interference or conflict of interest.

LEGAL & POLICY AUTHORITY:

MD Police Accountability Act of 2022

COMAR Title 12

SOP-PUB-10

SOP-PUB-34



Receive Notification Upon Final Investigation Disposition

You have the right to receive formal written notification when an investigation reaches final disposition. Notifications specify the administrative finding category (e.g., Unfounded, Exonerated, Not Sustained, Sustained, or Policy Failure) subject to statutory confidentiality requirements regarding specific personnel actions.

LEGAL & POLICY AUTHORITY:

MPIA § 4-311

SOP-PUB-12

SOP-PUB-13



Request Eligible Public Records

You have the right to inspect and request copies of disclosable public records, standard operating procedures, aggregate statistical reports, and open data publications pursuant to the Maryland Public Information Act (MPIA), subject only to lawful statutory exemptions.

LEGAL & POLICY AUTHORITY:

MPIA (State Gov't Art. § 4-101 et seq.)

SOP-PUB-01

SOP-PUB-16



Have Personal and Sensitive Information Protected

You have the right to privacy protections regarding your personal identifying information (PII), medical data, victim identity, and unlisted physical addresses. MATCOM enforces strict privacy filtering and address suppression protocols to safeguard sensitive public portal data.

LEGAL & POLICY AUTHORITY:

MPIA § 4-301 et seq.

SOP-PUB-03

SOP-PUB-15

SOP-PUB-30



Report an Immediate Emergency Through 911

You have the fundamental right to immediate emergency assistance. The Public Accountability Portal and administrative complaint intake channels are for non-emergency reporting and administrative oversight. Active crimes, medical emergencies, fires, or immediate threats to life and safety must always be reported directly to emergency dispatch by dialing 911 or MATCOM 24/7 Dispatch at 1-855-715-9911.

LEGAL & POLICY AUTHORITY:

MD Emergency Communications Standards

SOP-PUB-18



MARYLAND LEGAL COMPLIANCE FRAMEWORK & GOVERNING AUTHORITY

This Charter is established pursuant to and in full compliance with the laws of the State of Maryland and federal civil rights standards:

Maryland Public Information Act (MPIA)

MD Code Ann., State Gov't Art. § 4-101 et seq. (Public records inspection & exemptions).

MD Security Guards Act & Regulations

MD Business Regulation Art., Title 12, Subtitle 1; COMAR 12.10.01 & 12.10.02.

Police Accountability Act of 2022

MD statutory standards for complaint intake, misconduct investigation, and public reporting.

MPCTC Training Standards

COMAR Title 12, Subtitle 12 (Mandatory security guard & officer standards).

Maryland Wiretap Act

MD Cts. & Jud. Proc. Code Ann. § 10-402 (Audio/video evidence recording compliance).

Constitutional Guarantees

MD Declaration of Rights & US Constitution (Due process, equal protection, free speech).

Disability & Accessibility Standards

Americans with Disabilities Act (ADA), Section 504, and MD Accessibility Statutes.

Title VI Civil Rights Protection

Title VI of the Civil Rights Act of 1964 (Equal access and language translation).

CONTACT & INTAKE DIRECTORY

Organization: Matcom Office of
Public Safety LLC

HQ Address: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD
21207

Administrative Phone:
701-809-9911

24/7 Dispatch Hotline:
1-855-715-9911

Email Intake:
Oga@matcomops.org

Web Portal: www.matcomops.org

EXECUTIVE AUTHORIZATION

This Public Bill of Rights is promulgated under the executive authority of the Chief Executive Officer and is binding upon all personnel operating under Matcom Office of Public Safety LLC.

Dr. Brian C. Askew
**CHIEF EXECUTIVE OFFICER &
APPROVING AUTHORITY**

License: 24PLU-SGPD4620 (Exp. Jan 31,
2028) | NAICS: 561612

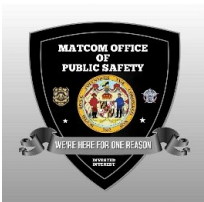
MATCOM OFFICE OF PUBLIC SAFETY LLC — PUBLIC ACCOUNTABILITY & TRANSPARENCY PORTAL

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911 | Admin:
701-809-9911

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed) • Effective Date: August 13, 2026

This document is a public declaration of principles and rights. It is maintained electronically on the Matcom
Transparency Portal.

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
MD Security Guard Agency License: 24PLU-SGPD4620 (Armed & Unarmed) | Exp: Jan 31, 2028
24/7 Dispatch: 1-855-715-9911 | Admin: 701-809-9911 | Email: Oga@matcomops.org |
NAICS: 561612

STANDARD OPERATING PROCEDURE

SOP-PUB-01: Public Transparency & Open Data Policy

Policy Number	SOP-PUB-01	Title	Public Transparency & Open Data Policy
Effective Date	August 13, 2026	Revision Date	August 13, 2026
Approving Authority	Dr. Brian C. Askew, CEO	Responsible Division	Office of Governmental Affairs
Classification	Public	Supersedes	None (Initial Issue)
Review Date	August 13, 2027	License Reference	MD License 24PLU-SGPD4620

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes the official policy and operational guidelines governing the proactive disclosure, publishing, and management of open public safety data by the Matcom Office of Public Safety LLC ("MATCOM"). MATCOM is committed to operating with complete transparency, accountability, and legal compliance under Maryland law, fostering community trust while safeguarding individual privacy and operational security.

1.2 Scope: This policy applies to all personnel, dispatchers, security officers, supervisors, data custodians, information technology staff, and executive officers operating under or on behalf of MATCOM (MD License 24PLU-SGPD4620). It governs all dataset releases through the MATCOM Public Safety Transparency Portal, open data APIs, public reports, and statutory disclosure requests.

2.0 AUTHORITY & LEGAL REFERENCES

This procedure is promulgated under the authority of the Chief Executive Officer of MATCOM and adheres strictly to the statutory and regulatory requirements of the State of Maryland, including but not limited to:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Government Article, § 4-101 et seq. (Mandating public access to public records while providing statutory exemptions for personal privacy and confidential investigations).
- **Maryland Security Guards Act:** Md. Code Ann., Business Regulation Article, Title 19, Subtitle 1 et seq.
- **COMAR 12.10.01 & 12.10.02:** Code of Maryland Regulations governing Security Guard Licensing, Agency Operations, and Mandatory Training Standards.
- **Maryland Police Accountability Act of 2022:** Establishing standards for record transparency, complaint tracking, and public accountability.
- **MPCTC Training & Operational Guidelines:** Maryland Police and Correctional Training Commissions (COMAR Title 12, Subtitle 12).
- **Maryland Courts & Judicial Proceedings Code § 10-402:** Wiretap and Electronic Surveillance Act regarding dispatch line audio disclosure rules.
- **Maryland State Police Licensing Division Rules:** Administrative guidelines governing private security guard company disclosures.

3.0 DEFINITIONS

3.1 Open Data: Non-confidential digital data produced or collected by MATCOM during public safety operations, rendered in machine-readable and human-readable formats, available to the public without fee or restriction.

3.2 Public Safety Transparency Portal: The official web-based repository (accessible via www.matcomops.org) where MATCOM publishes calls-for-service logs, aggregated crime statistics, policy documents, and performance metrics.

3.3 Personally Identifiable Information (PII): Any information that can be used to distinguish or trace an individual's identity, including names, Social Security Numbers, driver's license numbers, home addresses, phone numbers, date of birth, or biometric data.

3.4 Data Custodian: The designated official within the Office of Governmental Affairs responsible for auditing, redacting, and authorizing dataset publications.

3.5 Data Sanitization / Redaction: The irreversible process of removing or masking protected, confidential, or sensitive information from datasets before public release.

4.0 POLICY DIRECTIVES

4.1 Default to Transparency: All operational data generated by MATCOM CAD (Computer-Aided Dispatch) and incident reporting systems shall be presumed public unless explicit statutory exemption, privacy mandate, or tactical security override applies under Maryland law.

4.2 Equal Access: Open data shall be made available simultaneously to all members of the public, news media, researchers, and government agencies via the Transparency Portal free of charge.

4.3 Protection of Privacy & Vulnerable Parties: Proactive disclosure shall under no circumstances compromise victim confidentiality, juvenile records, medical privacy (HIPAA), domestic violence protections, or active criminal investigations.

4.4 Prohibition of Commercial Exploitation: MATCOM open datasets are published for public transparency and community safety; commercial scraping for predatory marketing or harassment is strictly prohibited by Portal Terms of Use.

5.0 DATA PUBLISHING CATEGORIES & SCHEDULES

MATCOM shall publish data according to the standardized publication matrix below:

Dataset Category	Description & Content	Publishing Frequency	Responsible Division
Daily Dispatch Log	CAD incident call records including call ID, call type, block address, assigned unit, status, and disposition code.	Daily at 06:00 EST (covering prior 24h)	Communications & CAD Division
Weekly Incident Summaries	Aggregated call volumes, response times, patrol coverage metrics, and property security incident trends.	Weekly (Mondays by 08:00 EST)	Office of Governmental Affairs
Monthly Operations Report	Comprehensive crime statistics, alarm responses, trespass enforcement actions, and inter-agency coordination.	Monthly (5th calendar day)	Office of Governmental Affairs
Quarterly IA & Complaints	De-identified public complaint intake numbers, investigation dispositions, and disciplinary summaries.	Quarterly (15th of Jan/Apr/Jul/Oct)	Professional Standards / IA
Annual Transparency Audit	Full annual review of security operations, licensing compliance, and public feedback.	Annually (by February 15)	Office of Executive Director / CEO

Dataset Category	Description & Content	Publishing Frequency	Responsible Division
	open data accuracy, and community engagement.		

6.0 DATA ACCURACY, VALIDATION & CORRECTION PROTOCOLS

6.1 Validation Pipeline: Prior to publishing any dataset to the Public Safety Transparency Portal, the data must undergo a two-tier validation check:

1. Automated Validation: CAD scripts verify data schema, check for missing fields, and auto-flag sensitive incident codes or addresses requiring suppression under SOP-PUB-03.
2. Data Custodian Review: A designated Office of Governmental Affairs analyst performs spot-check audits for syntax errors, improper redactions, or misclassified calls.

DATA CORRECTION SERVICE LEVEL AGREEMENT (SLA): If an error, typographical defect, or inaccurate entry is identified in a published public dataset, MATCOM shall issue an official Errata Notice on the portal and correct the dataset within **24 hours** of verification.

7.0 PRIVACY PROTECTIONS & REDACTION FRAMEWORK

7.1 Absolute Redactions: The following data fields shall NEVER be published in open public datasets:

- Full names, home street address numbers, or telephone numbers of reporting parties, victims, or witnesses.
- Social Security Numbers, Driver's License Numbers, or government identity numbers.
- Names or identifying details of juveniles (individuals under 18 years of age).
- Medical condition details, mental health emergency notes, or EMT patient status (protected under HIPAA and state health privacy rules).
- Exact street address numbers for sensitive incidents governed under SOP-PUB-03 (e.g., domestic violence, sexual assault, shelters).

8.0 PUBLIC INFORMATION REMOVAL & REDACTION REQUESTS

8.1 Formal Petitions: Any individual who believes a published MATCOM dataset contains confidential, inaccurate, or privacy-violating information may submit a

Public Data Redaction Petition via email to Oga@matcomops.org or in writing to MATCOM Headquarters.

8.2 Review Timeline: The Office of Governmental Affairs shall acknowledge receipt within **24 hours** and render a formal determination regarding suppression or correction within **5 business days**.

9.0 RESPONSIBILITIES

9.1 Chief Executive Officer (Dr. Brian C. Askew): Exercises ultimate approving authority over transparency policies, annual reviews, and legal disclosures.

9.2 Director of Governmental Affairs: Serves as Chief Data Custodian; oversees dataset publication schedules, privacy compliance, and MPIA petition processing.

9.3 Communications & CAD Administrator: Manages daily CAD log ingestion, automated redaction filters, and real-time portal feeds.

9.4 Field Supervisors & Officers: Ensure accurate, objective, and timely entry of CAD dispatch notes and incident details at the field level.

10.0 COMPLIANCE, ENFORCEMENT & TRAINING

10.1 Compliance Standard: Unlawful disclosure of confidential victim information or intentional withholding of legally mandated open public data constitutes a violation of MATCOM policy and COMAR 12.10.01 standards.

10.2 Mandatory Training: All MATCOM personnel shall complete annual training on Open Data Protocols, MPIA compliance, and Privacy Protection Rules during scheduled MPCTC re-certification hours.

11.0 RECORDS RETENTION & DOCUMENT CONTROL

All open public datasets, validation logs, and redaction audit records shall be retained electronically for a minimum of **five (5) years** in accordance with Maryland State Archives records retention schedules for public safety agencies.

12.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure takes effect on **August 13, 2026**, and supersedes all prior guidelines. It shall be reviewed annually on or before **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

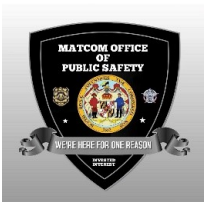
Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
MD Security Guard Agency License: 24PLU-SGPD4620 (Armed & Unarmed) | Exp: Jan 31, 2028
24/7 Dispatch: 1-855-715-9911 | Admin: 701-809-9911 | Email: Oga@matcomops.org |
NAICS: 561612

STANDARD OPERATING PROCEDURE

SOP-PUB-02: Public Calls-for-Service Information Release

Policy Number	SOP-PUB-02	Title	Public Calls-for-Service Information Release
Effective Date	August 13, 2026	Revision Date	August 13, 2026
Approving Authority	Dr. Brian C. Askew, CEO	Responsible Division	Communications & CAD Division
Classification	Public	Supersedes	None (Initial Issue)
Review Date	August 13, 2027	License Reference	MD License 24PLU-SGPD4620

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure defines the policies, rules, and technical workflows for the release of Computer-Aided Dispatch (CAD) calls-for-service information to the public, media, and community oversight stakeholders. The objective is to maintain public awareness of security operations while protecting victim identity, officer safety, and operational security.

1.2 Scope: This SOP applies to all dispatchers, communications supervisors, CAD systems administrators, and public information officers within MATCOM's 24/7 Communications Center (1-855-715-9911) operating under MD License 24PLU-SGPD4620.

2.0 AUTHORITY & LEGAL REFERENCES

This policy is authorized pursuant to MATCOM Executive Directives and complies with state statutory requirements:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Government Article, § 4-101 et seq.
- **Maryland Courts & Judicial Proceedings Code § 10-402:** Wiretap and Electronic Surveillance Act (governing audio dispatch recordings and text disclosures).
- **COMAR 12.10.01 & 12.10.02:** Regulations governing security guard company operations and dispatch communications.
- **Maryland Business Regulation Article, Title 19:** Private Security Agencies licensing compliance.
- **Maryland Police Accountability Act of 2022:** Public transparency mandates for dispatch call logs.

3.0 DEFINITIONS

3.1 Call for Service (CFS): Any incident, request for assistance, alarm signal, or officer-initiated security patrol recorded in the MATCOM CAD system.

3.2 CAD Incident Record: The digital record created by dispatch containing time stamps, unit assignments, caller details, location coordinates, and event disposition.

3.3 Block Address: A truncated geographic location where the exact house or building number is rounded down to the nearest hundred block (e.g., "6340 Security Blvd" becomes "6300 Block Security Blvd").

3.4 Real-Time Public CAD Feed: A near-real-time digital feed published to the Public Safety Transparency Portal, subject to mandatory operational delay filters.

4.0 STANDARD AUTHORIZED CAD PUBLIC FIELDS

Only specific CAD data fields are authorized for public release. The table below outlines the disclosure status for each standard CAD field:

CAD Field Name	Public Release Status	Format / Modification Requirement
Incident Control Number (CAD ID)	FULL RELEASE	Unique alphanumeric tracking number (e.g., MAT-2026-0813-0042).
Call Nature / Category	FULL RELEASE	Standard call code (e.g., Area Patrol, Trespass Notice, Burglar Alarm, Property Security).

CAD Field Name	Public Release Status	Format / Modification Requirement
Date & Call Received Time	FULL RELEASE	ISO format date and time stamp (YYYY-MM-DD HH:MM:SS EST).
Assigned Unit ID	FULL RELEASE	Unit identifier (e.g., Mobile Patrol Unit 104, K9 Unit 2).
Incident Location	MODIFIED (TRUNCATED)	Converted to 100-Block address. Exact suite or house numbers removed.
Call Status & Response Times	FULL RELEASE	Dispatched, En-Route, On-Scene, Cleared; response duration in minutes.
Final Disposition Code	FULL RELEASE	Standard clearance code (e.g., Advised/Cleared, Report Taken, Trespass Warning Issued).
Caller Name / Phone Number	ALWAYS REDACTED	Strictly suppressed to protect reporting citizen privacy.
Officer CAD Narrative Notes	REDACTED / RESTRICTED	Internal officer narrative withheld from automated public feeds.

5.0 ADDRESS TRUNCATION & ANONYMIZATION PROCEDURES

5.1 Truncation Algorithm: The CAD system shall automatically convert exact street addresses into 100-block ranges prior to public transmission:

- Residential/Commercial Example: 6340 Security Blvd, Suite 100 → converted to **6300 Block Security Blvd**.
- Intersection Example: Security Blvd & Rolling Rd → displayed as **Security Blvd / Rolling Rd (Intersection)**.
- Multi-Family Property Example: Apartment or suite numbers are purged entirely.

6.0 OPERATIONAL DELAY & TACTICAL WITHHOLDING RULES

6.1 Mandatory 15-Minute Operational Delay Feed: All real-time public CAD map feeds displayed on the portal shall operate on a mandatory **15-minute time delay**. This delay prevents tactical compromise during ongoing incidents and protects field officers from perimeter interference.

6.2 Complete Incident Withholding: CAD information shall be completely suppressed from public feeds while an active incident falls into any of the following emergency categories:

- Active Armed Suspect / Active Shooter Threat

- Officer in Distress / Emergency Backup Requested
- In-Progress Felonies, Burglaries, or Robberies
- Domestic Violence or Intimate Partner Disputes (governed by SOP-PUB-03)
- Sexual Assault or Crimes Involving Minors
- Active Tactical, Undercover, or Joint Law Enforcement Operations

TACTICAL OVERRIDE NOTICE: A Communications Supervisor or Executive Officer may manually toggle a CAD incident to "FULL SUPPRESSION" at any time if public release could imperil officer safety, victim safety, or property security.

7.0 DISPATCH AUDIO & RECORD DISCLOSURE RULES

7.1 Audio Broadcast Disclosure: Audio recordings of MATCOM dispatch channels are subject to the Maryland Wiretap Act (MD Courts & Judicial Proceedings § 10-402). Recorded phone calls from callers are strictly confidential and shall not be released to the public without a valid court order or MPIA determination signed by Legal Counsel.

7.2 Formal CAD Record Requests: Citizens requesting certified copies of CAD logs for legal, insurance, or MPIA purposes must submit a formal request to Oga@matcomops.org. Certified CAD logs are processed within 3 business days.

8.0 RESPONSIBILITIES

8.1 Communications Center Manager: Oversees CAD system public feed configurations, delays, and address truncation filters.

8.2 Duty Dispatchers: Responsible for proper call classification, entry of accurate disposition codes, and applying tactical suppression flags when required.

8.3 Director of Governmental Affairs: Reviews contested CAD release requests and audits public dispatch feed compliance.

9.0 COMPLIANCE & ENFORCEMENT

Willful circumvention of address suppression rules or unauthorized dissemination of confidential caller details is a major disciplinary offense resulting in immediate termination and reporting to the Maryland State Police Licensing Division under COMAR 12.10.01.

10.0 EFFECTIVE DATE & REVIEW

This SOP is effective as of **August 13, 2026**, and shall be reviewed annually on **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

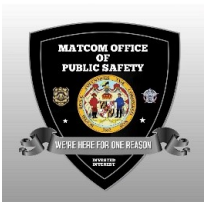
Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Communications & CAD Division
Matcom Office of Public Safety LLC

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
MD Security Guard Agency License: 24PLU-SGPD4620 (Armed & Unarmed) | Exp: Jan 31, 2028
24/7 Dispatch: 1-855-715-9911 | Admin: 701-809-9911 | Email: Oga@matcomops.org |
NAICS: 561612

STANDARD OPERATING PROCEDURE

SOP-PUB-03: Sensitive Incident & Address Suppression

Policy Number	SOP-PUB-03	Title	Sensitive Incident & Address Suppression
Effective Date	August 13, 2026	Revision Date	August 13, 2026
Approving Authority	Dr. Brian C. Askew, CEO	Responsible Division	Office of Governmental Affairs
Classification	Public	Supersedes	None (Initial Issue)
Review Date	August 13, 2027	License Reference	MD License 24PLU-SGPD4620

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure establishes mandatory protocols for suppressing exact location addresses, victim identifiers, and sensitive operational details from public CAD logs, transparency feeds, media releases, and open data portals. The primary objective is to safeguard crime victims, vulnerable populations, juveniles, confidential locations, and tactical security operations.

1.2 Scope: This policy applies across all MATCOM divisions, including field security officers, dispatchers, administrative personnel, and executive leadership operating under MD License 24PLU-SGPD4620.

2.0 AUTHORITY & LEGAL REFERENCES

This procedure is mandated pursuant to Maryland state statutes and executive public safety regulations:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Government Article, § 4-310 (Mandatory exemptions for records disclosing the location of domestic violence shelters and victim personal safety records).
- **Maryland Police Accountability Act of 2022:** Provisions protecting crime victim privacy and sensitive operational files.
- **Federal Violence Against Women Act (VAWA):** Privacy mandates prohibiting public disclosure of victim personally identifiable information.
- **Maryland Criminal Law Article & COMAR 12.10.01:** Statutory confidentiality protections for sexual assault, domestic violence, and juvenile records.
- **Health Insurance Portability and Accountability Act (HIPAA):** 45 CFR Part 160/164 (Protection of medical emergency and mental health crisis response data).

3.0 DEFINITIONS

3.1 Sensitive Incident: Any call for service, security dispatch, or incident investigation where public disclosure creates a foreseeable risk of physical harm, retaliation, trauma, or privacy violation to victims or officers.

3.2 Address Suppression: The complete masking or removal of geographic coordinates, street names, block numbers, and facility identifiers from public data views.

3.3 Protected Facility: Any domestic violence shelter, safehouse, crisis intervention center, juvenile facility, or undercover law enforcement facility.

3.4 Suppression Flag: A mandatory digital toggle in the MATCOM CAD system that prevents automated data export to public portals.

4.0 CATEGORIES MANDATING ADDRESS SUPPRESSION

The CAD system and publishing workflows shall automatically apply **FULL ADDRESS SUPPRESSION** for all incidents falling into the following statutory categories:

Category Code	Incident Type / Category	Suppression Directive	Public Display Format
CAT-01	Domestic Violence & Intimate Partner Abuse	Full Address & Location Masking	SUPPRESSED - SENSITIVE INCIDENT
CAT-02	Sexual Assault, Rape & Sex Crimes	Full Address & Location Masking	SUPPRESSED - SENSITIVE INCIDENT

Category Code	Incident Type / Category	Suppression Directive	Public Display Format
CAT-03	Crimes Involving Minors & Juveniles	Full Address & Name Suppression	SUPPRESSED - JUVENILE INCIDENT
CAT-04	Medical Emergencies, Overdose & Mental Health Crises	Full Location & Medical Data Masking	SUPPRESSED - MEDICAL / HEALTH CRISIS
CAT-05	Human Trafficking & Stalking Complaints	Full Address & Location Masking	SUPPRESSED - SENSITIVE INCIDENT
CAT-06	Protected Shelters, Safehouses & Crisis Centers	500-Yard Geofence Masking	SUPPRESSED - PROTECTED FACILITY
CAT-07	Active Tactical / SWAT / Undercover Operations	Full Tactical Operational Masking	SUPPRESSED - ACTIVE OPERATION
CAT-08	Witness Protection & Confidential Investigations	Permanent Executive Suppression	SUPPRESSED - RESTRICTED RECORD

5.0 OPERATIONAL SUPPRESSION MECHANICS & GEOFENCING

5.1 Automated CAD Auto-Flagging: When a call is entered into CAD with any nature code corresponding to Categories CAT-01 through CAT-08, the system shall automatically attach a [SUPPRESS_PUBLIC_FEED] tag. This tag blocks the record from exporting to the Transparency Portal.

5.2 Protected Facility Geofencing: A 500-yard digital geofence buffer shall be maintained around all registered domestic violence shelters and crisis facilities within MATCOM's operational jurisdiction. Any call dispatched within this geofenced perimeter shall automatically mask the address to SUPPRESSED - PROTECTED FACILITY regardless of call type.

6.0 ADMINISTRATIVE OVERRIDE & UNMASKING PROTOCOLS

RESTRICTED UNMASKING PROTOCOL: Unmasking or releasing a suppressed address requires formal written authorization from the Chief Executive Officer or Director of Governmental Affairs. Unauthorized unmasking is strictly illegal under MPIA § 4-310.

6.1 Subpoena & Court Order Exception: Suppressed records requested pursuant to a judicial subpoena or court order shall undergo mandatory legal review by MATCOM Legal Counsel prior to disclosure. All victim PII shall be redacted using permanent black-box redaction software before court filing.

6.2 Audit Trail Logging: Any manual override, unmasking event, or modification of a suppression flag generates an immutable entry in the MATCOM Security Audit Log, recording the employee ID, timestamp, justification, and authorizing official.

7.0 RESPONSIBILITIES

7.1 Director of Governmental Affairs: Maintains the official list of protected facility geofences and conducts monthly suppression compliance audits.

7.2 CAD System Administrator: Validates automated suppression rules and ensures CAD software security patches are maintained.

7.3 Communications Staff: Mandatory duty to manually apply suppression flags if an incoming call reveals sensitive victim or shelter details not automatically caught by nature codes.

8.0 COMPLIANCE & PENALTIES

Failure to apply address suppression rules or unauthorized release of protected victim addresses constitutes severe misconduct under MATCOM Disciplinary Regulations, punishable by suspension, termination, and civil/criminal liability under Maryland law.

9.0 EFFECTIVE DATE & REVIEW

Effective Date: **August 13, 2026**. Annual Review Date: **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
MD Security Guard Agency License: 24PLU-SGPD4620 (Armed & Unarmed) | Exp: Jan 31, 2028
24/7 Dispatch: 1-855-715-9911 | Admin: 701-809-9911 | Email: Oga@matcomops.org |
NAICS: 561612

STANDARD OPERATING PROCEDURE

SOP-PUB-04: Public Complaint Intake & Acceptance

Policy Number	SOP-PUB-04	Title	Public Complaint Intake & Acceptance
Effective Date	August 13, 2026	Revision Date	August 13, 2026
Approving Authority	Dr. Brian C. Askew, CEO	Responsible Division	Professional Standards / Internal Affairs
Classification	Public	Supersedes	None (Initial Issue)
Review Date	August 13, 2027	License Reference	MD License 24PLU-SGPD4620

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure establishes a transparent, accessible, and rigorous process for receiving, accepting, acknowledging, and triaging public complaints alleging misconduct, excessive force, unprofessional behavior, or statutory violations by MATCOM security officers, dispatchers, supervisors, or administrative employees.

1.2 Scope: This procedure applies to all members of the public and all MATCOM personnel operating under MD Security Guard Agency License 24PLU-SGPD4620. MATCOM maintains a strict open-door policy: Every complaint from any source shall be accepted and investigated.

2.0 AUTHORITY & LEGAL REFERENCES

This policy is promulgated under the authority of the CEO and complies with state oversight laws:

- **Maryland Police Accountability Act of 2022:** Public complaint intake standards, police accountability mandates, and anti-retaliation provisions.
- **COMAR 12.10.01 & COMAR 12.10.02:** Security Guard Licensee Standards, Code of Conduct, and Mandatory Disciplinary Reporting.
- **Maryland Business Regulation Article, Title 19:** Mandating licensee response to public misconduct allegations.
- **Maryland Constitutional Due Process Provisions:** Ensuring fair treatment for complainants and accused personnel.

3.0 DEFINITIONS

3.1 Public Complaint: Any expression of dissatisfaction, grievance, or allegation of improper conduct, policy violation, discourtesy, or criminal act submitted by a citizen, property owner, or visitor.

3.2 Anonymous Complaint: Any complaint submitted where the complainant declines or omits to provide their identity or contact details.

3.3 Incident Control Number (ICN): A unique, auto-generated tracking ID assigned to every complaint upon initial intake.

3.4 Retaliation: Any adverse action, harassment, intimidation, or discriminatory treatment directed against any person for filing a complaint in good faith.

4.0 POLICY DIRECTIVES & UNIVERSAL ACCEPTANCE

4.1 No-Barrier Intake: MATCOM prohibits any employee from refusing to accept a complaint, discouraging a citizen from filing a complaint, or requiring notarization or sworn affidavits as a precondition to complaint acceptance.

4.2 Anonymous & Third-Party Complaints: Anonymous complaints and third-party complaints (submitted by witnesses, legal counsel, or family members) shall be accepted and investigated with the same thoroughness as named complaints.

5.0 MULTI-CHANNEL INTAKE METHODS

Complainants may file a complaint 24 hours a day, 7 days a week, through any of the following intake channels:

Intake Channel	Access Method / Location	Processing Timeframe
Online Public Safety Portal	Web form at www.matcomops.org/complaints	Immediate Auto-Receipt; 24h IA Assignment
24/7 Telephone Intake Hotline	Call Dispatch at 1-855-715-9911 or Admin 701-809-9911	Immediate Call Intake Logged into CAD
Email Intake	Direct email to 0ga@matcomops.org	Acknowledged within 24 Hours
In-Person Intake	MATCOM HQ: 6340 Security Blvd, Suite 100-1071, Gwynn Oak, MD 21207	Field / Supervisor Complaint Form Intake
Mail / Written Form	Attn: Division of Professional Standards, 6340 Security Blvd, Suite 100-1071	Logged upon receipt

6.0 INFORMATION GATHERING GUIDELINES

To assist in a prompt investigation, intake officers shall attempt to collect the following information (though missing details shall NOT invalidate a complaint):

- Date, time, and specific physical location of the incident.
- Name, badge number, uniform description, or vehicle identification of involved personnel.
- Detailed factual narrative of the conduct or incident.
- Names, phone numbers, or addresses of any witnesses.
- Photographic, audio, video, or physical evidence (if available).

7.0 ACKNOWLEDGMENT & TRACKING PROTOCOLS

7.1 Auto-Receipt & Tracking Number: Every complaint received electronically or by phone shall immediately generate an automated receipt containing an **Incident Control Number (ICN)** (e.g., IA-2026-0813-009).

7.2 Formal Acknowledgment Letter: Within **three (3) business days** of receipt, the Division of Professional Standards shall issue an official written acknowledgment letter to the complainant via email or certified mail containing the ICN, assigned investigator contact details, and expected investigation timeline.

8.0 STRICT ANTI-RETALIATION SAFEGUARDS

PROHIBITION OF RETALIATION: Any MATCOM officer or employee who engages in retaliation, intimidation, surveillance, or harassment against a complainant or witness shall

be subject to **IMMEDIATE TERMINATION OF EMPLOYMENT** and referral to the Maryland State Police for criminal prosecution where applicable.

9.0 INVESTIGATION TRIAGE & DISPOSITIONS

9.1 Investigation Timeline: All public complaints shall undergo preliminary assessment within **5 business days** and full investigation completion within **30 calendar days**.

9.2 Investigation Disposition Classifications: Upon investigation completion, findings shall be categorized into one of five official findings:

- **Sustained:** Investigation revealed sufficient evidence to prove the alleged misconduct occurred.
- **Unfounded:** Investigation proved the alleged misconduct did not occur or allegation is factually false.
- **Exonerated:** The incident occurred, but the officer's actions were lawful, proper, and within policy.
- **Not Sustained:** Investigation failed to disclose sufficient evidence to prove or disprove the allegation.
- **Policy Failure:** The officer's action was consistent with policy, but the policy itself is flawed and requires revision.

9.3 Complainant Notification: Within **5 business days** of final executive sign-off, the complainant shall receive written notification of the official disposition.

10.0 RESPONSIBILITIES

10.1 Commander, Professional Standards / Internal Affairs: Responsible for intake logging, assigning investigators, tracking timelines, and maintaining IA records.

10.2 Field Supervisors: Duty to immediately accept complaints in the field, issue paper complaint receipts, and forward reports to IA within 12 hours.

11.0 EFFECTIVE DATE & REVIEW

Effective Date: **August 13, 2026**. Review Date: **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

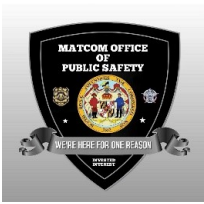
Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Professional Standards / Internal Affairs
Matcom Office of Public Safety LLC

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
MD Security Guard Agency License: 24PLU-SGPD4620 (Armed & Unarmed) | Exp: Jan 31, 2028
24/7 Dispatch: 1-855-715-9911 | Admin: 701-809-9911 | Email: Oga@matcomops.org |
NAICS: 561612

STANDARD OPERATING PROCEDURE

SOP-PUB-05: Public Commendation & Employee Praise Program

Policy Number	SOP-PUB-05	Title	Public Commendation & Employee Praise Program
Effective Date	August 13, 2026	Revision Date	August 13, 2026
Approving Authority	Dr. Brian C. Askew, CEO	Responsible Division	Office of Governmental Affairs / Human Resources
Classification	Public	Supersedes	None (Initial Issue)
Review Date	August 13, 2027	License Reference	MD License 24PLU-SGPD4620

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure establishes the formal framework for receiving, verifying, documenting, and honoring public commendations, citizen praise, and formal recognitions awarded to security officers, dispatchers, supervisors, administrative staff, and operational units of Matcom Office of Public Safety LLC.

1.2 Scope: This program applies to all active personnel across MATCOM operating under MD License 24PLU-SGPD4620. Recognizing exemplary performance promotes high morale, reinforces professional excellence, and strengthens positive community relations.

2.0 AUTHORITY & REFERENCES

This policy is authorized by the Chief Executive Officer under MATCOM HR Directives and complies with state standards:

- **COMAR 12.10.01:** Security Guard Licensee Professional Standards.
- **Maryland Business Regulation Article, Title 19:** Security Agency Professional Ethics and Recognition Guidelines.
- **MPCTC Professionalism Guidelines:** Standards for public safety employee recognition and career advancement.
- **MATCOM Employee Handbook & Merit System Regulations:** Guidelines for personnel awards and commendations.

3.0 DEFINITIONS

3.1 Public Commendation: A written or verbal expression of praise, gratitude, or recognition submitted by a citizen, property manager, client, or agency partner recognizing exceptional service.

3.2 Citizen Praise Card: Standardized physical form provided to officers to distribute to citizens upon request to facilitate feedback.

3.3 Commendation Review Committee: Joint committee comprising representatives from the Office of Governmental Affairs and Human Resources responsible for reviewing and verifying praise submissions.

4.0 SUBMISSION CHANNELS FOR PUBLIC PRAISE

Members of the public may submit officer commendations through multiple accessible channels:

Submission Channel	Contact / Portal Detail	Initial Processing Unit
Online Praise Portal	Form at www.matcomops.org/commendations	Office of Governmental Affairs
Direct Email Intake	Email to Oga@matcomops.org	Office of Governmental Affairs
Telephone Recognition Line	Call 701-809-9911 or Dispatch 1-855-715-9911	Communications Center Intake Log
Citizen Praise Cards / Mail	Mailed to HQ: 6340 Security Blvd, Suite 100-1071	Human Resources Division

5.0 VERIFICATION & REVIEW WORKFLOW

To ensure authenticity and integrity, all public commendations shall follow a 4-step verification process:

- 1. **Intake & Logging:** The Office of Governmental Affairs logs the commendation within **24 hours** of receipt and issues a tracking ID.
- 2. **Operational Verification:** Within **3 business days**, OGA verifies CAD incident records, patrol logs, or supervisor reports matching the date, time, and location reported.
- 3. **Employee & Supervisory Notification:** Once verified, a copy of the commendation is sent immediately to the employee, their direct supervisor, and the Division Commander.
- 4. **Personnel File Recording:** Human Resources places an official copy of the commendation into the employee's permanent personnel file.

6.0 AWARD CATEGORIES & RECOGNITION HIERARCHY

Public commendations are evaluated for inclusion in MATCOM's formal award hierarchy:

Award Tier	Award Title	Criteria & Eligibility	Recognition Provided
Tier 1	Official Certificate of Commendation	Verified public praise for exceptional customer service, courtesy, or diligence.	Certificate signed by CEO; Personnel file entry.
Tier 2	Employee / Dispatcher of the Month	Highest commended employee during a calendar month based on public & peer reviews.	Framed Award; \$250 Bonus; Designated Parking.
Tier 3	Life Saving / De-Escalation Merit Ribbon	Commendation involving life-saving intervention or exceptional crisis de-escalation.	Uniform Merit Ribbon; Formal CEO Ceremony.
Tier 4	CEO Distinguished Service Award	Annual award presented for extraordinary service representing MATCOM's highest ideals.	Engraved Plaque; Commendation Medal; Annual Gala.

CAREER ADVANCEMENT WEIGHTING: Verified public commendations are directly weighted during annual performance evaluations and carry positive promotional credit points for merit-based promotions to Supervisory and Command ranks.

7.0 PUBLIC TRANSPARENCY & HONOR ROLL PUBLICATION

7.1 Public Honor Roll: With the consent of the honored employee, verified public commendations (with citizen PII redacted) shall be published on the Public Safety Transparency Portal's monthly Honor Roll & Citizen Praise page.

8.0 RESPONSIBILITIES

8.1 Director of Human Resources: Maintains official award records, issues commendation certificates, and administers promotional credit points.

8.2 Director of Governmental Affairs: Manages online commendation portal, verifies records against CAD logs, and publishes monthly Honor Roll summaries.

9.0 EFFECTIVE DATE & ANNUAL REVIEW

Effective Date: **August 13, 2026**. Review Date: **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Office of Governmental Affairs / HR
Matcom Office of Public Safety LLC



MATCOM OFFICE OF PUBLIC SAFETY LLC

**LICENSED MARYLAND SECURITY GUARD
AGENCY • MD LICENSE 24PLU-SGPD4620**

Headquarters: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Web: www.matcomops.org | **Email:**
Oga@matcomops.org

STANDARD OPERATING PROCEDURE

SOP-PUB-06: Complaint Case Number & Tracking Procedure

POLICY NUMBER	SOP-PUB-06
TITLE	Complaint Case Number & Tracking Procedure
EFFECTIVE DATE	August 13, 2026
REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO
RESPONSIBLE DIVISION	Professional Standards / Internal Affairs
PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes a uniform, objective, and cryptographically secure complaint intake, case numbering, electronic receipt, and public status tracking system for Matcom Office of Public Safety LLC (hereinafter "Matcom"). The primary purpose is to guarantee that every complaint submitted against Matcom personnel, operations, or administrative procedures is immediately captured, assigned a standardized Case Identification Number (CIN), verified via an electronic receipt, and made trackable by the complainant through a

secure online portal while protecting operational integrity and individual privacy rights.

1.2 Scope: This procedure applies universally across all divisions, operational contracts, facilities, and personnel of Matcom Office of Public Safety LLC, including armed and unarmed security guards, special police officers, dispatch personnel, field supervisors, administrative staff, and executive leadership. It governs all complaints submitted by members of the public, commercial clients, property owners, government liaisons, or internal whistleblowers.

1.3 Public Commitment: Matcom maintains an absolute open-door public accountability framework. No employee or representative of Matcom possesses the authority to refuse, reject, delay, or suppress a public complaint. All submissions must enter the automated Case Management System (CMS) immediately upon intake.

2.0 AUTHORITY & LEGAL REFERENCES

2.1 Statutory Authority: This policy is issued under the authority of Dr. Brian C. Askew, CEO, in compliance with federal, state, and local statutory standards governing licensed private security agencies in the State of Maryland.

2.2 Primary Maryland Statutory References:

- **Maryland Business Regulation Article, Title 13 (Maryland Security Guard Act):** Statutory standards governing private security agency licensing, duty of oversight, and disciplinary recordkeeping.
- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02:** Licensing requirements, mandatory reporting rules, and operational conduct standards enforced by the Maryland State Police (MSP) Licensing Division.
- **Maryland Public Information Act (MPIA), State Government Article § 4-101 et seq.:** Framework governing public disclosure, confidentiality exemptions (§ 4-311 regarding personnel records), and inspection of public administrative records.
- **Maryland Police Accountability Act of 2022:** State public transparency principles, public complaint tracking expectations, and disciplinary reporting standards.
- **Maryland Police and Correctional Training Commissions (MPCTC) Standards (COMAR Title 12, Subtitle 12):** Professional standards benchmarks for law enforcement and special public safety entities.

- **Constitutional Due Process:** Article 24 of the Maryland Declaration of Rights and the Fourteenth Amendment to the United States Constitution guaranteeing procedural due process for complainants and subject employees.

3.0 DEFINITIONS

3.1 Case Identification Number (CIN): A unique, sequential 10-character alphanumeric identifier generated automatically by the CMS upon receipt of a complaint, structured as 2026-XXXX (e.g., 2026-0042 or prefixed as CMP-2026-0042).

3.2 Secure Access Code (SAC): A randomized, cryptographically generated 12-character alphanumeric PIN (e.g., K9x-72M-pQ4-L8v) issued exclusively to the complainant alongside the CIN to permit secure portal login and status verification.

3.3 Electronic Receipt: An immutable digital document generated instantly upon complaint submission, containing the CIN, SAC, submission date/time (EST/EDT and UTC), summary of submitted items, intake channel, and public tracking instructions.

3.4 Complainant Tracking Portal: A secure web interface hosted at www.matcomops.org/tracking enabling complainants to enter their CIN and SAC to view real-time case progression, assigned division status, and approved investigative updates.

3.5 Master Internal Affairs Tracking Log (MIATL): An encrypted, access-restricted database maintained by the Professional Standards / Internal Affairs Division containing full case files, unredacted witness statements, officer personnel data, and investigative logs.

4.0 POLICY

4.1 Mandatory Intake & Zero Suppression: Every complaint, whether received via online web portal, email, 24/7 dispatch phone, physical mail, or in-person delivery, shall be entered into the CMS within sixty (60) minutes of receipt by dispatch or administrative staff. Suppressing, altering, failing to report, or discouraging a complaint constitutes gross misconduct punishable by immediate termination and regulatory notification to the Maryland State Police Licensing Division.

4.2 Standardized Numbering Mandate: All complaints received within the calendar year 2026 shall strictly utilize the 2026-XXXX numbering protocol. Legacy

numbering systems are permanently retired. Case numbers shall be strictly sequential and system-assigned without manual overrides.

4.3 Complainant Transparency & Confidentiality Balance: Complainants are entitled to real-time status visibility regarding the stage of investigation. However, pursuant to the Maryland Public Information Act (MPIA) § 4-311 and Maryland employment due process law, internal investigative deliberations, personal medical data, unredacted officer home addresses, social security numbers, and confidential informant details are strictly exempt from public portal display.

5.0 PROCEDURES

5.1 Multi-Channel Complaint Intake & Ingestion

Complaints are received and automatically ingested into the CMS through four primary pathways:

1. **Secure Web Portal:** Direct electronic submission via www.matcomops.org/complaints. Automated script triggers immediate record creation, CIN generation, and SAC provisioning.
2. **Email Submissions:** Emails sent to Oga@matcomops.org or ia@matcomops.org are processed by an automated parser or logged manually by the IA intake officer within one (1) hour of receipt.
3. **24/7 Dispatch Hotline (1-855-715-9911):** Dispatch operators log telephonic complaints into the electronic intake dashboard while caller is on the line, instantly issuing a CIN/SAC verbally and via SMS/email if contact info is provided.
4. **In-Person or Postal Mail (6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207):** Written complaints are timestamped upon physical receipt, scanned into PDF format, and entered into the CMS within twenty-four (24) hours.

5.2 Case Identification Number (CIN) Structure

The standard CIN format for all matters initiated in 2026 is defined as follows:

STANDARDIZED CASE NUMBER FORMAT STRUCTURE

CMP-2026-XXXX (Public/General Complaint Tracking)

IA-2026-XXXX (Internal Affairs Misconduct Tracking)

Where:

- CMP or IA designates the initial administrative classification.
- 2026 designates the active calendar year.
- XXXX designates the sequential four-digit increment (e.g., 0001 to 9999).

5.3 Automated Electronic Receipt Issuance

Immediately upon database entry, the CMS generates a standardized Electronic Receipt containing:

- Official Header: Matcom Office of Public Safety LLC (MD Lic. 24PLU-SGPD4620).
- Assigned Case Identification Number (CIN) and Secure Access Code (SAC).
- Date and Exact Timestamp of Ingestion (EST/EDT and UTC).
- Intake Channel Identifier (Web, Phone, Mail, In-Person).
- Complainant Contact Information (or designated as "ANONYMOUS").
- Summary Statement of Allegation (verbatim text or phone log summary).
- Direct Hyperlink to Public Tracking Portal and Instructions.

5.4 Complainant Portal Access & Status Stages

By entering the CIN and SAC at www.matcomops.org/tracking, the complainant can monitor the active stage of the matter. The system displays six standardized, plain-language operational stages:

STAGE CODE	STAGE NAME	PUBLIC DISPLAY STATUS DESCRIPTION	TARGET SLA TIMELINE
STAGE 1	Intake & Preliminary Review	Complaint received and validated. Under initial review by Professional Standards Commander for triage and jurisdiction.	1 to 2 Business Days
STAGE 2	Classified & Assigned	Complaint classified (Class I-IV). Formally assigned to Lead Investigator / Internal Affairs Division.	2 to 3 Business Days
STAGE 3	Active Investigation	Evidence collection, video review, witness interviews, and officer interrogations actively underway.	15 to 30 Calendar Days
STAGE 4	Command & Legal Review	Investigative report completed. Under formal evaluation by Command Staff and Office of General Counsel.	5 to 10 Business Days
STAGE 5	Adjudication & Findings	Executive finding rendered by CEO / Approving Authority. Disposition letter generated and dispatched.	3 Business Days
STAGE 6	Referred / Case Closed	Matter concluded, administrative action implemented, or formally referred to outside law enforcement / MSP.	Final Disposition

5.5 Complainant Information Visibility Matrix

To comply with Maryland law, information displayed on the complainant tracking portal is divided into public visibility items and restricted internal items:

INFORMATION FIELD	COMPLAINANT VISIBLE?	LEGAL / ADMINISTRATIVE BASIS
Case Number (CIN) & Filing Timestamp	YES	Public Accountability Standard
Current Investigation Stage (Stages 1-6)	YES	Transparency Directive SOP-PUB-06
Assigned Division & Lead Investigator Badge #	YES	Administrative Accountability
Estimated Completion / SLA Target Date	YES	Customer Service Standard
Uploaded Evidence Receipt List (Filenames & Hashes)	YES	SOP-PUB-07 / SOP-PUB-08 Proof of Intake
Final Disposition Category (Sustained, Unfounded, etc.)	YES	Public Notice Right
Subject Officer Home Address / SSN / Personal Phone	NO (RESTRICTED)	MPIA § 4-311 / Maryland Privacy Law
Internal IA Deliberations & Legal Counsel Notes	NO (RESTRICTED)	Attorney-Client Privilege / Work Product
Unredacted Witness Identity (where safety risk exists)	NO (RESTRICTED)	Witness Protection Protocol

5.6 Automated Notification Triggers

The CMS automatically dispatches email and SMS alerts to the complainant upon the occurrence of any of the following milestones:

- Initial Case Creation & Receipt Transmission.
- Transition between Investigation Stages (e.g., Stage 2 to Stage 3).
- Request for Supplemental Evidence or Additional Information.
- Scheduling of Formal Witness Interview (if applicable).
- Issuance of Final Case Finding and Executive Notice.

5.7 Multi-Party Linkage & Re-opening Protocols

If multiple complaints stem from a single operational incident, the CMS establishes a "Master Incident Linkage" where each individual complaint retains its unique CIN for tracking while sharing underlying investigative findings. In cases where new, material evidence is submitted post-closure, the Professional Standards Division Commander may authorize re-opening the case, moving the status from Stage 6 back to Stage 3 with an updated suffix (e.g., CMP-2026-0042-R1).

6.0 RESPONSIBILITIES

6.1 Chief Executive Officer (Dr. Brian C. Askew): Exercises ultimate executive oversight, approves all disposition findings, and ensures company compliance with Maryland state licensing laws.

6.2 Commander, Professional Standards / Internal Affairs: Administers the CMS, ensures sequential CIN allocation, monitors SLA compliance, conducts audit reviews, and oversees secure portal functionality.

6.3 24/7 Dispatch Supervisor: Manages real-time telephonic complaint intake, ensures immediate CMS entry, and provides callers with initial verbal CIN/SAC credentials.

6.4 Lead Investigators: Update case status stage markers in real time, upload investigation milestones, and compile redacted updates for complainant portal transmission.

7.0 COMPLIANCE & ENFORCEMENT

Strict compliance with this SOP is mandatory. Any attempt by a Matcom officer or employee to manipulate case numbers, bypass intake protocols, delete records, intimidate complainants, or withhold receipt issuance shall result in severe disciplinary sanctions up to immediate summary termination of employment, revocation of company credentials, civil action, and referral to the Maryland State Police Licensing Division for statutory enforcement under Title 13 of the Maryland Business Regulation Article.

8.0 RECORDS & DOCUMENTATION

All electronic tracking records, transaction logs, audit trails, and electronic receipts shall be preserved in Write-Once-Read-Many (WORM) immutable digital storage for a

minimum of seven (7) years following case closure, or longer if subject to active civil litigation, MPIA administrative appeals, or law enforcement subpoena.

9.0 EFFECTIVE DATE & REVIEW

This SOP shall take effect on August 13, 2026, superseding all prior informal tracking procedures. It shall be subject to mandatory annual review on or before August 13, 2027 by the Professional Standards Division and Office of General Counsel.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC



MATCOM OFFICE OF PUBLIC SAFETY LLC

**LICENSED MARYLAND SECURITY GUARD
AGENCY • MD LICENSE 24PLU-SGPD4620**

Headquarters: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Web: www.matcomops.org | **Email:**
Oga@matcomops.org

STANDARD OPERATING PROCEDURE

SOP-PUB-07: Public Evidence Submission & Supplemental Evidence

POLICY NUMBER	SOP-PUB-07
TITLE	Public Evidence Submission & Supplemental Evidence
EFFECTIVE DATE	August 13, 2026
REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO
RESPONSIBLE DIVISION	Professional Standards / Evidence Unit
PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure establishes clear, accessible, legally sound, and technically rigorous channels for complainants, witnesses, clients, and members of the public to submit digital and physical evidence supporting or supplementing a complaint filed with Matcom Office of Public Safety LLC. This SOP details file intake standards, encryption, anti-malware isolation, HIPAA-compliant medical record intake, and compliance with Maryland evidence laws.

1.2 Scope: This procedure applies to all initial and supplemental evidence submissions associated with active or re-opened complaint files (format 2026-XXXX).

It governs all forms of tangible and digital evidence, including digital photographs, mobile phone video recordings, dashcam/CCTV footage, audio recordings, text messages, social media screenshots, medical reports, repair invoices, written witness declarations, and physical media items delivered to Matcom headquarters or field investigators.

2.0 AUTHORITY & LEGAL REFERENCES

2.1 Statutory Authority: Promulgated under the authority of Dr. Brian C. Askew, CEO, in compliance with Maryland regulatory mandates governing security agency oversight and digital evidence preservation.

2.2 Primary Legal References:

- **Maryland Courts & Judicial Proceedings Article § 10-402 (Maryland Wiretap Act):** Governs wiretapping and electronic surveillance. Requires strict compliance regarding audio recording consent and handling illegally intercepted communications.
- **Maryland Rules of Evidence (Rule 5-901 & 5-902):** Authentication and self-authentication standards for electronic records, digital photos, and computer-generated media.
- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02:** Record preservation and operational evidence requirements for security guard agencies.
- **Health Insurance Portability and Accountability Act (HIPAA), 45 CFR § 164:** Standards for secure intake and encryption of protected health information (PHI) submitted as medical evidence.
- **Maryland Public Information Act (MPIA), State Gov't Art. § 4-101 et seq.:** Confidentiality requirements governing evidentiary records held by administrative agencies.

3.0 DEFINITIONS

3.1 Digital Evidence: Any information or data of evidentiary value that is stored or transmitted in binary form, including video, audio, digital photos, electronic mail, text messages, and digital document files.

3.2 Supplemental Evidence: Additional evidentiary materials submitted after the initial complaint filing, appended to an existing active Case Identification Number (CIN: 2026-XXXX).

3.3 Secure Evidence Ingestion Gateway (SEIG): Matcom's TLS 1.3 encrypted web intake portal that validates, virus-scans, time-stamps, and cryptographically hashes uploaded files upon arrival.

3.4 Cryptographic Hash (SHA-256): A unique 64-character hexadecimal algorithm string produced from the exact binary content of a digital file, serving as a digital fingerprint to detect any subsequent alteration or tampering.

3.5 Malware Quarantine Container: An isolated, sandboxed virtual environment where incoming digital files are executed and analyzed for malicious payloads prior to database ingestion.

4.0 POLICY

4.1 Open Evidence Access Policy: Matcom maintains a open evidence submission policy. Any complainant or witness possesses the unconditional right to submit supporting evidentiary material at any point during an active investigation, prior to final executive adjudication.

4.2 Evidence Non-Alteration Mandate: All digital and physical evidence submitted to Matcom shall be stored in its raw, unaltered, native format. No Matcom employee shall edit, trim, filter, adjust, compress, or delete any public evidence submission.

4.3 Wiretap Act Compliance Advisory: Pursuant to Maryland Courts & Judicial Proceedings § 10-402, Maryland is a two-party (all-party) consent state for recording oral private communications where a reasonable expectation of privacy exists. However, audio recorded in public places where no expectation of privacy exists, or video recordings without audio, are lawful. Matcom's intake portal provides statutory advisories regarding audio recordings.

5.0 PROCEDURES

5.1 Public Evidence Submission Pathways

Members of the public may submit initial or supplemental evidence through four approved pathways:

SUBMISSION PATHWAY	ACCESS POINT / OPERATIONAL LOCATION	OPERATING HOURS & PROCESSING TIME
1. Secure Online Web Portal	www.matcomops.org/evidence	24/7/365 Availability; Instant automated processing

SUBMISSION PATHWAY	ACCESS POINT / OPERATIONAL LOCATION	OPERATING HOURS & PROCESSING TIME
2. Direct Email Intake	evidence@matcomops.org	24/7 Ingestion; Logged within 2 hours by Evidence Unit
3. In-Person Headquarters Drop-off	6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207	Mon-Fri 08:00 - 17:00 EST; Immediate physical receipt issued
4. Investigator Field Collection	On-site / Field Interview Location	By appointment; Investigator issues paper/digital receipt

5.2 File Category Specifications & Technical Parameters

The SEIG platform supports a wide spectrum of digital file categories and formats:

EVIDENCE CATEGORY	ACCEPTED FILE FORMATS	MAX FILE SIZE LIMIT	SPECIAL TECHNICAL INSTRUCTIONS
Digital Photographs	JPEG, PNG, HEIC, TIFF, RAW, BMP	100 MB per file	Preserve original EXIF metadata (GPS, timestamp, camera model). Do not screenshot.
Video Footage	MP4, MOV, AVI, WMV, MKV, M4V, 3GP	5 GB per session	Upload raw uncompressed clip from phone/dashcam/CCTV. Do not export through social apps.
Audio Recordings	MP3, WAV, M4A, AAC, OGG, FLAC	500 MB per file	Indicate whether recording occurred in public space or with participant consent.
Medical Records & Bills	PDF, JPEG, PNG	200 MB per file	Uploaded via HIPAA 256-bit AES encrypted channel. Protected health data restricted to IA.
Text & Chat Logs	PDF, PNG, JPEG, TXT, MSG, EML	100 MB per file	Include full header/sender details and timestamps where possible.
Written Documents	PDF, DOCX, RTF, TXT	100 MB per file	Signed witness statements or expert evaluations.

5.3 Supplemental Evidence Submission Workflow

To append supplemental evidence to an existing case, complainants execute the following steps:

1. Navigate to www.matcomops.org/evidence and select **"Add Supplemental Evidence."**
2. Input the assigned Case Identification Number (e.g., 2026-0042) and the 12-character Secure Access Code (SAC).
3. Select the Evidence Category from the drop-down menu (e.g., "Medical Records", "Supplemental Video").
4. Drag and drop files or select files from local device storage.
5. Enter a brief descriptive annotation for each file (e.g., "Photo showing bruise on left wrist taken Aug 14, 2026 at 09:00").
6. Click **"Submit Evidence Securely."**

5.4 Automated Automated Ingestion, Virus Screening & Hashing Protocol

Upon receipt of any digital file, the SEIG automatically executes a 4-step security and integrity workflow:

AUTOMATED TECHNICAL INGESTION SEQUENCE

Step 1: Anti-Malware Sandboxing: File is routed to an isolated quarantine container and scanned with dual anti-virus engines. If infected, the file is safely contained, quarantined, and flagged for IT Security review without corrupting the system.

Step 2: MIME-Type & Header Validation: System verifies file extensions against binary headers to prevent executable code execution masked as media files.

Step 3: SHA-256 Hashing: An automated algorithm calculates the SHA-256 cryptographic hash of the exact binary payload.

Step 4: Master Inventory Logging: File is moved to WORM (Write-Once-Read-Many) encrypted storage and assigned an Evidence Identifier (e.g., EVD-2026-0042-01).

5.5 Physical Media Intake Protocols

When physical media items (USB flash drives, SD cards, CD/DVDs, external hard drives, or original paper documents) are delivered to Matcom Headquarters or field investigators:

- The receiving officer immediately completes Form EVD-101 (Physical Evidence Intake Log).

- The physical item is placed into a tamper-evident, anti-static evidence bag and sealed in the presence of the submitter where feasible.
- A unique barcode label corresponding to the CIN is affixed to the bag.
- The submitter receives a duplicate physical receipt signed by the receiving officer with official agency stamp.
- The media is transferred to the Evidence Vault within two (2) hours for forensic imaging.

5.6 Automated Proof of Evidence Receipt

Within sixty (60) seconds of successful upload, the portal generates a downloadable, print-ready "Proof of Evidence Receipt" (PDF) dispatched to the complainant's email containing:

- Official Agency Header & MD License Number (24PLU-SGPD4620).
- Associated Case Identification Number (CIN).
- Exact Timestamp of Upload Completion (UTC and Eastern Standard/Daylight Time).
- Original File Name and Uploaded Byte Size.
- Calculated Cryptographic SHA-256 Hash String.
- Assigned Evidence Identifier (e.g., EVD-2026-0042-01).

5.7 Maryland Wiretap Act Compliance Procedures

If a submitted audio file appears to contain private oral communications recorded without clear multi-party consent:

- The SEIG system displays a statutory disclosure warning prior to upload.
- If uploaded, the file is flagged with a WIRETAP-REVIEW-REQUIRED tag.
- The Lead Investigator immediately consults the Office of General Counsel prior to listening to or utilizing the audio recording in investigative proceedings.
- If determined to violate MD Cts & Jud Proc § 10-402, the recording is segregated in a restricted legal vault and evaluated under statutory administrative conduct exceptions.

6.0 RESPONSIBILITIES

6.1 Commander, Evidence Unit: Oversees the SEIG platform, maintains physical evidence vault security, audits hash verification routines, and manages evidence retention schedules.

6.2 IT / Cyber Security Administrator: Maintains server encryption protocols (TLS 1.3, AES-256), performs anti-malware engine updates, and ensures 99.9% uptime for public upload portals.

6.3 Professional Standards Investigators: Review submitted evidence within twenty-four (24) hours of receipt, integrate verified evidence into active investigative case files, and request supplemental documentation when necessary.

7.0 COMPLIANCE & ENFORCEMENT

Any employee who deliberately conceals, alters, tampers with, fails to log, or unlawfully disposes of public evidence submissions shall be terminated immediately for cause and subjected to criminal prosecution under Maryland Criminal Law Article § 9-307 (Tampering with Physical Evidence) and reported to the Maryland State Police Licensing Division.

8.0 RECORDS & DOCUMENTATION

All digital evidence, cryptographic hash manifests, physical media intake logs, and upload receipts shall be retained in immutable storage for a minimum of seven (7) years following case closure, adhering strictly to COMAR 12.10.01 evidence standards.

9.0 EFFECTIVE DATE & REVIEW

This SOP takes effect on August 13, 2026. It shall be reviewed annually on or before August 13, 2027 by the Professional Standards Division Commander, Evidence Unit Supervisor, and Office of General Counsel.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC



MATCOM OFFICE OF PUBLIC SAFETY LLC

**LICENSED MARYLAND SECURITY GUARD
AGENCY • MD LICENSE 24PLU-SGPD4620**

Headquarters: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Web: www.matcomops.org | **Email:**
Oga@matcomops.org

STANDARD OPERATING PROCEDURE

SOP-PUB-08: Evidence Integrity & Chain of Custody

POLICY NUMBER	SOP-PUB-08
TITLE	Evidence Integrity & Chain of Custody
EFFECTIVE DATE	August 13, 2026
REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO
RESPONSIBLE DIVISION	Professional Standards / Evidence Unit
PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure defines the mandatory technical architecture, administrative rules, security standards, and physical protocols required to ensure the absolute integrity and unbroken Chain of Custody (CoC) for all evidence collected by or submitted to Matcom Office of Public Safety LLC. This policy establishes cryptographic verification, automated audit tracking, role-based access controls, time-stamping standards, and secure retention mechanics necessary to satisfy criminal and civil court admissibility thresholds under Maryland law.

1.2 Scope: This SOP governs all digital evidence (video, audio, photographs, electronic logs, system backups) and physical evidence (weapons, clothing, paper documents, physical media storage devices) held within Matcom's Digital Evidence Management System (DEMS) or Physical Evidence Vault. It applies to all Matcom employees, investigators, evidence custodians, supervisors, and executive officers.

2.0 AUTHORITY & LEGAL REFERENCES

2.1 Statutory Authority: Promulgated by Dr. Brian C. Askew, CEO, pursuant to Maryland security agency regulatory mandates and forensic evidence standards.

2.2 Primary Legal & Technical Standards:

- **Maryland Rules of Evidence (Rule 5-901, 5-902, 5-1001 through 5-1008 - Best Evidence Rule):** Governing authentication, original document rules, and digital record admissibility.
- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02:** Security guard agency recordkeeping, physical security, and evidence handling regulations.
- **ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence:** International benchmark for digital forensic integrity.
- **NIST Special Publication 800-86:** Guide to Integrating Forensic Techniques into Incident Response.
- **Maryland Business Regulation Article Title 13 (Maryland Security Guards Act):** Mandatory recordkeeping and regulatory compliance standards.
- **Maryland Public Information Act (MPIA), State Gov't Art. § 4-101 et seq.:** Statutory rules regarding public evidence disclosure and confidentiality exemptions.

3.0 DEFINITIONS

3.1 Chain of Custody (CoC): The chronological, unbroken, legally defensible written and electronic documentation showing the receipt, custody, control, transfer, analysis, and disposition of physical and digital evidence.

3.2 Evidence Identifier: A unique 16-character alphanumeric code formatted as EVD-2026-XXXX-YYYY (Year-Case Number-Item Number) permanently bound to each evidence item.

3.3 Cryptographic Hash Verification: The process of generating a unique SHA-256 binary string upon intake and continuously recalculating it during storage to prove that no bit, byte, or frame of data has been altered.

3.4 Write-Once-Read-Many (WORM) Storage: Unalterable cloud and local storage architecture preventing any file modification, overwrite, or premature deletion once committed.

3.5 Stratum-1 Time Synchronization: Network Time Protocol (NTP) server synchronization linked to the United States Naval Observatory (USNO) atomic clock, guaranteeing ISO 8601 timestamp accuracy within ± 1 millisecond.

3.6 Immutable Audit Trail: An unalterable system ledger recording every user interaction with an evidence file, including view, play, export, transfer, permission change, or metadata inspection.

4.0 POLICY

4.1 Inviolability of Chain of Custody: Every item of evidence entering Matcom's possession must have an unbroken Chain of Custody. Any gap, unrecorded transfer, missing hash check, or unauthorized access compromises the evidence and shall trigger an immediate Internal Affairs investigation.

4.2 Dual-Storage Cryptographic Hash Mandate: Digital evidence must be hashed using SHA-256 at the point of ingestion and stored across dual geographically redundant WORM locations. Original raw media files must never be edited, transcoded, or overwritten.

4.3 Least Privilege Access Control: Access to evidence items is restricted strictly on a Need-to-Know / Least Privilege basis. No employee, regardless of rank, possesses default access to evidence files outside their assigned active investigations.

5.0 PROCEDURES

5.1 Evidence Identification System

Every evidence item is assigned a standardized Evidence Identifier upon intake:

STANDARDIZED EVIDENCE IDENTIFIER PROTOCOL

EVD-2026-XXXX-YYYY

Example: EVD-2026-0042-0001 (First evidence item associated with Case 2026-0042)

- EVD: Global Evidence Tag

- 2026: Active Case Year
- XXXX: Sequential Case Tracking Number (0001 - 9999)
- YYYY: Individual Item Sequence Number (0001 - 9999)

5.2 Cryptographic Hash Integrity Mechanics

To satisfy Maryland evidence authentication rules (Rule 5-901), the DEMS executes the following hashing protocol:

1. **Primary Hash Generation:** Immediately upon upload completion or forensic drive imaging, the system computes a primary SHA-256 hash (64-character hex string).
2. **Secondary Hash Verification:** A secondary MD5 hash is calculated concurrently to provide cross-algorithm redundancy.
3. **Database Registration:** Hash values are written into an immutable, append-only database table cryptographically signed by the agency's root security key.
4. **Automated Integrity Cron-Audits:** Every thirty (30) days, an automated background job recalculates the SHA-256 hash of all stored files and compares it against the initial intake hash. Any variance triggers an instant priority security alert to the Chief Information Security Officer (CISO).

5.3 Stratum-1 Time Synchronization Standards

All server hardware, video recorders, body-worn cameras, dispatch terminals, and evidence workstations must synchronize clock timers every sixty (60) seconds with Matcom's primary Stratum-1 NTP server. Timestamps appended to CoC log entries strictly adhere to ISO 8601 standard: YYYY-MM-DDTHH:MM:SS.sss-04:00 (Eastern Time Zone with UTC offset).

5.4 Access Controls & Role-Based Permission Matrix

System access to evidence files within DEMS is managed strictly via Role-Based Access Control (RBAC):

USER ROLE	VIEW / STREAM	DOWNLOAD RAW FILE	EXPORT REDACTED COPY	MODIFY METADATA	DELETE FILE
Public Complainant (via Portal)	YES (Watermarked)	NO	NO	NO	NO
Field Security Guard	Upload Only	NO	NO	NO	NO

USER ROLE	VIEW / STREAM	DOWNLOAD RAW FILE	EXPORT REDACTED COPY	MODIFY METADATA	DELETE FILE
Lead IA Investigator	YES	YES (Logged)	YES (Logged)	NO (Notes Only)	NO
Evidence Unit Custodian	YES	YES	YES	Tagging Only	NO
Professional Standards Commander	YES	YES	YES	YES (Admin Tags)	NO
Chief Executive Officer (CEO)	YES	YES	YES	YES	Authorization Only

5.5 Immutable Audit Log Structure

Every interaction with an evidence file generates an immutable audit record containing eight mandatory data points:

- **Log Entry Sequence ID:** Auto-incrementing 64-bit integer.
- **Exact Timestamp:** ISO 8601 Stratum-1 synchronized time.
- **User Account ID & Badge Number:** Authenticated operator identity.
- **Source IP & MAC Address:** Physical network workstation identifier.
- **Evidence Identifier:** Target EVD-2026-XXXX-YYYY.
- **Action Executed:** (VIEW, PLAY, DOWNLOAD_RAW, EXPORT_REDACTED, PERMISSION_CHANGE).
- **SHA-256 Post-Action Verification:** Hash check confirmation post-access.
- **Reason for Access:** Mandatory text field entered by investigator prior to file unlock.

5.6 Physical Evidence Vault Protocols

For physical evidence items (weaponry, uniform items, physical media, paper records):

- **Vault Location:** Matcom Headquarters (6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207), Secure Evidence Vault.
- **Physical Security:** Solid steel door, dual-custody biometric keycard lock, 24/7 high-definition CCTV coverage with 365-day video retention.

- **Temporary Drop Box:** Field officers submit after-hours evidence into heavy-gauge one-way drop lockers. Once closed, lockers can only be opened by the Evidence Unit Custodian.
- **Physical Log Form EVD-102:** Every physical transfer requires physical signatures from both releasing and receiving parties, recording date, exact time, and reason for transfer.

5.7 Evidence Retention, Disposal & Litigation Holds

Evidence is retained according to strict legal schedules:

CLASSIFICATION / CASE TYPE	MANDATORY RETENTION PERIOD	STATUTORY AUTHORITY
General Public Complaints (Class III/IV)	7 Years Post-Closure	COMAR 12.10.01 Standard
Serious Misconduct / Excessive Force (Class I)	10 Years Post-Closure	Maryland Police Accountability Act / Civil Statute
Active Civil Litigation / Subpoena Matter	Indefinite Hold (Litigation Hold)	Judicial Order / COMAR Rule
Criminal Investigation Referral	Permanent / Until Statute of Limitations Expires	MD Criminal Procedure Code

Certified Destruction Mechanics: Upon expiration of mandatory retention periods and absence of active litigation holds, digital evidence undergo DoD 5220.22-M cryptographic wipe. Physical items are incinerated or shredded by a certified contractor. Certified Certificates of Destruction are signed by the Evidence Custodian and CEO and preserved permanently in the CMS.

6.0 RESPONSIBILITIES

6.1 CEO (Dr. Brian C. Askew): Authorizes evidence destruction, enforces agency-wide evidentiary compliance, and approves external law enforcement transfers.

6.2 Chief Information Security Officer (CISO): Maintains DEMS cryptographic infrastructure, monitors automated hash audit routines, and audits network access logs.

6.3 Evidence Unit Custodian: Maintains physical vault inventory, manages physical CoC forms, conducts monthly physical audits, and handles court subpoena transfers.

6.4 IA Investigators: Adhere to least privilege rules, record precise access justifications, and ensure initial field evidence is properly cataloged and hashed.

7.0 COMPLIANCE & ENFORCEMENT

Falsifying chain of custody logs, tampering with cryptographic hashes, granting unauthorized evidence access, or destroying evidence subject to active inquiry constitutes gross official misconduct resulting in immediate employment termination, civil litigation, and criminal prosecution under MD Criminal Law Art. § 9-307.

8.0 RECORDS & DOCUMENTATION

Chain of Custody ledgers, hash verification manifests, access audit logs, and Certificates of Destruction are permanent administrative records retained indefinitely in Matcom's master archive.

9.0 EFFECTIVE DATE & REVIEW

This SOP takes effect on August 13, 2026, and shall undergo annual joint review by the Evidence Unit, CISO, and Office of General Counsel on or before August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC



MATCOM OFFICE OF PUBLIC SAFETY LLC

**LICENSED MARYLAND SECURITY GUARD
AGENCY • MD LICENSE 24PLU-SGPD4620**

Headquarters: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Web: www.matcomops.org | **Email:**
Oga@matcomops.org

STANDARD OPERATING PROCEDURE

SOP-PUB-09: Complaint Classification & Referral Procedure

POLICY NUMBER	SOP-PUB-09
TITLE	Complaint Classification & Referral Procedure
EFFECTIVE DATE	August 13, 2026
REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO
RESPONSIBLE DIVISION	Professional Standards / Internal Affairs
PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure defines the objective screening criteria, risk-based classification hierarchy, and mandatory referral routing protocols for all complaints, reports of misconduct, and administrative grievances submitted to Matcom Office of Public Safety LLC. The primary objective is to ensure that every complaint is evaluated promptly, classified accurately, and routed to the proper internal investigative division, executive body, or external regulatory/law enforcement authority without delay or bias.

1.2 Scope: This procedure applies to all initial complaints logged into the Case Management System (CMS) under format 2026-XXXX. It governs routing decisions across Internal Affairs, Professional Standards, Field Operations Supervision, Human Resources, Office of General Counsel, Risk Management, local law enforcement agencies, State's Attorney Offices, and the Maryland State Police Licensing Division.

2.0 AUTHORITY & LEGAL REFERENCES

2.1 Statutory Authority: Promulgated under the executive authority of Dr. Brian C. Askew, CEO, pursuant to Maryland private security statutory oversight regulations.

2.2 Primary Statutory References:

- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02:** Mandatory reporting requirements for security guard agencies, including mandatory notification to the Maryland State Police Licensing Division for security guard arrests, weapon discharges, or serious license qualification violations.
- **Maryland Business Regulation Article, Title 13 (Maryland Security Guards Act):** Regulatory enforcement standards and agency disciplinary oversight rules.
- **Maryland Police Accountability Act of 2022:** Mandatory public transparency, complaint triage standards, and external referral mandates.
- **Maryland Criminal Procedure Article § 2-101 et seq.:** Statutory criteria governing mandatory referral of criminal allegations to sworn law enforcement entities and State's Attorney Offices.
- **Maryland Public Information Act (MPIA), State Gov't Art. § 4-101 et seq.:** Public disclosure and agency record-sharing regulations.

3.0 DEFINITIONS

3.1 Complaint Triage: The initial administrative screening conducted within twenty-four (24) hours of complaint intake to analyze allegations, determine legal jurisdiction, evaluate immediate risk, and assign a binding Classification Tier.

3.2 Class I Misconduct (Serious / High-Risk): Allegations involving excessive or illegal force, unauthorized discharge of a firearm, criminal acts, sexual misconduct/harassment, constitutional violations, corruption, or false imprisonment.

3.3 Class II Administrative Violation: Allegations involving operational policy non-compliance, equipment misuse, uniform deficiencies, tardiness, insubordination, or minor report errors.

3.4 Class III Customer Service Misunderstanding: Grievances related to perceived rudeness, interpersonal miscommunication, tone of voice, or minor client service dissatisfaction.

3.5 Class IV Frivolous / Duplicate Complaint: Filings demonstrably lacking factual basis, duplicate entries, or unsubstantiated claims clearly refuted by objective initial evidence.

3.6 Mandatory External Referral: A statutory obligation requiring Matcom to transfer investigative jurisdiction or provide immediate notice to external bodies (e.g., Maryland State Police, local Police Department, State's Attorney, or MD Civil Rights Commission).

4.0 POLICY

4.1 Mandatory 24-Hour Screening: All complaints logged in the CMS shall be reviewed and classified by the Professional Standards Division Commander within twenty-four (24) hours of ingestion.

4.2 Mandatory Criminal Referral: If initial intake screening or subsequent investigation reveals reasonable suspicion that a crime has been committed by Matcom personnel, the CEO and Office of General Counsel shall immediately refer the matter to the appropriate local law enforcement agency and State's Attorney Office.

4.3 Mandatory Regulatory Reporting to MSP: Pursuant to COMAR 12.10.01, Matcom shall submit formal written notification to the Maryland State Police Licensing Division within twenty-four (24) hours whenever a licensed security guard is involved in a firearm discharge, arrest, felony charge, or serious licensing violation.

5.0 PROCEDURES

5.1 Complaint Screening & Triage Process

Upon receipt of a new complaint (CIN: 2026-XXXX), the Professional Standards Intake Officer executes a 3-step screening process:

1. **Jurisdictional Review:** Verifies whether the alleged incident involves Matcom personnel, contracted property, or official duties.

2. **Immediate Risk Assessment:** Evaluates whether an ongoing safety threat exists. If active safety risks are identified, the subject officer is immediately suspended from field duty pending investigation.
3. **Tier Assignment:** Formally assigns a Classification Tier (Class I, II, III, or IV) in the CMS.

5.2 Four-Tier Classification Hierarchy

Allegations are categorized according to the following strict classification criteria:

CLASSIFICATION TIER	ALLEGATION CRITERIA & EXAMPLES	PRIMARY INVESTIGATIVE UNIT	MANDATORY EXECUTIVE / EXTERNAL NOTICES
CLASS I (Serious Misconduct)	• Excessive / Unlawful Use of Force • Firearm / Less-Lethal Weapon Discharge • Alleged Criminal Offenses (Theft, Assault, Extortion) • Sexual Harassment / Sexual Assault • False Arrest / Unlawful Detention • Civil Rights Violations / Bias Offenses	Internal Affairs Division (IA)	• CEO (Immediate) • Office of General Counsel • MD State Police Licensing Div. • Local Police (if criminal)
CLASS II (Administrative / Operational)	• Failure to Follow Post Orders • Unauthorized Absence / Sleeping on Duty • Uniform & Equipment Violations • Insubordination / Disrespect to Supervisor • Incomplete Shift Incident Reports	Field Operations Supervision / Operations Commander	• Professional Standards Division • Operations Manager
CLASS III (Customer Service)	• Unprofessional Demeanor / Tone of Voice • Perceived Lack of	Site Supervisor / Customer Service Unit	• Operations Manager

CLASSIFICATION TIER	ALLEGATION CRITERIA & EXAMPLES	PRIMARY INVESTIGATIVE UNIT	MANDATORY EXECUTIVE / EXTERNAL NOTICES
	Assistance • Interpersonal Miscommunication • Minor Client Service Disputes		• Client Liaison Officer
CLASS IV (Frivolous / Duplicate)	• Demonstrably False on Face (Refuted by Video) • Duplicate Submission for Same Incident • Incoherent or Nonsensical Submissions	Internal Affairs Intake Officer	• Professional Standards Commander (Closure Sign-off)

5.3 Comprehensive Referral Routing Matrix

Based on the assigned Tier and subject matter, complaints are routed according to the following matrix:

TARGET UNIT / ENTITY	REFERRAL TRIGGER & CRITERIA	ACTION REQUIRED
Internal Affairs Division	Class I Misconduct; complex multi-officer incidents	Conduct formal IA investigation under SOP-PUB-10
Field Operations Supervision	Class II Administrative & Class III Service matters	Conduct supervisory review, counselling, or retraining
Human Resources Division	EEO claims, workplace discrimination, wage disputes	Execute HR labor review under Employee Handbook
Legal & Risk Management	Claims of bodily injury, property damage, civil notice	Initiate legal hold, notify insurance carrier
Local Police / State's Attorney	Probable criminal violations by staff or public	Formal criminal referral and evidence transfer
MD State Police Licensing Div.	Firearm discharge, security guard arrest, felony charge	Mandatory regulatory notice per COMAR 12.10.01

5.4 External Referral Mechanics & Notice Protocols

When a complaint triggers a mandatory external referral:

MANDATORY EXTERNAL REFERRAL WORKFLOW

1. Executive Authorization: The IA Commander drafts Form REF-201 (External Agency Referral Form) and submits it to CEO Dr. Brian C. Askew and Legal Counsel for sign-off within twelve (12) hours.

2. Evidence Packet Transmission: Complete evidence copies (including SHA-256 hash manifests) are compiled and delivered via secure encrypted transfer to the outside law enforcement agency or MSP Licensing Division.

3. Administrative Concurrent Hold: Matcom's administrative investigation may be paused or conducted concurrently as requested by prosecuting authorities to avoid interfering with criminal investigations.

5.5 Complainant Referral Notification Directive

Within twenty-four (24) hours of a referral decision, the CMS automatically transmits a formal "Notice of Referral" to the complainant detailing:

- The official Case Identification Number (CIN: 2026-XXXX).
- The specific division or external agency assuming primary investigative jurisdiction.
- Contact information (agency name, point of contact, phone number) for external referrals.
- Instructions on how to continue tracking the administrative component via www.matcomops.org/tracking.

6.0 RESPONSIBILITIES

6.1 CEO (Dr. Brian C. Askew): Approves all Class I classification decisions, signs mandatory criminal and Maryland State Police referrals, and directs immediate emergency suspensions.

6.2 Commander, Professional Standards / IA: Executes daily complaint screening within 24 hours, enforces classification consistency, and manages the referral matrix.

6.3 Director of Human Resources: Adjudicates EEO, labor, and workplace harassment referrals in coordination with IA.

6.4 Operations Managers: Resolve Class II and III referrals within fourteen (14) business days and submit supervisory resolution reports to IA.

7.0 COMPLIANCE & ENFORCEMENT

Failing to classify a Class I misconduct allegation, deliberately misclassifying serious misconduct as a minor administrative matter to bypass IA oversight, or concealing mandatory reporting events from the Maryland State Police constitutes gross insubordination and willful breach of statutory duty, resulting in immediate termination and regulatory sanction.

8.0 RECORDS & DOCUMENTATION

All classification worksheets, referral forms (REF-201), external agency transmittal receipts, and complainant referral notices shall be permanently attached to the CMS case file and preserved for seven (7) years in WORM storage.

9.0 EFFECTIVE DATE & REVIEW

This SOP shall become effective on August 13, 2026. It shall be reviewed annually on or before August 13, 2027 by the Professional Standards Division, Office of General Counsel, and Executive Leadership.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC



MATCOM OFFICE OF PUBLIC SAFETY LLC

**LICENSED MARYLAND SECURITY GUARD
AGENCY • MD LICENSE 24PLU-SGPD4620**

Headquarters: 6340 Security Blvd.,
Suite 100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Web: www.matcomops.org | **Email:**
Oga@matcomops.org

STANDARD OPERATING PROCEDURE

SOP-PUB-10: Internal Affairs Investigation Process

POLICY NUMBER	SOP-PUB-10
TITLE	Internal Affairs Investigation Process
EFFECTIVE DATE	August 13, 2026
REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO
RESPONSIBLE DIVISION	Professional Standards / Internal Affairs
PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure provides a plain-language, transparent, step-by-step public explanation of the complete lifecycle of an Internal Affairs (IA) investigation conducted by Matcom Office of Public Safety LLC. It outlines the exact investigative mechanics that occur from initial intake to final executive disposition, demonstrating how Matcom maintains rigorous public accountability, thorough evidence analysis, impartial fact-finding, and strict compliance with Maryland constitutional due process standards.

1.2 Scope: This procedure governs all Class I serious misconduct investigations and complex administrative inquiries assigned to the Professional Standards / Internal Affairs Division involving Matcom personnel, including armed and unarmed security guards, special police officers, field supervisors, dispatchers, and management personnel.

2.0 AUTHORITY & LEGAL REFERENCES

2.1 Statutory Authority: Promulgated under the executive authority of Dr. Brian C. Askew, CEO, in accordance with Maryland security agency regulatory laws.

2.2 Primary Legal References:

- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02:** Security guard agency oversight, mandatory investigation standards, and licensing rules.
- **Maryland Business Regulation Article, Title 13 (Maryland Security Guards Act):** Disciplinary oversight and professional standards regulations.
- **Maryland Police Accountability Act of 2022:** Standards for complaint investigation, investigative transparency, and formal disciplinary findings.
- **Maryland Constitutional Due Process (Declaration of Rights, Art. 24) & U.S. Constitution (14th Amendment):** Guaranteeing procedural due process rights for subject employees and complainants.
- **Garrity v. New Jersey, 385 U.S. 493 (1967):** Legal principles governing compelled administrative statements and protection against self-incrimination.
- **Cleveland Board of Education v. Loudermill, 470 U.S. 532 (1985):** Pre-disciplinary due process hearing rights for employees.
- **Maryland Public Information Act (MPIA), State Gov't Art. § 4-101 et seq.:** Confidentiality rules and public disclosure parameters for completed investigation summaries.

3.0 DEFINITIONS

3.1 Internal Affairs Investigation: A formal administrative inquiry conducted by designated Professional Standards investigators to determine whether a Matcom employee violated company policies, post orders, civil rights laws, or state security guard regulations.

3.2 Lead Investigator: An experienced Professional Standards investigator assigned by the IA Commander to manage evidence collection, interview witnesses, interrogate subject officers, and draft the final Report of Investigation (ROI).

3.3 Subject Employee: The specific Matcom security officer, supervisor, or staff member against whom allegations of misconduct have been formally lodged.

3.4 Preponderance of the Evidence: The legal standard of proof required in administrative IA adjudications, meaning that the evidence shows that it is "more likely true than not" (greater than 50% probability) that the alleged misconduct occurred.

3.5 Garrity Disclosure / Compelled Statement: A formal administrative warning advising a subject employee that they are required to answer questions truthfully regarding their official duties, but that their compelled administrative statements cannot be used against them in subsequent criminal prosecution.

4.0 POLICY

4.1 Commitment to Objective Impartiality: All Internal Affairs investigations shall be conducted thoroughly, objectively, and without bias or preconceived conclusions. Investigators serve as neutral finders of fact.

4.2 Standard 30-Day Resolution Timeline: Internal Affairs investigations shall be completed within thirty (30) calendar days from formal assignment. If extraordinary circumstances require an extension (e.g., awaiting forensic analysis or criminal prosecution holds), the IA Commander must submit a written request to the CEO for a maximum 30-day extension, notifying the complainant in writing.

4.3 Standard of Proof & Executive Approval: Adjudication findings must be supported by a Preponderance of the Evidence. All final investigative dispositions and proposed disciplinary actions require formal written approval from CEO Dr. Brian C. Askew.

5.0 PROCEDURES

5.1 Ten-Stage Lifecycle of an Internal Affairs Investigation

Every accepted complaint assigned to the Internal Affairs Division progresses through ten distinct operational stages:

THE 10 OPERATIONAL STAGES OF AN IA INVESTIGATION

Stage 1: Intake & Preliminary Assessment — Verification of case details, jurisdiction check, and CIN allocation.

Stage 2: Investigator Assignment & Conflict Check — Appointment of Lead Investigator free of personal/professional conflicts.

Stage 3: Investigative Planning & Evidence Gathering — Review of CCTV, Body-Worn Camera (BWC), GPS, radio logs, and dispatch tapes.

Stage 4: Witness & Complainant Interviews — Formal audio-recorded interviews and sworn written statements.

Stage 5: Subject Employee Notice & Interrogation — Written notice of charges, Garrity advisement, and recorded interrogation.

Stage 6: Investigative Analysis & Timeline Reconstruction — Synthesis of physical evidence, statement matrices, and policy analysis.

Stage 7: Report of Investigation (ROI) Assembly — Drafting comprehensive written ROI detailing facts and evidence.

Stage 8: Command & Legal Review — Legal review by Office of General Counsel and IA Commander approval.

Stage 9: Executive Adjudication & Finding Rendered — Formal adjudication by CEO Dr. Brian C. Askew.

Stage 10: Complainant Notification & Closing Transmittal — Public portal update, formal notice letter, and regulatory notices.

5.2 Evidence Collection Standards

During Stage 3, the Lead Investigator systematically collects and secures all relevant evidence pursuant to SOP-PUB-07 and SOP-PUB-08:

- **Digital Video & Audio:** Closed-circuit television (CCTV) footage, mobile phone videos, dashcam clips, and body-worn camera recordings. All video is hashed (SHA-256) upon retrieval.
- **Electronic Operational Logs:** Computer-Aided Dispatch (CAD) incident logs, electronic tour-verification guard tour scanner data, radio voice transmissions, and GPS vehicle tracking history.
- **Documentary Evidence:** Daily Shift Logs, Incident Reports, Visitor Register Sheets, Property Handover Logs, and training certification records.

5.3 Witness & Subject Employee Interview Protocols

During Stages 4 and 5, formal interviews are conducted under strict procedural standards:

1. **Complainant & Witness Interviews:** Conducted in person or via secure video conference. Interviews are digitally recorded, transcribed, and incorporated into the master case file. Complainants may be accompanied by a representative.
2. **Subject Employee Notice:** The subject employee receives Form IA-102 (Notice of Internal Affairs Investigation) at least forty-eight (48) hours prior to interrogation, specifying the exact policy provisions allegedly violated.

3. **Garrity Advisement:** Prior to interrogation, the subject employee is provided written Garrity Disclosures. Employees are obligated to answer truthfully; failure to cooperate constitutes insubordination leading to employment termination.

5.4 The Five Standardized Adjudication Findings

Upon evaluating all gathered evidence against policy provisions, the investigation concludes with one of five binding disposition categories:

FINDING CATEGORY	OFFICIAL LEGAL / ADMINISTRATIVE DEFINITION	ADMINISTRATIVE OUTCOME
SUSTAINED	The investigation disclosed sufficient evidence to prove by a Preponderance of the Evidence that the subject employee committed the alleged misconduct.	Formal disciplinary sanction issued; mandatory retraining, suspension, or termination.
UNFOUNDED	The investigation proved by clear evidence that the alleged act(s) did not occur or that the subject employee was not involved.	Employee exonerated; record cleared; no disciplinary action taken.
EXONERATED	The evidence established that the incident occurred, but the subject employee's actions were lawful, proper, justified, and fully within company policy.	Employee exonerated; incident deemed proper tactical/operational response.
NOT SUSTAINED	The investigation failed to discover sufficient evidence to clearly prove or disprove the allegation by a preponderance of the evidence.	Inconclusive finding; no formal disciplinary action; case closed without prejudice.
POLICY FAILURE	The evidence showed that the incident occurred, but revealed a flaw, ambiguity, or inadequacy in agency SOPs or training standards.	Policy revised; agency-wide retraining ordered; employee not disciplined.

5.5 Executive Adjudication & Disciplinary Framework

In Stage 9, the complete Report of Investigation is presented to CEO Dr. Brian C. Askew. If a finding of **SUSTAINED** is rendered, the CEO selects progressive disciplinary sanctions based on severity:

- **Level 1: Written Reprimand & Mandatory Retraining:** For minor administrative infractions.
- **Level 2: Suspension Without Pay (1 to 30 Days):** For moderate policy violations or repeated infractions.

- **Level 3: Demotion in Rank / Loss of Special Credentials:** Removal from supervisory or armed guard status.
- **Level 4: Summary Termination of Employment:** For gross misconduct, excessive force, firearms violations, or criminal conduct.

5.6 Complainant Closing Notice & Public Transparency

Within three (3) business days of executive adjudication (Stage 10):

- A formal written disposition letter is dispatched to the complainant via certified mail and email, signed by CEO Dr. Brian C. Askew.
- The letter details the official finding category (Sustained, Unfounded, Exonerated, Not Sustained, or Policy Failure) and confirms that appropriate administrative action has been implemented.
- The public tracking portal at www.matcomops.org/tracking is updated to Stage 6 (Case Closed).
- Pursuant to COMAR 12.10.01, required regulatory notifications are transmitted to the Maryland State Police Licensing Division.

6.0 RESPONSIBILITIES

6.1 CEO (Dr. Brian C. Askew): Serves as sole Approving Authority for final adjudication findings, issues executive disciplinary decisions, and signs formal disposition letters.

6.2 Commander, Internal Affairs: Supervises IA investigators, enforces 30-day investigation SLAs, reviews Reports of Investigation for objective rigor, and conducts quality assurance.

6.3 Lead Investigators: Execute impartial fact-finding, maintain chain of custody, conduct recorded interviews, and compile comprehensive Reports of Investigation.

7.0 COMPLIANCE & ENFORCEMENT

Any investigator or supervisor who intentionally falsifies investigative findings, fails to interview key witnesses, coerces statements, or leaks confidential investigative materials shall be terminated immediately for gross breach of duty and subjected to civil litigation and regulatory reporting.

8.0 RECORDS & DOCUMENTATION

All Reports of Investigation, audio recordings, witness transcripts, and executive disposition notices shall be preserved permanently in Matcom's secure, restricted Internal Affairs vault, with redacted summaries accessible pursuant to the Maryland Public Information Act (MPIA).

9.0 EFFECTIVE DATE & REVIEW

This SOP takes effect on August 13, 2026. It shall be reviewed annually on or before August 13, 2027 by the Internal Affairs Commander, Office of General Counsel, and Chief Executive Officer.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

MATCOM OFFICE OF PUBLIC SAFETY



LICENSED MARYLAND SECURITY GUARD AGENCY — MD LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — PUBLIC SAFETY GOVERNANCE

Policy Number:	SOP-PUB-11	Effective Date:	August 13, 2026
Policy Title:	Criminal Misconduct Referral Procedure	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Legal Liaison	Supersedes:	None (Initial Issue)
Classification:	Public	Jurisdiction:	State of Maryland (COMAR / MD Code)

1.0 PURPOSE & SCOPE

1.1 Purpose: Standard Operating Procedure SOP-PUB-11 establishes mandatory administrative and operational protocols for identifying, evaluating, and referring allegations or findings of criminal misconduct involving employees, contractors, or security personnel of Matcom Office of Public Safety LLC ("MATCOM"). Additionally, this policy establishes strict separation mechanisms ("Taint Walls") to isolate administrative internal inquiries from criminal law enforcement investigations, safeguarding constitutional rights and evidentiary integrity.

1.2 Scope: This procedure applies universally to all MATCOM personnel, including armed and unarmed security guards, special duty officers, dispatchers, field supervisors, internal affairs investigators, and administrative executives operating within the State of Maryland under MD Security Guard Agency License #24PLU-SGPD4620.

2.0 AUTHORITY & STATUTORY REFERENCES

This policy is promulgated under the authority of the CEO of MATCOM and complies with federal and Maryland law, including:

- **Maryland Code, Business Regulation Article, Title 19** (Security Guard Agencies).
- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02** (Security Guard Certification and Conduct).
- **Maryland Public Information Act (MPIA)**, MD Code Ann., Gen. Prov. § 4-101 et seq.
- **Maryland Police Accountability Act of 2022** (statutory frameworks governing investigative accountability).
- **Maryland Courts & Judicial Proceedings Article § 10-402** (Maryland Wiretap and Electronic Surveillance Act).
- **Garrity v. New Jersey**, 385 U.S. 493 (1967) (constitutional rules against compelled self-incrimination).
- **Maryland Declaration of Rights, Article 24** (Due Process).

3.0 DEFINITIONS

3.1 Administrative Investigation: An internal inquiry conducted by MATCOM's Professional Standards Division to determine compliance with corporate rules, client contracts, and COMAR regulatory standards, where employment sanctions may result.

3.2 Criminal Misconduct: Any act or omission by an employee that constitutes a misdemeanor or felony under the Maryland Criminal Law Article or federal criminal statutes (e.g., unlawful force amounting to assault/battery, theft, extortion, falsification of official logs, wiretap violations, or civil rights violations).

3.3 Criminal Referral: The formal transmission of physical evidence, incident logs, and investigative summaries to a law enforcement agency having primary criminal jurisdiction (e.g., Baltimore County Police Department, Maryland State Police) or prosecuting authority (State's Attorney's Office).

3.4 Garrity Warning: An administrative notice advising an employee that failure to answer questions during an administrative inquiry may result in job termination, but that compelled answers cannot be used against the employee in a criminal trial.

3.5 Taint Wall / Information Firewall: Operational and physical barriers prohibiting administrative investigators from sharing Garrity-protected statements or compelled disclosures with criminal prosecutors or police investigators.

4.0 POLICY STATEMENTS

4.1 Absolute Duty to Refer: MATCOM maintains a strict zero-tolerance policy for criminal acts committed by its personnel. Whenever a complaint or internal review reveals credible evidence of criminal misconduct, MATCOM shall immediately refer the matter to the appropriate law enforcement authority having territorial jurisdiction and notify the Maryland State Police Licensing Division as required by law.

4.2 Criminal Primacy: Criminal investigations conducted by sworn law enforcement agencies take precedence over internal administrative inquiries. MATCOM shall pause administrative interrogations when requested by investigating police agencies to protect criminal evidence.

CONSTITUTIONAL MANDATE — GARRITY ISOLATION

Compelled administrative statements obtained under threat of termination shall NEVER be disclosed to criminal police officers, State's Attorneys, or grand juries. Violating this firewall invalidates criminal prosecutions and triggers severe regulatory action under COMAR Title 12.

5.0 DETAILED OPERATING PROCEDURES

5.1 Threshold Determination & Screening Matrix

Upon intake of any complaint or occurrence report, the Professional Standards Division shall evaluate the facts against the Criminal Referral Threshold Matrix below:

Allegation Category	Criminal Threshold Examples	Immediate Mandatory Action
Use of Force	Force causing serious bodily injury, unauthorized firearm discharge, chokeholds.	Notify Local Police & MSP Licensing Division within 4 hours. Freeze BWC footage.
Property / Financial	Theft of client property, extortion, grand larceny, intentional property damage.	Refer to local law enforcement precinct. Secure physical evidence & logs.

Allegation Category	Criminal Threshold Examples	Immediate Mandatory Action
Integrity & Public Safety	Tampering with evidence, falsifying state security logs, illegal wiretapping/recording.	Administrative suspension; refer to State's Attorney Special Investigations.

5.2 Step-by-Step Referral Protocol

1. **Immediate Scene & Digital Preservation:** Secure scene, impound firearms/equipment, export Body-Worn Camera (BWC) files, CAD dispatch records, and access control logs.
2. **Executive Notification:** Notify CEO Dr. Brian C. Askew and Legal Liaison within two (2) hours of criminal threshold determination.
3. **Formal Referral:** Submit formal written Criminal Referral Form (Form MATCOM-CR-01) to the law enforcement agency with geographic jurisdiction (e.g., Baltimore County Police Department).
4. **MSP Licensing Division Notice:** Transmit regulatory notification to the Maryland State Police Licensing Division within five (5) business days pursuant to COMAR 12.10.01.

5.3 Separation of Administrative & Criminal Files

MATCOM maintains two segregated case file systems:

- a) **Criminal File:** Contains uncompelled third-party witness statements, physical evidence logs, CCTV video, and CAD reports—accessible to police.
- b) **Administrative File:** Contains employee personnel records, internal supervisory memos, and Garrity-protected interview recordings—strictly locked and barred from police access.

6.0 ROLES & RESPONSIBILITIES

6.1 CEO (Dr. Brian C. Askew): Approves all external criminal referrals and emergency employee suspensions.

6.2 Legal Liaison: Serves as single point of contact with State's Attorneys and law enforcement agencies; enforces Taint Wall integrity.

6.3 Field Supervisors: Responsible for immediate scene management, weapon impoundment, and preliminary evidence preservation.

7.0 COMPLIANCE, OVERSIGHT & ENFORCEMENT

Failure by any employee or manager to report suspected criminal misconduct, or any attempt to obstruct a criminal referral, shall result in immediate termination of employment and referral to the Maryland State Police for certification revocation.

8.0 RECORDS & DOCUMENTATION

All criminal misconduct referral files shall be retained securely by the Legal Liaison for a minimum of seven (7) years or until all statute of limitations and litigation holds expire.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISION HISTORY

Effective August 13, 2026. Annual review scheduled for August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew, Chief Executive Officer

Approving Authority, Matcom Office of Public Safety LLC
Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY



LICENSED MARYLAND SECURITY GUARD AGENCY — MD LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — PUBLIC SAFETY GOVERNANCE

Policy Number:	SOP-PUB-12	Effective Date:	August 13, 2026
Policy Title:	Complaint Findings & Dispositions	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Internal Affairs	Supersedes:	None (Initial Issue)
Classification:	Public	Jurisdiction:	State of Maryland (COMAR / MD Code)

1.0 PURPOSE & SCOPE

1.1 Purpose: Standard Operating Procedure SOP-PUB-12 establishes standardized definitions, evidentiary standards, and formal adjudication classifications for all administrative complaints processed by Matcom Office of Public Safety LLC ("MATCOM"). This policy ensures public accountability, consistency, and clear citizen communication regarding investigative outcomes.

1.2 Scope: This procedure governs all formal disposition determinations rendered by the Professional Standards Division concerning security personnel, armed officers, special agents, and corporate staff licensed under MD Security Guard Agency License #24PLU-SGPD4620.

2.0 AUTHORITY & STATUTORY REFERENCES

- **Maryland Code, Business Regulation Article, Title 19** (Security Guard Agencies).

- **COMAR 12.10.01 & 12.10.02** (Security Guard Certification, Conduct, and Administrative Sanctions).
- **Maryland Public Information Act (MPIA)**, MD Code Ann., Gen. Prov. § 4-101 et seq.
- **Maryland Police Accountability Act of 2022** (standardized disposition framework principles).
- **Maryland Declaration of Rights, Article 24** (Due Process and Procedural Fairness).

3.0 DEFINITIONS

3.1 Preponderance of the Evidence: The evidentiary standard applied in all MATCOM administrative adjudications. A finding is proven by a preponderance of the evidence when the weight of credible evidence demonstrates that the allegation is more likely true than not true (greater than 50% probability).

3.2 Subject Personnel: The employee or contractor against whom a complaint or allegation of policy non-compliance is filed.

3.3 Complainant: Any citizen, client representative, public official, or employee who submits a formal or informal complaint regarding MATCOM operations or staff.

4.0 POLICY STATEMENTS

4.1 Uniform Disposition Classifications: Every administrative investigation conducted by MATCOM shall conclude with one of the nine (9) authorized disposition classifications defined in Section 5.0. No custom or hybrid dispositions are permitted.

4.2 Objective & Impartial Adjudication: Investigative findings must be grounded solely in verifiable facts, physical/digital evidence, witness statements, and applicable COMAR regulations without bias or speculation.

5.0 DETAILED OPERATING PROCEDURES

The Professional Standards Division shall assign exactly one of the following nine official dispositions to each allegation in a complaint:

Disposition Term	Official Legal / Operational Definition	Corrective / Operational Action Required
SUSTAINED		Disciplinary action, suspension, retraining, or

Disposition Term	Official Legal / Operational Definition	Corrective / Operational Action Required
	The investigation disclosed sufficient evidence to prove the allegation by a preponderance of the evidence.	termination; licensing report to MSP.
NOT SUSTAINED	The investigation failed to disclose sufficient evidence to prove or disprove the allegation.	Case closed without employee discipline; maintained in confidential record.
UNFOUNDED	The investigation proved conclusively that the alleged act(s) did not occur, or that the subject officer was not involved.	Case closed; complete exoneration of personnel.
EXONERATED	The alleged conduct occurred, but was lawful, proper, justified, and fully compliant with MATCOM policy and Maryland law.	Case closed; action validated as lawful and within policy.
POLICY FAILURE	The alleged action occurred and complied with existing policy, but the policy itself was flawed, inadequate, or produced an unintended outcome.	Immediate policy suspension/ revision; retraining of staff; client notification.
TRAINING ISSUE	The conduct occurred due to a performance deficiency attributable to gaps in training rather than intentional misconduct.	Mandatory remedial training through MPCTC-approved module; performance tracking.
REFERRED	The matter was formally referred to an outside law enforcement agency, licensing board, or regulatory authority for primary jurisdiction.	Administrative hold pending external disposition.
ADMINISTRATIVE CLOSURE	Investigation terminated due to lack of jurisdiction, withdrawal, or employee resignation prior to initiation (notated in file).	Permanent notation in personnel licensing file regarding separation pending investigation.
INSUFFICIENT INFORMATION	Inadequate details provided by complainant, who remained unreachable after 3 documented attempts over 15 business days.	Administrative closure pending submission of further information.

PUBLIC TRANSPARENCY PRINCIPLE

Citizen complainants receive formal written notices containing the official disposition term and a plain-language factual summary, ensuring transparency while respecting statutory privacy laws under MPIA § 4-311.

6.0 ROLES & RESPONSIBILITIES

6.1 Internal Affairs Lead Investigator: Conducts factual inquiries, analyzes evidence against COMAR standards, and submits recommended dispositions.

6.2 Professional Standards Review Board: Audits investigative findings for objectivity, evidentiary sufficiency, and consistent application of disposition terms.

6.3 Chief Executive Officer (Dr. Brian C. Askew): Approves or modifies all final dispositions for sustained cases, policy failures, and employment terminations.

7.0 COMPLIANCE, OVERSIGHT & ENFORCEMENT

Arbitrary alteration of investigative findings or failure to apply the preponderance of evidence standard shall result in administrative review. Quarterly public summary reports of dispositions shall be compiled by Governmental Affairs.

8.0 RECORDS & DOCUMENTATION

All disposition records, investigative reports, and supervisory concurrence memos shall be indexed by Control Number and retained in the Professional Standards database for a minimum of seven (7) years.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISION HISTORY

Effective August 13, 2026. Annual review scheduled for August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew, Chief Executive Officer

Approving Authority, Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY



LICENSED MARYLAND SECURITY GUARD AGENCY — MD LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — PUBLIC SAFETY GOVERNANCE

Policy Number:	SOP-PUB-13	Effective Date:	August 13, 2026
Policy Title:	Complaint Response, Notification & Final Letter	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Office of Governmental Affairs / Professional Standards	Supersedes:	None (Initial Issue)
Classification:	Public	Jurisdiction:	State of Maryland (COMAR / MD Code)

1.0 PURPOSE & SCOPE

1.1 Purpose: Standard Operating Procedure SOP-PUB-13 specifies mandatory protocols, strict timelines, public privacy safeguards, and standardized letter formats governing communications with complainants. It ensures all citizens receiving security services from Matcom Office of Public Safety LLC ("MATCOM") are kept fully informed of the progress and final disposition of public complaints.

1.2 Scope: Applies to all public communications, notices, status updates, and downloadable response packages issued by the Office of Governmental Affairs and Professional Standards Division under MD License #24PLU-SGPD4620.

2.0 AUTHORITY & STATUTORY REFERENCES

- **Maryland Public Information Act (MPIA)**, MD Code Ann., Gen. Prov. § 4-101 et seq. (personnel privacy restrictions § 4-311).

- **COMAR 12.10.01 & 12.10.02** (Security Guard Agency Administrative Regulations).
- **Maryland Business Regulation Article, Title 19.**
- **Maryland Constitutional Due Process Provisions** (Declaration of Rights, Art. 24).

3.0 DEFINITIONS

3.1 Complaint Control Number (CCN): A unique alphanumeric identifier assigned to every public complaint upon intake (e.g., MATCOM-CMP-2026-001) used for tracking and public correspondence.

3.2 Formal Acknowledgement: Written communication issued to the complainant confirming receipt of a complaint and providing the CCN.

3.3 Final Disposition Letter: The official executive response transmitted to the complainant detailing the investigation's factual summary, findings, and disposition classification.

4.0 POLICY STATEMENTS

4.1 Guaranteed Communication Milestones: MATCOM guarantees four mandatory communication touchpoints for every formal complaint: Receipt Acknowledgement, 30-Day Progress Update(s), Request for Information (if applicable), and Final Disposition Response.

4.2 Balance of Transparency and Privacy: Letters shall provide clear factual details regarding the incident and disposition while redacting confidential employee personnel records protected under MPIA § 4-311.

5.0 DETAILED OPERATING PROCEDURES

5.1 Timelines & Communication Matrix

Notice Type	Mandatory Target Timeline	Delivery Channel	Required Elements
Acknowledgement Letter	Within 3 Business Days of Intake	Certified Mail or Secure Email	Complaint Control Number (CCN), Assigned Investigator Name, Contact Info.
Periodic Status Update	Every 30 Calendar Days	Email / Postal Mail	

Notice Type	Mandatory Target Timeline	Delivery Channel	Required Elements
			Current investigative stage, anticipated completion window.
Info Request Notice	As Needed (10 Business Day Window)	Email / Telephone Follow-up	Specific missing facts, deadline for response, consequences of non-response.
Final Disposition Letter	Within 5 Business Days of Executive Approval	Certified Mail & Downloadable Portal	Factual summary, official disposition, policy changes implemented, CEO signature.

5.2 Standardized Public Communication Templates

Template A: Formal Intake Acknowledgement Letter

MATCOM OFFICE OF PUBLIC SAFETY LLC — OFFICE OF GOVERNMENTAL AFFAIRS

Date: [Date]

To: [Complainant Name]

Address: [Complainant Address]

Subject: ACKNOWLEDGEMENT OF FORMAL COMPLAINT — CONTROL NO: [CCN]

Dear [Complainant Name],

This letter serves as official confirmation that the Matcom Office of Public Safety LLC Professional Standards Division has received your complaint dated [Date] regarding security operations at [Location]. Your matter has been assigned Complaint Control Number [CCN].

Lead Investigator [Investigator Name] has been assigned to conduct a thorough and impartial inquiry. You may expect periodic status updates every 30 days until resolution. If you have additional documents, videos, or witness information, please contact our Office at 701-809-9911 or via email at Oga@matcomops.org quoting your Control Number.

Sincerely,

Office of Governmental Affairs / Professional Standards Division

Matcom Office of Public Safety LLC

Template B: Final Executive Disposition Response Letter

MATCOM OFFICE OF PUBLIC SAFETY LLC — EXECUTIVE OFFICE

Date: [Date]

To: [Complainant Name]

Subject: FINAL DETERMINATION & DISPOSITION NOTICE — CONTROL NO: [CCN]

Dear [Complainant Name],

The Professional Standards Division has completed its comprehensive administrative investigation into Complaint Control Number **[CCN]**. Following a multi-tier supervisory review and executive evaluation, a final determination has been rendered by Chief Executive Officer Dr. Brian C. Askew.

INVESTIGATIVE SUMMARY:

[Insert plain-language summary of physical evidence reviewed, Body-Worn Camera audit, CAD logs, and interviewed witnesses].

OFFICIAL FINDING & DISPOSITION:

Based upon a preponderance of the evidence, the disposition of your complaint is classified as: **[INSERT DISPOSITION: SUSTAINED / NOT SUSTAINED / UNFOUNDED / EXONERATED / POLICY FAILURE]**.

CORRECTIVE / SYSTEMIC ACTIONS TAKEN:

[Insert appropriate public summary of corrective actions, policy updates, or training measures implemented].

MATCOM remains committed to professional excellence and public safety across the State of Maryland.

Respectfully submitted,

Dr. Brian C. Askew, Chief Executive Officer

Matcom Office of Public Safety LLC (MD License # 24PLU-SGPD4620)

6.0 ROLES & RESPONSIBILITIES

6.1 Governmental Affairs Specialist: Logs incoming complaints, issues acknowledgements within 3 business days, and manages complainant correspondence.

6.2 Chief Executive Officer: Personally signs all Final Disposition Letters sent to citizen complainants.

7.0 COMPLIANCE, OVERSIGHT & ENFORCEMENT

Failure to meet mandatory communication timelines shall trigger an administrative review by the Professional Standards Commander. All outbound correspondence is audited monthly.

8.0 RECORDS & DOCUMENTATION

All transmitted notices, postal receipts, and secure portal download logs are archived in the CCN master record and preserved for a mandatory 7-year retention period.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISION HISTORY

Effective August 13, 2026. Annual review scheduled for August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew, Chief Executive Officer

Approving Authority, Matcom Office of Public Safety LLC
Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY



LICENSED MARYLAND SECURITY GUARD AGENCY — MD LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — PUBLIC SAFETY GOVERNANCE

Policy Number:	SOP-PUB-14	Effective Date:	August 13, 2026
Policy Title:	Complaint Review, Approval & Quality Assurance	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Command Staff	Supersedes:	None (Initial Issue)
Classification:	Public	Jurisdiction:	State of Maryland (COMAR / MD Code)

1.0 PURPOSE & SCOPE

1.1 Purpose: Standard Operating Procedure SOP-PUB-14 mandates a rigorous multi-tier supervisory review, quality control audit, and executive approval process for all administrative investigative reports and public response letters produced by Matcom Office of Public Safety LLC ("MATCOM"). It establishes quality assurance standards to guarantee objectivity, thoroughness, and statutory compliance prior to case closure.

1.2 Scope: Applies to all internal affairs investigations, supervisory inquiry reports, quality assurance audits, and public disposition releases managed by Command Staff and the Professional Standards Division under MD Security Guard Agency License #24PLU-SGPD4620.

2.0 AUTHORITY & STATUTORY REFERENCES

- **Code of Maryland Regulations (COMAR) 12.10.01 & 12.10.02.**
- **Maryland Code, Business Regulation Article, Title 19.**

- **Maryland Police Training and Standards Commission (MPCTC)** quality audit guidelines (COMAR 12.12).
- **Maryland Public Information Act (MPIA)**, MD Code Ann., Gen. Prov. § 4-101 et seq.

3.0 DEFINITIONS

3.1 Investigative Summary Report (ISR): The primary administrative document prepared by an investigator containing allegations, witness summaries, evidence analysis, policy analysis, and recommended findings.

3.2 Quality Assurance Checklist (QAC): A mandatory 10-point audit form completed by supervisory staff verifying evidence completeness, legal compliance, and logical consistency before executive review.

3.3 Early Intervention System (EIS): An automated administrative tracking mechanism that flags officers or post locations accumulating multiple complaints within a specified timeframe for proactive intervention.

4.0 POLICY STATEMENTS

4.1 Mandatory Four-Tier Approval Chain: No investigative report or public disposition letter may be finalized, released, or filed without passing through the complete four-tier review hierarchy.

4.2 Zero Tolerance for Investigative Gaps: Investigations featuring unverified statements, missing BWC footage audits, unaddressed witness leads, or logical contradictions shall be rejected and remanded for additional field work.

5.0 DETAILED OPERATING PROCEDURES

5.1 Four-Tier Review & Approval Hierarchy

Review Tier	Responsible Level	Core Audit Responsibilities
TIER 1	Lead Internal Affairs Investigator	Completes field investigation, collects digital evidence, interviews witnesses, authors draft Investigative Summary Report (ISR).
TIER 2	Professional Standards Supervisor	Conducts technical quality review using Form MATCOM-QA-100; verifies evidence chain of custody and COMAR compliance.

Review Tier	Responsible Level	Core Audit Responsibilities
TIER 3	Legal & Governmental Affairs Liaison	Reviews report for statutory liability, MPIA redaction compliance, and prepares public disposition response draft.
TIER 4	Chief Executive Officer (Dr. Brian C. Askew)	Final executive review and approval; signs official disposition letters and authorizes administrative/disciplinary actions.

5.2 Quality Assurance Audit Checklist (Form MATCOM-QA-100 Criteria)

Supervisors conducting Tier 2 audits must evaluate and sign off on the following 10 mandatory quality controls:

1. **Complainant Contact:** Direct contact made with complainant within required timeframes?
2. **Witness Coverage:** All identified third-party witnesses interviewed or documented unreachability?
3. **Digital Evidence Audit:** Body-Worn Camera (BWC), CCTV, and GPS dispatch data fully audited?
4. **Policy Mapping:** Allegations precisely mapped to specific COMAR regulations or MATCOM SOP clauses?
5. **Evidentiary Standard:** Recommended findings supported by a Preponderance of the Evidence?
6. **Garrity Integrity:** Complete isolation between administrative statements and criminal law enforcement?
7. **Tone & Objectivity:** Report maintains neutral, factual, and non-judgmental professional language?
8. **MPIA Redaction Review:** Employee personal identifying details protected per MPIA § 4-311?
9. **EIS Evaluation:** Subject officer's 12-month complaint history audited for EIS pattern triggers?
10. **Action Plan:** Remedial training or policy adjustments identified for sustained/policy failure findings?

5.3 Early Intervention System (EIS) Triggers

PROACTIVE QUALITY OVERSIGHT — EIS THRESHOLDS

Any security officer or operational team accumulating **three (3) or more administrative complaints within a rolling 12-month period**—regardless of

disposition—shall automatically trigger an EIS Command Review. The Command Staff shall evaluate officer performance and order mandatory retraining, shift reassignment, or psychological fitness evaluation.

6.0 ROLES & RESPONSIBILITIES

6.1 Command Staff / Division Commanders: Monitor investigative quality, enforce review deadlines, and oversee EIS intervention plans.

6.2 Chief Executive Officer: Holds sole authority to execute final case approvals, modify findings, or issue corrective orders.

7.0 COMPLIANCE, OVERSIGHT & ENFORCEMENT

The Professional Standards Division shall conduct semi-annual random quality audits of 20% of all closed files to ensure consistent adherence to SOP-PUB-14 standards.

8.0 RECORDS & DOCUMENTATION

Completed Quality Assurance Checklists (Form MATCOM-QA-100) shall be permanently attached to the master case file and retained for seven (7) years.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISION HISTORY

Effective August 13, 2026. Annual review scheduled for August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew, Chief Executive Officer

Approving Authority, Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY



LICENSED MARYLAND SECURITY GUARD AGENCY — MD LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Phone: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — PUBLIC SAFETY GOVERNANCE

Policy Number:	SOP-PUB-15	Effective Date:	August 13, 2026
Policy Title:	Public Records, Privacy & Confidential Information	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Office of Governmental Affairs / Legal	Supersedes:	None (Initial Issue)
Classification:	Public	Jurisdiction:	State of Maryland (COMAR / MD Code)

1.0 PURPOSE & SCOPE

1.1 Purpose: Standard Operating Procedure SOP-PUB-15 establishes administrative policies governing public record requests, statutory disclosure limits, and privacy protection controls for Matcom Office of Public Safety LLC ("MATCOM"). It delineates information that may be publicly released under Maryland law from confidential personnel, intelligence, medical, juvenile, and security-sensitive information requiring strict protection.

1.2 Scope: Applies to all corporate records, incident logs, complaint files, Body-Worn Camera (BWC) footage, dispatch tapes, and personnel records maintained under MD Security Guard Agency License #24PLU-SGPD4620.

2.0 AUTHORITY & STATUTORY REFERENCES

- **Maryland Public Information Act (MPIA)**, MD Code Ann., Gen. Prov. § 4-101 through § 4-601.

- **Personnel Records Exemption**, MD Code Ann., Gen. Prov. § 4-311 (Mandatory denial of personnel files).
- **Medical Records Exemption**, MD Code Ann., Gen. Prov. § 4-329 & HIPAA (45 CFR Part 164).
- **Investigatory Records Exemption**, MD Code Ann., Gen. Prov. § 4-351 (Active law enforcement/investigative files).
- **Maryland Courts & Judicial Proceedings Article § 10-402** (Maryland Wiretap Act).
- **Maryland Courts & Judicial Proceedings Article § 3-8A-27** (Confidentiality of Juvenile Records).
- **COMAR 12.10.01 & 12.10.02** (Security Guard Agency Licensing Rules).

3.0 DEFINITIONS

3.1 Public Record: Any documentary material in any format created, received, or maintained by MATCOM in connection with the transaction of public safety business that is not statutorily exempt from disclosure.

3.2 Redaction: The removal or obscurement of confidential, exempt, or personally identifiable information from an otherwise public record prior to disclosure.

4.0 POLICY STATEMENTS

4.1 Policy of Openness with Statutory Controls: MATCOM supports public transparency while upholding statutory privacy mandates protecting security staff, crime victims, juveniles, and client site security plans.

4.2 Duty to Protect Confidential Information: Employees who unlawfully disclose protected personnel, medical, or security-sensitive data face immediate termination and potential criminal prosecution under Maryland law.

5.0 DETAILED OPERATING PROCEDURES

5.1 Record Disclosure Categories & Privacy Controls

Record Classification	Legal Status under MPIA / MD Law	Disclosure Protocol & Specific Restrictions
Personnel Records	Mandatory Confidential (Gen. Prov. § 4-311)	Home addresses, SSNs, performance reviews, internal discipline files strictly withheld. Factual disposition summaries permitted.

Record Classification	Legal Status under MPIA / MD Law	Disclosure Protocol & Specific Restrictions
Criminal Intelligence & Active Files	Exempt from Release (Gen. Prov. § 4-351)	Withheld while investigation/prosecution is active to prevent evidence contamination or fair trial impairment.
Medical & Psychological Data	Mandatory Confidential (Gen. Prov. § 4-329)	Drug testing results, medical leave notes, physical fitness reports strictly protected under HIPAA.
Juvenile Identifying Data	Mandatory Confidential (MD CJP § 3-8A-27)	All names, images, addresses, or identifying details of persons under 18 completely redacted.
Victim & Witness PII	Protected Personal Identifiable Information	Personal phone numbers, home addresses, financial details redacted to protect safety and privacy.
Security-Sensitive Information (SSI)	Confidential Infrastructure Record	Client floor plans, alarm codes, guard post shift orders, tactical maps, radio frequencies strictly withheld.
Body-Worn Camera (BWC) Audio/Video	Conditional Disclosure / Wiretap Act Compliance	Redacted for uninvolved bystanders, private residence interiors, medical emergencies, and wiretap audio (§ 10-402).

5.2 Public Records Request Processing & Fee Schedule

Request Submission & Timelines

MPIA requests must be submitted in writing to the Office of Governmental Affairs at Oga@matcomops.org. MATCOM adheres to statutory response timelines:

- **Acknowledgement:** Issued within 10 business days of receipt.
- **Final Determination / Production:** Provided within 30 calendar days.

Fee Schedule & Search Costs

Pursuant to MPIA § 4-206, MATCOM establishes the following fee schedule for record searches, redaction, and copying:

- **First Two Hours of Search/Redaction:** Free of charge.
- **Clerical/Staff Labor Rate:** \$35.00 per hour after initial two free hours.
- **Duplication / Copying Fee:** \$0.15 per standard page; digital transmittal via email/portal free.

Administrative Appeals & Redaction Log

Whenever information is redacted or a request is denied in whole or part, MATCOM shall provide a written **Redaction Log** citing the specific Maryland statutory

exemption (e.g., MPIA § 4-311). Requesters have the right to file an administrative appeal with CEO Dr. Brian C. Askew within 30 days.

6.0 ROLES & RESPONSIBILITIES

6.1 Public Information Officer (PIO) / Legal Counsel: Processes MPIA requests, applies statutory redactions, and prepares Redaction Logs.

6.2 Records Custodian: Maintains secure electronic archives, access logs, and fee accounting ledgers.

7.0 COMPLIANCE, OVERSIGHT & ENFORCEMENT

Unauthorized release of confidential records or non-compliance with MPIA disclosure orders shall result in administrative disciplinary action and legal review.

8.0 RECORDS & DOCUMENTATION

All MPIA requests, redaction logs, postal receipts, and written appeal determinations shall be archived for seven (7) years in the Governmental Affairs registry.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISION HISTORY

Effective August 13, 2026. Annual review scheduled for August 13, 2027.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew, Chief Executive Officer

Approving Authority, Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | Phone: 701-809-9911 | 24/7 Dispatch:
1-855-715-9911

Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed Security, Exp. Jan 31, 2028)

POLICY NUMBER	SOP-PUB-16	EFFECTIVE DATE	August 13, 2026
POLICY TITLE	Public Records Request Procedure	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	REVIEW DATE	August 13, 2027
RESPONSIBLE DIVISION	Office of Governmental Affairs / Legal	PUBLIC/ RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)		

SOP-PUB-16: PUBLIC RECORDS REQUEST PROCEDURE

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes official administrative and operational guidelines for processing public records requests submitted to Matcom Office of Public Safety LLC ("MATCOM"). MATCOM is committed to operating with high standards of public transparency, regulatory accountability, and open governance while preserving statutory protections for sensitive security blueprints, proprietary operational protocols, personal identifying information (PII), and ongoing internal or law enforcement investigations.

1.2 Scope: This procedure applies to all administrative units, division heads, operational personnel, security officers, records custodians, and legal representatives

of MATCOM. It governs the receipt, tracking, legal evaluation, fee calculation, redaction, fulfillment, and appeal handling for all public records requests originating from citizens, news media organizations, legal counsel, non-profit advocacy bodies, or government agencies.

1.3 Target Audience: Office of Governmental Affairs, Legal Division, IT Infrastructure Group, Professional Standards / Internal Affairs, and the general public seeking official MATCOM documentation.

2.0 STATUTORY & REGULATORY AUTHORITY

This policy is promulgated under and strictly enforced in accordance with the following state statutes, administrative regulations, and organizational mandates:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., General Provisions Article, § 4-101 through § 4-601.
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 and COMAR 12.10.02 (Security Guard Licensing, Certification, and Operational Standards).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Security Guard Agencies and Certification).
- **Maryland Police Training and Standards Commission (MPCTC):** Training and recordkeeping standards pursuant to COMAR Title 12, Subtitle 12.
- **Maryland Police Accountability Act of 2022:** Provisions governing disciplinary records transparency, public oversight, and record disclosure standards.
- **Maryland Courts and Judicial Proceedings Article:** § 10-402 (Interception of Communications / Wiretap Act compliance regarding audio/video media disclosures).
- **Maryland State Government Article:** § 10-1101 et seq. (Language Access Requirements for State and Quasi-Public Entities).
- **Title II of the Americans with Disabilities Act (ADA):** Ensuring public records request mechanisms are fully accessible to individuals with disabilities.

3.0 OPERATIONAL DEFINITIONS

- **Public Record:** The original or any copy of any documentary material—including written correspondence, electronic mail, Computer Aided Dispatch (CAD) logs, incident reports, policy manuals, audio recordings, or body-worn camera (BWC) media—made or received by MATCOM in connection with the transaction of public safety operations.

- **Custodial Record:** Any record currently held within MATCOM's physical archive, electronic document management system (EDMS), or remote cloud database.
- **MPIA Officer:** The designated MATCOM official within the Office of Governmental Affairs responsible for receiving, logging, coordinating, and responding to public records requests.
- **Applicant / Requester:** Any individual, citizen, corporation, media organization, or legal entity submitting a formal request to inspect or copy public records.
- **Redaction:** The lawful masking, blotting, or digital removal of exempt, confidential, or legally protected text, figures, audio frequencies, or video frames prior to releasing records.
- **Indigent Person:** An applicant whose net annual income falls below 125% of the federal poverty guidelines or who qualifies for state public assistance, making them eligible for fee waivers.
- **Commercial Purpose:** Any request submitted with the primary intent of utilizing disclosed records for direct commercial solicitation, marketing, or monetary resale.

4.0 GENERAL POLICY STATEMENT

It is the explicit policy of MATCOM to honor the spirit and letter of the Maryland Public Information Act. Public records maintained by MATCOM shall be made available for inspection and copying at reasonable times and without unnecessary delay, subject only to specific statutory exemptions required to safeguard individual privacy, security tactics, and active law enforcement investigations. Access to public records shall not be unreasonably denied, nor shall requesters be required to demonstrate a special interest or justification to inspect non-exempt records.

5.0 OPERATING PROCEDURES & WORKFLOWS

5.1 Submission Channels

Requesters may submit public records requests through any of the following official intake portals:

- **Online Portal:** Electronic submission via MATCOM Public Access Web Portal at www.matcomops.org/public-records.
- **Electronic Mail:** Direct submission to the Office of Governmental Affairs at Oga@matcomops.org with subject line "MPIA Public Records Request".

- **United States Postal Mail or Hand Delivery:** Written requests delivered to MATCOM Office of Public Safety LLC, Attn: Public Records Officer, 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207.

5.2 Intake, Logging & Acknowledgment Protocol

STEP 1: Immediate System Logging

Upon receipt of any request, the MPIA Officer shall immediately log the request into the Master MPIA Tracking Register, capturing requester contact data, date received, description of records sought, and assigning a unique tracking code (e.g., MPIA-2026-00101).

STEP 2: Statutory Acknowledgment (10-Day Requirement)

Within ten (10) business days of receipt, the MPIA Officer shall issue a formal written Acknowledgment Letter to the applicant confirming receipt, providing the unique tracking code, and stating whether the request is granted, denied, or requires fee estimation / time extension.

5.3 Timeline Standards & Multi-Track Processing

In accordance with Md. Code Ann., Gen. Prov. § 4-203, MATCOM shall adhere to the following strict timeline standards:

Request Track	Description & Scope	Maximum Fulfillment Timeline
Simple Track	Routine policy files, standard published reports, basic incident stats requiring no complex legal redaction.	Within 10 business days of receipt.
Standard Track	CAD logs, officer incident statements, contracts, or records requiring moderate redaction of PII.	Within 30 calendar days of receipt.
Complex Track	Voluminous multi-year archives, extensive BWC video footage requiring frame-by-frame redaction, or complex legal review.	30 calendar days initial; extended up to 30 additional days upon written agreement with requester.

5.4 Fee Schedule & Indigent Waiver Protocol

MATCOM applies standard, transparent fee rates authorized under MPIA § 4-206:

- **First Two (2) Hours:** Staff search, legal review, and record preparation time is provided **FREE of charge**.
- **Additional Staff Time:** Charged at \$25.00 per hour for clerical search/prep, or actual salary rate for specialized technical/legal analysis.
- **Reproduction / Printing:** \$0.15 per page for standard black & white copies; actual media cost (\$5.00 per USB drive) for digital disclosures.
- **Indigent Fee Waiver:** Fees shall be waived in full upon submission of proof of indigency (e.g., Maryland Food Supplement Program, SSI statement, or affidavit of income below 125% federal poverty line).
- **Public Interest Waiver:** The MPIA Officer may waive fees if disclosure primarily benefits the general public rather than a commercial interest.

5.5 Legal Review & Exemption/Redaction Standards

Before releasing any record, the Legal Division and MPIA Officer shall review the material and apply mandatory or discretionary redactions pursuant to MPIA § 4-301 through § 4-355:

MANDATORY EXEMPTION / REDACTION CATEGORIES

- **Personal Identifying Information (PII):** Social Security Numbers, driver's license numbers, home addresses, personal phone numbers, financial accounts, and medical records.
- **Security Blueprints & Tactical Protocols:** Building alarm codes, physical security vulnerability assessments, guard patrol route frequencies, and active tactical radio frequencies.
- **Ongoing Investigations:** Active Internal Affairs personnel files, open criminal investigation files, and confidential informant disclosures.
- **Wiretap & Electronic Interception Data:** Audio recordings subject to Maryland Wiretap Act prohibitions under CJP § 10-402.
- **Juvenile Records:** Names and identifying data of minors involved in incidents.

5.6 Delivery & Production Methods

Records shall be delivered via secure digital transfer link (download portal), encrypted email attachment, certified postal delivery, or held for in-person inspection

at MATCOM Headquarters in Gwynn Oak, MD during normal business hours (Monday through Friday, 0900–1700 hours).

5.7 Administrative & Judicial Appeals

If MATCOM denies a request in whole or in part, or if the requester disputes a fee assessment, the requester has the statutory right to:

1. Submit a petition for dispute resolution to the **State Public Information Act Ombudsman** (Office of the Attorney General of Maryland).
2. File an administrative appeal with the **State Public Information Act Compliance Board** regarding fee disputes exceeding \$350.00.
3. File a civil action in the **Circuit Court for Baltimore County** or the circuit court in the jurisdiction where the applicant resides or has a principal place of business.

5.8 Language Access & ADA Accommodation

In compliance with Maryland State Government Article § 10-1101 and Title II of the ADA, MATCOM provides free translation services for records request forms into Spanish and other primary languages, as well as alternative formats (large print, audio-assisted text) for individuals with visual or hearing impairments.

6.0 ORGANIZATIONAL ROLES & RESPONSIBILITIES

Role / Division	Primary Responsibilities
CEO (Dr. Brian C. Askew)	Executive oversight, final policy authority, authorization for high-level legal appeals.
MPIA Public Records Officer	Central intake, tracking, inter-divisional coordination, fee assessment, issuing formal decision letters.
Legal Division Counsel	Legal review of redactions, claim of statutory privilege, representation in Ombudsman and Circuit Court proceedings.
IT Systems Manager	EDMS database query execution, digital video frame-by-frame redaction, maintaining secure download infrastructure.
Records Management Custodian	Physical file retrieval, archive management, document scanning, hardcopy reproduction.

7.0 COMPLIANCE, MONITORING & ENFORCEMENT

Failure of MATCOM personnel to comply with this SOP, deliberate concealment or destruction of public records subject to an active request, or unauthorized disclosure of protected PII constitutes a severe disciplinary offense. Violators shall be subject to administrative discipline up to and including immediate termination of employment, revocation of security officer clearance under COMAR 12.10.01, and potential civil or criminal penalties under Maryland law.

8.0 RECORDS MANAGEMENT & DATA RETENTION

The Office of Governmental Affairs shall maintain a permanent **Master MPIA Log** containing records of all requests, acknowledgment letters, fee assessments, redaction logs, and written final responses. All physical and electronic files associated with a specific MPIA request shall be retained for a minimum of **three (3) years** following final disposition or resolution of all judicial appeals.

9.0 REVIEW, APPROVAL & VERSION HISTORY

This procedure shall be audited annually by the Office of Governmental Affairs and Legal Division to ensure full alignment with legislative updates to the Maryland Public Information Act and state court rulings. Next scheduled review date: **August 13, 2027**.

ADMINISTRATIVE APPROVAL & AUTHORIZATION

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the Chief Executive Officer of Matcom Office of Public Safety LLC. It carries full operational authority and applies to all personnel, contractors, and administrative divisions.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving
Authority

Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | Phone: 701-809-9911 | 24/7 Dispatch:
1-855-715-9911

Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed Security, Exp. Jan 31, 2028)

POLICY NUMBER	SOP-PUB-17	EFFECTIVE DATE	August 13, 2026
POLICY TITLE	Transparency Portal Data Correction Procedure	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	REVIEW DATE	August 13, 2027
RESPONSIBLE DIVISION	Office of Governmental Affairs / IT	PUBLIC/ RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)		

SOP-PUB-17: TRANSPARENCY PORTAL DATA CORRECTION PROCEDURE

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) defines the mandatory operational protocol for receiving, investigating, verifying, executing, and auditing public requests for data correction on MATCOM’s Public Transparency Portal and Interactive Dashboard. MATCOM maintains public-facing digital platforms to display aggregated incident metrics, security officer licensing verifications, community engagement statistics, and complaint dispositions. This SOP guarantees that the public has a transparent, legally binding mechanism to challenge and rectify inaccurate, incomplete, or outdated data published on these platforms.

1.2 Scope: This policy applies to all personnel within the Office of Governmental Affairs, IT Infrastructure Group, Professional Standards / Internal Affairs Division, Communications Center, and operational management responsible for generating, managing, or auditing public dashboard datasets.

1.3 Target Audience: Public safety researchers, journalists, impacted citizens, MATCOM IT data stewards, and executive leadership.

2.0 STATUTORY & REGULATORY AUTHORITY

This procedure is executed pursuant to authority under:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., Gen. Prov. § 4-101 et seq. (Public data transparency and statutory accuracy requirements).
- **Maryland Police Accountability Act of 2022:** Mandatory recordkeeping and public reporting mandates for security and law enforcement functions.
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 & 12.10.02 (Guard agency administrative record integrity).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Licensed security guard operational accountability).
- **Maryland Courts and Judicial Proceedings Article:** § 10-402 (Electronic data verification and recording restrictions).
- **Maryland Constitutional Due Process and Equal Protection Clauses:** Guaranteeing fair administrative standards in government-grade data publishing.
- **State Language Access & ADA Standards:** Ensuring equal access to portal correction mechanisms.

3.0 OPERATIONAL DEFINITIONS

- **Transparency Portal / Dashboard:** MATCOM's public website interface (www.matcomops.org/transparency) displaying operational statistics, incident maps, complaint outcomes, and licensing verifications.
- **Data Error / Material Inaccuracy:** Any published data point—including officer certification status, date/time of reported incidents, incident classification codes, or complaint resolution statuses—that deviates from verified primary source records.
- **Petitioner / Requester:** Any citizen, employee, or organization submitting a formal petition for public data correction.

- **Data Steward:** The designated IT / Governmental Affairs specialist assigned responsibility for maintaining database integrity and executing validated portal corrections.
- **Primary Source Record:** Original, immutable operational documentation including CAD call logs, certified field incident reports, body-worn camera metadata, or state licensing board files.
- **Correction Tracking Log:** An encrypted database tracking all submitted correction petitions, investigation notes, determinations, and executed database modifications.

4.0 GENERAL POLICY STATEMENT

MATCOM maintains an unyielding commitment to published data integrity. Public confidence in private public-safety organizations depends on transparent, verifiable facts. MATCOM guarantees that any published material inaccuracy on its public portal shall be investigated thoroughly, verified against primary source records, and corrected within specified operational timelines without bias or administrative friction.

5.0 OPERATING PROCEDURES & WORKFLOWS

5.1 Submission of Data Correction Petitions

Citizens and interested parties may file a petition for data correction through the following dedicated channels:

- **Online Correction Form:** Accessible directly via the Transparency Portal at www.matcomops.org/transparency/correct-data.
- **Electronic Mail Submission:** Sent directly to Oga@matcomops.org with subject header "Data Correction Petition - [Portal ID]".
- **Written Petition by Mail:** Addressed to MATCOM IT / Governmental Affairs Division, 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207.

Petitions must specify: (a) the exact URL or dashboard element containing the disputed data; (b) the specific data point alleged to be inaccurate; (c) the corrected data proposed; and (d) any supporting documentation or primary reference numbers (e.g., CAD Incident Number).

5.2 Intake, Logging & Triage

STEP 1: Registration (Within 24 Hours)

IT Data Management receives the petition, logs it into the Master Correction Log, and issues an automated confirmation receipt containing a unique Data Petition ID (e.g., DCR-2026-0042).

STEP 2: Preliminary Assessment (Within 3 Business Days)

The Office of Governmental Affairs reviews the petition to verify that it involves published portal data and contains sufficient detail for investigation. Unsubstantiated claims or duplicate filings are triaged accordingly.

5.3 Investigative Verification Workflow

The assigned Data Steward shall execute a multi-source audit to verify the claim:

VERIFICATION STEPS

1. Query primary source CAD dispatch logs and original security officer field incident reports.
2. Review body-worn camera metadata or GPS vehicle tracking records if time/location is disputed.
3. Cross-reference state licensing database records (MSP Licensing Division) for officer status disputes.
4. Consult with the reporting supervisor or Internal Affairs division if complaint status is disputed.

5.4 Determination Standards & Correction Timelines

Determination Outcome	Criteria & Standard of Proof	Required Operational Action	Execution Timeline
Granted in Full	Primary source records confirm published portal data is factually incorrect.	Execute database script update; publish errata note if data was public >30 days.	Within 5 business days of determination.
Partially Granted	Partial inaccuracy verified; remaining published elements proven accurate.	Correct verified error; provide detailed explanation of retained elements.	Within 7 business days of determination.
Denied	Published data matches verified primary source records; claim unproven.	Maintain published data; issue formal written Notice of Findings with evidence overview.	Within 10 business days of determination.

5.5 System Update & Errata Notice Standards

When a correction is executed, the IT Data Steward shall update the backend SQL repository and clear system caching. If the corrected data was publicly visible for longer than thirty (30) days, an Errata Tag shall be attached to the portal entry for a period of fourteen (14) days, reading: "Data updated on [Date] following administrative review under SOP-PUB-17."

5.6 Written Notice to Petitioner

Within ten (10) business days of final determination, the Office of Governmental Affairs shall issue a formal Written Determination Notice to the petitioner via email or postal mail detailing the findings, actions taken, database modifications executed, and options for administrative review.

5.7 Reconsideration & Administrative Appeal

If a petitioner disagrees with a denial, they may submit a **Request for Administrative Reconsideration** to the Chief Executive Officer within fifteen (15) calendar days. The CEO or designated Legal Counsel shall review the case file and render a final written agency decision within twenty (20) calendar days.

5.8 Language Access & ADA Digital Accessibility

All data correction interfaces shall comply with WCAG 2.1 AA digital accessibility standards and support multi-lingual screen-reader translation pursuant to Maryland Language Access guidelines.

6.0 ORGANIZATIONAL ROLES & RESPONSIBILITIES

Role / Division	Primary Responsibilities
Chief Executive Officer	Final administrative appeal authority, system integrity oversight.
CIO / IT Infrastructure Group	Portal backend administration, database correction script execution, maintaining audit trails.
Governmental Affairs Director	Public liaison, petition intake, issuing formal determination notices, regulatory reporting.
Internal Affairs / Quality Assurance	Providing verified complaint investigation outcomes for data cross-referencing.
Field & Dispatch Operations	Validating primary CAD dispatch and officer field report data during investigations.

7.0 COMPLIANCE, MONITORING & ENFORCEMENT

Deliberate tampering with portal data, intentional refusal to correct verified database errors, or falsification of primary source records by MATCOM employees is strictly prohibited. Violators face immediate disciplinary termination, license revocation referral under COMAR 12.10.01, and potential criminal prosecution under Maryland statutes governing official misconduct and record falsification.

8.0 RECORDS MANAGEMENT & DATA RETENTION

All correction petitions, primary source verification documents, IT modification transaction logs, and written determination notices shall be archived in the **Master Transparency Data Retention System** for a minimum of **five (5) years**.

9.0 REVIEW, APPROVAL & VERSION HISTORY

This policy shall undergo annual review by the CIO and Office of Governmental Affairs to incorporate evolving database technology standards and statutory public transparency amendments. Next review date: **August 13, 2027**.

ADMINISTRATIVE APPROVAL & AUTHORIZATION

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the Chief Executive Officer of Matcom Office of Public Safety LLC. It carries full operational authority and applies to all personnel, contractors, and administrative divisions.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving
Authority

Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | Phone: 701-809-9911 | 24/7 Dispatch:
1-855-715-9911

Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed Security, Exp. Jan 31, 2028)

POLICY NUMBER	SOP-PUB-18	EFFECTIVE DATE	August 13, 2026
POLICY TITLE	Public Emergency vs. Non-Emergency Reporting	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	REVIEW DATE	August 13, 2027
RESPONSIBLE DIVISION	Communications & CAD Division	PUBLIC/RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)		

SOP-PUB-18: PUBLIC EMERGENCY VS. NON-EMERGENCY REPORTING

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes strict operational protocols for differentiating between active life-safety emergencies requiring immediate public safety response and non-emergency administrative matters, customer inquiries, or policy complaints. It provides clear guidance to the public and operational staff regarding correct communication channel utilization, and mandates automated safeguards to handle misrouted emergency reports received via digital portals.

1.2 Scope: Applies to MATCOM's 24/7 Communications & CAD Division, field operations personnel, website administration, public intake web portals, email servers, and public safety dispatchers.

1.3 Target Audience: General public, security dispatchers, CAD operators, field supervisors, and portal administrators.

2.0 STATUTORY & REGULATORY AUTHORITY

This SOP is established in compliance with:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., Gen. Prov. § 4-101 et seq. (Public record disclosure and emergency portal recordkeeping).
- **Maryland Public Safety Article:** § 1-301 et seq. (Emergency Telephone System / 911 Public Safety Answering Point [PSAP] Governance).
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 & 12.10.02 (Security Guard Agency Operational & Dispatch Standards).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Security guard agency operations).
- **MPCTC Dispatch & Telecommunications Standards:** COMAR Title 12, Subtitle 12.
- **Maryland Police Accountability Act of 2022:** Call reporting and emergency protocol standards.
- **Maryland Courts and Judicial Proceedings Article:** § 10-402 (Wiretap Act compliance regarding recorded communications and call monitoring disclosures).
- **Americans with Disabilities Act (ADA) & Maryland Language Access Mandates:** TTY/TDD and accessible emergency telecommunication standards.

3.0 OPERATIONAL DEFINITIONS

- **Life-Safety Emergency:** Any active, ongoing, or imminent incident involving threat to human life, serious bodily injury, active violent crimes, structural fires, armed intrusions, or medical distress requiring immediate law enforcement, fire, or EMS response.
- **Urgent Security Incident:** Non-life-threatening active property security breaches, trespass incidents, or alarms at contract client facilities requiring immediate MATCOM security guard dispatch.

- **Public Safety Answering Point (PSAP):** The primary 911 emergency communications center operated by municipal or county police/fire agencies (e.g., Baltimore County / Baltimore City 911).
- **MATCOM 24/7 Dispatch Center:** MATCOM's central security communications hub reachable at **1-855-715-9911**.
- **Public Complaint / Reporting Portal:** MATCOM's non-emergency web-based administrative intake system used for policy complaints, public records requests, and data correction petitions.
- **Misrouted Emergency Report:** An emergency life-safety report inadvertently submitted via non-emergency web portals, email, or administrative phone lines.

4.0 GENERAL POLICY STATEMENT

CRITICAL MANDATE: MATCOM'S PUBLIC COMPLAINT PORTAL AND ADMINISTRATIVE EMAIL ACCOUNTS ARE NOT MONITORED FOR IMMEDIATE EMERGENCY RESPONSE. In any situation involving an active emergency, threat to life, or ongoing crime, citizens must immediately dial **911**. MATCOM maintains prominent, explicit emergency disclaimers across all digital touchpoints and mandates immediate, automated escalation protocols if an emergency report is detected on non-emergency channels.

5.0 OPERATING PROCEDURES & WORKFLOWS

5.1 Incident Classification & Reporting Channel Matrix

Incident Category	Examples of Incidents	PRIMARY Reporting Channel	Secondary / Backup Channel
CRITICAL EMERGENCY	Shots fired, active shooter, physical assault, structure fire, medical emergency, armed robbery, burglary in progress.	DIAL 911 IMMEDIATELY (Municipal/County PSAP)	MATCOM 24/7 Dispatch: 1-855-715-9911
URGENT SECURITY DISPATCH	Active trespass on client property, unverified security alarm, parking violation blocking access, property damage discovery.	MATCOM 24/7 Dispatch: 1-855-715-9911	MATCOM Dispatch Email: dispatch@matcomops.org
NON-EMERGENCY POLICE REPORT	Past theft, property damage with no suspect present, lost property, general police inquiries.	Local Law Enforcement Non-Emergency Number	MATCOM 24/7 Dispatch: 1-855-715-9911
ADMINISTRATIVE / COMPLAINT PORTAL	Officer conduct complaints, public records requests, data correction petitions, general business inquiries.	MATCOM Online Portal: www.matcomops.org	Email: Oga@matcomops.org Phone: 701-809-9911

5.2 Mandatory Digital Disclaimer Standards

MANDATORY PUBLIC WARNING DISPLAYED ON ALL WEB PORTALS

WARNING: DO NOT USE THIS ONLINE PORTAL TO REPORT AN ACTIVE EMERGENCY!

If you are experiencing a medical emergency, a crime in progress, a fire, or any immediate threat to life or safety, **STOP AND DIAL 911 IMMEDIATELY**. This web portal is processed during standard administrative business hours and is NOT monitored for real-time emergency dispatch.

5.3 Protocol for Handling Misrouted Emergency Reports

When an emergency report is submitted via an online form, email, or administrative telephone line, the receiving staff member or automated system shall execute the following emergency escalation procedure immediately:

PHASE 1: Immediate Interception & CAD Alert

The web portal keyword monitoring engine alerts the 24/7 CAD Communications Supervisor immediately upon detecting emergency keywords (e.g., "gun", "shot", "assault", "fire", "dying", "help").

PHASE 2: Direct Cross-Dispatch to 911 PSAP

The CAD Operator shall immediately contact the primary County/City 911 PSAP via direct line, transmit the caller's location, contact details, and incident description, and request emergency police/fire/EMS response.

PHASE 3: MATCOM Field Guard Dispatch

If the incident location falls within a MATCOM-contracted facility, MATCOM Dispatch shall simultaneously deploy on-duty armed/unarmed patrol supervisors to secure the scene and render aid pending 911 arrival.

PHASE 4: Emergency Incident Logging

The CAD Operator shall generate an Urgent Misrouted Escalation Ticket in the CAD system, recording exact timestamps of receipt, PSAP transfer, and operational resolution.

5.4 MATCOM 24/7 Dispatch Center Operations

MATCOM's Communications Division operates 24 hours a day, 365 days a year at **1-855-715-9911**. All incoming dispatch calls are recorded in compliance with Maryland Wiretap Act CJP § 10-402 under automated call recording disclaimers. Dispatchers are trained to perform rapid call triage and maintain direct radio contact with field officers and local police dispatch centers.

5.5 TTY/TDD & Multilingual Emergency Telecommunications

The Communications Division maintains full Next Generation 911 / TTY / TDD telecommunication relay integration for hearing-impaired citizens, alongside 24/7 on-demand translation support in over 200 languages.

6.0 ORGANIZATIONAL ROLES & RESPONSIBILITIES

Role / Division	Primary Responsibilities
CEO (Dr. Brian C. Askew)	Executive authority over public safety dispatch operations and inter-agency coordination.
Communications Director	Managing 24/7 Dispatch Center operations, CAD system integrity, dispatcher emergency triage training.
CAD Dispatch Operators	24/7 call receiving, emergency triage, immediate 911 cross-dispatching, logging misrouted emergency reports.
On-Duty Patrol Supervisors	Immediate scene response for urgent incidents on MATCOM property, coordination with arriving municipal police/EMS.
IT & Webmaster Team	Maintaining automated web disclaimer pop-ups, keyword emergency trigger scripts, portal server uptime.

7.0 COMPLIANCE, MONITORING & ENFORCEMENT

Failure of any MATCOM employee or dispatcher to immediately escalate a misrouted emergency report to 911 constitutes gross negligence and grounds for immediate termination of employment, forfeiture of dispatch certifications, and potential legal liability. The Communications Division conducts monthly Quality Assurance audits of all dispatch logs and misrouted report files.

8.0 RECORDS MANAGEMENT & DATA RETENTION

All CAD call logs, audio recordings, misrouted emergency escalation reports, and 911 cross-dispatch receipts shall be permanently preserved in the CAD secure digital repository for a minimum of **three (3) years**.

9.0 REVIEW, APPROVAL & VERSION HISTORY

This SOP shall be reviewed annually by the Communications Director and Legal Division in consultation with local public safety answering point (PSAP) authorities. Next scheduled review date: **August 13, 2027**.

ADMINISTRATIVE APPROVAL & AUTHORIZATION

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the Chief Executive Officer of Matcom Office of Public Safety LLC. It carries full operational authority and applies to all personnel, contractors, and administrative divisions.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving
Authority
Matcom Office of Public Safety LLC
Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC
Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | Phone: 701-809-9911 | 24/7 Dispatch:
1-855-715-9911

Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed Security, Exp. Jan 31, 2028)

POLICY NUMBER	SOP-PUB-19	EFFECTIVE DATE	August 13, 2026
POLICY TITLE	Anonymous & Confidential Complaint Procedure	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	REVIEW DATE	August 13, 2027
RESPONSIBLE DIVISION	Professional Standards / Internal Affairs	PUBLIC/ RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)		

SOP-PUB-19: ANONYMOUS & CONFIDENTIAL COMPLAINT PROCEDURE

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes comprehensive, legally binding guidelines for receiving, logging, evaluating, investigating, and resolving anonymous and confidential misconduct complaints submitted against MATCOM personnel, security guards, or administrative staff. MATCOM guarantees accessible reporting pathways that protect complainants from disclosure, fear of reprisal, or administrative barriers, while maintaining statutory standards of due process and evidentiary integrity.

1.2 Scope: Applies to all complaints alleging official misconduct, excessive force, illegal acts, discrimination, administrative non-compliance, or SOP violations involving MATCOM security officers, managers, or contractors.

1.3 Target Audience: Professional Standards / Internal Affairs Division (IAD), Legal Counsel, Human Resources, company employees, and members of the public.

2.0 STATUTORY & REGULATORY AUTHORITY

This SOP is authorized and governed by:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., Gen. Prov. § 4-101 et seq. (Confidentiality exemptions and public records disclosures).
- **Maryland Police Accountability Act of 2022:** Md. Code Ann., Public Safety Article § 3-101 et seq. (Complaint processing and oversight standards).
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 & 12.10.02 (Security guard misconduct investigation rules).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Security Guard Licensing discipline).
- **MPCTC Professional Standards Standards:** COMAR Title 12, Subtitle 12.
- **Maryland Courts and Judicial Proceedings Article:** § 10-402 (Wiretap Act compliance regarding confidential recorded statements).
- **Maryland Constitutional Due Process & Equal Protection Guarantees:** Balancing complainant protections with accused personnel rights.
- **Maryland Language Access & ADA Mandates:** Guaranteeing accessibility for all complainants.

3.0 OPERATIONAL DEFINITIONS

- **Anonymous Complaint:** A complaint submitted where the complainant intentionally withholds their name, contact details, or identity entirely.
- **Confidential Complaint:** A complaint where the complainant discloses their identity to Internal Affairs investigators but requests that their identity be withheld from the subject employee, the public, or external bodies to the maximum extent permitted by law.
- **Complainant Tracking Code (CTC):** A secure, system-generated 8-character alphanumeric key issued to anonymous complainants allowing them to track investigation progress and communicate securely without revealing identity.

- **Internal Affairs Division (IAD):** MATCOM's specialized investigative arm within Professional Standards responsible for investigating personnel misconduct.
- **Material Corroboration:** Independent physical, electronic, documentary, or testimonial evidence (e.g., body-worn camera video, CAD logs, GPS tracking) that substantiates allegations independent of complainant testimony.
- **Statutory Exceptions to Confidentiality:** Mandatory legal triggers requiring identity disclosure (e.g., court orders, criminal discovery, Brady/Giglio material disclosures, Police Accountability Board statutory filings).

4.0 GENERAL POLICY STATEMENT

MATCOM maintains an absolute zero-suppression policy regarding misconduct allegations. **ANONYMOUS AND CONFIDENTIAL COMPLAINTS SHALL BE INVESTIGATED WITH THE SAME RIGOR, COMPREHENSIVE EVIDENTIARY AUDITING, AND DILIGENCE AS SIGNED, NAMED COMPLAINTS.** No complaint shall be dismissed solely because the complainant chooses to remain anonymous or requests confidentiality.

5.0 OPERATING PROCEDURES & WORKFLOWS

5.1 Multi-Channel Intake Infrastructure

Complainants may submit anonymous or confidential reports through any of the following secure pathways:

- **24/7 Anonymous Hotline:** Toll-free telephone intake at **1-855-715-9911** (Option 4) featuring automated caller-ID scrubbing.
- **Encrypted Web Portal:** Submission via www.matcomops.org/complaints/ anonymous with encrypted SSL data transmission and automatic IP address stripping.
- **Secure Mail Drop:** Physical mail addressed to: MATCOM Internal Affairs Division, Private Drop Box 1071, 6340 Security Blvd., Suite 100, Gwynn Oak, MD 21207.
- **In-Person Confidential Interview:** Confidential appointment at IAD headquarters with private, secure access.

5.2 Distinguishing Anonymous vs. Confidential Reporting

Feature / Parameter	Anonymous Complaint	Confidential Complaint
Identity Status	Identity completely unknown to MATCOM investigators.	Identity known to IAD investigators only; withheld from subject officer.
Follow-Up Contact	Via Complainant Tracking Code (CTC) web interface only.	Direct encrypted phone, email, or in-person contact by IAD.
Legal Protection Standard	Absolute identity protection (no identity data exists to disclose).	Protected to maximum legal limit; subject to mandatory judicial subpoena exceptions.
Evidentiary Burden	Requires strong material corroboration (video, CAD, physical evidence).	Combines complainant testimony with material corroboration.

5.3 Investigative Protocol for Anonymous Complaints

Because anonymous complaints lack direct witness testimony at administrative hearings, IAD investigators shall follow an aggressive material corroboration strategy:

STEP 1: Preliminary Threshold Assessment (Within 24 Hours)

IAD reviews the anonymous allegation to determine if it describes a specific violation of law, COMAR regulations, or MATCOM SOPs with sufficient detail to investigate.

STEP 2: Independent Evidence Extraction

Investigators immediately preserve and review: (a) Body-Worn Camera (BWC) media; (b) CAD radio dispatch call logs and audio files; (c) Patrol vehicle GPS location data; (d) Facility CCTV video footage; (e) Electronic guard-tour pipe logs.

STEP 3: Witness & Supervisor Interviews

Investigators interview non-subject officers, client security directors, and third-party civilian witnesses who were present at the scene.

STEP 4: Findings Determination

Case findings are classified as: Sustained, Unfounded, Exonerated, or Not Sustained based strictly on independent physical and documentary evidence.

5.4 Statutory Limitations on Confidentiality

MANDATORY LEGAL DISCLOSURE TRIGGERS

While MATCOM guards complainant confidentiality vigorously, complainants must be informed that identity confidentiality may be overridden under the following narrow statutory circumstances:

- **Judicial Court Orders & Subpoenas:** A enforceable subpoena issued by a Maryland Circuit Court or Federal District Court judge.
- **Criminal Prosecution:** Discovery obligations under Maryland Rule 4-263 in criminal cases involving the subject officer.
- **Brady / Giglio Exculpatory Requirements:** Constitutional mandates requiring disclosure of material exculpatory or impeachment evidence to defense counsel.
- **Maryland Police Accountability Board Reporting:** Statutory reporting mandates under Pub. Safety § 3-101.

5.5 Complainant Tracking Code (CTC) System

Upon submitting an anonymous complaint online or via hotline, the system generates a unique 8-character alphanumeric key (e.g., CTC-89B42K). The complainant can enter this key at www.matcomops.org/complaint-status to view investigation progress, review public findings summaries, or submit additional evidence confidentially.

5.6 Information Security & Data Sanitization

All anonymous web portal submissions pass through an automated privacy proxy that permanently strips IP addresses, browser fingerprints, and metadata. Digital complaint files are stored in an encrypted vault accessible exclusively by authorized Internal Affairs personnel.

6.0 ORGANIZATIONAL ROLES & RESPONSIBILITIES

Role / Division	Primary Responsibilities
CEO (Dr. Brian C. Askew)	Final approving authority for sustained IA findings and administrative discipline.
Director of Internal Affairs	Overall management of anonymous intake systems, case assignment, confidential file security.
IA Lead Investigators	Conducting independent evidentiary investigations, BWC analysis, witness interviews, generating reports.
Legal Division Counsel	Subpoena defense, confidentiality court motions, Brady/Giglio compliance determinations.
IT Security Officer	Maintaining web portal encryption, automated IP scrubbing, CTC database security.

7.0 COMPLIANCE, MONITORING & ENFORCEMENT

Any MATCOM employee, supervisor, or investigator who improperly discloses the identity of a confidential complainant, attempts to trace an anonymous complainant, or compromises confidential IA files shall be immediately terminated for cause and subjected to legal prosecution under Maryland privacy and official misconduct laws.

8.0 RECORDS MANAGEMENT & DATA RETENTION

All anonymous and confidential complaint case files, BWC media, CAD logs, and CTC transaction histories shall be retained securely in the **Master IA Vault** for a minimum of **seven (7) years** following case closure.

9.0 REVIEW, APPROVAL & VERSION HISTORY

This SOP shall be reviewed annually by the Professional Standards Division and Legal Counsel to ensure full alignment with state accountability legislation and court precedent. Next review date: **August 13, 2027**.

ADMINISTRATIVE APPROVAL & AUTHORIZATION

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the Chief Executive Officer of Matcom Office of Public Safety LLC. It carries full operational authority and applies to all personnel, contractors, and administrative divisions.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving
Authority

Matcom Office of Public Safety LLC

Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC



STANDARD OPERATING PROCEDURE — PUBLIC SAFETY DIVISION

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | Phone: 701-809-9911 | 24/7 Dispatch:
1-855-715-9911

Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

MD Security Guard License: 24PLU-SGPD4620 (Armed & Unarmed Security, Exp. Jan 31, 2028)

POLICY NUMBER	SOP-PUB-20	EFFECTIVE DATE	August 13, 2026
POLICY TITLE	Anti-Retaliation & Complainant Protection	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	REVIEW DATE	August 13, 2027
RESPONSIBLE DIVISION	Professional Standards / Human Resources / Legal	PUBLIC/ RESTRICTED CLASSIFICATION	Public
SUPERSEDES	None (Initial Issue)		

SOP-PUB-20: ANTI-RETALIATION & COMPLAINANT PROTECTION

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes an unyielding, zero-tolerance policy prohibiting retaliation, intimidation, harassment, coercion, blacklisting, or adverse employment/service treatment against any individual—including citizens, security officers, administrative employees, contractors, or witnesses—who files a complaint, reports misconduct, or assists in any investigation involving MATCOM. This procedure provides immediate protective mechanisms, expedited investigative workflows, and severe administrative and legal consequences for retaliatory conduct.

1.2 Scope: Applies universally across all MATCOM divisions, operational sites, contract locations, executive leadership, field supervisors, security personnel, and administrative employees.

1.3 Target Audience: All MATCOM personnel, Human Resources, Internal Affairs Division, Legal Counsel, contract clients, and the public.

2.0 STATUTORY & REGULATORY AUTHORITY

This SOP is promulgated and enforced pursuant to:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., Gen. Prov. § 4-101 et seq. (Whistleblower record protection and privacy standards).
- **Maryland Police Accountability Act of 2022:** Md. Code Ann., Pub. Safety § 3-101 et seq. (Complainant protection and anti-retaliation mandates).
- **Maryland Criminal Law Article:** § 9-302 (Witness Intimidation, Retaliation, and Tampering Statute—Felony Offense).
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 & 12.10.02 (Guard agency ethical and professional standards).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Security guard licensee conduct).
- **Maryland Labor & Employment Article:** Whistleblower protection and anti-retaliation statutory provisions.
- **Maryland Constitutional Due Process & Equal Protection Clauses:** Guaranteeing protection of legal rights.
- **State Language Access & ADA Standards:** Ensuring accessible reporting of retaliation allegations.

3.0 OPERATIONAL DEFINITIONS

- **Retaliation:** Any adverse action, harassment, intimidation, demotion, termination, schedule penalization, assignment shift to undesirable posts, contract interference, verbal/physical coercion, or social blacklisting executed against an individual because they engaged in a protected activity.
- **Protected Activity:** Filing a complaint, reporting suspected misconduct, testifying in an IA or court proceeding, requesting public records, petitioning for data correction, or assisting in any investigation.

- **Adverse Action:** Any action that causes material detriment to an employee's working conditions, compensation, professional reputation, or a citizen's access to public safety services.
- **Good-Faith Complaint:** A complaint filed with an honest belief in its truthfulness, regardless of whether the ultimate investigation sustains the allegation.
- **Interim Protective Measures:** Immediate operational actions taken by MATCOM leadership to isolate and protect a complainant or witness during an active investigation.

4.0 GENERAL POLICY STATEMENT

MATCOM MAINTAINS AN ABSOLUTE ZERO-TOLERANCE POLICY AGAINST RETALIATION. Retaliation strikes at the core of organizational integrity and public trust. Any officer, supervisor, or employee who engages in, encourages, or condones retaliatory action against any complainant or witness shall face immediate administrative suspension, termination of employment, revocation of guard certification, and referral for felony criminal prosecution under Maryland Criminal Law § 9-302.

5.0 OPERATING PROCEDURES & WORKFLOWS

5.1 Reporting Allegations of Retaliation

Any individual who believes they are being subjected to retaliatory treatment may report the incident immediately via any of the following priority pathways:

- **Emergency Anti-Retaliation Hotline:** Direct 24/7 priority line at **1-855-715-9911** (Option 5).
- **Direct HR / IA Filing:** In-person or direct email to 0ga@matcomops.org with subject line "URGENT - RETALIATION COMPLAINT".
- **Online Complaint Portal:** Secure submission at www.matcomops.org/anti-retaliation.

5.2 Expedited Investigation Protocol (24-Hour Mandate)

PHASE 1: Immediate Launch (Within 24 Hours)

Upon receiving a retaliation complaint, Internal Affairs and HR shall launch an expedited investigation within twenty-four (24) hours, assigning a senior lead investigator.

PHASE 2: Immediate Interim Protective Orders

Within twelve (12) hours of receipt, HR shall issue binding Interim Protection Orders to safeguard the complainant (see Section 5.3).

PHASE 3: Fast-Track Evidentiary Review

Investigators audit schedule logs, email/messaging communications, supervisor shift notes, BWC audio, and witness statements to establish temporal proximity and retaliatory intent.

5.3 Mandatory Interim Protective Measures

To guarantee complete safety during an ongoing investigation, MATCOM leadership shall execute one or more of the following mandatory interim protective actions immediately:

AVAILABLE INTERIM PROTECTIVE MEASURES

- **Subject Reassignment / Administrative Suspension:** Immediate transfer or paid administrative leave for the accused supervisor/officer.
- **No-Contact Directives:** Issuance of formal, legally binding administrative No-Contact Orders prohibiting the subject from communicating with the complainant.
- **Shift & Location Stabilization:** Guaranteeing that the complainant's shift, pay rate, contract post, and duties remain strictly unchanged.
- **Safety Escorts & Security Monitoring:** Providing specialized security monitoring or escort details for complainants facing physical threats.

5.4 Disciplinary Sanctions & Criminal Referral

If an investigation sustains allegations of retaliation, MATCOM shall impose the following mandatory penalties:

Severity Level	Type of Retaliatory Conduct	Mandatory Sanction / Penalty
Category A (Severe)	Physical threats, termination, wage withholding, blacklisting, law enforcement misuse.	Immediate termination of employment; permanent bar from MATCOM; notification to MSP Licensing Division; criminal referral under MD Crim. Law § 9-302.
Category B (Moderate)	Schedule penalization, undesirable assignment transfer, verbal harassment, isolation.	30-day unpaid suspension; mandatory demotion; formal reprimand; 1-year probation; mandatory anti-retaliation retraining.
Category C (Minor)	Subtle workplace exclusion, uncooperative attitude, indirect negative remarks.	Written reprimand; mandatory counseling; strict monitoring; reassignment away from complainant.

5.5 Post-Investigation Monitoring Protocol

To prevent delayed retaliation, Human Resources and Internal Affairs shall conduct mandatory post-investigation check-ins with complainants according to the following schedule:

- **30-Day Check-in:** Formal interview and audit of work schedules/service interactions.
- **90-Day Check-in:** Performance appraisal review and supervisor feedback audit.
- **180-Day Check-in:** Comprehensive workplace environment audit.
- **1-Year Check-in:** Final compliance review and case file closure certification.

5.6 Employee Training & Onboarding Mandates

All newly hired security officers, administrative employees, and managers must complete mandatory Anti-Retaliation and Whistleblower Protection training during initial onboarding, with required annual recertification thereafter under COMAR 12.10.01 training protocols.

6.0 ORGANIZATIONAL ROLES & RESPONSIBILITIES

Role / Division	Primary Responsibilities
CEO (Dr. Brian C. Askew)	Ultimate enforcement authority, approval of immediate terminations and criminal referrals.
HR Director	Executing interim protective orders, job security guarantees, post-investigation monitoring audits.
Internal Affairs Director	Leading 24-hour fast-track retaliation investigations, collecting digital and testimonial evidence.
Legal Counsel	Interface with State's Attorney for criminal prosecutions under MD Crim. Law § 9-302.
Field Supervisors	Enforcing no-contact orders on duty posts, maintaining fair assignment schedules, reporting retaliation.

7.0 COMPLIANCE, MONITORING & ENFORCEMENT

Compliance with this SOP is monitored directly by the CEO and Legal Counsel. MATCOM publishes annual aggregated statistical reports detailing retaliation complaints received, investigation outcomes, and disciplinary actions taken, upholding full transparency with regulatory bodies and the public.

8.0 RECORDS MANAGEMENT & DATA RETENTION

All retaliation reports, interim protection orders, investigation case files, and post-investigation monitoring logs shall be preserved in the **Master HR/IA Confidential Retaliation Vault** for a minimum of **seven (7) years** following employee separation or incident resolution.

9.0 REVIEW, APPROVAL & VERSION HISTORY

This policy shall be reviewed annually by HR, IA, and Legal Counsel to reflect statutory amendments to Maryland labor laws and police accountability regulations. Next review date: **August 13, 2027**.

ADMINISTRATIVE APPROVAL & AUTHORIZATION

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the Chief Executive Officer of Matcom Office of Public Safety LLC. It carries full operational authority and applies to all personnel, contractors, and administrative divisions.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving
Authority
Matcom Office of Public Safety LLC
Date: August 13, 2026

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC
Date: August 13, 2026

MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT-GRADE SECURITY & PUBLIC SAFETY SERVICES

MD License: **24PLU-SGPD4620**

Armed & Unarmed Security

Exp: January 31, 2028

HQ: 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207

Admin:
701-809-9911

24/7 Dispatch:
1-855-715-9911

Web:
www.matcomops.org



Policy Number:	SOP-PUB-21	Effective Date:	August 13, 2026
Policy Title:	Accessibility, Disability Accommodation & Language Access		
Approving Authority:	Dr. Brian C. Askew, CEO	Revision Date:	August 13, 2026
Responsible Division:	Office of Governmental Affairs / ADA Coordinator	Review Date:	August 13, 2027
Classification:	Public	Supersedes:	None (Initial Issue)

STANDARD OPERATING PROCEDURE

SOP-PUB-21: ACCESSIBILITY, DISABILITY ACCOMMODATION & LANGUAGE ACCESS

1.0 PURPOSE & SCOPE

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish comprehensive, government-grade operational standards for ensuring full, equal, and non-discriminatory access to all public safety services, transparency portals, complaint mechanisms, and official records administered by Matcom Office of Public Safety LLC ("MATCOM"). MATCOM is committed to removing physical, communication, digital, and linguistic barriers so that members of the public—regardless of disability status or primary

language—can fully participate in public safety oversight, submit inquiries or concerns, and interact safely with MATCOM personnel.

1.2 Scope & Applicability

This policy applies universally across all operational divisions, administrative offices, field security assignments, customer service touchpoints, digital portals, and public transparency services maintained by MATCOM within the State of Maryland. It governs all MATCOM employees, licensed security officers, supervisory staff, administrative personnel, subcontractors, and designated agents.

1.3 Public Transparency Commitment

MATCOM affirms that public safety services and public transparency portals must be accessible to every member of the community. Accessibility is not an afterthought; it is a core legal responsibility and ethical mandate embedded into every standard operating workflow.

2.0 AUTHORITY & LEGAL REFERENCES

This SOP is promulgated under the authority of the Chief Executive Officer of Matcom Office of Public Safety LLC and derives its mandate from federal, state, and administrative legal authorities, including but not limited to:

- **Title II and Title III of the Americans with Disabilities Act (ADA) of 1990** (42 U.S.C. § 12101 et seq.) and implementing Department of Justice regulations (28 C.F.R. Parts 35 & 36).
- **Section 504 of the Rehabilitation Act of 1973** (29 U.S.C. § 794), prohibiting discrimination on the basis of disability in federally funded programs and public services.
- **Title VI of the Civil Rights Act of 1964** (42 U.S.C. § 2000d et seq.) and Executive Order 13166 ("Improving Access to Services for Persons with Limited English Proficiency").
- **Maryland Public Information Act (MPIA)**, Md. Code Ann., State Government Article § 4-101 et seq., establishing public rights to access government records in accessible formats.
- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01 and 12.10.02), governing Maryland Security Guard Licensees, standards of conduct, and public safety duties under MD License 24PLU-SGPD4620.

- **Maryland Police Accountability Act of 2022**, reinforcing standards for public accountability, transparent reporting, and non-discriminatory service delivery.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, governing private security agencies and public interaction mandates.
- **Maryland Constitutional Rights** regarding Due Process and Equal Protection of the Laws (MD Declaration of Rights, Arts. 24 & 46).
- **Web Content Accessibility Guidelines (WCAG) 2.1, Level AA Standards**, as adopted for public agency digital accessibility.

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following terms are defined:

- **Auxiliary Aids and Services:** Includes qualified interpreters (on-site or VRI), note-takers, computer-aided transcription services, written materials, audio recordings, captioning, large print or Braille documents, assistive listening devices, and accessible electronic document formats.
- **Disability:** A physical or mental impairment that substantially limits one or more major life activities, a record of such impairment, or being regarded as having such impairment, as defined under 42 U.S.C. § 12102.
- **Limited English Proficiency (LEP):** Refers to individuals who do not speak English as their primary language and who have a limited ability to read, speak, write, or understand English.
- **Language Access Plan (LAP):** An operational framework detailing protocols for providing immediate, qualified language assistance to LEP individuals free of charge.
- **Reasonable Accommodation:** Any necessary modification or adjustment to a policy, practice, or operational procedure that enables an individual with a disability to access services, participate in public reporting, or communicate effectively with MATCOM personnel.
- **Screen-Reader Compatibility:** Technical compliance of electronic documents (HTML, PDF, forms) with assistive technology software (e.g., JAWS, NVDA, VoiceOver) adhering to WCAG 2.1 Level AA specifications.
- **Qualified Interpreter:** An interpreter who is able to interpret effectively, accurately, and impartially, both receptively and expressively, using any necessary specialized vocabulary, certified through recognized bodies (e.g., RID or state credentialing).

4.0 POLICY STATEMENT

It is the absolute policy of Matcom Office of Public Safety LLC that no individual shall be excluded from participation in, denied the benefits of, or subjected to discrimination in any MATCOM service, program, activity, or public disclosure on the grounds of disability, race, color, national origin, or primary language. MATCOM shall proactively provide reasonable accommodations, auxiliary aids, and language assistance services free of charge to all members of the public who request or require them.

CORE MANDATE: FREE & IMMEDIATE AUXILIARY ASSISTANCE

All accommodation and translation services provided under SOP-PUB-21 are rendered at **zero cost** to the requesting member of the public. MATCOM personnel are strictly prohibited from imposing surcharges, delays, or administrative burdens on individuals seeking accessibility accommodations or language assistance.

5.0 STANDARD OPERATING PROCEDURES

5.1 Public Accommodation Request Protocol

MATCOM maintains multiple accessible channels for members of the public to request disability accommodations or alternative document formats:

1. **24/7 Intake Portal:** Requests may be submitted at any time via the official MATCOM portal at www.matcomops.org or via email to Oga@matcomops.org.
2. **Telephonic Request Line:** Individuals may contact 24/7 Dispatch at **1-855-715-9911** or Administrative Headquarters at **701-809-9911**. Dispatchers are trained to log accommodation requests immediately into the CAD system.
3. **In-Person / Postal Request:** Written requests may be delivered to 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207.

Service Request Type	Standard Response SLA	Fulfillment Authority
Alternate Document Format (Large Print, Screen-Reader PDF)	Within 3 Business Days	ADA Coordinator / OGA
On-Site or Telephonic Sign Language Interpreter	Within 24 Hours (Immediate in emergencies)	24/7 Dispatch Center
	Immediate (< 2 Minutes)	24/7 Dispatch Center

Service Request Type	Standard Response SLA	Fulfillment Authority
LEP Telephonic Language Translation (200+ Languages)		
Web / Dashboard Technical Accessibility Fix	Within 5 Business Days	IT & Data Analytics Division

5.2 Language Assistance Services & LEP Management

MATCOM utilizes an automated multi-lingual routing system integrated into its 24/7 Dispatch Operations Center (1-855-715-9911). When an LEP individual contacts MATCOM:

- Dispatchers immediately connect the call to a certified multi-lingual translation contract vendor supporting over 200 languages.
- All vital public documents—including Complaint Forms, Service Concern Intakes, Public Transparency Guides, and MPIA Request Forms—shall be published in English, Spanish, French, Amharic, Chinese, and Korean.
- Field security officers are equipped with mobile translation applications and "I Speak" language identification cards to facilitate immediate field communication.

5.3 Digital Accessibility & Web Content (WCAG 2.1 AA Compliance)

All digital public transparency portals, complaint dashboards, downloadable SOPs, statistical reports, and public forms published on www.matcomops.org must strictly conform to WCAG 2.1 Level AA standards. Technical requirements include:

- Full keyboard navigation capability without visual focus traps.
- All non-text visual content (images, charts, badges) must feature descriptive alt text attributes.
- Color contrast ratios must meet or exceed 4.5:1 for standard text and 3:1 for large headings (using MATCOM Navy #1B2A4A and Gold #B88A2E on compliant backgrounds).
- PDF documents published for public viewing must be fully tagged, structured, and tested with JAWS and NVDA screen readers.

5.4 Field Operations & Security Officer Conduct

When interacting with individuals who are deaf, hard of hearing, blind, visually impaired, or experiencing cognitive disabilities during duty assignments:

- MATCOM officers shall maintain a calm, respectful demeanor, utilize written notes or electronic mobile typing tools when appropriate, and allow service animals in all public spaces without interruption.
- Officers shall NEVER separate an individual with a disability from their service animal or necessary mobility device, unless an immediate physical safety threat exists.
- Officers conducting field contacts shall verify effective communication before concluding an interaction.

5.5 ADA Grievance & Service Denial Appeal Procedure

If an individual believes MATCOM has failed to provide a reasonable accommodation, auxiliary aid, or language assistance service, the individual may file an ADA Grievance with the ADA Coordinator within 60 days of the incident.

1. **Filing:** Submit form or statement in writing, by email (Oga@matcomops.org), or verbally via dispatch.
2. **Investigation:** The ADA Coordinator shall initiate an investigation within 3 business days and render a written determination within 10 business days.
3. **Executive Appeal:** If unsatisfied with the determination, the complainant may appeal to Dr. Brian C. Askew, CEO, whose decision shall constitute final administrative action for MATCOM within 10 business days.

6.0 ROLES & RESPONSIBILITIES

Role / Position	Primary Administrative & Operational Responsibilities
Dr. Brian C. Askew, CEO	Executive oversight; final appellate authority for ADA grievances; approval of annual accessibility audits and budget allocations.
ADA Coordinator / OGA Director	Direct oversight of accommodation requests; management of language translation contracts; conducting quarterly WCAG audits; maintaining request logs.
24/7 Dispatch Shift Supervisors	Immediate execution of telephonic interpretation routing; logging real-time accessibility requests; dispatching field auxiliary support.

Role / Position	Primary Administrative & Operational Responsibilities
Field Security Officers (Armed & Unarmed)	Direct compliance with field communication protocols; assisting individuals with disabilities; respecting service animals; utilizing translation tools.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE SANCTIONS

Strict compliance with this SOP is mandatory for all personnel. Failure of MATCOM employees or contractors to provide mandatory language access, refusal to honor reasonable accommodation requests without legal justification, or discriminatory treatment of individuals with disabilities constitutes grave misconduct. Violations will result in disciplinary sanctions up to and including termination of employment and revocation of security guard assignments under COMAR 12.10.01.

8.0 RECORDS MANAGEMENT, ARCHIVING & RETENTION

All accommodation logs, language assistance usage reports, digital compliance audits, and ADA grievance files shall be maintained in a secure, confidential electronic database managed by the Office of Governmental Affairs.

- Medical or disability data collected during accommodation requests shall be stored separately from general public records, strictly complying with MPIA confidentiality exemptions and federal privacy laws.
- All accessibility and language access records shall be retained for a minimum of **seven (7) years** from the date of record creation.

9.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure takes effect on August 13, 2026, and supersedes all prior directives regarding accessibility and language access. It shall be formally reviewed annually by the ADA Coordinator and the CEO.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026
MD License: 24PLU-SGPD4620

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch:
1-855-715-9911

This official document is classified as PUBLIC and published for community transparency and regulatory compliance under
COMAR 12.10.01.

MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT-GRADE SECURITY & PUBLIC SAFETY SERVICES

MD License: **24PLU-SGPD4620**
Armed & Unarmed Security
Exp: January 31, 2028

HQ: 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
Admin: 701-809-9911
24/7 Dispatch: 1-855-715-9911
Web: www.matcomops.org



Policy Number:	SOP-PUB-22	Effective Date:	August 13, 2026
Policy Title:	Community Feedback & Service Concern Resolution		
Approving Authority:	Dr. Brian C. Askew, CEO	Revision Date:	August 13, 2026
Responsible Division:	Office of Governmental Affairs / Community Relations	Review Date:	August 13, 2027
Classification:	Public	Supersedes:	None (Initial Issue)

STANDARD OPERATING PROCEDURE

SOP-PUB-22: COMMUNITY FEEDBACK & SERVICE CONCERN RESOLUTION

1.0 PURPOSE & SCOPE

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish a accessible, transparent, and structured mechanism for receiving, evaluating, conciliating, and resolving community feedback, general customer service concerns, delayed response queries, and neighborhood operational issues that do not rise to the level of formal officer misconduct. Matcom Office of Public Safety LLC ("MATCOM") believes that responsive

community feedback management is essential to fostering public trust, maintaining high operational standards, and continually improving security guard operations across Maryland.

1.2 Scope & Applicability

This SOP applies to all community members, commercial clients, property managers, residents, visitors, and public stakeholders interacting with MATCOM field security officers, dispatch staff, and administrative personnel within the State of Maryland.

1.3 Misconduct vs. Service Concern Threshold

This policy specifically governs non-disciplinary service inquiries and operational feedback. Allegations involving physical force, criminal conduct, severe civil rights violations, unlawful searches, or corrupt acts are governed by Professional Standards / Internal Affairs under SOP-PUB-25 and formal disciplinary procedures.

2.0 AUTHORITY & LEGAL REFERENCES

This SOP is issued under the executive authority of the Chief Executive Officer of Matcom Office of Public Safety LLC and complies with relevant state statutory and regulatory standards, including:

- **Maryland Police Accountability Act of 2022** principles regarding public input, transparency, and responsive community relations.
- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01 and 12.10.02), governing security guard agency licensing, supervisory duties, and public standards under MD License 24PLU-SGPD4620.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, regulating security guard agencies, customer service standards, and contract performance.
- **Maryland Public Information Act (MPIA)**, Md. Code Ann., State Government Article § 4-101 et seq., governing public access to non-confidential feedback logs and aggregate service performance statistics.
- **MATCOM Quality Assurance & Client Relations Directives.**

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following definitions apply:

- **Community Feedback:** Any expression of opinion, inquiry, commendation, suggestion, or general observation regarding MATCOM services, officer presence, or operational protocols submitted by a member of the public.
- **Service Concern:** A formal notification from a citizen or client expressing dissatisfaction with a non-disciplinary operational aspect of MATCOM's performance, such as response delays, officer demeanor/politeness, patrol coverage schedules, parking enforcement clarity, or uniform neatness.
- **Misconduct Complaint:** An allegation that, if proven true, would constitute a violation of state law, COMAR regulations, or MATCOM disciplinary policies (e.g., excessive force, theft, illegal search, false arrest).
- **Conciliation / Early Resolution:** An informal, non-punitive process led by Community Relations to address a service concern through direct communication, clarification of policy, operational adjustments, or supervisory coaching.
- **Service Quality Tracking Number (SQTN):** A unique tracking code generated upon receipt of any community feedback or concern to track its progress from intake through resolution.

4.0 POLICY STATEMENT

MATCOM welcomes community feedback and views service concerns as vital opportunities for agency improvement. MATCOM guarantees that all community feedback will be acknowledged promptly, evaluated impartially, and resolved in good faith. No individual shall suffer retaliation, harassment, or service disruption for submitting feedback or raising a service concern.

PUBLIC SERVICE ASSURANCE

MATCOM pledges to acknowledge every submitted service concern within **24 hours** and complete a full review with a written or verbal resolution within **10 business days**.

5.0 STANDARD OPERATING PROCEDURES

5.1 Intake Multi-Channel Accessibility

Community members may submit feedback or service concerns through any of the following official intake channels:

- **Digital Community Feedback Portal:** Online form at www.matcomops.org/feedback accessible 24/7.
- **Email Submission:** Directly to the Community Relations Division at Oga@matcomops.org.
- **24/7 Telephone Intake:** Contacting Dispatch at **1-855-715-9911** or Administration at **701-809-9911**.
- **Patrol Vehicle QR Codes:** Scanning the public feedback QR code displayed on all MATCOM marked patrol vehicles.
- **Written Correspondence:** Mail to MATCOM Office of Public Safety LLC, Attn: Community Relations, 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207.

5.2 Intake Triage & Classification Protocol

Upon receipt of any submission, the Community Relations Division shall conduct an immediate triage evaluation within 24 hours:

Classification	Criteria / Nature of Incident	Routing & Next Steps
Commendation / General Feedback	Positive officer praise, policy suggestions, general neighborhood inquiries.	Logged; Commendation letter forwarded to officer and placed in personnel file; response sent within 48 hours.
Service Concern (Level I)	Minor customer service issues, uniform neatness, response time inquiries, parking clarification.	Assigned SQTN; reviewed by Field Operations Supervisor; conciliated within 5 business days.
Service Concern (Level II)	Repeated response delays, property manager client disputes, officer unprofessional communication.	Assigned SQTN; reviewed by Community Relations Manager & OGA; client/citizen conference within 10 business days.
Misconduct Allegation (Escalation)	Excessive force, unlawful detention, theft, civil rights violation, criminal act.	IMMEDIATE TRANSFER to Professional Standards / Internal Affairs (SOP-PUB-25); citizen notified of IA case number within 12 hours.

5.3 Investigation & Conciliation Workflow

For all Level I and Level II Service Concerns, the assigned Community Relations Officer shall:

1. Review Computer-Aided Dispatch (CAD) call logs, GPS patrol tracking history, and officer shift reports related to the date and location of the concern.
2. Interview the assigned field security officer and immediate Field Supervisor to obtain a complete context of the occurrence.
3. Contact the community member to discuss their perspective, clarify operational policies, and explore informal conciliation options.
4. Determine whether operational adjustments, supervisor coaching, site post-order updates, or remedial training are warranted.

5.4 Resolution Pathways & Remedies

When a service concern is validated, MATCOM may implement one or more of the following corrective actions:

- **Supervisory Counseling & Coaching:** Direct retraining of the officer on communication, de-escalation, or customer service standards.
- **Post Order Revision:** Updating site-specific security instructions to resolve neighborhood confusion or improve response protocols.
- **Reassignment:** Adjusting officer field placements to better match site requirements.
- **Formal Explanation / Apology:** Issuing a written explanation detailing MATCOM's findings and offering a formal corporate apology when MATCOM standards were not met.

5.5 Community Analytics & Dashboard Integration

All feedback data—categorized by nature, site location, response time, and disposition—shall be aggregated quarterly by the Data Analytics Division. Summarized, non-confidential feedback trends shall be published on the MATCOM Public Transparency Dashboard pursuant to SOP-PUB-24.

6.0 ROLES & RESPONSIBILITIES

Role / Unit	Assigned Responsibilities
Dr. Brian C. Askew, CEO	

Role / Unit	Assigned Responsibilities
	Executive oversight of community relations policies; final approval of systemic operational changes resulting from feedback trends.
Community Relations Manager (OGA)	Overall administration of the Service Concern Resolution process; managing SQTN tracking logs; conducting conciliation conferences.
Field Operations Supervisors	Investigating assigned service concerns; interviewing officers; auditing CAD/ GPS records; conducting officer coaching.
Internal Affairs Commander	Receiving immediate escalations from OGA when feedback indicates potential officer misconduct.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE SANCTIONS

All MATCOM employees are required to cooperate fully with Community Relations investigations and conciliation reviews. Failure to report service concerns, concealment of community complaints, or any act of retaliation against a citizen filing a concern shall result in immediate disciplinary action up to and including termination of employment and referral to the Maryland State Police Licensing Division.

8.0 RECORDS MANAGEMENT, ARCHIVING & RETENTION

The Office of Governmental Affairs shall maintain a secure electronic database of all community feedback, service concerns, SQTN files, supervisor investigation reports, and written resolution letters.

- Service concern records shall be retained for a minimum of **five (5) years** from the date of case closure.
- Aggregated, anonymized statistics shall be preserved permanently for trend analysis and transparency reporting.

9.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure is effective August 13, 2026, and shall be formally reviewed every twelve (12) months by the Community Relations Manager and the Chief Executive Officer.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026
MD License: 24PLU-SGPD4620

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch:
1-855-715-9911

This official document is classified as PUBLIC and published for community transparency and regulatory compliance under
COMAR 12.10.01.

MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT-GRADE SECURITY & PUBLIC SAFETY SERVICES

MD License: **24PLU-SGPD4620**
Armed & Unarmed Security
Exp: January 31, 2028

HQ: 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207
Admin: 701-809-9911
24/7 Dispatch: 1-855-715-9911
Web: www.matcomops.org



Policy Number:	SOP-PUB-23	Effective Date:	August 13, 2026
Policy Title:	Officer/Employee Identification & Public Information		
Approving Authority:	Dr. Brian C. Askew, CEO	Revision Date:	August 13, 2026
Responsible Division:	Office of Governmental Affairs / Legal	Review Date:	August 13, 2027
Classification:	Public	Supersedes:	None (Initial Issue)

STANDARD OPERATING PROCEDURE

SOP-PUB-23: OFFICER / EMPLOYEE IDENTIFICATION & PUBLIC INFORMATION

1.0 PURPOSE & SCOPE

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to define clear, legally sound, and operational standards governing officer field identification and the release or masking of officer personal identifying information (PII) on MATCOM's public transparency portal, open databases, and public records disclosures. This SOP strictly balances public accountability, citizen oversight, and statutory transparency mandates with officer safety, privacy rights, and security protections under Maryland law.

1.2 Scope & Applicability

This SOP applies to all licensed security guards (armed and unarmed), special police officers, field supervisors, administrative staff, and executive leadership employed by Matcom Office of Public Safety LLC ("MATCOM") under Maryland License 24PLU-SGPD4620.

2.0 AUTHORITY & LEGAL REFERENCES

This policy is issued pursuant to the legal authority of the CEO of Matcom Office of Public Safety LLC and complies with statutory and regulatory mandates including:

- **Maryland Public Information Act (MPIA)**, Md. Code Ann., State Government Article § 4-101 et seq., specifically § 4-311 (Personnel Records Exemption) and § 4-351 (Investigative Records Exemption).
- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01.04 & 12.10.02.06), specifying mandatory security guard identification card display, badge standards, and uniform requirements.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, governing security guard agency obligations and employee record management.
- **Maryland Police Accountability Act of 2022**, regarding public disclosure of officer disciplinary records, complaint outcomes, and identification standards.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Maryland Wiretap Act), governing visual and audio recordings in public interactions.
- **Maryland Constitutional Protections** regarding privacy, equal protection, and due process.

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following definitions apply:

- **Badge / Unit Identifier:** A unique numeric or alphanumeric call sign (e.g., "Unit-402", "Badge-812") assigned to an individual MATCOM officer for public tracking, dispatch CAD logging, and transparency reporting.
- **Personal Identifying Information (PII):** Sensitive personal data including home address, social security number, personal cellular number, personal email address, date of birth, medical records, financial details, and emergency contact information.

- **Duty Nameplate & Insignia:** Uniform standard identification including the officer's last name, company badge, and MATCOM corporate shoulder patches required during field operations.
- **Public Transparency Portal Schema:** The standardized layout used on www.matcomops.org where public statistics, calls for service, and complaint dispositions are published using anonymized unit identifiers rather than full employee legal names, except where disclosure is mandated by law.
- **Officer Safety Exception:** A formal administrative determination made by Legal Counsel or the CEO withholding officer name disclosure due to credible safety threats, active stalking, protective orders, or active undercover assignments.

4.0 POLICY STATEMENT

MATCOM enforces a strict policy of transparent field identification while safeguarding employee personal safety and statutory privacy rights. While performing duty in uniform, every MATCOM officer shall clearly display their identity to the public. On public internet portals and published statistical reports, MATCOM utilizes standardized Unit Identifiers to ensure complete accountability without exposing personnel to external harassment, doxxing, or safety threats. Full officer names shall be disclosed in public records only when mandated by the Maryland Public Information Act, court orders, or formal legal processes.

FIELD IDENTIFICATION MANDATE

Except during tactical emergencies or active undercover operations approved in writing by the CEO, every MATCOM officer on duty **must** state their last name, unit number, and present their MATCOM duty card upon request by any member of the public.

5.0 STANDARD OPERATING PROCEDURES

5.1 Field Officer Identification Standards

All MATCOM security officers operating in uniform must strictly adhere to standard identification dress codes pursuant to COMAR 12.10.01:

- **Uniform Badge & Nameplate:** Must wear an official MATCOM metal or embroidered chest badge displaying the company name and license number, paired with a standard metallic nameplate showing the officer's last name.

- **Duty Security Guard Card:** Must carry their current Maryland State Police Security Guard Identification Card at all times on duty and display or present it upon lawful request.
- **Verbal Identification:** Upon citizen inquiry, the officer shall state: "I am Security Officer [Last Name], Unit [Number], with Matcom Office of Public Safety."

5.2 Transparency Portal Identification Schema & Unit Masking

To protect officer personal security while maintaining 100% public accountability, MATCOM's public-facing transparency dashboard (SOP-PUB-24) publishes incident logs, call logs, use-of-force summaries, and complaint dispositions according to the following disclosure matrix:

Data / Record Category	Public Portal Display Format	MPIA Disclosure Status
Calls for Service & CAD Incident Logs	Unit Number / Call Sign (e.g., Unit-204)	Disclosable with PII redacted
Sustained Misconduct Complaints (Formal Disciplinary)	Unit Number & Officer Name (if final action)	Disclosable under MPPA 2022 standards
Unfounded / Exonerated Complaint Dispositions	Unit Number Only (Anonymized)	Redacted under MPIA § 4-351
Officer Personal Data (Address, SSN, Phone, Medical)	STRICTLY PROHIBITED FROM PUBLICATION	EXEMPT under MPIA § 4-311
Use-of-Force Incident Summaries	Unit Number, Shift, Incident ID	Disclosable summary; names released upon final UFRB report if sustained

5.3 MPIA Public Records Processing & Redaction Protocol

All formal requests under the Maryland Public Information Act seeking officer records shall be forwarded immediately to the Legal Division at Oga@matcomops.org:

1. Legal Counsel shall conduct a statutory review under Md. Code Ann. Gen. Prov. § 4-101 et seq. within 10 days of receipt.
2. All home addresses, social security numbers, personal phone numbers, bank details, medical records, and family information shall be permanently redacted.

3. If an investigation is active and pending, personnel records shall be temporarily withheld under MPIA § 4-351 until final administrative closure.
4. The requesting party shall receive a formal response within 30 days specifying all redactions and statutory justifications.

5.4 Officer Safety Exception & Threat Protocols

If an officer is subject to credible physical threats, domestic violence, active stalking, or retaliatory harassment:

- The officer or supervisor may submit an emergency request to the Legal Division for an "Officer Safety Exception."
- Upon approval by the CEO, the officer's legal name shall be masked in all public releases, replaced exclusively with their confidential Unit Identifier across all portal entries.

5.5 Wiretap Act Compliance & Citizen Video Recording

Pursuant to Md. Courts & Judicial Proceedings § 10-402, citizens have the constitutional right to audio and video record MATCOM officers performing public duties in public spaces. MATCOM officers shall NOT order citizens to stop recording, confiscate recording devices, or demand deletion of media, provided the citizen does not physically obstruct officer operations or compromise scene safety.

6.0 ROLES & RESPONSIBILITIES

Role / Unit	Assigned Responsibilities
Dr. Brian C. Askew, CEO	Executive approval of Officer Safety Exceptions; final administrative review of contested MPIA record disclosures.
Legal Division Counsel (OGA)	Direct management of MPIA record requests; conducting statutory redactions; maintaining secure mapping tables linking Unit Identifiers to employee names.
Field Security Supervisors	Enforcing uniform identification standards (badges, nameplates, security guard cards); inspecting officer turnout prior to shift start.
Data Analytics Division	Ensuring public transparency dashboards display only authorized Unit Identifiers and redacted public summaries.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE SANCTIONS

Failure to wear required identification, refusal to state name and unit number to a citizen, unauthorized release of employee PII, or tampering with public portal mapping tables constitutes severe misconduct. Violators are subject to disciplinary action up to termination of employment and civil liability.

8.0 RECORDS MANAGEMENT, ARCHIVING & RETENTION

The Legal Division shall maintain a confidential mapping database linking all public Unit Identifiers to employee master records. Access is restricted to authorized legal and executive personnel.

- MPIA request logs, redacted release files, and officer identification registers shall be retained for a minimum of **seven (7) years**.
- Mapping keys for unit call signs shall be preserved permanently to enable retrospective auditing.

9.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure takes effect on August 13, 2026, and shall be reviewed annually by Legal Counsel and the CEO.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026
MD License: 24PLU-SGPD4620

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch:
1-855-715-9911

This official document is classified as PUBLIC and published for community transparency and regulatory compliance under
COMAR 12.10.01.

MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT-GRADE SECURITY & PUBLIC SAFETY SERVICES

MD License: **24PLU-SGPD4620**
Armed & Unarmed Security
Exp: January 31, 2028

HQ: 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 **Admin:** 701-809-9911 **24/7 Dispatch:** 1-855-715-9911 **Web:** www.matcomops.org



Policy Number:	SOP-PUB-24	Effective Date:	August 13, 2026
Policy Title:	Public Transparency Dashboard Statistics		
Approving Authority:	Dr. Brian C. Askew, CEO	Revision Date:	August 13, 2026
Responsible Division:	Office of Governmental Affairs / Data Analytics	Review Date:	August 13, 2027
Classification:	Public	Supersedes:	None (Initial Issue)

STANDARD OPERATING PROCEDURE

SOP-PUB-24: PUBLIC TRANSPARENCY DASHBOARD STATISTICS

1.0 PURPOSE & SCOPE

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish rigorous, standardized methodologies for capturing, validating, aggregating, calculating, and publishing operational public safety data on the MATCOM Public Transparency Dashboard. Matcom Office of Public Safety LLC ("MATCOM") believes that open, machine-readable, and mathematically sound statistical reporting reinforces public

accountability, demonstrates service efficiency, and validates compliance with Maryland public safety licensing standards.

1.2 Scope & Applicability

This policy applies to all operational data generated across MATCOM's 24/7 Computer-Aided Dispatch (CAD) system, Incident Management Database, Professional Standards / Internal Affairs tracking system, and Customer Feedback records. It governs the Data Analytics Division, Office of Governmental Affairs, and IT infrastructure personnel.

2.0 AUTHORITY & LEGAL REFERENCES

This SOP is promulgated under the authority of the CEO of Matcom Office of Public Safety LLC and in strict compliance with federal and state open data principles:

- **Maryland Public Information Act (MPIA)**, Md. Code Ann., State Government Article § 4-101 et seq., mandating proactive public release of government-grade aggregate statistical data.
- **Maryland Police Accountability Act of 2022**, establishing data transparency standards for public safety response, misconduct disposition reporting, and use-of-force analytics.
- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01 and 12.10.02), governing security guard operational reporting and record-keeping mandates under MD License 24PLU-SGPD4620.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, regulating security agency administrative reporting.
- **NAICS 561612 Security Guard & Patrol Service Standards** for statistical reporting.

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following definitions apply:

- **Call for Service (CFS):** Any incident logged into MATCOM CAD originating from a citizen emergency call, client request, dispatch assignment, or officer-initiated patrol activity.
- **Dispatch Response Time:** The precise elapsed time measured in seconds from the moment a call for service is answered by 24/7 Dispatch to the timestamped arrival of the first MATCOM patrol unit on scene.

- **Complaint Disposition Categories:** Sustained, Unfounded, Exonerated, Not Sustained, and Administrative Closure.
- **Commendation Rate:** The percentage ratio of formal positive citizen commendations relative to total public interactions.
- **Statistical Suppression Rule:** A privacy control method wherein any reporting cell containing fewer than five (5) aggregate occurrences is masked (e.g., "<5") on public displays to prevent individual re-identification.

4.0 POLICY STATEMENT

MATCOM pledges complete open data transparency. All public safety performance metrics shall be updated and published on a strict quarterly schedule at www.matcomops.org/transparency. Published statistics must be accurate, audited by the Data Analytics Division prior to release, free of administrative bias, and downloadable in machine-readable formats (CSV and JSON).

OPEN DATA COMMITMENT & SLA

Quarterly transparency datasets shall be published no later than **15 calendar days** following the conclusion of each calendar quarter. Datasets shall be permanently archived and accessible without fees or login barriers.

5.0 STANDARD OPERATING PROCEDURES

5.1 Core Published Metric Categories

The Data Analytics Division shall aggregate and calculate seven (7) primary operational metric categories for public release:

Metric Category	Data Source System	Published Breakdown Parameters
1. Calls for Service (CFS)	24/7 CAD Dispatch Log	Total volume by zone, time of day, priority level, and call type (emergency vs. routine).
2. Dispatch Response Times	CAD Automated Timestamps	Mean, median, and 90th percentile response times in minutes/seconds for Priority 1 calls.
3. Complaint Totals & Dispositions	Professional Standards IA Database	Count of complaints, citizen vs. internal origin, and disposition percentage breakdown.

Metric Category	Data Source System	Published Breakdown Parameters
4. Use-of-Force Occurrences	Use-of-Force Review Log (SOP-PUB-25)	Incidents by force level (Soft Hand, Less-Lethal, Firearm), officer unit, subject injury status.
5. Commendations & Service Praise	Community Relations Database	Total formal praises received, commendation-to-complaint ratio.
6. Vehicle Patrol & Pursuits	GPS Fleet Telematics	Patrol mileage logged, traffic contacts, zero-pursuit compliance confirmations.
7. Accessibility & Language Access	OGA Accommodation Log (SOP-PUB-21)	LEP translation call volume by language, ADA accommodation requests fulfilled.

5.2 Calculation Methodologies & Formulas

To ensure mathematical consistency across all reporting periods, the Data Analytics Division shall utilize standard statistical calculations for Average Response Time (ART), Sustained Disposition Percentage (SDP), Use-of-Force Rate per 1,000 Calls for Service, and Commendation-to-Complaint Ratio.

5.3 Data Quality Control, Validation & Anonymization Audit

Prior to publishing any dataset on www.matcomops.org, a multi-stage audit must be completed:

- 1. Automated Data Extraction:** Scripts pull raw data from CAD, IA, and CRM databases on the 1st day of the month following quarter-end.
- 2. Validation Audit:** Data analysts verify data completeness, eliminate duplicate CAD logs, and reconcile pending IA investigations.
- 3. Privacy & Anonymization Check:** The Legal Division reviews datasets to ensure all Personal Identifying Information (PII) is removed. Applying the Cell Suppression Rule, any aggregate demographic or geographical subgroup count less than 5 is replaced with "<5" to prevent re-identification.
- 4. Executive Certification:** The CEO signs off on the final dataset certificate prior to web deployment.

5.4 Dashboard Publication Schedule & Open Data API

Reporting Period	Data Coverage Dates	Mandatory Publication Deadline
First Quarter (Q1)	January 1 – March 31	April 15

Reporting Period	Data Coverage Dates	Mandatory Publication Deadline
Second Quarter (Q2)	April 1 – June 30	July 15
Third Quarter (Q3)	July 1 – September 30	October 15
Fourth Quarter (Q4) / Annual	October 1 – December 31	January 15 (Annual Report: Feb 1)

6.0 ROLES & RESPONSIBILITIES

Role / Position	Assigned Data & Dashboard Responsibilities
Dr. Brian C. Askew, CEO	Executive approval of quarterly transparency reports; certifying data accuracy to Maryland licensing authorities.
Data Analytics Division Director	Lead data scientist; executing calculation scripts; managing database integrations; enforcing formula accuracy.
Legal Division Counsel	Conducting privacy anonymization audits; enforcing MPIA compliance and cell suppression rules.
IT Administrator	Maintaining web dashboard uptime, database security, interactive chart elements, and downloadable CSV/JSON links.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE SANCTIONS

Falsification, deliberate alteration, selective omission, or unauthorized delay of transparency dashboard statistics constitutes severe administrative fraud. Personnel involved in manipulating public statistics will face immediate termination of employment, civil legal action, and criminal referral under Maryland state law.

8.0 RECORDS MANAGEMENT, ARCHIVING & RETENTION

The Data Analytics Division shall maintain an immutable digital archive of all raw source extraction tables, calculation sheets, audit logs, and published report files.

- Published quarterly statistical summaries and annual reports shall be preserved **permanently** on the MATCOM web archive.
- Raw CAD, IA, and CRM aggregated source data tables shall be retained for a minimum of **ten (10) years**.

9.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure takes effect on August 13, 2026, and shall be formally reviewed every twelve (12) months by the Data Analytics Division and the CEO.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026
MD License: 24PLU-SGPD4620

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch:
1-855-715-9911

This official document is classified as PUBLIC and published for community transparency and regulatory compliance under
COMAR 12.10.01.

MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT-GRADE SECURITY & PUBLIC SAFETY SERVICES

MD License: **24PLU-SGPD4620**

Armed & Unarmed Security

Exp: January 31, 2028

HQ: 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207

Admin:
701-809-9911

24/7 Dispatch:
1-855-715-9911

Web:
www.matcomops.org



Policy Number:	SOP-PUB-25	Effective Date:	August 13, 2026
Policy Title:	Public Use-of-Force Transparency		
Approving Authority:	Dr. Brian C. Askew, CEO	Revision Date:	August 13, 2026
Responsible Division:	Professional Standards / Internal Affairs	Review Date:	August 13, 2027
Classification:	Public	Supersedes:	None (Initial Issue)

STANDARD OPERATING PROCEDURE

SOP-PUB-25: PUBLIC USE-OF-FORCE TRANSPARENCY

1.0 PURPOSE & SCOPE

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to establish rigorous, unyielding public transparency standards regarding any use of physical, less-lethal, or lethal force by security officers employed by Matcom Office of Public Safety LLC ("MATCOM"). MATCOM is committed to maintaining the highest ethical and legal standards in force application, enforcing de-escalation mandates, conducting independent internal reviews of every force incident, and publishing comprehensive public summaries and aggregate statistics on the MATCOM Public Transparency Portal.

1.2 Scope & Applicability

This SOP applies to all armed and unarmed security guards, special police officers, field supervisors, and command staff operating under Maryland Security Guard License 24PLU-SGPD4620.

2.0 AUTHORITY & LEGAL REFERENCES

This SOP is promulgated under the authority of the CEO of Matcom Office of Public Safety LLC and derives its legal framework from Maryland statutes, regulations, and constitutional standards:

- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01 and 12.10.02), specifically regulating armed security guard force limits, mandatory firearm discharge reporting to the Maryland State Police Licensing Division within 24 hours, and duty equipment standards.
- **Maryland Police Accountability Act of 2022**, establishing proportional force standards, statutory de-escalation requirements, and public disclosure guidelines for force investigations.
- **MPCTC Training Standards (COMAR Title 12, Subtitle 12)** regarding defensive tactics, less-lethal force application, and de-escalation protocols.
- **Maryland Public Information Act (MPIA)**, Md. Code Ann., State Government Article § 4-101 et seq., governing public access to finalized use-of-force review records and statistical reports.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Maryland Wiretap Act), governing public audio/video recording of officers during force incidents.
- **Fourth Amendment / Article 26 Objective Reasonableness Standard** (Graham v. Connor, 490 U.S. 386).

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following definitions apply:

- **Use of Force:** Any physical force applied by a MATCOM officer to compel compliance, overcome physical resistance, defend self or others, or effect a lawful detention or arrest. Force is categorized into three levels:
 - **Level 1 (Soft Force):** Escort holds, soft hand controls, joint manipulations, non-injurious pressure points, and physical guiding techniques.

- **Level 2 (Hard / Less-Lethal Force):** Takedowns, hard hand strikes, chemical agents (OC spray), Conducted Energy Weapons (Taser deployment), or impact batons.
- **Level 3 (Lethal / Critical Force):** Firearm discharge, or force causing death, severe bodily harm, loss of consciousness, or bone fracture.
- **De-Escalation:** Tactical, verbal, and spatial techniques employed by officers to stabilize a scene, reduce immediacy of threats, and gain voluntary compliance without resorting to physical force.
- **Use of Force Review Board (UFRB):** An internal executive board convened by MATCOM to conduct formal administrative reviews of every Level 2 and Level 3 force occurrence.
- **Critical Incident Public Briefing:** An official, redacted public summary report published on www.matcomops.org detailing the facts, timeline, video availability, and administrative status of a Level 3 critical force incident.

4.0 POLICY STATEMENT

It is the strict policy of MATCOM that security officers shall use only the minimum force that is objectively reasonable, necessary, and proportional under the totality of circumstances to achieve a legitimate public safety objective. De-escalation must be attempted whenever safe and feasible. Every application of force—without exception—is subject to mandatory internal reporting, independent administrative investigation, Use of Force Review Board audit, and transparent public reporting pursuant to SOP-PUB-24.

MANDATORY REPORTING & STATE NOTIFICATION

Any discharge of a firearm by a MATCOM officer (other than range training) must be reported to 24/7 Dispatch immediately, to the CEO within **1 hour**, and formally submitted to the Maryland State Police Licensing Division within **24 hours** pursuant to COMAR 12.10.02.

5.0 STANDARD OPERATING PROCEDURES

5.1 Mandatory Incident Notification & Internal Escalation

When any level of physical force is applied by a MATCOM officer during a field assignment:

1. **Immediate Scene Stabilization & Medical Aid:** The officer shall immediately render emergency first aid and request EMS via 24/7 Dispatch (1-855-715-9911) if any subject or officer sustains injury or requests medical evaluation.
2. **Dispatcher Notification (Within 15 Minutes):** The officer must notify 24/7 Dispatch, detailing scene location, subject condition, and requesting an immediate Field Operations Supervisor response.
3. **Written Force Report Filing (Within 12 Hours):** The officer shall complete and submit a formal MATCOM Use of Force Incident Report prior to the end of their shift or within 12 hours max.

5.2 Use of Force Review Board (UFRB) Investigation Workflow

Force Level	Investigative Body	Review Timeline	Public Disclosure Outcome
Level 1 (Soft Force)	Field Operations Supervisor	Completed within 3 Business Days	Aggregated into Quarterly Public Transparency Statistics (SOP-PUB-24).
Level 2 (Less-Lethal Force)	Internal Affairs / UFRB Panel	Completed within 10 Business Days	Detailed case summary published on portal upon case closure; aggregated stats.
Level 3 (Firearm / Critical)	CEO, IA Commander, Legal Counsel & MSP Homicide/Licensing	UFRB convenes within 7 Days; final report within 30 Days	Critical Incident Public Briefing published within 14 days; full report upon final disposition.

5.3 Public Release Protocol for Critical Force Incidents

In the event of a Level 3 critical force incident:

- **Preliminary Public Release (Within 14 Days):** MATCOM shall publish an official Critical Incident Public Briefing on www.matcomops.org detailing date, time, location, unit identifier, call summary, force type, medical actions taken, and current administrative status of the officer (e.g., Paid Administrative Leave).

- **Video / Audio Media Release Guidelines:** Dashcam, body-worn camera, or CCTV footage associated with a force incident shall be evaluated for public release by Legal Counsel. Media shall be released unless prohibited by court order, ongoing criminal prosecution rights, or mandatory witness privacy protections under MPIA § 4-351.

5.4 Citizen Force Review Request & Complaint Rights

Any member of the public who believes a MATCOM officer utilized excessive, unnecessary, or unprovoked force may lodge a formal complaint or request a force review:

- Complaints may be filed via www.matcomops.org/complaint, email to Oga@matcomops.org, phone at 1-855-715-9911, or mail to Gwynn Oak Headquarters.
- Every citizen force complaint triggers an automatic Professional Standards Internal Affairs investigation under SOP-PUB-25.
- Complainants shall receive a unique case tracking number within 24 hours and a formal written notification letter upon investigation completion.

6.0 ROLES & RESPONSIBILITIES

Role / Unit	Assigned Force Transparency Responsibilities
Dr. Brian C. Askew, CEO	Executive Chair of Use of Force Review Board; final administrative authority on officer discipline; signatory on critical incident public releases.
Internal Affairs Commander	Lead investigator for Level 2 and Level 3 force incidents; securing evidence and bodycam media; filing MSP licensing reports within 24 hours.
Legal Division Counsel	Reviewing video/audio media for public release under MPIA; liaising with Maryland State Police and state prosecutors.
Field Operations Supervisors	Immediate scene response for force incidents; taking officer statements; impounding equipment; submitting Level 1 supervisor reviews.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE SANCTIONS

Failure to report use of force, submitting false force statements, concealing bodycam media, or using excessive force constitutes grounds for immediate termination of employment, revocation of Maryland security guard credentials under COMAR 12.10.01, and potential criminal prosecution under Maryland state law.

8.0 RECORDS MANAGEMENT, ARCHIVING & RETENTION

The Professional Standards Division shall maintain a secure, encrypted repository of all Use of Force Incident Reports, UFRB hearing minutes, video/audio evidence files, and public briefing releases.

- Critical Level 3 force incident files and firearm discharge records shall be retained **permanently**.
- Level 1 and Level 2 use of force records and UFRB audit logs shall be retained for a minimum of **twenty-five (25) years**.

9.0 EFFECTIVE DATE, PERIODIC REVIEW & APPROVAL

This Standard Operating Procedure takes effect on August 13, 2026, and shall be formally reviewed every twelve (12) months by Professional Standards and the CEO.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026
MD License: 24PLU-SGPD4620

Matcom Office of Public Safety LLC | 6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch:
1-855-715-9911

This official document is classified as PUBLIC and published for community transparency and regulatory compliance under
COMAR 12.10.01.



MATCOM OFFICE OF PUBLIC SAFETY LLC

STANDARD OPERATING PROCEDURE & PUBLIC DIRECTIVE

HQ: 6340 Security Blvd., Suite
100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Email: Oga@matcomops.org |
Web: www.matcomops.org
MD License: 24PLU-SGPD4620 |
NAICS: 561612

OFFICIAL PUBLIC DIRECTIVE — UNRESTRICTED DISTRIBUTION

Policy Number	SOP-PUB-26	Effective Date	August 13, 2026
Policy Title	Public Emergency Vehicle Transparency & Absolute Pursuit Prohibition		
Revision Date	August 13, 2026	Review Date	August 13, 2027
Approving Authority	Dr. Brian C. Askew, CEO	Supersedes	None (Initial Issue)
Responsible Division	Professional Standards / Operations Division	Classification	Public

1.0 PURPOSE & SCOPE

1.1 Purpose: The purpose of this Standard Operating Procedure (SOP) is to establish clear, comprehensive, and legally sound guidelines governing the transparency of emergency vehicle operations, mobile patrol safety data, and vehicular response metrics maintained by Matcom Office of Public Safety LLC ("MATCOM"). **It is the absolute policy of MATCOM that the agency does not engage in vehicular pursuits of any kind, under any circumstances, whatsoever.** This SOP documents that prohibition, establishes the framework for emergency vehicle response transparency, and ensures that all vehicular operations are conducted with the highest standard of public accountability, officer safety, and community trust.

1.2 Scope: This policy applies to all sworn and unsworn operational personnel, mobile patrol officers, field supervisors, fleet management officers, Professional Standards Division investigators, and executive management operating under MATCOM's Maryland Security Guard Agency License (MD License # 24PLU-SGPD4620). This procedure encompasses all emergency vehicle operations, routine mobile patrols, client property

perimeter security responses, inter-agency emergency assistance actions, and public transparency disclosures.

2.0 AUTHORITY & STATUTORY REFERENCES

This policy is promulgated under the executive authority of the Chief Executive Officer of MATCOM and is governed by applicable federal, state, and local statutory frameworks, including but not limited to:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Gov't Art. § 4-101 et seq. (governing public access to official records and statutory disclosure exemptions).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Security Guard Agencies and Certification Standards).
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 and 12.10.02 (Security Guard Licensing, Code of Conduct, and Operational Training Requirements).
- **Maryland Transportation Article:** Title 21, Subtitle 106 (Authorized Emergency Vehicles, Privileges, and Due Regard Standards).
- **Maryland Police Accountability Act of 2022:** Provisions promoting public transparency, incident reporting standards, and law enforcement alignment.
- **MPCTC Training Standards:** Maryland Police and Correctional Training Commissions guidelines (COMAR Title 12, Subtitle 12) regarding driver training and public safety principles.
- **Maryland Declaration of Rights:** Article 26 (Protection of constitutional rights during public interactions).

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following terms shall have the specified meanings:

- **Code 1 (Routine Operation):** Normal vehicular transit compliant with all statutory speed limits, traffic control devices, and standard motor vehicle laws without emergency equipment activated.
- **Code 3 (Emergency Response Driving):** The operation of an authorized MATCOM patrol vehicle equipped with emergency lights and sirens during an immediate, life-safety emergency, executed in strict accordance with MD Transportation Art. § 21-106.

- **Vehicular Pursuit:** An active, continuous attempt by a mobile patrol unit to apprehend a fleeing driver in a motor vehicle who is willfully ignoring audible and visual signals to stop. **MATCOM does not engage in vehicular pursuits of any kind, under any circumstances. This prohibition is absolute and without exception. All fleeing suspects shall be documented and reported to the appropriate law enforcement agency for apprehension.**
- **Administrative Safety Review (ASR):** A mandatory internal review conducted by the Professional Standards Division following any Code 3 emergency response, vehicle collision, or pursuit-related incident.
- **Telematics Monitoring System (TMS):** GPS-enabled onboard telemetry hardware and software that continuously captures vehicle speed, acceleration, braking, route mapping, and emergency light activation.
- **Public Emergency Driving Transparency Report:** An annual, publicly available statistical compilation detailing emergency vehicle responses, safety outcomes, and fleet safety findings published on MATCOM's public portal. This report shall affirmatively document that MATCOM engaged in zero (0) vehicular pursuits during the reporting period, in accordance with the agency's absolute prohibition on pursuits.

4.0 POLICY STATEMENT

It is the absolute policy of MATCOM that public safety and the preservation of human life outweigh all other operational considerations. **MATCOM does not engage in vehicular pursuits of any kind, under any circumstances, whatsoever.** As a licensed private security guard agency operating under Maryland Security Guard Agency License #24PLU-SGPD4620 and COMAR 12.10, MATCOM personnel are neither authorized nor trained to conduct vehicular pursuits. All fleeing suspects shall be documented with vehicle descriptions, direction of travel, and license plate information (where safely observable) and immediately reported to the appropriate law enforcement agency. The decision to pursue rests exclusively with sworn law enforcement officers acting under their respective agency policies and Maryland law.

To foster community trust and comply with Maryland transparency principles, MATCOM commits to collecting, auditing, and publishing accurate annual statistics regarding all emergency response driving, multi-agency assistance incidents, and vehicle accidents. MATCOM shall provide these public disclosures without compromising ongoing criminal investigations, revealing tactical operational blueprints, or disclosing protected officer personal information under MPIA § 4-311.

ABSOLUTE PROHIBITION: NO PURSUITS — NO EXCEPTIONS
MATCOM does not engage in vehicular pursuits of any kind, under any

circumstances, whatsoever. No MATCOM officer, supervisor, or contractor shall initiate, join, or continue a vehicular pursuit for any reason — including but not limited to property crimes, traffic infractions, misdemeanors, felonies, or flee-and-elude situations. This prohibition is absolute and applies to all MATCOM personnel without exception. Violation of this directive constitutes a severe breach of policy and may result in immediate termination, loss of security guard certification referral to the Maryland State Police, and criminal prosecution where applicable. All fleeing vehicles shall be documented and immediately reported to 911 or the appropriate law enforcement agency. Emergency response driving (Code 3) is permitted only when responding to an immediate threat of death or serious bodily harm on or immediately adjacent to client properties — this is not a pursuit.

5.0 OPERATING PROCEDURES & DETAILED REQUIREMENTS

5.1 Emergency Vehicle Operation & Absolute Pursuit Prohibition

5.1.1 Authorization Criteria: Mobile patrol officers may only activate emergency lights and sirens (Code 3) when responding to a verified active violent incident, robbery in progress, active shooter, or severe medical emergency where seconds count to prevent loss of life.

5.1.2 Due Regard Requirement: Pursuant to MD Transportation Art. § 21-106, emergency driving privileges do not relieve the officer from the duty to drive with due regard for the safety of all persons. Drivers must slow down at intersections, clear each lane before proceeding against traffic signals, and adjust speed for weather and road conditions.

5.1.3 Termination Mandate: An officer must immediately terminate Code 3 driving or multi-agency assistance if directed by a field supervisor, if weather/traffic conditions pose an unreasonable hazard, or if the risk to the public outweighs the immediate need for emergency arrival.

5.2 Mandatory Immediate Incident Reporting

Whenever a MATCOM vehicle is involved in a Code 3 emergency response, an attempted flee situation, or any vehicular collision (regardless of damage level), the operator must complete the following protocol within two (2) hours of the incident:

1. Notify 24/7 Dispatch (1-855-715-9911) immediately to log exact time, location, and nature of emergency response.
2. Submit an Electronic Vehicular Incident Report (Form MAT-VIR-100) detailing vehicle speed, route, environmental conditions, supervisor authorization, and outcome.

3. Ensure dashcam video, rear-seat video, and telematics data are auto-uploaded to the secure Professional Standards Division server.

5.3 Data Collection Architecture for Public Transparency

The Professional Standards Division shall maintain a standardized database capturing mandatory data points for every Code 3 emergency response. The database shall affirmatively record the total number of vehicular pursuits engaged in by MATCOM personnel, which shall always be zero (0) in accordance with the absolute pursuit prohibition established in this SOP:

Data Field Category	Specific Telematics & Operational Indicators Tracked	Public Disclosure Status
Incident Identifiers	Date, time of day, general geographic location (jurisdiction/zip code).	Fully Public
Initiating Cause	Initial reason for emergency response (e.g., violent felony in progress, medical emergency, multi-agency assistance).	Fully Public
Operational Metrics	Maximum speed attained, total distance, duration of response, road/weather conditions.	Fully Public (Aggregated)
Incident Outcome	Successful resolution, voluntary stop, termination by supervisor, collision, property damage, injuries.	Fully Public
Administrative Finding	PSD Review Disposition: Within Policy, Out of Policy, Policy Revision Recommended, Remedial Training Ordered.	Fully Public (Aggregated)
Officer & Unit Identifiers	Officer name, badge number, vehicle VIN, internal tactical call sign.	Restricted under MPIA § 4-311

5.4 Annual Public Transparency Reporting Schedule

5.4.1 Publication Deadline: MATCOM shall compile and publish the annual Public Pursuit & Emergency Driving Transparency Report on its official website (www.matcomops.org) no later than March 15th of each calendar year, covering the preceding year's operational data.

5.4.2 Content Standards: The report shall include quarterly statistical summaries, total Code 3 responses, an affirmative statement that zero (0) vehicular pursuits were conducted during the reporting period, any incidents where suspects fled from MATCOM personnel (documented for law enforcement referral), collision rates per 100,000 miles driven, percentage of incidents compliant with policy, and a narrative summary of systemic fleet safety enhancements.

5.5 Redaction Guidelines & MPIA Safe Harbor Provisions

Pursuant to the Maryland Public Information Act (MPIA), State Gov't Art. § 4-101 et seq., specific information shall be redacted prior to public release to protect ongoing legal proceedings and officer safety:

- **MPIA § 4-310 Exemption:** Information that would reveal specialized tactical maneuvers, active undercover operations, or compromise an active criminal prosecution handled by local law enforcement.
- **MPIA § 4-311 Exemption:** Personal identifiers of individual security officers, personnel evaluation records, or medical records resulting from an incident.
- **MPIA § 4-351 Exemption:** Specific security measures, fleet GPS hardware serial numbers, or client proprietary vault location details.

6.0 ROLES & RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Exercises ultimate approving authority over this SOP and ensures agency resources are allocated for fleet telemetry, safety training, and public compliance.

6.2 Director of Operations: Oversees daily mobile patrol operations, enforces Code 3 parameters, and ensures immediate supervisory oversight during emergency responses.

6.3 Professional Standards Division (PSD) Commander: Audits all vehicular incident reports, conducts administrative reviews, verifies telematics accuracy, and drafts the Annual Public Transparency Report.

6.4 Mobile Patrol Officers: Complies with all emergency driving limits, operates patrol vehicles with due regard, uploads dashcam data, and submits Form MAT-VIR-100 within required timeframes.

6.5 Public Information Officer (PIO) / IT Director: Formats, validates, and publishes approved transparency reports on the public portal in accessible, machine-readable formats.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE PROVISIONS

7.1 Mandatory Compliance: Compliance with this SOP is mandatory for all MATCOM personnel. **Any engagement in a vehicular pursuit by MATCOM personnel is an immediate and absolute violation of agency policy.** Engaging in a pursuit, failing to report a Code 3 response, or failing to report a fleeing suspect to law enforcement constitutes a severe breach of professional conduct and is grounds for immediate

disciplinary action up to and including termination, and referral to the Maryland State Police for potential licensing action.

7.2 Disciplinary Sanctions: Violations of this policy shall result in progressive administrative action, up to and including immediate termination of employment, revocation of driver authorization, and reporting to the Maryland State Police Licensing Division pursuant to COMAR 12.10.01.

8.0 RECORDS MANAGEMENT, RETENTION & REPORTING

All telematics data, dashcam recordings, Form MAT-VIR-100 reports, and PSD review findings shall be permanently stored in MATCOM's encrypted digital archive and retained for a minimum of seven (7) years in compliance with Maryland record retention guidelines for public safety entities. Published annual reports shall remain permanently accessible in the online Public Directive Library archive.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISIONS

This Standard Operating Procedure takes effect on August 13, 2026, and shall undergo formal administrative review by the Executive Management Board annually on or before August 13, 2027. Any required statutory amendments resulting from changes in COMAR or Maryland General Assembly enactments shall be incorporated immediately.

AUTHORIZATION & EXECUTIVE APPROVAL

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the executive management of Matcom Office of Public Safety LLC in full accordance with Maryland law and regulatory standards.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Managing Director
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

Matcom Office of Public Safety LLC • Licensed Maryland Security Guard Agency
(License # 24PLU-SGPD4620)

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 • 24/7 Dispatch:

1-855-715-9911 • www.matcomops.org

Document Identifier: SOP-PUB-26 • Classification: Public • Published Pursuant to Maryland
Public Information Act & Transparency Guidelines



MATCOM OFFICE OF PUBLIC SAFETY LLC

STANDARD OPERATING PROCEDURE & PUBLIC DIRECTIVE

HQ: 6340 Security Blvd., Suite
100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Email: Oga@matcomops.org |
Web: www.matcomops.org
MD License: 24PLU-SGPD4620 |
NAICS: 561612

OFFICIAL PUBLIC DIRECTIVE — UNRESTRICTED DISTRIBUTION

Policy Number	SOP-PUB-27	Effective Date	August 13, 2026
Policy Title	Early Intervention System Public Explanation		
Revision Date	August 13, 2026	Review Date	August 13, 2027
Approving Authority	Dr. Brian C. Askew, CEO	Supersedes	None (Initial Issue)
Responsible Division	Professional Standards / Human Resources	Classification	Public

1.0 PURPOSE & SCOPE

1.1 Purpose: The purpose of this Standard Operating Procedure (SOP) is to provide a transparent, publicly accessible explanation of MATCOM's Early Intervention System (EIS). This policy outlines how MATCOM proactively monitors operational patterns, public complaints, force applications, vehicular incidents, and training indicators to identify personnel who may benefit from non-disciplinary professional guidance, retraining, or wellness support before conduct issues arise.

1.2 Scope: This procedure applies to all active security personnel, armed guards, mobile patrol units, field supervisors, dispatchers, and administrative employees operating under MATCOM's Maryland Security Guard Agency License (MD License # 24PLU-SGPD4620). It defines the operational thresholds, evaluation mechanics, supportive interventions, and public transparency disclosures associated with the EIS.

2.0 AUTHORITY & STATUTORY REFERENCES

This policy is promulgated under the authority of the CEO of MATCOM and complies with Maryland public safety statutes, including:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Gov't Art. § 4-311 (Mandatory Exemption Protecting Personnel and Performance Records from Public Disclosure).
- **Maryland Police Accountability Act of 2022:** Best practice recommendations regarding Early Intervention System implementation and officer wellness frameworks.
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 and 12.10.02 (Security Guard Training, Supervision, and Professional Standards).
- **Maryland Business Regulation Article:** Title 12, Subtitle 1 (Agency Licensing and Oversight).
- **MPCTC Training Guidelines:** COMAR Title 12, Subtitle 12 standards regarding performance management and supervisory intervention.

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following terms shall apply:

- **Early Intervention System (EIS):** A structured, data-driven, non-disciplinary administrative management tool designed to identify performance patterns and assist employees through supportive intervention, retraining, or counseling.
- **EIS Alert / Trigger:** An automated administrative notification generated when an employee reaches a predefined numerical threshold of monitored indicators within a specified time window.
- **Non-Disciplinary Remediation:** Supportive administrative actions—such as peer mentoring, specialized tactical retraining, stress management counseling, or supervisory coaching—that do not constitute formal disciplinary sanctions or adverse employment actions.
- **Individual Intervention Plan (IIP):** A customized, time-bound development plan formulated by Professional Standards and HR to support an employee flagged by an EIS alert.
- **Public EIS Transparency Summary:** An annual anonymized statistical summary published on MATCOM's portal reporting overall EIS activity without disclosing individual employee identities.

4.0 POLICY STATEMENT

MATCOM is firmly committed to maintaining professional excellence, officer well-being, and community accountability. MATCOM recognizes that high-stress security environments can impact employee performance. The Early Intervention System operates as a supportive, proactive risk-management mechanism designed to catch potential performance concerns at the earliest possible stage.

CRITICAL PUBLIC PRINCIPLE: EIS IS NOT MISCONDUCT OR DISCIPLINE

An EIS alert is an administrative threshold flag generated automatically by software.

An EIS alert IS NOT a finding of misconduct, fault, policy violation, or disciplinary guilt. High operational activity levels (e.g., working high-volume posts) can trigger an alert purely due to exposure frequency. An alert simply prompts a supervisory review to determine if support or training is beneficial.

MATCOM balances public transparency with statutory privacy requirements. While individual EIS records are protected personnel files under MPIA § 4-311, MATCOM annually publishes aggregate EIS program statistics to reassure the public that proactive oversight is continuously active.

5.0 OPERATING PROCEDURES & DETAILED REQUIREMENTS

5.1 Monitored Performance Indicators & System Thresholds

The Professional Standards Division continuously inputs data into the secure EIS database. An automated alert is generated whenever an employee meets or exceeds any of the following threshold combinations:

Monitored Indicator Category	Numerical Threshold Trigger	Evaluation Timeframe	Primary Administrative Objective
Use of Force Incidents	2 or more recorded force applications	90 Rolling Days	Evaluate de-escalation tactics, verbal commands, and post stress factors.
Public / Citizen Complaints	2 or more formal or informal complaints	180 Rolling Days	Assess customer service, communication style, and conflict resolution.
Vehicle Accidents / Fleet Claims	2 or more preventable vehicle incidents	12 Rolling Months	Review defensive driving skills, fatigue, and telematics reports.

Monitored Indicator Category	Numerical Threshold Trigger	Evaluation Timeframe	Primary Administrative Objective
Policy / Administrative Infractions	3 or more minor infractions (tardiness, uniform)	90 Rolling Days	Identify personal stress, scheduling conflicts, or burnout.
Commendations & Recognition	Logged continuously	Ongoing	Provide positive context and balance operational evaluations.
Training & Certification Deficiencies	1 missed mandatory recertification date	Immediate Trigger	Ensure 100% COMAR training compliance prior to post assignment.

5.2 Supervisory Review Workflow

When an EIS alert is generated, the following mandatory review process is executed within fourteen (14) calendar days:

- 1. Automated Notification:** The EIS software notifies the Professional Standards Division Manager and the employee's direct Field Supervisor.
- 2. Contextual Preliminary Review:** The Supervisor and PSD Manager review the underlying incident reports, shift logs, client post assignment difficulty, and past commendations.
- 3. Informal Employee Conference:** The Supervisor conducts a non-disciplinary meeting with the employee to discuss the alert, review operational conditions, and listen to employee feedback regarding post challenges or personal stressors.
- 4. Determination of Action:**
 - No Action Required: The alert was driven solely by high-density routine activity with zero policy concerns. Case closed with rationale logged.
 - Supportive Action Recommended: Formulation of an Individual Intervention Plan (IIP).

5.3 Supportive Intervention Pathways

If supportive intervention is warranted, MATCOM provides tailored resources without financial cost to the employee:

- **Specialized Tactical Retraining:** One-on-one instruction in verbal de-escalation, defensive tactics, conflict resolution, or defensive driving.
- **Peer Mentoring Program:** Assignment to a senior Field Training Officer (FTO) for co-patrol duties and guidance.

- **Employee Assistance Program (EAP) Referral:** Confidential access to professional counseling, stress management, financial advice, or mental health support.
- **Post Reassignment:** Temporary rotation to a lower-density security post to alleviate operational burnout.

5.4 Public Explanation & Transparency Reporting Framework

To ensure the public fully understands MATCOM's early intervention efforts without violating employee privacy under MPIA § 4-311, MATCOM publishes an Annual EIS Public Summary Report on www.matcomops.org by April 30th of each year.

Report Content: Total EIS alerts generated agency-wide, total IIPs implemented, breakdown of alerts by indicator category, percentage of successful intervention completions, and systemic training improvements instituted as a result of aggregate EIS trends. No personnel names, badge numbers, or specific incident locations shall be disclosed.

6.0 ROLES & RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Provides executive oversight, ensures funding for EAP and training resources, and reviews annual aggregate EIS reports.

6.2 Director of Human Resources: Coordinates EAP referrals, oversees individual support plans, and ensures personnel privacy is protected in full compliance with MPIA § 4-311.

6.3 Professional Standards Division Manager: Administers the EIS database, conducts weekly data audits, facilitates supervisory review workflows, and compiles annual transparency reports.

6.4 Field Supervisors: Conduct constructive, non-disciplinary employee conferences, monitor IIP progress, and foster a supportive command environment.

6.5 Security Personnel: Actively participate in recommended retraining or mentorship programs and communicate operational challenges openly with supervisors.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE PROVISIONS

7.1 Administrative Integrity: Field supervisors who fail to conduct mandatory EIS reviews within statutory timelines or attempt to use EIS alerts as a punitive measure shall be subject to administrative review for failure to execute managerial duties.

7.2 Non-Punitiveness Protection: An employee's participation in an EIS intervention plan shall not be recorded as a disciplinary sanction and shall not prohibit eligibility for promotion or commendation.

8.0 RECORDS MANAGEMENT, RETENTION & REPORTING

All individual EIS alerts, supervisor conference notes, and Individual Intervention Plans shall be maintained in a secure, encrypted EIS database separate from standard employee personnel files. In accordance with Maryland administrative record guidelines, individual EIS records shall be retained for five (5) years following closure, after which they shall be purged unless active litigation applies.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISIONS

This Standard Operating Procedure takes effect on August 13, 2026, and shall undergo annual review on or before August 13, 2027. Revisions shall be approved by the CEO and updated in the Public Directive Library.

AUTHORIZATION & EXECUTIVE APPROVAL

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the executive management of Matcom Office of Public Safety LLC in full accordance with Maryland law and regulatory standards.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Managing Director
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

Matcom Office of Public Safety LLC • Licensed Maryland Security Guard Agency
(License # 24PLU-SGPD4620)

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 • 24/7 Dispatch:
1-855-715-9911 • www.matcomops.org

Document Identifier: SOP-PUB-27 • Classification: Public • Published Pursuant to Maryland
Public Information Act & Transparency Guidelines



MATCOM OFFICE OF PUBLIC SAFETY LLC

STANDARD OPERATING PROCEDURE & PUBLIC DIRECTIVE

HQ: 6340 Security Blvd., Suite
100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Email: Oga@matcomops.org |
Web: www.matcomops.org
MD License: 24PLU-SGPD4620 |
NAICS: 561612

OFFICIAL PUBLIC DIRECTIVE — UNRESTRICTED DISTRIBUTION

Policy Number	SOP-PUB-28	Effective Date	August 13, 2026
Policy Title	Public Policy Directive Library		
Revision Date	August 13, 2026	Review Date	August 13, 2027
Approving Authority	Dr. Brian C. Askew, CEO	Supersedes	None (Initial Issue)
Responsible Division	Office of Governmental Affairs / Legal	Classification	Public

1.0 PURPOSE & SCOPE

1.1 Purpose: The purpose of this Standard Operating Procedure (SOP) is to establish standard governance, classification criteria, version control protocols, digital archiving procedures, and public publication standards for MATCOM's online Public Policy Directive Library hosted at www.matcomops.org. MATCOM is committed to operating with complete institutional openness, making its governing rules, standards of conduct, force policies, and administrative directives accessible to the public, clients, regulatory authorities, and public safety partners.

1.2 Scope: This procedure governs all written directives, Standard Operating Procedures (SOPs), Special Orders, Administrative Bulletins, and Operational Guidelines issued by MATCOM. It establishes criteria for determining public versus security-restricted classification, formatting standards, revision workflows, and public document request management under the Maryland Public Information Act (MPIA).

2.0 AUTHORITY & STATUTORY REFERENCES

This SOP is issued pursuant to executive management authority and aligns with state and federal legal mandates:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Gov't Art. § 4-101 et seq. (establishing right of public inspection and specific statutory exemptions).
- **Maryland Police Accountability Act of 2022:** Transparency mandates requiring public accessibility of agency policy manuals and operational guidelines.
- **Code of Maryland Regulations (COMAR):** COMAR 12.10.01 and 12.10.02 (Security Guard Agency Regulatory Standards).
- **Maryland State Archives Record Standards:** Guidelines for electronic document preservation, indexing, and permanent historical archiving.
- **Web Content Accessibility Guidelines (WCAG 2.1 AA):** Standards ensuring digital public policy libraries are accessible to individuals with disabilities.

3.0 DEFINITIONS

For the purposes of this Standard Operating Procedure, the following terms shall apply:

- **Public Policy Directive:** An official MATCOM policy, SOP, or code of conduct that governs general operations, public interactions, complaint procedures, ethics, or transparency, approved for unrestricted public distribution.
- **Restricted / Security-Sensitive Directive:** A operational directive containing tactical response codes, active armory security protocols, high-security client vault blueprints, or IT cyber defense architecture exempt from disclosure under MPIA § 4-310/351 to protect public and facility safety.
- **Active Directive Library:** The current, fully effective collection of MATCOM policies hosted on the official public web portal.
- **Superseded Directive Archive:** The historical online repository containing past, replaced versions of MATCOM policies, maintained to preserve full institutional lineage and transparency.
- **Semantic Versioning Architecture:** A standardized numbering system (e.g., v1.0, v1.1) denoting major policy overhauls versus minor administrative updates.

4.0 POLICY STATEMENT

MATCOM operates under a presumption of open government and public transparency. It is the official policy of MATCOM that all written directives governing employee conduct,

public safety protocols, citizen interaction standards, and administrative accountability shall be classified as **Public** and maintained in the online Policy Directive Library.

Exemptions from public publication shall be limited strictly to directives where disclosure would compromise physical security, expose tactical vulnerabilities, or violate statutory confidentiality requirements under Maryland law. When a directive contains both public principles and sensitive tactical details, MATCOM shall publish a redacted or summary version rather than withholding the entire document.

5.0 OPERATING PROCEDURES & DETAILED REQUIREMENTS

5.1 Policy Classification Framework

Prior to promulgation, every proposed directive shall be reviewed by the Classification Committee (comprising the General Counsel, Director of Governmental Affairs, and Director of Operations) to assign one of two official classifications:

Classification Category	Defining Criteria & Policy Types Included	Public Access & Publishing Rule
Public Directive (Unrestricted)	SOPs governing public interaction, ethics, Complaint Procedures, Use of Force policy summaries, Early Intervention, Public Portals, and Privacy Notices.	Published immediately on www.matcomops.org in PDF & HTML formats. Available for download without registration.
Restricted Security Directive (Confidential)	Directives containing active tactical entry codes, SWAT co-response blueprints, high-security cash-in-transit routes, armory key controls, or IT firewall configurations.	Restricted to authorized personnel. Redacted public summary version published if feasible under MPIA § 4-310.

5.2 Standardized Document Structure & Formatting

All SOPs written for MATCOM must adhere strictly to the standardized 10-part document hierarchy to ensure uniformity and legal clarity:

- 1. Standardized Header Banner & Contact Details:** License # 24PLU-SGPD4620, HQ address, phone, email, web.
- 2. Standardized Front Page Metadata Table:** Policy Number, Title, Effective Date, Revision Date, Approving Authority, Responsible Division, Classification, Supersedes, Review Date.
- 3. 1.0 Purpose & Scope**
- 4. 2.0 Authority & Statutory References** (Full Maryland code citations)

5. **3.0 Definitions**
6. **4.0 Policy Statement**
7. **5.0 Operating Procedures & Detailed Requirements**
8. **6.0 Roles & Responsibilities**
9. **7.0 Compliance, Enforcement & Administrative Provisions**
10. **8.0 Records Management, Retention & Reporting**
11. **9.0 Effective Date, Review Cycle & Revisions**
12. **Signature Block & Regulatory Footer:** CEO execution line and license expiration metadata.

5.3 Version Control & Publishing Protocol

5.3.1 Indexing Convention: Directives shall follow a structured alphanumeric identifier (e.g., SOP-PUB-28 for Public SOPs, SOP-OPS-12 for Operations SOPs).

5.3.2 Version Revision Tracking: Minor grammar or statutory cross-reference updates increment the decimal (v1.0 to v1.1). Substantive policy modifications increment the integer (v1.0 to v2.0) and require fresh executive signature execution.

5.3.3 Web Publishing Timeline: Upon execution by Dr. Brian C. Askew, CEO, the IT Division shall publish the new SOP to the online library within five (5) business days.

5.4 Maintenance of the Superseded Policy Archive

To preserve institutional history and ensure accountability for past operational incidents, MATCOM maintains an online Superseded Policy Archive. When a policy is revised or superseded:

- The active library document is updated to the new version.
- The previous version is stamped "SUPERSEDED — HISTORICAL REFERENCE ONLY" across the header in red text.
- The superseded document is moved to the public archive section of www.matcomops.org and retained for a minimum of ten (10) years.

5.5 MPIA Public Policy Request Pipeline

Members of the public requesting unreleased policy documents or unredacted versions may submit a formal request under the Maryland Public Information Act to Oga@matcomops.org. Requests shall be processed by General Counsel within thirty (30) days in full accordance with Md. Code Ann., State Gov't Art. § 4-203.

6.0 ROLES & RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Retains final authority over policy approvals, classification overrides, and public promulgation.

6.2 General Counsel / Legal Division: Reviews all directives for Maryland statutory compliance, evaluates MPIA exemption applicability, and manages formal public information requests.

6.3 Director of Governmental Affairs: Serves as primary liaison with state licensing boards, oversight bodies, and the public regarding policy accessibility.

6.4 Policy Coordinator / Webmaster: Maintains the online digital portal, verifies WCAG 2.1 AA compliance, formats document metadata, and manages the Superseded Policy Archive.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE PROVISIONS

7.1 Public Accessibility Mandate: Failure to publish an approved Public SOP or deliberate withholding of non-exempt public directives constitutes an administrative violation subject to executive review.

7.2 Protection of Restricted Data: Unauthorized public dissemination of Restricted Security Directives by MATCOM employees is strictly prohibited and constitutes grounds for immediate termination and civil legal remedies under Maryland law.

8.0 RECORDS MANAGEMENT, RETENTION & REPORTING

Master electronic files of all active and superseded policies shall be maintained permanently in MATCOM's secure cloud repository. Web server download logs for the Policy Library shall be retained for three (3) years to monitor public engagement and system performance.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISIONS

This Standard Operating Procedure takes effect on August 13, 2026, and shall undergo formal annual review on or before August 13, 2027.

AUTHORIZATION & EXECUTIVE APPROVAL

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the executive management of Matcom Office of Public Safety LLC in full accordance with Maryland law and regulatory standards.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Managing Director
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC
Date: August 13, 2026

Matcom Office of Public Safety LLC • Licensed Maryland Security Guard Agency
(License # 24PLU-SGPD4620)

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 • 24/7 Dispatch:
1-855-715-9911 • www.matcomops.org

Document Identifier: SOP-PUB-28 • Classification: Public • Published Pursuant to Maryland
Public Information Act & Transparency Guidelines



MATCOM OFFICE OF PUBLIC SAFETY LLC

STANDARD OPERATING PROCEDURE & PUBLIC DIRECTIVE

HQ: 6340 Security Blvd., Suite
100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Email: Oga@matcomops.org |
Web: www.matcomops.org
MD License: 24PLU-SGPD4620 |
NAICS: 561612

OFFICIAL PUBLIC DIRECTIVE — UNRESTRICTED DISTRIBUTION

Policy Number	SOP-PUB-29	Effective Date	August 13, 2026
Policy Title	Website & Public Portal Terms of Use		
Revision Date	August 13, 2026	Review Date	August 13, 2027
Approving Authority	Dr. Brian C. Askew, CEO	Supersedes	None (Initial Issue)
Responsible Division	Office of Governmental Affairs / IT / Legal	Classification	Public

1.0 PURPOSE & SCOPE

1.1 Purpose: The purpose of this Standard Operating Procedure (SOP) and Terms of Use agreement is to establish legally binding standards, operational rules, digital evidence submission criteria, acceptable use parameters, and cyber defense protocols governing all public access to and interaction with MATCOM's web interfaces, public portals, community tip lines, and client portals hosted at www.matcomops.org.

1.2 Scope: This policy applies to all external visitors, public users, clients, media entities, community informants, and automated web traffic accessing MATCOM's digital infrastructure. It covers website browsing, electronic tip submissions, digital media/evidence uploads, policy directive downloads, public dashboard views, and interactive client account management interfaces.

2.0 AUTHORITY & STATUTORY REFERENCES

This policy is promulgated under the corporate and legal authority of MATCOM and is backed by state and federal criminal and civil statutes:

- **Maryland Criminal Law Article:** Md. Code Ann., Crim. Law § 9-501 (Prohibiting False Statements to Public Safety/Security Officials) & § 9-503 (False Reports of Crimes).
- **Maryland Computer Crimes Act:** Md. Code Ann., Crim. Law § 6-301 et seq. (Unauthorized Access, System Intrusion, and Denial of Service Offences).
- **Maryland Courts and Judicial Proceedings Article:** Md. Code Ann., Cts. & Jud. Proc. § 10-402 (Maryland Wiretap Act - Prohibiting Audio Interception without All-Party Consent).
- **Maryland Personal Information Protection Act (MPIPA):** Md. Code Ann., Com. Law § 14-3501 et seq. (Data Security and Breach Notification Framework).
- **Federal Computer Fraud and Abuse Act (CFAA):** 18 U.S.C. § 1030 (Federal Cyber Intrusion Sanctions).
- **Digital Millennium Copyright Act (DMCA):** 17 U.S.C. § 512 (Protection of Intellectual Property and Media Submissions).

3.0 DEFINITIONS

For the purposes of this Terms of Use agreement, the following terms shall apply:

- **Public Portal:** Any web-based domain, sub-domain, or interactive portal operated by MATCOM (including www.matcomops.org) accessible to the public or authorized clients.
- **Automated Scraping / Extraction:** The use of bots, spiders, web crawlers, AI scraping tools, or automated scripts to systematically download, index, harvest, or aggregate portal data without express written authorization.
- **Digital Evidence Submission:** Any electronic media, image, video file, document, or written account uploaded to MATCOM by a public user regarding a security incident, crime tip, or property complaint.
- **Malicious Upload / Intrusion:** The transmission of malware, trojans, ransomware, executable code, SQL injection scripts, or fraudulent reports intended to compromise MATCOM's IT network or disrupt public safety operations.
- **Public Dashboard Data Disclaimer:** The explicit legal notice governing the informational "AS IS" status of statistical summaries published on MATCOM public portals.

4.0 POLICY STATEMENT

Access to MATCOM's public web portals is a conditional privilege granted strictly in accordance with these Terms of Use. MATCOM welcomes legitimate public interaction, crime tip submissions, policy review, and client engagement. However, MATCOM maintains a ZERO-TOLERANCE posture toward cyber attacks, unauthorized automated data harvesting, submission of false or malicious reports, and violations of Maryland privacy laws.

CRITICAL STATUTORY WARNING: FALSE REPORTING IS A CRIME

Submitting false, fraudulent, or fictitious crime tips, emergency alerts, or complaints through MATCOM public portals is strictly prohibited. Pursuant to **Maryland Criminal Law § 9-501**, making a false statement or report to security and public safety officials is a criminal offense punishable by imprisonment and monetary fines. All submissions log IP addresses and metadata for law enforcement prosecution.

5.0 OPERATING PROCEDURES & DETAILED REQUIREMENTS

5.1 Acceptable Use Standards

Public users are authorized to browse public pages, download published Public Policy Directives, review transparency reports, submit legitimate community security tips, and access client account features using standard web browsers.

5.2 Express Prohibitions & Cyber Security Restrictions

Users accessing MATCOM portals are strictly prohibited from engaging in any of the following activities:

1. **Automated Data Scraping:** Utilizing automated software, bots, AI scraping tools, or scripts to harvest text, graphics, statistical tables, or portal data for commercial aggregation or AI model training without written consent from MATCOM CEO.
2. **System Probing & Intrusion:** Attempting to probe, scan, or test the vulnerability of MATCOM servers, bypass authentication barriers, execute SQL injections, or launch Distributed Denial of Service (DDoS) attacks.
3. **Illegal Audio Recordings (Wiretap Compliance):** Uploading video or audio media captured in violation of **Md. Cts. & Jud. Proc. § 10-402 (Maryland Wiretap Act)**, which mandates all-party consent for recording private audio communications in Maryland.
4. **Malicious Media Uploads:** Uploading executable files (.exe, .bat, .js), corrupted media, obscene material, or content infringing third-party intellectual property rights.

5.3 Conditions for Digital Evidence & Tip Submissions

By submitting digital photos, video recordings, documents, or tip descriptions to MATCOM through the portal:

Submission Term Category	Legal Requirement & Operational Protocol
Irrevocable Investigation License	The user grants MATCOM a non-exclusive, royalty-free, worldwide license to review, store, analyze, and transfer submitted media to law enforcement authorities (Maryland State Police, local police departments) for criminal investigation and prosecution.
Chain of Custody Acknowledgment	Submitted media becomes part of an official security record archive. Submissions cannot be deleted or retracted by the user once uploaded.
Anonymous Reporting Option	Users may submit tips anonymously; however, IP telemetry is logged internally for security defense and false report investigation under Md. Crim. Law § 9-501.

5.4 Public Dashboard & Information Disclaimer

All statistical data, pursuit summaries, Early Intervention explanations, and public dashboard figures published on www.matcomops.org are provided **"AS IS" and "AS AVAILABLE"** for general public information purposes only. While MATCOM makes every effort to ensure accuracy:

- Dashboard figures do not constitute formal judicial findings or binding legal admissions.
- Official certified records for evidentiary or legal proceedings must be requested through formal MPIA submission procedures.
- MATCOM disclaims liability for minor typographical errors or temporary portal downtime.

5.5 Intellectual Property Rights

The MATCOM name, logo, official agency seal, standard operating procedure contents, and website design are the exclusive intellectual property of Matcom Office of Public Safety LLC. Unauthorized commercial reproduction or impersonation of MATCOM seal is strictly prohibited under Maryland law.

5.6 Enforcement, IP Banning & Law Enforcement Escalation

MATCOM employs automated Firewall and Intrusion Prevention Systems (IPS) that continuously monitor portal traffic. In the event of a breach of these Terms of Use:

- **Immediate Technical Block:** The offending IP address, subnet, or user account shall be permanently banned from MATCOM systems.
- **Civil Claims:** MATCOM reserves the right to seek damages and injunctive relief against illegal scrapers or cyber attackers.
- **Criminal Referral:** Cyber intrusions or false reports shall be immediately referred to the Maryland State Police Cyber Crimes Unit and the Federal Bureau of Investigation (FBI).

6.0 ROLES & RESPONSIBILITIES

6.1 Chief Information Officer (CIO): Manages website infrastructure, configures web application firewalls, implements rate-limiting, and logs cyber intrusion attempts.

6.2 General Counsel: Enforces Terms of Use, initiates civil legal action against unauthorized scrapers, and manages law enforcement referrals.

6.3 Public Information Officer (PIO): Ensures public disclaimer notices are prominently displayed on all interactive forms and public dashboards.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE PROVISIONS

Continued use of MATCOM public portals constitutes explicit acceptance of these Terms of Use. MATCOM reserves the right to update these terms at any time without individual notice by publishing the updated SOP to the Policy Library.

8.0 RECORDS MANAGEMENT, RETENTION & REPORTING

All web server access logs, firewall security alerts, tip submission metadata, and IP tracking records shall be maintained in secure digital storage for a minimum of three (3) years for cyber audit and evidentiary purposes.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISIONS

This Standard Operating Procedure takes effect on August 13, 2026, and shall undergo annual review on or before August 13, 2027.

AUTHORIZATION & EXECUTIVE APPROVAL

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the executive management of Matcom Office of Public Safety LLC in full accordance with Maryland law and regulatory standards.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Managing Director
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC

Date: August 13, 2026

Matcom Office of Public Safety LLC • Licensed Maryland Security Guard Agency
(License # 24PLU-SGPD4620)
6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 • 24/7 Dispatch:
1-855-715-9911 • www.matcomops.org
Document Identifier: SOP-PUB-29 • Classification: Public • Published Pursuant to Maryland
Public Information Act & Transparency Guidelines



MATCOM OFFICE OF PUBLIC SAFETY LLC

STANDARD OPERATING PROCEDURE & PUBLIC DIRECTIVE

HQ: 6340 Security Blvd., Suite
100-1071
Gwynn Oak, MD 21207
24/7 Dispatch: 1-855-715-9911 |
Office: 701-809-9911
Email: Oga@matcomops.org |
Web: www.matcomops.org
MD License: 24PLU-SGPD4620 |
NAICS: 561612

OFFICIAL PUBLIC DIRECTIVE — UNRESTRICTED DISTRIBUTION

Policy Number	SOP-PUB-30	Effective Date	August 13, 2026
Policy Title	Public Portal Privacy Notice & Data Collection		
Revision Date	August 13, 2026	Review Date	August 13, 2027
Approving Authority	Dr. Brian C. Askew, CEO	Supersedes	None (Initial Issue)
Responsible Division	Office of Governmental Affairs / IT / Legal	Classification	Public

1.0 PURPOSE & SCOPE

1.1 Purpose: The purpose of this Standard Operating Procedure (SOP) and Public Privacy Notice is to establish a robust, government-grade data governance framework detailing how MATCOM collects, processes, stores, protects, and discloses personal information and telemetry data acquired through its public web portals, tip submission interfaces, job application portals, and digital communications at www.matcomops.org.

1.2 Scope: This procedure covers all digital data collection points operated by MATCOM. It governs Personally Identifiable Information (PII), technical telemetry, IP routing data, cookie files, crime tip submissions, employment applications, and client account data. It applies to all IT personnel, data processors, administrative staff, and third-party cloud service vendors supporting MATCOM's infrastructure.

2.0 AUTHORITY & STATUTORY REFERENCES

This Privacy Notice and data collection policy is governed by applicable federal, state, and administrative legal frameworks:

- **Maryland Public Information Act (MPIA):** Md. Code Ann., State Gov't Art. § 4-101 et seq. (protecting personal information including § 4-331 preference data, § 4-338 identity details, and § 4-311 personnel files).
- **Maryland Personal Information Protection Act (MPIPA):** Md. Code Ann., Com. Law § 14-3501 et seq. (mandating reasonable security measures for PII and statutory breach notification timelines).
- **Maryland Courts and Judicial Proceedings Article:** Md. Code Ann., Cts. & Jud. Proc. § 10-402 (Maryland Wiretap Act).
- **COMAR Security Guard Regulations:** COMAR 12.10.01 (Record Keeping and Confidentiality Standards for Licensed Security Agencies).
- **NIST Cybersecurity Framework / NIST SP 800-88:** Guidelines for Media Sanitization and Electronic Data Destruction.

3.0 DEFINITIONS

For the purposes of this Privacy Notice & Data Collection SOP, the following definitions apply:

- **Personally Identifiable Information (PII):** Any data point that can directly or indirectly identify an individual, including full name, home address, personal telephone number, email address, Social Security Number, driver's license number, IP address, or uploaded photograph.
- **Technical Telemetry Data:** System-generated technical metadata captured during portal interactions, including browser type, operating system, referrer URL, device identifier, session duration, and request timestamps.
- **Cookie / Session Token:** A small text file stored on a user's device that enables secure portal navigation, user authentication, and preference retention.
- **Data Controller:** Matcom Office of Public Safety LLC, which determines the legal purpose and administrative means for processing portal data.
- **Data Processor:** Vetted third-party cloud hosting providers, IT infrastructure contractors, or software vendors operating under binding data protection agreements with MATCOM.

4.0 POLICY STATEMENT

MATCOM respects the fundamental privacy rights of citizens, clients, job applicants, and public portal users. MATCOM operates under the core privacy principle of **Data Minimization**: MATCOM collects only the personal information strictly necessary to provide public safety services, execute contractual security duties, fulfill public transparency mandates, and defend its digital network against cyber threats.

MATCOM NEVER sells, rents, leases, or trades user personal data or contact lists to third-party commercial marketers. All PII collected through MATCOM portals is protected by government-grade encryption and access controls in strict compliance with the Maryland Personal Information Protection Act (MPIPA).

5.0 OPERATING PROCEDURES & DETAILED REQUIREMENTS

5.1 Categories of Data Collected

MATCOM collects two distinct categories of information through its public digital portals:

Data Collection Category	Specific Data Elements Captured	Method of Collection & User Consent
Active Voluntary Submissions	Name, telephone number, email address, incident details, physical location, uploaded photo/video media, job applicant resumes, and client billing details.	Provided directly and voluntarily by the user through online forms, tip submission fields, or portal uploads.
Passive Technical Telemetry	Public IP address, geolocation (city/zip level), user-agent string, browser version, pages visited, session duration, HTTP response codes, and essential security cookies.	Captured automatically by web server firewalls and session management logging upon accessing www.matcomops.org .

5.2 Primary Legal & Business Purposes of Collection

Information collected by MATCOM is processed strictly for legitimate public safety and administrative purposes:

- Security Operations & Incident Response:** Investigating reported crime tips, client property incidents, and emergency dispatch requests.
- Public Transparency Reporting:** Generating anonymized statistical reports required by SOP-PUB-26 and SOP-PUB-27.

3. **Employment Vetting:** Processing security officer employment applications in compliance with COMAR 12.10.01 background check mandates.
4. **Cyber Security Defense:** Detecting and mitigating unauthorized intrusion, rate-limiting, scraping attempts, and DDoS attacks.

5.3 Data Retention & Destruction Schedule

MATCOM maintains strict data retention schedules to ensure information is not retained longer than legally required. Electronic records are permanently purged according to **NIST SP 800-88** sanitization standards:

Record Category	Mandatory Retention Period	Disposition & Sanitization Method
Web Server Access & Firewall Logs	Twelve (12) Months	Automated cryptographic overwrite after 365 days.
Community Tips & Incident Media	Five (5) Years (Min.)	Permanent digital archive if linked to active prosecution; otherwise purged after 5 years.
Job Applicant PII & Resumes	Three (3) Years	Purged from HR database 3 years post-submission pursuant to EEOC/COMAR rules.
General Public Portal Inquiries	Three (3) Years	Secure electronic purge.

5.4 Third-Party Disclosure Conditions & Exemptions

MATCOM shall not disclose personal information collected through its portals to external entities except under the following specific, lawful circumstances:

- **Law Enforcement Escalation:** Disclosure to local police departments, Maryland State Police, or federal agencies pursuant to an active criminal investigation, valid subpoena, or court order.
- **Maryland Public Information Act (MPIA) Requests:** If portal records are requested under MPIA, MATCOM's General Counsel shall strictly redact all personal identifiers, email addresses, phone numbers, and PII pursuant to **Md. Code Ann., State Gov't Art. § 4-331 and § 4-338** prior to document release.
- **Imminent Threat to Life:** Immediate emergency disclosure to public safety authorities to prevent imminent death or severe bodily injury.

5.5 Cybersecurity Safeguards & Technical Controls

MATCOM implements government-grade technical, physical, and administrative safeguards to protect portal data:

- **Encryption in Transit:** All website traffic and form submissions are encrypted using Transport Layer Security (TLS 1.3 / 256-bit SSL).
- **Encryption at Rest:** Database repositories containing PII are encrypted using Advanced Encryption Standard (AES-256).
- **Access Control:** Strict Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) limit employee data access strictly on a "need-to-know" operational basis.
- **Vulnerability Audits:** Annual third-party vulnerability scans and penetration testing.

5.6 User Rights & Privacy Contact

Users wishing to inquire about personal data submitted through MATCOM portals, request correction of inaccurate PII, or file a privacy concern may contact MATCOM's Data Privacy Officer:

Matcom Office of Public Safety LLC — Data Privacy Officer

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207

Email: Oga@matcomops.org | Telephone: 701-809-9911

6.0 ROLES & RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Maintains ultimate executive accountability for agency data privacy compliance and approves major data governance policies.

6.2 Data Privacy Officer (DPO) / General Counsel: Audits data collection practices, oversees MPIA redactions, handles privacy inquiries, and manages MPIPA breach notifications.

6.3 Chief Information Officer (CIO): Implements TLS/AES encryption, configures firewall access controls, enforces NIST data purging schedules, and monitors cyber telemetry.

7.0 COMPLIANCE, ENFORCEMENT & ADMINISTRATIVE PROVISIONS

7.1 Employee Misuse Sanctions: Any MATCOM employee or contractor who accesses, misuses, or discloses portal PII without authorization shall face immediate termination, revocation of security credentials, and potential legal prosecution under Maryland law.

8.0 RECORDS MANAGEMENT, RETENTION & REPORTING

Privacy audit logs, consent records, and data destruction certificates shall be maintained by the IT Division for seven (7) years in secure digital format.

9.0 EFFECTIVE DATE, REVIEW CYCLE & REVISIONS

This Standard Operating Procedure takes effect on August 13, 2026, and shall undergo annual review on or before August 13, 2027.

AUTHORIZATION & EXECUTIVE APPROVAL

This Standard Operating Procedure has been reviewed, approved, and officially promulgated by the executive management of Matcom Office of Public Safety LLC in full accordance with Maryland law and regulatory standards.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Managing Director
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental Affairs
Matcom Office of Public Safety LLC
Date: August 13, 2026

Matcom Office of Public Safety LLC • Licensed Maryland Security Guard Agency
(License # 24PLU-SGPD4620)

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 • 24/7 Dispatch:
1-855-715-9911 • www.matcomops.org

Document Identifier: SOP-PUB-30 • Classification: Public • Published Pursuant to Maryland
Public Information Act & Transparency Guidelines



MATCOM OFFICE OF PUBLIC SAFETY LLC

LICENSED MARYLAND SECURITY GUARD AGENCY — LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Direct: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — OFFICIAL ADMINISTRATIVE DIRECTIVE

Policy Number:	SOP-PUB-31	Effective Date:	August 13, 2026
Title:	Cybersecurity & Fraudulent Submission Protection	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	IT Division / Office of Governmental Affairs	Classification:	Public
Supersedes:	None (Initial Issue)	Distribution:	All Divisions & Public Web Portal

SOP-PUB-31 — CYBERSECURITY & FRAUDULENT SUBMISSION PROTECTION

PUBLIC SAFETY INTAKE INFRASTRUCTURE & INFORMATION ASSURANCE STANDARD

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes mandatory technical, operational, and administrative controls for Matcom Office of Public Safety LLC ("MATCOM") to protect public-facing complaint portals, official web systems, case management databases, and administrative communications against cyber threats, malicious software, fraudulent complaint submissions, automated bot attacks, impersonation, phishing, ransomware, and unauthorized access attempts.

1.2 Scope: This policy applies to all electronic intake systems, web forms, portal endpoints, email servers, digital storage repositories, and physical information systems operated or controlled by MATCOM. It governs all personnel, including executive leadership, sworn/licensed security guards, administrative staff, IT personnel, third-party contractors, and members of the public utilizing MATCOM's public safety intake portals.

2.0 AUTHORITY & REFERENCES

This policy is issued under the authority of the Chief Executive Officer pursuant to Maryland law and professional security guard agency standards:

- **Maryland Code Ann., Commercial Law § 14-3501 et seq.:** Maryland Personal Information Protection Act (MPIPA).
- **Maryland Code Ann., State Government § 10-1301 et seq.:** Cybersecurity and Data Breach Notification Standard for State Entities and Contractors.
- **Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. § 4-101 et seq.:** Specific provisions under § 4-338 regarding exemption of cybersecurity plans, system vulnerabilities, and network infrastructure records.
- **Maryland Criminal Law Code Ann. § 7-302:** Maryland Crimes Against Computers Law (Unauthorized Access, Malware Distribution, Fraud).
- **COMAR Title 12, Subtitle 10, Chapters 01 & 02:** Maryland State Police Licensing Division Regulations for Security Guard Agencies.
- **Maryland Courts & Judicial Proceedings Code Ann. § 10-402:** Wiretap and Electronic Communications Protections.
- **NIST SP 800-53 Rev. 5:** Security and Privacy Controls for Information Systems and Organizations.

3.0 DEFINITIONS

3.1 Automated Submission Bot: Software applications configured to execute automated scripts across web forms to submit high volumes of spam, malicious payloads, or false data.

3.2 Content Disarm and Reconstruction (CDR): A cybersecurity technology that strips embedded active code, macros, and hidden scripts from incoming digital attachments, converting them into safe, sanitized flat files.

3.3 Fraudulent Submission: An intentionally false, fabricated, forged, or spoofed complaint, feedback, or evidence file submitted to MATCOM with intent to deceive, harass, disrupt operations, or compromise technical infrastructure.

3.4 Web Application Firewall (WAF): A security barrier that filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application to prevent attacks such as SQL injection, cross-site scripting (XSS), and buffer overflows.

4.0 POLICY

4.1 Policy Statement: It is the explicit policy of MATCOM to maintain a zero-trust, high-integrity digital environment for public safety operations. While MATCOM guarantees full accessibility for legitimate public grievances, citizen complaints, and operational feedback, MATCOM strictly forbids the use of its public intake infrastructure for malicious cyber activities, automated spam campaigns, impersonation, or submission of fraudulent records.

4.2 Information Assurance Commitment: MATCOM shall employ robust encryption, continuous monitoring, web application firewalls, automated malware sandboxing, and strict access controls to ensure that citizen complaints are preserved with complete confidentiality and integrity while protecting the agency's systems against disruption or compromise.

5.0 PROCEDURES

5.1 Technical Intake Controls & Perimeter Defense

All public-facing web portals, forms, and digital communication endpoints operated by MATCOM shall enforce the following perimeter defenses:

1. **Transport Layer Encryption:** End-to-end TLS 1.3 encryption for all web form submissions, preventing interception or tampering during transit.
2. **Web Application Firewall (WAF):** Deployment of an enterprise WAF configured to inspect all incoming HTTP/HTTPS requests for malicious signatures, cross-site scripting (XSS), SQL injection (SQLi), and command injection attempts.
3. **Automated Bot Prevention:** Mandatory integration of enterprise CAPTCHA / bot challenge software (e.g., Cloudflare Turnstile or reCAPTCHA Enterprise) on every public submission form.
4. **Rate Limiting:** Hard limits restricting submission frequency to a maximum of 3 submissions per IP address per hour, preventing Denial of Service (DoS) attacks and brute-force flooding.

5.2 File Attachment Inspection & Sanitization

Public complaint forms that accept uploaded evidence files (photos, video, documents) must subject all attachments to multi-stage technical inspection prior to storage:

Mandatory File Upload Restrictions:

Permitted extensions: .PDF, .JPG, .JPEG, .PNG, .MP4, .MOV, .DOCX.

Prohibited

extensions: .EXE, .BAT, .VBS, .PS1, .ZIP, .RAR, .JS, .HTML, .DLL, .MSI, .SCR.
Maximum file size: 25 MB per individual file upload; 100 MB aggregate per submission.

1. **Automated Antivirus/Malware Sandboxing:** All uploaded files must be routed directly to an isolated cloud sandbox and scanned by at least two independent signature/heuristic anti-malware engines.
2. **Content Disarm and Reconstruction (CDR):** Document files (.PDF, .DOCX) shall undergo CDR processing to neutralize active macros, dynamic script execution, and embedded object links before analyst viewing.
3. **Storage Isolation:** Uploaded attachments shall be stored in an isolated, non-executable, encrypted cloud storage bucket (AES-256) separated from operational databases.

5.3 Identity Verification & Impersonation Detection

To protect against false-identity submissions while respecting citizen privacy under Maryland law:

- **Email Verification Requirement:** Non-anonymous submissions require automated 2-step email verification (one-time verification token sent to complainant's email) before the complaint is logged into the active investigation queue.
- **Domain Verification:** System automated checks for SPF, DKIM, and DMARC alignment on incoming email communications to flag spoofed domain addresses.
- **Anonymous Complaint Protocol:** Anonymous complaints are permitted in accordance with public accountability principles, but are subjected to heightened internal screening to verify factual plausibility prior to allocating investigative resources.

5.4 Detection & Triage of Fraudulent Submissions

The IT Division and Internal Affairs shall utilize automated and manual screening workflows to classify incoming web submissions:

Classification Level	Indicator Criteria	Automated Action	Investigative Routing
Level 1: Valid Intake	Passed WAF, clean file scan, valid email token, coherent content.	Assigned Case ID & Receipt Generated.	Routed to Professional Standards IA Queue.
Level 2: Suspicious / Low Quality	Duplicate IP address, high spam score, missing contact details, gibberish.	Flagged for Manual Review.	Held in Hold Queue for 48 hours for IA Supervisory Triage.

Classification Level	Indicator Criteria	Automated Action	Investigative Routing
Level 3: Fraudulent / Harassment	Identified impersonation, fabricated identities, extortion text, malicious intent.	Quarantined & Sender Logged.	Forwarded to Office of Governmental Affairs & Legal.
Level 4: Malicious Cyber Attack	Exploit payload detected, malware attachment, active attack attempt.	Immediate IP Block & Session Terminated.	Alert sent to CISO; Incident Logged for Criminal Referral.

5.5 System Access Control & Data Protection

Access to complaint records, citizen personal data, and investigative case files is governed by strict Zero-Trust and Role-Based Access Control (RBAC) principles:

1. **Multi-Factor Authentication (MFA):** Mandatory hardware key or authenticator app MFA for all MATCOM staff accessing the internal case management database.
2. **Audit Logging:** System logs must record every access, view, modification, export, or deletion of complaint records. Audit logs must be tamper-evident, append-only, and retained for 7 years.
3. **Data Encryption:** All data at rest encrypted using AES-256; all data in transit encrypted via TLS 1.3.

5.6 Incident Response & Breach Notification Protocols

In the event of a confirmed or suspected cybersecurity breach, unauthorized access, or database compromise:

MANDATORY STATUTORY BREACH NOTIFICATION (Md. Code Ann., State Gov't § 10-1301 et seq.):

If personal information is compromised, the IT Division shall immediately notify the CEO. MATCOM shall report the breach to the **Office of the Attorney General of Maryland** and the **State Chief Information Security Officer** within the statutory timeframes established by Maryland law.

5.7 Criminal Referral of Malicious Cyber Activity

Where an individual or entity deliberately submits malicious code, executes a cyber attack, or submits forged documents with intent to obstruct justice or defraud MATCOM:

- The CISO shall assemble a digital forensic package containing IP headers, payload analysis, time stamps, and system logs.

- MATCOM Legal Counsel shall formally refer the matter to the **Maryland State Police Cyber Crime Unit**, the **Federal Bureau of Investigation (FBI) IC3**, and the **Baltimore County State's Attorney's Office** for prosecution under Md. Crim. Law § 7-302.

6.0 RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Exercises ultimate oversight of information security policies, approves major system architecture changes, and authorizes law enforcement referrals for cyber crimes.

6.2 IT Division / Chief Information Security Officer (CISO): Responsible for maintaining firewalls, malware scanners, CDR systems, access controls, audit logs, and conducting annual penetration testing.

6.3 Professional Standards / Internal Affairs (IA): Responsible for reviewing flagged suspicious submissions, ensuring evidence integrity, and maintaining strict confidentiality of valid complaints.

6.4 Office of Governmental Affairs & Legal Counsel: Manages statutory breach notifications to Maryland state authorities and coordinates external agency communications.

7.0 COMPLIANCE & ENFORCEMENT

7.1 Internal Enforcement: Any MATCOM employee who bypasses cybersecurity controls, shares system credentials, disables antivirus protections, or opens unauthorized suspicious attachments shall be subject to immediate administrative discipline, up to and including termination of employment and revocation of security guard license authorization.

7.2 Audits: The IT Division shall conduct quarterly vulnerability scans and an annual comprehensive cybersecurity compliance audit in accordance with NIST SP 800-53 standards.

8.0 RECORDS & DOCUMENTATION

All cybersecurity logs, firewall traffic archives, malicious file quarantine records, breach reports, and WAF audit trails shall be securely retained for a minimum of **seven (7) years** pursuant to COMAR 12.10.01 and MATCOM's master document retention policy, after which they may be securely purged in compliance with state standards.

9.0 EFFECTIVE DATE & REVIEW

This Standard Operating Procedure takes effect on **August 13, 2026**, and supersedes all prior administrative issuances concerning digital intake and cybersecurity. This policy shall be formally reviewed on or before **August 13, 2027**.

OFFICIAL EXECUTIVE APPROVAL & ADOPTION

Brian C. Askeew, Ph.D.

DR. BRIAN C. ASKEW

CHIEF EXECUTIVE OFFICER & APPROVING AUTHORITY
MATCOM OFFICE OF PUBLIC SAFETY LLC

Daune Simpkins

DAUNE SIMPKINS

DEPUTY DIRECTOR, GOVERNMENTAL AFFAIRS
MATCOM OFFICE OF PUBLIC SAFETY LLC
DATE: AUGUST 13, 2026 | LICENSE: 24PLU-SGPD4620



MATCOM OFFICE OF PUBLIC SAFETY LLC

LICENSED MARYLAND SECURITY GUARD AGENCY — LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Direct: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — OFFICIAL ADMINISTRATIVE DIRECTIVE

Policy Number:	SOP-PUB-32	Effective Date:	August 13, 2026
Title:	Complaint Withdrawal & Continued Investigation	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Internal Affairs	Classification:	Public
Supersedes:	None (Initial Issue)	Distribution:	All Divisions & Public Web Portal

SOP-PUB-32 — COMPLAINT WITHDRAWAL & CONTINUED INVESTIGATION

ADMINISTRATIVE STANDARDS FOR COMPLAINANT WITHDRAWAL REQUESTS & AGENCY-INITIATED PROCEEDINGS

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes official policy and procedural protocols governing requests by citizens, employees, or third parties to withdraw previously submitted administrative complaints against Matcom Office of Public Safety LLC ("MATCOM") security officers, supervisors, or operational staff. It mandates strict safeguards to ensure withdrawal requests are voluntary, free from coercion, intimidation, or improper financial settlement, and defines the legal and operational thresholds under which MATCOM maintains an independent obligation to continue investigating serious misconduct regardless of a complainant's desire to withdraw.

1.2 Scope: Applies to all internal affairs investigations, citizen grievances, public complaints, and administrative reviews initiated within MATCOM. All Professional

Standards personnel, Internal Affairs (IA) investigators, command staff, and licensed security personnel must adhere strictly to these standards.

2.0 AUTHORITY & REFERENCES

This directive is promulgated pursuant to state statutory mandates, administrative regulations, and organizational governance standards:

- **Maryland Police Accountability Act of 2022 (Md. Code Ann., Public Safety § 3-101 et seq.):** Oversight principles, mandatory administrative investigation procedures, and complaint disposition standards.
- **COMAR Title 12, Subtitle 10, Chapters 01 & 02:** Maryland State Police Licensing Division Regulations for Licensed Security Guard Agencies and Duty to Report Misconduct.
- **Maryland Business Regulation Article, Title 12, Subtitle 1:** Licensing requirements and agency standards for private security providers.
- **Maryland Constitution, Declaration of Rights, Article 24:** Constitutional due process guarantees for complainants and accused personnel.
- **Maryland Criminal Law Code Ann. § 9-302 & § 9-303:** Intimidation of Witnesses, Coercion, and Retaliation Prohibitions.
- **Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. § 4-101 et seq.:** Public disclosure and confidentiality rules for administrative investigation records.

3.0 DEFINITIONS

3.1 Agency-Initiated Investigation: An administrative investigation continued or converted under MATCOM's sole authority when public safety, policy integrity, or legal mandates require resolution despite a complainant's withdrawal request.

3.2 Coercion / Intimidation: Any direct or indirect act, threat, harassment, financial inducement, or pressure exerted upon a complainant to force, induce, or influence them into withdrawing a complaint.

3.3 Discretionary Dismissal: The administrative closure of a minor, non-criminal, non-force grievance following a verified voluntary withdrawal request where no systemic policy violation or public harm exists.

3.4 Withdrawal Request: A formal, written declaration submitted by a complainant requesting that MATCOM cease administrative proceedings regarding a previously filed complaint.

4.0 POLICY

4.1 Policy Statement: MATCOM recognizes the right of a complainant to submit a request to withdraw a formal complaint. However, a complaint filed against a licensed security guard or agency employee is a matter of public accountability and internal administrative discipline, not merely a private dispute between two individuals. MATCOM maintains an absolute duty to uphold public trust, enforce professional security standards, and protect the community from security officer misconduct.

4.2 Duty to Continue Investigation: MATCOM shall not automatically terminate an administrative investigation simply because a complainant requests withdrawal. MATCOM shall independently review every withdrawal request and shall continue investigating serious allegations—including use of force, firearms discharges, civil rights violations, criminal conduct, or recurring misconduct—regardless of the complainant's wishes.

4.3 Zero Tolerance for Retaliation or Pressure: MATCOM maintains zero tolerance for any attempt by security personnel, supervisors, or third parties to contact, pressure, bribe, or intimidate a complainant into withdrawing a complaint. Any such action constitutes severe misconduct resulting in immediate termination and referral for criminal prosecution under Md. Crim. Law § 9-302.

5.0 PROCEDURES

5.1 Processing Written Requests for Complaint Withdrawal

When a complainant contacts MATCOM requesting to withdraw or dismiss a pending complaint, the following mandatory steps shall be executed:

- 1. Mandatory Withdrawal Form (Form SOP-PUB-32-A):** The complainant must complete and execute MATCOM Form SOP-PUB-32-A (Complaint Withdrawal Request Form), specifying the exact reasons for the withdrawal request.
- 2. Verification of Identity:** The IA investigator must verify the complainant's identity (via government-issued photo ID or digital 2-step authentication) to prevent fraudulent withdrawals by unauthorized third parties.

3. **Mandatory Voluntariness Interview:** The lead investigator or IA Supervisor shall conduct a recorded audio/video interview (in person or via secure teleconference) with the complainant to confirm that the withdrawal is entirely voluntary.

5.2 Anti-Coercion & Retaliation Screening

During the voluntariness interview, the IA investigator shall explicitly inquire into and document responses regarding potential coercion:

Mandatory Voluntariness Inquiry Questions:

1. "Has any employee of MATCOM, or anyone acting on their behalf, contacted you regarding this complaint?"
2. "Have you been offered money, gifts, employment benefits, or any financial settlement to withdraw this complaint?"
3. "Has anyone threatened, intimidated, or made you feel unsafe if you continued with this complaint?"
4. "Are you withdrawing this complaint of your own free will without any pressure or external influence?"

5.3 Evaluation Criteria: Discretionary Dismissal vs. Mandatory Continued Investigation

Upon completion of the voluntariness screening, the IA Commander and Legal Counsel shall evaluate the complaint against MATCOM's continuation thresholds:

Category	Allegation Threshold	Action & Disposition Standard
Discretionary Dismissal Permitted	• Minor customer service disputes (e.g., tone of voice, minor uniform non-compliance). • Factual misunderstanding resolved through mutual explanation. • Absence of force, injury, criminal act, or policy breach. • Complainant confirms full voluntary satisfaction.	Approved Withdrawal: Case closed as "Closed-Withdrawn by Complainant." Notice sent to CEO and subject officer.
Mandatory Continued Investigation Required	• Allegations involving Use of Force or Excessive Force. • Unlawful Brandishing or Discharge of Firearm / Less-Lethal Weapons. • Allegations of Criminal Acts (Assault, Theft, Extortion, Trespass). • Civil Rights Violations,	Withdrawal Denied: Converted immediately to "MATCOM Agency-Initiated Administrative Investigation." Investigation proceeds to full formal adjudication.

Category	Allegation Threshold	Action & Disposition Standard
	Discrimination, or Unlawful Detention. • Subject officer has prior sustained disciplinary history. • Evidence of Coercion, Intimidation, or Unlawful Settlement. • Independent evidence (Body-Worn Camera, CCTV) supports the allegation.	

5.4 Transition to Agency-Initiated Administrative Investigation

When a withdrawal request is denied under Section 5.3:

1. **Re-Classification:** The case title is formally re-designated in the Internal Affairs tracking system as: "MATCOM IA Agency-Initiated Investigation Case # [YYYY-IA-XXXX]".
2. **Notification to Complainant:** The complainant is sent written notice explaining that while their personal participation is no longer required, MATCOM has an administrative obligation under state regulatory standards to complete the investigation.
3. **Evidence Preservation:** Independent evidence—including Body-Worn Camera (BWC) footage, station dispatch audio, CAD logs, electronic access control records, and third-party CCTV—shall be secured and evaluated independently of complainant testimony.

5.5 Case Disposition & Licensing Authority Reporting

Upon completion of an Agency-Initiated Investigation, the case shall be adjudicated under standard findings:

- **Sustained:** Misconduct proven by a preponderance of the evidence; disciplinary action imposed up to termination and license revocation notice to the Maryland State Police Licensing Division.
- **Not Sustained:** Insufficient evidence to prove or disprove the allegation.
- **Exonerated:** The incident occurred, but the officer's actions were lawful, proper, and within policy.
- **Unfounded:** The allegation was demonstrably false or factually impossible.

6.0 RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Retains sole authority to review and approve IA Commander recommendations for case closures involving executive officers or critical use-of-force incidents.

6.2 Internal Affairs Commander: Oversees all withdrawal screening interviews, determines whether a complaint meets mandatory continuation criteria, and re-classifies cases as Agency-Initiated.

6.3 Lead IA Investigator: Conducts voluntariness interviews, completes Form SOP-PUB-32-A, investigates potential officer coercion, and gathers independent corroborating evidence.

6.4 Security Personnel & Supervisors: Strictly prohibited from discussing complaints with complainants or soliciting withdrawals. Must immediately report any withdrawal request communicated directly to field personnel.

7.0 COMPLIANCE & ENFORCEMENT

7.1 Mandatory Disciplinary Action: Any security officer, supervisor, or employee found to have solicited, requested, incentivized, coerced, or intimidated a complainant to withdraw a complaint shall face immediate suspension, administrative charge for Gross Misconduct, summary termination, and referral to the Maryland State Police Licensing Division for permanent guard card revocation.

7.2 Supervisory Oversight: Internal Affairs shall conduct semi-annual audits of all closed withdrawal cases to verify compliance with screening protocols.

8.0 RECORDS & DOCUMENTATION

All withdrawal forms (SOP-PUB-32-A), recorded voluntariness interviews, IA decision memos, BWC footage, and Agency-Initiated case files shall be permanently archived in the secure Professional Standards database and retained for a minimum of **seven (7) years** pursuant to COMAR 12.10.01 and Maryland record retention standards.

9.0 EFFECTIVE DATE & REVIEW

This Standard Operating Procedure takes effect on **August 13, 2026**, superseding all prior agency memos or unwritten policies regarding complaint withdrawals. This policy shall be reviewed annually on or before **August 13, 2027**.

OFFICIAL EXECUTIVE APPROVAL & ADOPTION

Brian C. Askeew, Ph.D.

DR. BRIAN C. ASKEW
CHIEF EXECUTIVE OFFICER & APPROVING AUTHORITY
MATCOM OFFICE OF PUBLIC SAFETY LLC

Daune Simpkins

DAUNE SIMPKINS
DEPUTY DIRECTOR, GOVERNMENTAL AFFAIRS
MATCOM OFFICE OF PUBLIC SAFETY LLC
DATE: AUGUST 13, 2026 | LICENSE: 24PLU-SGPD4620



MATCOM OFFICE OF PUBLIC SAFETY LLC

LICENSED MARYLAND SECURITY GUARD AGENCY — LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Direct: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — OFFICIAL ADMINISTRATIVE DIRECTIVE

Policy Number:	SOP-PUB-33	Effective Date:	August 13, 2026
Title:	External Agency Referral & Jurisdictional Complaints	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Office of Governmental Affairs	Classification:	Public
Supersedes:	None (Initial Issue)	Distribution:	All Divisions & Public Web Portal

SOP-PUB-33 — EXTERNAL AGENCY REFERRAL & JURISDICTIONAL COMPLAINTS

INTER-AGENCY ROUTING, JURISDICTIONAL BOUNDARY PROTOCOLS & PUBLIC TRANSPARENCY

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) defines mandatory administrative protocols for Matcom Office of Public Safety LLC ("MATCOM") when receiving, processing, and transferring complaints, grievances, or reports of misconduct that fall outside MATCOM's direct administrative or operational jurisdiction, or that involve external municipal police departments, county sheriff offices, state law enforcement, third-party security companies, public agencies, client organizations, contractors, prosecutors, or judicial entities.

1.2 Scope: This procedure applies to all administrative complaints, incident reports, citizen grievances, and legal inquiries received by MATCOM. It binds all Professional

Standards personnel, Governmental Affairs liaison officers, dispatchers, and intake staff across MATCOM's operational footprint in Maryland.

2.0 AUTHORITY & REFERENCES

This directive operates under Maryland statutory provisions and regulatory agency mandates governing private security licensing and inter-agency cooperation:

- **Maryland Business Regulation Article, Title 12, Subtitle 1:** Scope of Authority and Regulatory Boundaries for Licensed Security Guard Agencies.
- **COMAR Title 12, Subtitle 10, Chapters 01 & 02:** Licensing Division Standards and Mandatory Misconduct Reporting to the Maryland State Police.
- **Maryland Police Accountability Act of 2022 (Md. Code Ann., Public Safety § 3-101 et seq.):** Coordination with County Police Accountability Boards (PAB) and Administrative Charging Committees (ACC).
- **Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. § 4-351:** Inter-agency transfer of public safety and investigatory records.
- **COMAR Title 12, Subtitle 12:** Maryland Police Training and Standards Commission (MPCTC) Administrative Rules.

3.0 DEFINITIONS

3.1 External Jurisdiction: The lawful authority vested in a separate public law enforcement agency, regulatory body, client property owner, or external corporate entity outside MATCOM's corporate governance.

3.2 Inter-Agency Referral: The formal administrative transfer of a complaint, case file, evidence package, or citizen grievance from MATCOM to an external agency of proper jurisdiction.

3.3 Non-Jurisdictional Complaint: Any complaint filed with MATCOM that alleges misconduct or requests action regarding individuals, officers, employees, or entities not employed, contracted, or licensed under MATCOM's agency license (# 24PLU-SGPD4620).

3.4 Licensing Authority: The Maryland State Police (MSP) Licensing Division, responsible for state oversight and guard card issuance under COMAR 12.10.01.

4.0 POLICY

4.1 Policy Statement: MATCOM is committed to absolute transparency, inter-agency cooperation, and ensuring that no public complaint falls into an administrative vacuum. MATCOM shall promptly evaluate every incoming complaint to determine proper jurisdiction. When a complaint involves an external agency, municipal police department, third-party security company, or client entity, MATCOM shall formally transfer the complaint to the appropriate authority within strict timeframes while providing written confirmation and guidance to the complainant.

4.2 Duty to Assist Citizens: MATCOM personnel shall never dismiss a citizen complaint with a simple refusal or verbal rejection. Staff must provide constructive assistance by facilitating the referral, identifying the correct agency contact details, and documenting the transfer in MATCOM's master inter-agency referral log.

5.0 PROCEDURES

5.1 Initial Jurisdictional Assessment & Categorization

Upon receipt of any complaint or grievance, the Professional Standards intake officer shall conduct an immediate jurisdictional determination within **twenty-four (24) hours**:

- Personnel Verification:** Check subject name, badge number, and deployment location against MATCOM's master roster and scheduling database.
- Entity Classification:** Categorize the subject entity as (a) MATCOM Employee/Guard, (b) Sworn Police Officer/Sheriff, (c) External Private Security Agency, (d) Client / Property Management Personnel, or (e) Third-Party Government Contractor.

5.2 Referral Protocols by External Target Agency

Once non-jurisdiction is established, the Office of Governmental Affairs shall route the case file according to the following mandatory target matrix:

Target Entity Category	Primary Destination Agency	Referral Method & Timeframe
Sworn Local Police / Sheriff (e.g., Baltimore County PD, Baltimore City PD)	Internal Affairs Division of target Law Enforcement Agency & Local Police Accountability Board (PAB).	Encrypted Electronic Transfer & Direct IA Call within 24 Hours (Immediate if active crime).
State Police / Special Police (e.g., MSP, MD	Maryland State Police Internal Affairs / MSP Licensing Division.	Secure Portal / Formal Written Memorandum within 48 Hours .

Target Entity Category	Primary Destination Agency	Referral Method & Timeframe
Transportation Authority)		
External Private Security Guard Agency	Maryland State Police Licensing Division & Executive Management of Target Security Company.	Certified Mail & Encrypted Email to MSP Licensing within 2 Business Days .
Client Property Management / Landlord	Client Designated Corporate Safety / Property Operations Manager.	Written Notice & Transmittal Summary within 3 Business Days .
State's Attorney / Prosecutor	Local State's Attorney's Office (Special Investigations / Integrity Unit).	Hand-Delivered / Secure Legal Transmittal within 24 Hours .

5.3 Referrals to Regulatory Bodies & Police Accountability Boards

In compliance with the Maryland Police Accountability Act of 2022 and COMAR 12.10.01:

- **Police Accountability Board (PAB) Coordination:** If a complaint alleges misconduct involving sworn police officers acting in conjunction with MATCOM special operations, a copy of the referral package shall be transmitted to the local County Police Accountability Board within **3 business days**.
- **MSP Licensing Division Reporting:** Complaints alleging unlicensed security guard activity, handgun permit violations, or gross statutory violations by third-party guard companies shall be reported directly to the MSP Licensing Division.

5.4 Concurrent Jurisdiction & Joint Operational Complaints

Where an incident involves both MATCOM security guards and external personnel (e.g., joint response with local police or client staff):

Dual-Track Investigation Protocol:

1. MATCOM shall retain administrative jurisdiction over MATCOM employees and conduct an internal review under SOP-PUB-35.
2. MATCOM shall formally coordinate with the external agency's Internal Affairs unit.
3. MATCOM shall share video evidence, CAD logs, and officer statements in accordance with MPIA § 4-351 while preserving statutory due process rights.

5.5 Mandatory Citizen Notification & Guidance

Within **five (5) business days** of completing an external referral, the Office of Governmental Affairs shall issue a formal written Notice of Inter-Agency Referral to the complainant containing:

1. Formal confirmation that MATCOM has reviewed the complaint and determined jurisdictional responsibility lies with an external entity.
2. Exact name, address, telephone number, email, and web portal link of the destination agency's Internal Affairs or oversight division.
3. MATCOM's internal Tracking Reference Number (e.g., REF-2026-EXT-XXXX) and the external agency's receipt/case number (if available).
4. Information regarding public records rights under the Maryland Public Information Act (MPIA).

6.0 RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Authorizes formal inter-agency Memoranda of Understanding (MOUs) and signs high-level referral transmittals to State's Attorneys and state oversight boards.

6.2 Director of Governmental Affairs: Serves as primary agency liaison to external police departments, MSP Licensing Division, and municipal bodies; oversees all outgoing referral transmittals.

6.3 Professional Standards / IA Commander: Conducts initial jurisdictional reviews, segregates dual-agency evidence, and ensures compliance with 24-hour criminal referral deadlines.

7.0 COMPLIANCE & ENFORCEMENT

Failure by MATCOM personnel to properly process, log, or refer an external complaint within mandated timeframes constitutes an administrative dereliction of duty. Supervisors failing to forward non-jurisdictional complaints to Governmental Affairs within 24 hours shall face administrative reprimand.

8.0 RECORDS & DOCUMENTATION

The Office of Governmental Affairs shall maintain an immutable Master Inter-Agency Referral Register recording every external transfer. All referral transmittal letters,

agency receipt confirmations, certified mail receipts, and citizen notices shall be retained for **seven (7) years** under COMAR 12.10.01 archive standards.

9.0 EFFECTIVE DATE & REVIEW

This Standard Operating Procedure takes effect on **August 13, 2026**, and shall undergo annual administrative review on or before **August 13, 2027**.

OFFICIAL EXECUTIVE APPROVAL & ADOPTION

Brian C. Askeew, Ph.D.

DR. BRIAN C. ASKEW

CHIEF EXECUTIVE OFFICER & APPROVING AUTHORITY
MATCOM OFFICE OF PUBLIC SAFETY LLC

Daune Simpkins

DAUNE SIMPKINS

DEPUTY DIRECTOR, GOVERNMENTAL AFFAIRS
MATCOM OFFICE OF PUBLIC SAFETY LLC
DATE: AUGUST 13, 2026 | LICENSE: 24PLU-SGPD4620



MATCOM OFFICE OF PUBLIC SAFETY LLC

LICENSED MARYLAND SECURITY GUARD AGENCY — LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Direct: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — OFFICIAL ADMINISTRATIVE DIRECTIVE

Policy Number:	SOP-PUB-34	Effective Date:	August 13, 2026
Title:	Conflict of Interest & Independent Review	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Legal / Command Staff	Classification:	Public
Supersedes:	None (Initial Issue)	Distribution:	All Divisions & Public Web Portal

SOP-PUB-34 — CONFLICT OF INTEREST & INDEPENDENT REVIEW

ETHICAL DISQUALIFICATION STANDARDS, EXECUTIVE RECUSAL & EXTERNAL REVIEW PROTOCOLS

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) mandates strict ethical guidelines, conflict disqualification rules, and independent external review mechanisms for Matcom Office of Public Safety LLC ("MATCOM"). It guarantees that every internal affairs investigation, citizen complaint, or administrative disciplinary action is conducted with absolute impartiality, free from actual, potential, or perceived bias, self-interest, executive command pressure, or personal conflict.

1.2 Scope: This procedure governs all administrative investigations involving executive leadership (Chief Executive Officer, Chiefs, Division Directors), Professional Standards / Internal Affairs (IA) personnel, lead investigators, and any complaint where a command-line or personal conflict exists.

2.0 AUTHORITY & REFERENCES

This directive is issued in compliance with Maryland statutory ethics rules, constitutional due process requirements, and licensing standards:

- **Maryland Public Ethics Law, Md. Code Ann., General Provisions Title 5:** Statutory standards governing conflict of interest, self-dealing, and administrative impartiality.
- **Maryland Police Accountability Act of 2022 (Md. Code Ann., Public Safety § 3-101 et seq.):** Principles of independent administrative oversight and charging committee integrity.
- **COMAR Title 12, Subtitle 10, Chapters 01 & 02:** Licensing Division Integrity Rules for Private Security Guard Agencies.
- **Maryland Constitution, Declaration of Rights, Article 24:** Fundamental due process rights requiring a neutral, detached administrative tribunal.
- **Maryland Whistleblower Protection Act, Md. Code Ann., State Pers. & Pens. § 5-301 et seq.:** Protections for employees reporting executive or administrative wrongdoing.

3.0 Definitions

3.1 Conflict of Interest: Any personal, financial, familial, romantic, supervisory, or professional relationship that impairs, or reasonably appears to impair, an investigator's, supervisor's, or executive's ability to render an impartial administrative judgment.

3.2 Independent Special Investigator: An external, un-conflicted third-party professional—such as a retired judge, licensed private investigator, or special legal counsel—retained by MATCOM to conduct an administrative investigation free from agency influence.

3.3 Recusal Wall: Administrative and technical barriers established within MATCOM's case management infrastructure to completely isolate a conflicted officer or executive from accessing, viewing, or discussing a specific investigation.

3.4 Command-Line Conflict: A scenario where an accused employee is in the direct chain of command of the investigating officer or where the investigator reports directly to the subject of the investigation.

4.0 POLICY

4.1 Policy Statement: MATCOM enforces a strict, uncompromising prohibition against conflict of interest in all internal investigations and disciplinary reviews. No employee,

supervisor, investigator, or executive officer shall investigate, adjudicate, review, or attempt to influence any case in which they have a personal, financial, supervisory, or institutional conflict.

4.2 Mandatory Recusal & Independent Referral: Whenever a conflict of interest is identified—or when a complaint directly names executive leadership or Internal Affairs personnel—the conflicted individual must immediately recuse themselves, and the matter shall be referred forthwith to an Independent Special Investigator or external review body.

5.0 PROCEDURES

5.1 Conflict Identification & Mandatory Disclosure

Prior to initiating any administrative investigation, every assigned IA investigator and reviewing supervisor must complete MATCOM Form SOP-PUB-34-A (Conflict Disclosures Certification). Mandatory disqualifying conflicts include:

Conflict Category	Specific Disqualifying Criteria	Mandatory Administrative Action
Familial & Household	Spouse, domestic partner, child, parent, sibling, relative, or co-habitant of accused or complainant.	Immediate Mandatory Recusal & Reassignment.
Romantic / Personal	Current or past dating, intimate, or close personal friendship with involved parties.	Immediate Mandatory Recusal & Reassignment.
Financial & Business	Joint business ventures, private loans, employment outside MATCOM, or financial interest in outcome.	Immediate Mandatory Recusal & Reassignment.
Command & Supervisory	Direct line-of-command supervisor, direct subordinate, or annual evaluation author of subject officer.	Reassignment to Alternate Division or External Review.
Party / Witness Status	Investigator was a witness, participant, or decision-maker in the underlying incident.	Immediate Mandatory Recusal as Investigator.
Executive Level	Complaint names CEO, Division Director, IA Commander, or Executive Staff member.	Automatic Referral to Independent Special Investigator.

5.2 Recusal Protocols & Information Barriers ("Recusal Wall")

Upon formal recusal or identification of a conflict:

1. **System Lockout:** IT Division shall immediately adjust access permissions in the Internal Affairs database, placing the file in a restricted vault inaccessible to the recused individual.
2. **Prohibition of Discussion:** Recused personnel are strictly prohibited from discussing the investigation, requesting updates, or reviewing drafts with the assigned investigator.
3. **Documented Wall Certificate:** An official Recusal Wall Notice shall be filed in the case record signed by the IT Director and Legal Counsel.

5.3 Special Protocols for Complaints Involving Executive Leadership (CEO & Command Staff)

When a complaint alleges misconduct against the Chief Executive Officer, Chief of Security, or IA Commander:

EXECUTIVE COMPLAINT INDEPENDENT PROTOCOL:

1. The Internal Affairs Division is automatically disqualified from handling the investigation.
2. Within **forty-eight (48) hours**, the complaint shall be transmitted directly to MATCOM's External Legal Counsel and Board of Managers.
3. Legal Counsel shall retain an qualified **Independent Special Investigator** within **five (5) business days**.

5.4 Qualification Standards for Independent Special Investigators

To ensure absolute independence, any external investigator retained under this policy must satisfy the following minimum criteria:

- Must be a licensed Maryland Private Investigator, retired judge, former federal special agent, or external legal counsel specializing in administrative oversight.
- Must have zero current or prior financial, employment, or personal ties to MATCOM, its officers, or the complainant.
- Must execute a sworn Affidavit of Independence prior to receiving case materials.

5.5 Independent Adjudication & Reporting Transmittal

The Independent Special Investigator shall possess full authority to sub-poena agency records, interview personnel under oath, examine BWC footage, and issue a binding Independent Investigative Report containing findings of fact and disciplinary recommendations.

The final report shall be submitted directly to External Legal Counsel and the Board of Managers, bypass internal executive command review, and be transmitted to the Maryland State Police Licensing Division if statutory licensing violations are sustained.

5.6 Whistleblower Protections & Anti-Retaliation

Any MATCOM employee who reports a conflict of interest, discloses executive misconduct, or cooperates with an Independent Special Investigator is fully protected under the Maryland Whistleblower Protection Act. Any retaliation or adverse employment action taken against a reporting employee shall result in immediate termination of the retaliating official.

6.0 RESPONSIBILITIES

6.1 Board of Managers & External Legal Counsel: Responsible for selecting and retaining Independent Special Investigators for CEO / Executive complaints and ensuring case isolation.

6.2 Chief Executive Officer (CEO): Mandatory self-recusal upon receipt of any complaint naming the CEO; prohibited from interfering with independent reviews.

6.3 Professional Standards / IA Commander: Enforces conflict screening for all staff investigators and logs recusal orders.

7.0 COMPLIANCE & ENFORCEMENT

Failure to declare a known conflict of interest, attempting to circumvent a Recusal Wall, or exerting improper influence over an investigation constitutes severe administrative misconduct punishable by immediate termination for cause and reporting to state licensing authorities.

8.0 RECORDS & DOCUMENTATION

All Conflict Certification Forms (Form SOP-PUB-34-A), Recusal Wall Notices, Independent Investigator contracts, and final external reports shall be retained in secure legal archives for a minimum of **seven (7) years** pursuant to COMAR 12.10.01 standards.

9.0 EFFECTIVE DATE & REVIEW

This Standard Operating Procedure takes effect on **August 13, 2026**, and shall undergo annual review on or before **August 13, 2027**.

OFFICIAL EXECUTIVE APPROVAL & ADOPTION

Brian C. Askeew, Ph.D.

DR. BRIAN C. ASKEW
CHIEF EXECUTIVE OFFICER & APPROVING AUTHORITY
MATCOM OFFICE OF PUBLIC SAFETY LLC

Daune Simpkins

DAUNE SIMPKINS
DEPUTY DIRECTOR, GOVERNMENTAL AFFAIRS
MATCOM OFFICE OF PUBLIC SAFETY LLC
DATE: AUGUST 13, 2026 | LICENSE: 24PLU-SGPD4620



MATCOM OFFICE OF PUBLIC SAFETY LLC

LICENSED MARYLAND SECURITY GUARD AGENCY — LICENSE # 24PLU-SGPD4620

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207 | 24/7 Dispatch: 1-855-715-9911
Direct: 701-809-9911 | Email: Oga@matcomops.org | Web: www.matcomops.org | NAICS: 561612

STANDARD OPERATING PROCEDURE — OFFICIAL ADMINISTRATIVE DIRECTIVE

Policy Number:	SOP-PUB-35	Effective Date:	August 13, 2026
Title:	Complaint Investigation Timelines & Delayed Cases	Revision Date:	August 13, 2026
Approving Authority:	Dr. Brian C. Askew, CEO	Review Date:	August 13, 2027
Responsible Division:	Professional Standards / Internal Affairs	Classification:	Public
Supersedes:	None (Initial Issue)	Distribution:	All Divisions & Public Web Portal

SOP-PUB-35 — COMPLAINT INVESTIGATION TIMELINES & DELAYED CASES

OPERATIONAL LIFECYCLE BENCHMARKS, FORMAL DELAY APPROVALS & COMPLAINANT NOTICE STANDARDS

1.0 PURPOSE & SCOPE

1.1 Purpose: This Standard Operating Procedure (SOP) establishes binding operational timeframes, target benchmarks, formal extension protocols, and mandatory citizen communication standards for all administrative complaints and internal investigations conducted by Matcom Office of Public Safety LLC ("MATCOM"). It eliminates administrative backlogs, guarantees due process for accused personnel, and ensures citizens are kept continuously informed when a case requires extended investigation.

1.2 Scope: Governs all complaint processing stages within MATCOM's Professional Standards / Internal Affairs (IA) Division, including intake, triage, investigation, command review, adjudication, and final disposition reporting.

2.0 AUTHORITY & REFERENCES

This directive is promulgated under state statutory mandates and administrative standards governing security guard agency operations:

- **Maryland Police Accountability Act of 2022 (Md. Code Ann., Public Safety § 3-101 et seq.):** Statutory timeframes and due process benchmarks for administrative investigations.
- **COMAR Title 12, Subtitle 10, Chapters 01 & 02:** Maryland State Police Licensing Division Regulations for Security Guard Agencies.
- **Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. § 4-203:** Response timeframes for public records and administrative case statuses.
- **Maryland Constitution, Declaration of Rights, Article 24:** Constitutional due process rights guaranteeing prompt resolution of administrative accusations.

3.0 DEFINITIONS

3.1 Lifecycle Timeframe: The total elapsed time from the initial receipt of a complaint by MATCOM to the transmission of the final written disposition letter to the complainant and subject officer.

3.2 Tolling Event: A legally recognized external circumstance—such as an active criminal prosecution or court stay—that temporarily pauses MATCOM's administrative investigation clock.

3.3 Extension Order: A formal written authorization issued by the CEO or IA Commander granting additional time beyond standard benchmarks to complete a complex investigation.

4.0 POLICY

4.1 Policy Statement: MATCOM is committed to prompt, rigorous, and transparent resolution of all public and internal complaints. Unreasonable administrative delay undermines public confidence, compromises evidence, and violates constitutional due process.

4.2 Standard Lifecycle Benchmark: Standard administrative investigations shall be completed and adjudicated within **sixty (60) calendar days** of initial receipt.

4.3 Mandatory Citizen Updates: If an investigation exceeds 30 calendar days due to complexity or tolling, MATCOM shall issue a mandatory written status update to the complainant every 30 days until final disposition.

5.0 PROCEDURES

5.1 Target Operational Benchmarks by Lifecycle Phase

Internal Affairs personnel shall adhere to the following mandatory phase timeframes:

Lifecycle Phase	Operational Activity	Mandatory Timeframe	Responsible Authority
Phase 1: Intake & Ack.	Issue formal written receipt & case tracking ID to complainant.	24-48 Hours (Max 2 Business Days)	IA Intake Clerk / Portal System
Phase 2: Triage & Assign	Conduct preliminary review, verify jurisdiction, assign Lead Investigator.	3 Business Days	IA Commander
Phase 3: Field Investigation	Interview witnesses, collect BWC/ CCTV evidence, interrogate subject, draft report.	30 Calendar Days	Lead IA Investigator
Phase 4: Adjudication Review	Command staff review of findings, legal concurrence, disciplinary decision.	15 Calendar Days	IA Commander / CEO / Legal
Phase 5: Final Disposition Notice	Issue formal written disposition notice to complainant, subject officer, and MSP Licensing.	5 Business Days post-review	Office of Governmental Affairs
MAXIMUM STANDARD LIFECYCLE (PHASES 1-5):		60 CALENDAR DAYS TOTAL	

5.2 Formal Extension Request & Tolling Protocols

When an investigation cannot be completed within the 30-day Phase 3 benchmark due to extraordinary circumstances, the Lead Investigator must submit Form SOP-PUB-35-A (Investigation Extension Request) prior to Day 25.

Permissible Grounds for Extension / Tolling:

- 1. Tolling for Concurrent Criminal Prosecution:** Pending criminal investigation or prosecution by local police/State's Attorney arising from the same incident.
- 2. Forensic Lab Analysis:** Delays in external laboratory testing (e.g., ballistics, toxicological, digital forensics).
- 3. Witness Unavailability:** Essential witness incapacitated, hospitalized, deployed, or

uncooperative.

4. **Complex / Multi-Subject Cases:** Cases involving multiple officers, complex financial audits, or extensive digital evidence.

Extensions may be granted in **30-day increments** up to a maximum total lifecycle of 180 calendar days, requiring express written approval from the CEO.

5.3 Complainant Status Update Notifications

For any case exceeding 30 calendar days:

1. **30-Day Progress Letter:** Issued on Day 30 informing the complainant that the investigation remains active under an authorized extension.
2. **Recurring Monthly Updates:** Issued every 30 calendar days thereafter until case closure.
3. **Content Standard:** Status updates shall provide meaningful progress information without disclosing confidential investigatory strategies or sensitive personal employee data exempt under MPIA § 4-351.

5.4 Supervisory Audits & Aging Case Management

The IA Commander shall enforce the following audit tracking controls:

- **21-Day Dashboard Alert:** Automated system warning generated on Day 21 for any uncompleted Phase 3 investigation.
- **Bi-Weekly IA Command Audit:** IA Commander shall conduct bi-weekly status reviews of all open cases exceeding 45 days.
- **Supervisory Reassignment:** If an investigator fails to demonstrate reasonable diligence, the IA Commander shall reassign the case and initiate an administrative inquiry into the investigator's performance.

5.5 Annual Metrics & Public Transparency Disclosures

Within forty-five (45) days of the end of each calendar year, MATCOM's Professional Standards Division shall publish an annual summary report detailing:

- Total administrative complaints received.
- Average completion lifecycle time (in calendar days).
- Percentage of cases closed within 60-day standard vs. extended cases.
- Summary breakdown of dispositions (Sustained, Unfounded, Exonerated, Not Sustained, Withdrawn).

6.0 RESPONSIBILITIES

6.1 Chief Executive Officer (CEO): Sole authority to approve extension requests beyond 60 calendar days and review annual performance metrics.

6.2 Internal Affairs Commander: Manages daily timeline compliance, reviews extension requests, conducts bi-weekly audits, and ensures status letters are issued.

6.3 Lead IA Investigator: Responsible for executing field investigations within 30 days, logging time entries, and submitting extension requests promptly.

7.0 COMPLIANCE & ENFORCEMENT

Unexcused neglect of case timelines or failure to issue required complainant status updates shall result in administrative discipline for the responsible investigator or supervisor under MATCOM performance standards.

8.0 RECORDS & DOCUMENTATION

All case timeline logs, extension requests (Form SOP-PUB-35-A), status update letters, and annual metric reports shall be archived in the Professional Standards database and retained for **seven (7) years** pursuant to COMAR 12.10.01 standards.

9.0 EFFECTIVE DATE & REVIEW

This Standard Operating Procedure takes effect on **August 13, 2026**, and shall undergo annual review on or before **August 13, 2027**.

OFFICIAL EXECUTIVE APPROVAL & ADOPTION

Brian C. Askeew, Ph.D.

DR. BRIAN C. ASKEW

CHIEF EXECUTIVE OFFICER & APPROVING AUTHORITY
MATCOM OFFICE OF PUBLIC SAFETY LLC

Daune Simpkins

DAUNE SIMPKINS

DEPUTY DIRECTOR, GOVERNMENTAL AFFAIRS
MATCOM OFFICE OF PUBLIC SAFETY LLC
DATE: AUGUST 13, 2026 | LICENSE: 24PLU-SGPD4620



MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT & COMMERCIAL SECURITY OPERATIONS

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD
21207 | 24/7 Dispatch: 1-855-715-9911

OFFICIAL STANDARD OPERATING PROCEDURE

MD License: 24PLU-SGPD4620
NAICS: 561612 | HQ:
701-809-9911

POLICY NUMBER	SOP-PUB-36		
TITLE	SOP-PUB-36 — Public Communication During Critical Incidents		
EFFECTIVE DATE	August 13, 2026	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	RESPONSIBLE DIVISION	Office of Governmental Affairs / Communications Division / Command Staff
CLASSIFICATION	Public	SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027	LEGAL BASIS	COMAR 12.10.01 / MD State Govt Art. § 4-101 et seq.

STANDARD OPERATING PROCEDURE: PUBLIC COMMUNICATION DURING CRITICAL INCIDENTS

Mandatory Protocols Governing Transparency Portal Emergency Alerts, Real-Time Public Messaging, Crisis Communications, and Incident Information Release

1.0 PURPOSE & SCOPE

1.1 Purpose

This Standard Operating Procedure (SOP) establishes strict operational protocols for public communication, real-time alerts, and Transparency Portal disclosures during critical incidents handled by or involving Matcom Office of Public Safety LLC (hereinafter "MATCOM"). The objective is to maintain public safety, prevent mass panic, ensure factual accuracy, preserve operational security, protect individual privacy rights, and uphold government-grade transparency standards in full alignment with Maryland state law.

1.2 Scope

This policy applies to all active critical incidents occurring at MATCOM-protected client properties, public safety contracts, or operational zones across the State of Maryland. It governs all communications issued by MATCOM personnel, including the Chief Executive Officer, Public Information Officers (PIO), Operations Commanders, Dispatch Supervisors, Field Supervisors, and IT System Administrators managing MATCOM's Public Transparency Portal.

MANDATORY OPERATING PRINCIPLE

During active critical incidents, MATCOM personnel must balance the public's immediate right to know with the paramount requirement to protect human life, preserve tactical security, prevent perpetrator escape, and protect the integrity of ongoing criminal investigations conducted by primary law enforcement agencies.

2.0 AUTHORITY & STATUTORY REFERENCES

This procedure is issued pursuant to the executive authority of the Chief Executive Officer and is governed by the statutory, administrative, and constitutional standards of the State of Maryland and federal operational guidelines:

- **Maryland Public Information Act (MPIA)**, Maryland Code, State Government Article § 4-101 et seq., governing public records disclosures, statutory exemptions, law enforcement record protections, and investigative file safeguards.

- **Code of Maryland Regulations (COMAR) Title 12, Subtitle 10** (COMAR 12.10.01 & 12.10.02), establishing licensing, operational control, and regulatory compliance standards for private security guard agencies under the Maryland State Police Licensing Division.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, regulating security guard agencies and guard operations within Maryland.
- **Maryland Police Accountability Act of 2022** (Chapter 59, Acts of 2021 / House Bill 670), setting public accountability, use-of-force transparency, and incident reporting expectations across public safety entities in Maryland.
- **Maryland Police and Correctional Training Commissions (MPCTC) Standards** (COMAR Title 12, Subtitle 12), providing benchmark guidelines for incident command, public notifications, and tactical communications.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Maryland Wiretap and Electronic Surveillance Act), establishing statutory restrictions regarding two-party consent for wire, oral, and electronic communications recording and publication.
- **Maryland Constitution**, Declaration of Rights, Articles 24 and 26, ensuring due process and protection against illegal searches and unauthorized disclosures.
- **Federal Emergency Management Agency (FEMA) Incident Command System (ICS) / National Incident Management System (NIMS)** standards for Public Information Systems (NIMS Component 3).

3.0 KEY DEFINITIONS

For the purposes of this SOP, the following definitions apply:

- **Critical Incident:** Any extraordinary operational event presenting an immediate threat to life, public safety, or major property, including but not limited to active shooter threats, weapon discharges, officer-involved shootings, mass-casualty incidents, hostage/barricade situations, major fires, hazardous material spills, severe civil disturbances, bomb threats, or sudden structural collapses.
- **Public Transparency Portal:** MATCOM's official, web-accessible public safety information portal hosted at www.matcomops.org/transparency, configured to publish verified incident advisories, real-time safety warnings, and public safety data.

- **Public Information Officer (PIO):** An authorized spokesperson designated by the CEO or Command Staff to formulate, verify, and disseminate official public communications.
- **Initial Incident Advisory:** A rapid, verified initial statement published to alert the public of an active critical threat, providing mandatory safety instructions and geographic avoidance perimeters.
- **Redacted Public Summary:** An official post-incident document cleared for public release following the removal of sensitive tactical details, personal identifying information (PII), juvenile records, and protected criminal investigative data.

4.0 GENERAL POLICY

It is the firm policy of MATCOM to maintain maximum achievable transparency regarding critical incidents while upholding strict operational integrity. Standardized protocols ensure that public communications released during high-stress critical incidents are verified, objective, timely, legal, and coordinated with primary emergency services.

No individual field officer, dispatch operator, or non-designated employee is authorized to issue public statements, post on social media, or communicate with news media personnel regarding a MATCOM critical incident without explicit clearance from the Chief Public Information Officer or the CEO.

5.0 PROCEDURES

5.1 Critical Incident Tier Classification

Upon notification of a critical incident, the On-Duty Incident Commander or Dispatch Supervisor shall immediately classify the event according to the MATCOM Incident Escalation Matrix:

Tier Level	Incident Category	Examples	Public Communication Action
Tier 1: High Operational Severity	Localized Incident / Contained Threat	Burglary in progress, localized medical emergency, contained physical dispute, property damage.	Standard incident logging; no public emergency alert required unless public movement is directly impacted.

Tier Level	Incident Category	Examples	Public Communication Action
Tier 2: Major Public Safety Event	Significant Ongoing Hazard	Active fire, structural damage, hazardous chemical release, localized perimeter closure, active perimeter search.	Issue Public Safety Advisory on Transparency Portal within 30 minutes; broadcast traffic/perimeter advisories.
Tier 3: Critical / Extreme Danger	Active Threat / Life Safety Emergency	Active shooter, weapon discharge, officer-involved shooting, hostage situation, mass-casualty event, bomb threat.	Immediate Crisis Alert broadcast within 15 minutes; activate Transparency Portal Emergency Banner; notify Lead LEO Agency.

5.2 Timeline for Public Disclosures During Critical Incidents

When a Tier 3 Critical Incident occurs, the following strict timeline shall govern public disclosures:

- 1. Initial Advisory (0 - 15 Minutes):** Focus exclusively on life safety. Publish an Emergency Safety Advisory via the Transparency Portal and official social channels stating:
 - Nature of hazard (e.g., "Active Security Operation / Avoid Area").
 - Exact geographic location / boundary perimeter to avoid.
 - Actionable public protection instructions (e.g., "Shelter in Place," "Evacuate Zone B").
 - Confirmation that primary emergency services (911 / Police / Fire) are on scene or responding.
- 2. Preliminary Verified Fact Sheet (1 Hours - 2 Hours):** Once the scene is stabilized or primary law enforcement establishes Incident Command, release a preliminary fact sheet detailing:
 - Confirmed non-sensitive operational facts.
 - Current operational status (e.g., "Scene Contained," "Suspect in Custody by Baltimore County Police").
 - Status of MATCOM personnel (e.g., "Officers securing outer perimeter").
 - Location of designated Media Staging Area and Family Reintegration Center.

3. **Comprehensive Post-Incident Debrief (24 Hours - 72 Hours):** Publish a comprehensive Redacted Public Summary on the Transparency Portal following executive legal review.

5.3 Transparency Portal Emergency Banner Management

The Transparency Portal features an automated Red/Gold Emergency Banner system. During a Tier 2 or Tier 3 event, the designated PIO or Systems Administrator shall trigger the Emergency Banner with a single-click authorization protocol. The banner shall display high-visibility alerts with direct emergency guidance and timestamped updates.

5.4 Mandatory Redactions and Information Withholdings

In accordance with the Maryland Public Information Act (MPIA § 4-311, § 4-351) and COMAR standards, the following information shall **NEVER** be released to the public or displayed on the Transparency Portal during or after a critical incident:

- Identities of deceased or critically injured victims prior to official Next-of-Kin (NOK) notification verified by the Medical Examiner or Lead Police Agency.
- Identities, photos, or personal details of involved juvenile victims, witnesses, or subjects.
- Tactical positions, sniper perimeters, SWAT entry routes, radio frequency bands, or specific surveillance camera blind spots.
- Proprietary client security plans, alarm codes, structural blueprints, or access control vulnerabilities.
- Unverified speculation, rumors, or unconfirmed casualty counts.
- Audio or video recordings prohibited from release under the Maryland Wiretap Act (MD CJ § 10-402) without prior statutory authorization or redaction.

5.5 Coordination with Primary Law Enforcement Agencies

Whenever a critical incident involves responding primary law enforcement agencies (e.g., Maryland State Police, Baltimore County Police Department, Baltimore City Police Department, MD Transportation Authority Police), MATCOM operates under the National Incident Management System (NIMS) Joint Information System (JIS) principles.

MATCOM PIOs shall immediately align all public messaging with the Lead Law Enforcement Agency's Public Information Officer. MATCOM shall not release details regarding criminal suspects, tactical actions, or criminal evidence without express prior clearance from the Lead Investigative Agency.

6.0 RESPONSIBILITIES & ADMINISTRATIVE CONTROL

Role / Title	Operational Responsibilities During Critical Incidents
Chief Executive Officer (Dr. Brian C. Askew)	Retains ultimate approval authority for all major crisis press statements, official agency stance, and major Transparency Portal releases during Tier 3 events.
Chief Public Information Officer (PIO)	Drafts, verifies, and disseminates initial alerts; interfaces directly with news media; coordinates Joint Information Center (JIC) operations with law enforcement.
Incident Commander / Field Supervisor	Provides accurate, verified ground-truth facts to the Communications Division; establishes physical media staging boundaries on scene.
24/7 Dispatch Operations (1-855-715-9911)	Maintains incident log timelines; routes urgent press inquiries directly to the PIO on-call; posts initial emergency alerts when authorized by Command.
IT / Portal Administrator	Ensures Transparency Portal uptime, activates crisis banner systems, and enforces data encryption and portal security during high-traffic events.

7.0 COMPLIANCE, ENFORCEMENT & PENALTIES

Strict compliance with this SOP is a mandatory condition of employment and operational licensing. Unauthorized release of confidential incident information, unauthorized social media postings, leaking of body-worn camera footage, or making false public statements during a critical incident constitutes a severe disciplinary violation.

Violations will result in immediate suspension pending an Internal Affairs investigation, potential termination for cause, civil liability under client non-disclosure agreements, and immediate referral to the Maryland State Police Licensing Division for security license suspension or revocation under COMAR 12.10.01.

8.0 RECORDS & RETENTION REQUIREMENTS

All critical incident communications, including press release drafts, Transparency Portal update logs, social media postings, media inquiry logs, and broadcast audio clips, shall be permanently archived in MATCOM's Secure Document Repository pursuant to Maryland records retention guidelines (State Government Article § 10-608 et seq.) and MATCOM SOP-PUB-39.

9.0 EFFECTIVE DATE, ANNUAL REVIEW & EXECUTIVE AUTHORIZATION

This Standard Operating Procedure takes effect on **August 13, 2026**, superseding all prior informal directives. It shall undergo formal review annually on or before **August 13, 2027**, by the Office of Governmental Affairs and Internal Audit.

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental
Affairs

Matcom Office of Public Safety
LLC

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Date: August 13, 2026

MD License: 24PLU-SGPD4620

Status: Active & Binding



MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT & COMMERCIAL SECURITY OPERATIONS

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD
21207 | 24/7 Dispatch: 1-855-715-9911

OFFICIAL STANDARD OPERATING PROCEDURE

MD License: 24PLU-SGPD4620
NAICS: 561612 | HQ:
701-809-9911

POLICY NUMBER	SOP-PUB-37		
TITLE	SOP-PUB-37 — Media & Public Information Release		
EFFECTIVE DATE	August 13, 2026	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	RESPONSIBLE DIVISION	Office of Governmental Affairs / Public Information Officer
CLASSIFICATION	Public	SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027	LEGAL BASIS	MD State Govt Art. § 4-101 / COMAR 12.10.01

STANDARD OPERATING PROCEDURE: MEDIA & PUBLIC INFORMATION RELEASE

Comprehensive Directives Governing Press Inquiries, Spokesperson Authorization, Misinformation Management, Inter-Agency Coordination, and Official Public Statements

1.0 PURPOSE & SCOPE

1.1 Purpose

This Standard Operating Procedure establishes definitive regulations for preparing, approving, issuing, and archiving public statements, press releases, media briefings, and official website updates generated by Matcom Office of Public Safety LLC (MATCOM). It defines spokesperson designations, rapid misinformation correction protocols, and inter-agency media coordination procedures to ensure institutional transparency, accuracy, professional integrity, and full compliance with Maryland law.

1.2 Scope

This SOP applies to all media interactions, official press statements, digital broadcasts, and public disclosures conducted by MATCOM employees, sub-contractors, executive officers, and appointed representatives. It governs routine agency news as well as emergency press releases, routine incident inquiries, and partner-agency joint communications across Maryland.

2.0 AUTHORITY & STATUTORY REFERENCES

This policy is promulgated under the executive authority of the Chief Executive Officer in compliance with statutory provisions governing security guard companies and public record release in Maryland:

- **Maryland Public Information Act (MPIA)**, Maryland Code, State Government Article § 4-101 et seq., establishing public records disclosure requirements and statutory exemptions for investigative, personnel, and security records.
- **COMAR 12.10.01 & 12.10.02** (Maryland State Police Licensing Division Regulations for Security Guard Agencies), establishing operational standards, supervisory duties, and official recordkeeping.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, providing the statutory framework for licensed security guard entities in Maryland.
- **Maryland Police Accountability Act of 2022** (Chapter 59, Acts of 2021), promoting standardized public reporting and transparency.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Maryland Wiretap Act), governing the dissemination of recorded audio and video materials.

- **State Government Article § 10-608 et seq.**, governing the preservation and retention of official agency communications and public press releases.

3.0 KEY DEFINITIONS

- **Public Information Officer (PIO):** The designated MATCOM officer authorized to manage media inquiries, draft press releases, conduct press briefings, and interface with news organizations.
- **Official Media Statement:** Any written, audio, or video communication issued on MATCOM letterhead or via official MATCOM broadcast channels intended for public distribution.
- **On the Record:** Information provided to journalists that may be explicitly quoted and attributed to MATCOM or the named spokesperson.
- **On Background / Off the Record:** Non-attributable information provided solely to clarify complex operational context. Note: MATCOM personnel are strictly prohibited from providing off-the-record statements regarding active criminal investigations or use-of-force events.
- **Misinformation Rapid Response Protocol:** The structured operational procedure executed to correct false, misleading, or unverified public reports affecting public safety or agency operations.
- **Joint Information Center (JIC):** A physical or virtual command post established jointly with municipal, county, state, or federal law enforcement agencies during multi-agency operations.

4.0 GENERAL POLICY

MATCOM is dedicated to open, accurate, and prompt communication with news media outlets and the general public. However, to guarantee accuracy, protect active investigations, and respect individual privacy rights, all public statements must flow through designated, authorized channels.

EXCLUSIVE SPOKESPERSON REQUIREMENT

Only the Chief Executive Officer, designated Public Information Officers, or individuals specifically authorized in writing by the CEO may speak on behalf of MATCOM. Field security guards, supervisors, dispatchers, and administrative staff are strictly forbidden from issuing comments, answering press questions, or making social media posts regarding MATCOM operational affairs.

5.0 PROCEDURES

5.1 Designation & Authority of Public Information Officers

The Office of Governmental Affairs maintains a primary PIO and secondary (on-call) PIOs. The Chief Public Information Officer reports directly to the CEO. PIO responsibilities include:

- Serving as the single point of contact for all media outlets (broadcast, print, digital).
- Drafting press releases and organizing news conferences.
- Monitoring news broadcasts and digital platforms for agency-related reports.
- Maintaining press credentialing registers and media contacts.

5.2 Review & Approval Workflow for Press Releases

Prior to public issuance, every official statement or press release must complete the mandatory three-stage verification process:

Stage	Action Item	Responsible Authority	Required Standard
Stage 1: Fact Verification	Gather operational data from Field Incident Report and CAD dispatch logs.	Lead Operations Commander / PIO	100% factual accuracy; verified timestamps; cleared scene details.
Stage 2: Legal & MPIA Compliance	Review statement for statutory exemptions (MPIA § 4-351), PII redactions, and liability risks.	Office of Governmental Affairs / Legal Counsel	Compliance with MD Wiretap Act, privacy statutes, and client non-disclosure contracts.
Stage 3: Executive Approval	Final review and authorization signature for public release.	Dr. Brian C. Askew, CEO (or Executive Director)	Written sign-off recorded in PIO release log.

5.3 On-Scene Media Relations & Staging Protocol

When media representatives arrive at the scene of an active MATCOM security operation or critical incident, field personnel shall adhere to the following steps:

1. Immediately notify Dispatch (1-855-715-9911) and request contact with the On-Call PIO.
2. Establish a clear, safe **Media Staging Area (MSA)** outside the active operational perimeter and hot zone.
3. Direct media personnel to the designated MSA in a courteous and professional manner.
4. Do not block cameras or attempt to confiscate media equipment on public property. Respect First Amendment rights of media representatives.
5. Provide media personnel with the official PIO contact card (Email: Oga@matcomops.org | Phone: 701-809-9911).

5.4 Misinformation Correction Protocol

In the event that inaccurate, false, or viral misinformation is broadcast by media outlets or circulated on digital platforms regarding MATCOM operations or involved officers:

- The PIO shall immediately compile verified facts and prepare an official **Correction Advisory**.
- The PIO shall contact the news director, editor, or authoring journalist in writing, requesting an immediate formal correction or update.
- If viral social media misinformation threatens public safety or officer security, MATCOM shall issue a public fact-check statement on its official Transparency Portal within two (2) hours.

5.5 Inter-Agency Coordination (Joint Information System)

In situations involving partner public safety agencies (e.g., Maryland State Police, County Police, Local Fire Departments), MATCOM PIOs shall strictly coordinate press release contents with the Lead Agency PIO. MATCOM will not release details regarding criminal suspects, police tactical entries, or official medical examiner findings without express prior clearance from the primary agency.

5.6 Publishing to the Public Transparency Portal

All approved media releases, formal statements, and advisories shall simultaneously be uploaded to the official MATCOM Transparency Portal (www.matcomops.org/transparency). Uploaded documents shall be timestamped, assigned a unique press release tracking ID, and permanently stored for public audit.

6.0 RESPONSIBILITIES & ROLES

- **Chief Executive Officer:** Retains final authority over all strategic communications, crisis press conferences, and policy statements.
- **Public Information Officer:** Manages daily media inquiries, prepares initial press drafts, conducts press briefings, and monitors media accuracy.
- **Field Supervisors:** Enforce media staging perimeters on scene, courteously direct journalists, and report media presence to Dispatch.
- **Security Officers:** Maintain perimeter security, refrain from answering media questions, and immediately report media inquiries to supervisors.

7.0 COMPLIANCE & ENFORCEMENT

Strict compliance with this policy is mandatory. Employees who give unauthorized interviews, leak internal operational documents, post unauthorized videos or comments on social media, or misrepresent MATCOM during media inquiries face severe disciplinary action up to and including immediate termination of employment, civil litigation for breach of fiduciary duty, and formal report to the Maryland State Police Licensing Division.

8.0 RECORDS MANAGEMENT & ARCHIVAL

In compliance with Maryland State Government Article § 10-608 et seq., all press statements, media logs, broadcast recordings, correction letters, and PIO approval records shall be retained in the permanent agency archive for a minimum of seven (7) years in accessible digital format.

9.0 EFFECTIVE DATE, ANNUAL REVIEW & AUTHORIZATION

This policy takes effect on **August 13, 2026**. It shall be formally reviewed annually on or before **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental
Affairs
Matcom Office of Public Safety
LLC

Date: August 13, 2026

MD License: 24PLU-SGPD4620

Status: Active & Binding



MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT & COMMERCIAL SECURITY OPERATIONS

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD
21207 | 24/7 Dispatch: 1-855-715-9911

OFFICIAL STANDARD OPERATING PROCEDURE

MD License: 24PLU-SGPD4620
NAICS: 561612 | HQ:
701-809-9911

POLICY NUMBER	SOP-PUB-38		
TITLE	SOP-PUB-38 — Transparency Portal Audit & Accountability		
EFFECTIVE DATE	August 13, 2026	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	RESPONSIBLE DIVISION	Office of Governmental Affairs / Internal Audit
CLASSIFICATION	Public	SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027	LEGAL BASIS	MD State Govt Art. § 4-101 / COMAR 12.10.01

STANDARD OPERATING PROCEDURE: TRANSPARENCY PORTAL AUDIT & ACCOUNTABILITY

Mandatory Directives Establishing System Audit Trails, Record Suppression Review, Privacy Impact Assessments, Data Integrity Audits, and Access Control Inspections

1.0 PURPOSE & SCOPE

1.1 Purpose

This Standard Operating Procedure defines the mandatory technical and administrative audit protocols governing MATCOM's Public Transparency Portal. To maintain public trust and regulatory compliance, MATCOM enforces rigorous internal control standards to verify that all published public safety records are complete, accurate, unmanipulated, compliant with privacy statutes, and free from improper record suppression or unauthorized modifications.

1.2 Scope

This SOP applies to all data pipelines, database management systems, content publishing workflows, user access controls, record suppression decisions, and administrative modifications associated with the MATCOM Transparency Portal. It mandates oversight by the Internal Audit Division, Office of Governmental Affairs, IT Infrastructure Team, and Executive Leadership.

2.0 STATUTORY & ADMINISTRATIVE AUTHORITY

This procedure is issued under the executive authority of the Chief Executive Officer and incorporates statutory auditing, compliance, and privacy mandates under Maryland law:

- **Maryland Public Information Act (MPIA)**, Maryland Code, State Government Article § 4-101 et seq., governing public access, mandatory exemptions (§ 4-351), and official records custodianship.
- **COMAR 12.10.01 & 12.10.02** (Maryland State Police Licensing Division Regulations), requiring accurate operational recordkeeping and administrative accountability for private security guard agencies.
- **Maryland Police Accountability Act of 2022** (Chapter 59, Acts of 2021), mandating public reporting integrity and independent oversight mechanisms.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Wiretap Act), prohibiting unlawful publication of electronic communications.
- **Maryland Personal Information Protection Act (PIPA)**, MD Commercial Law Code Ann. § 14-3501 et seq., regulating the protection and audit of Personally Identifiable Information (PII).

- **State Government Article § 10-608 et seq.**, governing official public record preservation and audit retention schedules.

3.0 KEY DEFINITIONS

- **Immutable System Audit Trail:** A tamper-proof, cryptographic digital log that automatically captures every system event, user login, record creation, record edit, redaction, suppression, or deletion within the Transparency Portal database.
- **Record Suppression:** The deliberate administrative withholding, removal, or delayed publication of an incident record or field report on the Transparency Portal based on statutory exemptions or active law enforcement holds.
- **Data Integrity Audit:** A systematic cross-verification comparing CAD dispatch raw logs, field officer Incident Reports, and Transparency Portal public records to detect discrepancies or unauthorized alterations.
- **Privacy Impact Assessment (PIA):** A formal compliance review verifying that all published records have undergone proper automated and manual redactions for Personally Identifiable Information (PII) and protected juvenile data.
- **Role-Based Access Control (RBAC):** Technical access limitations restricting administrative edit and publishing privileges to designated authorized personnel.

4.0 GENERAL POLICY

MATCOM maintains an absolute commitment to data integrity and portal accountability. System administrators, communications staff, and executive officers are strictly prohibited from altering, suppressing, delaying, or deleting Transparency Portal records without formal legal justification and written authorization recorded in the system audit log.

ZERO-TOLERANCE TAMPERING POLICY

Any deliberate alteration, falsification, unauthorized deletion, or illegal suppression of public safety records on the Transparency Portal constitutes a major administrative violation resulting in immediate discharge, potential civil

liability, and formal referral to the State's Attorney's Office under MD Criminal Law § 8-606 (Falsification of Public Records).

5.0 PROCEDURES

5.1 Technical Audit Trail Specifications

The Transparency Portal platform must maintain an immutable, read-only audit log capturing the following parameters for 100% of portal transactions:

Logged Parameter	Description & Technical Standard
User Identity & IP Address	Exact user account ID, authenticated role, two-factor authentication token, and source IPv4/IPv6 address.
Timestamp & Operation Type	NTP-synchronized timestamp (millisecond precision) logging CREATE, READ, UPDATE, REDACT, SUPPRESS, or DELETE operations.
Pre- and Post-State Delta	Full cryptographic hash (SHA-256) of the record prior to and immediately following any administrative modification.
Authorization Reference ID	Mandatory link to the written MPIA Exemption Justification Form or CEO Sign-off ID for suppressed/redacted entries.

5.2 Record Suppression & Redaction Approval Workflow

When an incident record contains sensitive data requiring suppression under MPIA exemptions (e.g., active homicide investigation, ongoing undercover operation, juvenile victim identity):

1. The Lead Investigator or PIO must submit an electronic **Record Suppression Request Form (RSR-Form)** detailing the specific statutory exemption under MD State Govt. Art. § 4-351.
2. The Legal / Compliance Officer must review and concur with the legal statutory basis within twelve (12) hours.
3. The CEO must grant final digital authorization.
4. The system logs the suppression event, displaying a standardized public placeholder notice: "Record Restricted Pursuant to MD State Govt. Art. § 4-351 (Active Law Enforcement Investigation)."

5.3 Quarterly Internal Audit Schedule & Sampling Methodology

The Internal Audit Division shall execute quarterly audits according to the following schedule:

Audit Quarter	Target Audit Period	Audit Sample Size	Report Due Date
Q1 Audit	January 1 – March 31	100% of Suppressed Records + 20% Random Incident Sample	April 30
Q2 Audit	April 1 – June 30	100% of Suppressed Records + 20% Random Incident Sample	July 31
Q3 Audit	July 1 – September 30	100% of Suppressed Records + 20% Random Incident Sample	October 31
Q4 Audit	October 1 – December 31	100% of Suppressed Records + 20% Random Incident Sample	January 31

5.4 Public Complaint & Record Inquiry Handling

Members of the public or news media may submit a **Transparency Portal Accuracy Inquiry** regarding any published or suppressed record via the portal's online inquiry form. The Internal Audit Division shall:

- Acknowledge receipt of the inquiry within three (3) business days.
- Conduct an independent review comparing CAD records and original field logs against the published record.
- Issue a written response or publish a corrected public record within ten (10) business days.

5.5 Annual Third-Party Security & Compliance Review

In addition to internal audits, MATCOM shall retain an independent, certified cybersecurity and compliance auditing firm annually to perform a comprehensive vulnerability assessment, penetration test, and data integrity audit of the Transparency Portal infrastructure.

6.0 RESPONSIBILITIES & ACCOUNTABILITY MATRIX

- **Director of Internal Audit:** Directs quarterly portal audits, reviews suppression logs, investigates accuracy complaints, and drafts quarterly audit findings for the CEO.

- **Chief Information Officer (CIO):** Mainalities technical infrastructure, enforces RBAC system permissions, ensures immutable log backups, and oversees cybersecurity assessments.
- **Legal Counsel / Compliance Officer:** Reviews all suppression requests for statutory validity under MPIA and privacy statutes.
- **Chief Executive Officer:** Authorizes high-tier record suppressions and receives quarterly audit reports for executive action.

7.0 COMPLIANCE & ENFORCEMENT

Failure to comply with audit directives, attempting to bypass system audit trails, or making unauthorized record modifications constitutes severe official misconduct. Violators are subject to termination, civil action, and formal licensing sanctions reported to the Maryland State Police Licensing Division.

8.0 RECORDS & RETENTION REQUIREMENTS

All internal and external audit reports, suppression authorization logs, user access audit trails, and accuracy inquiry files shall be retained in secure digital format for a minimum of ten (10) years in accordance with MATCOM SOP-PUB-39 and Maryland records preservation standards.

9.0 EFFECTIVE DATE, ANNUAL REVIEW & EXECUTIVE AUTHORIZATION

This policy takes effect on **August 13, 2026**, and shall undergo annual formal review on or before **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental
Affairs
Matcom Office of Public Safety
LLC

Date: August 13, 2026

MD License: 24PLU-SGPD4620

Status: Active & Binding



MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT & COMMERCIAL SECURITY OPERATIONS

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD
21207 | 24/7 Dispatch: 1-855-715-9911

OFFICIAL STANDARD OPERATING PROCEDURE

MD License: 24PLU-SGPD4620
NAICS: 561612 | HQ:
701-809-9911

POLICY NUMBER	SOP-PUB-39		
TITLE	SOP-PUB-39 — Records Retention for Complaints, Commendations & Evidence		
EFFECTIVE DATE	August 13, 2026	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	RESPONSIBLE DIVISION	Office of Governmental Affairs / Legal / Records Management
CLASSIFICATION	Public	SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027	LEGAL BASIS	MD State Govt Art. § 10-608 / COMAR 12.10.01

STANDARD OPERATING PROCEDURE: RECORDS RETENTION FOR COMPLAINTS, COMMENDATIONS & EVIDENCE

Mandatory Schedules, Litigation Hold Directives, Digital Evidence Preservation, Chain of Custody, Protection of Case Materials, and Authorized Secure Destruction Protocols

1.0 PURPOSE & SCOPE

1.1 Purpose

This Standard Operating Procedure establishes a comprehensive, legally compliant Records Management Schedule for Matcom Office of Public Safety LLC (MATCOM). It defines mandatory retention periods, litigation hold procedures, electronic evidence preservation rules, chain-of-custody protocols, and secure destruction workflows governing internal affairs complaints, public commendations, use-of-force records, body-worn camera footage, dispatch audio, and operational case evidence.

1.2 Scope

This SOP applies to all physical paper documents, electronic data files, digital media recordings, computer-aided dispatch (CAD) logs, internal investigation files, personnel records, and physical evidence items under MATCOM's custody or control across all divisions and operational locations in Maryland.

2.0 STATUTORY & ADMINISTRATIVE AUTHORITY

This procedure is issued under executive authorization and complies strictly with Maryland statutory and regulatory requirements:

- **Maryland Records Management Act**, Maryland Code, State Government Article § 10-608 et seq., governing the preservation, retention, and disposition of public safety records.
- **Maryland Public Information Act (MPIA)**, Maryland Code, State Government Article § 4-101 et seq., mandating records disclosure and inspection standards.
- **COMAR Title 12, Subtitle 10** (COMAR 12.10.01 & 12.10.02), requiring licensed security guard agencies to maintain complete employee, incident, and complaint records for regulatory inspection by the Maryland State Police Licensing Division.
- **Maryland Police Accountability Act of 2022** (Chapter 59, Acts of 2021), mandating long-term retention of administrative complaint investigations and use-of-force documentation.
- **Maryland Courts and Judicial Proceedings Article § 10-402** (Maryland Wiretap Act), governing lawful recording storage and evidentiary handling.

- **Maryland Rules of Evidence (Title 5, Chapter 900)**, governing chain of custody, authentication, and digital evidence integrity.

3.0 KEY DEFINITIONS

- **Litigation Hold:** An immediate, mandatory directive issued by Legal Counsel requiring the freeze, preservation, and non-destruction of all paper and electronic records relevant to pending, threatened, or anticipated litigation, subpoena, administrative hearing, or regulatory investigation.
- **Master Retention Schedule:** The official administrative schedule specifying mandatory minimum storage timeframes for distinct agency record classes prior to authorized archival or secure destruction.
- **Internal Affairs File:** The complete investigative package compiled regarding an administrative complaint against a security officer, including citizen statements, supervisor findings, body camera video, dispatch audio, and final executive disposition.
- **Digital Evidence Management System (DEMS):** MATCOM's secure, encrypted cloud-based repository utilized for ingesting, cataloging, preserving, and tracking digital audio, video, and electronic evidence files.
- **Certificate of Destruction:** An official signed legal document certifying the permanent, secure destruction of specified records upon expiration of their mandatory retention period.

4.0 GENERAL POLICY

It is MATCOM's policy to systematically retain, organize, and safeguard all agency records in strict compliance with state legal standards. Records shall not be destroyed, discarded, altered, or deleted prior to the expiration of their applicable retention schedule. A Litigation Hold supersedes all routine retention schedules and completely halts any scheduled destruction.

5.0 MASTER RECORDS RETENTION SCHEDULE

All MATCOM personnel and records custodians shall adhere to the following mandatory Master Retention Schedule:

Record Category	Specific Record Type	Mandatory Retention Period	Final Disposition
Citizen & Internal Complaints	Internal Affairs investigations, sustained or unsustained officer misconduct complaints, disciplinary files.	7 Years Minimum (Sustained severe violations retained Permanently in officer master file).	Archived in Secure Legal Vault / Certified Destruction if non-sustained.
Officer Commendations	Public commendations, awards, letters of appreciation, merit citations.	5 Years Minimum (Cross-referenced in permanent employment record).	Permanent inclusion in Employee Master Record.
Use of Force Records	Use-of-Force Incident Reports, supervisory reviews, firearm discharge logs, defensive tactic evaluations.	10 Years Minimum from date of incident (Permanent if resulting in litigation or severe injury).	Permanent Digital Archival in Legal Vault.
Digital Evidence (BWC / CCTV)	Body-Worn Camera footage, vehicle dashcam video, facility CCTV exports (Routine / Non-Incident).	3 Years Standard (Unflagged routine patrol video).	Automated Secure Purge unless flagged for litigation hold.
Critical Incident Digital Evidence	Body-Worn Camera footage associated with critical incidents, officer injuries, arrests, or weapons discharge.	10 Years Minimum (or until final resolution of litigation/appeals).	Permanent Archive in DEMS Legal Hold.
Dispatch Audio & CAD Logs	Recorded 24/7 dispatch phone calls, radio transmissions, Computer-Aided Dispatch (CAD) incident logs.	3 Years Minimum for routine calls; 10 Years for critical incidents.	Secure Purge or Permanent Legal Hold.
General Incident Reports	Routine security incident reports, property damage logs, alarm response records, field interview cards.	5 Years Minimum from date of report creation.	Certified Shredding / Digital Purge.
Security Guard Licensing	MSP Security Guard license copies,	5 Years Past Termination of	Certified Destruction.

Record Category	Specific Record Type	Mandatory Retention Period	Final Disposition
	background check results, MPCTC training certifications, drug testing.	employment per COMAR 12.10.01.	

5.2 Litigation Hold Implementation Workflow

Upon receiving notice of actual or anticipated litigation, subpoena, or MPIA request, the Legal Department shall immediately:

1. Issue a written **Litigation Hold Notice (LHN)** to all relevant Division Commanders, IT Administrators, and Evidence Custodians.
2. Identify, locate, and isolate all paper files, emails, CAD logs, and BWC recordings relevant to the matter.
3. Apply an automated lock in DEMS and CAD databases preventing auto-deletion or user modification.
4. Maintain the Litigation Hold until formal written release is issued by Legal Counsel upon final conclusion of all legal proceedings and appeals.

5.3 Chain of Custody & Evidence Security

All physical evidence items (e.g., recovered property, confiscated items, physical documents) must be cataloged in the MATCOM Physical Evidence Vault. Every transfer of custody must be documented on Form EV-101 (Chain of Custody Log) recording the date, time, transferring officer, receiving custodian, and purpose of transfer.

5.4 Authorized Destruction & Certification Protocol

Records that have reached the expiration of their mandatory retention schedule and are free from active litigation holds may be destroyed under strict oversight:

- Paper records shall undergo cross-cut shredding compliant with DIN 66399 Level P-4 standards.
- Digital storage media shall undergo cryptographic erasure or physical demagnetization/destruction.
- The Records Manager and Legal Counsel must sign a formal **Certificate of Destruction** documenting record titles, date range, method of

destruction, and authorization date. Certificates of Destruction are retained permanently.

6.0 RESPONSIBILITIES & DIVISION ROLES

- **Records Management Officer:** Oversees daily record filing, maintains the Master Retention Schedule, executes authorized destruction, and issues Certificates of Destruction.
- **Legal Counsel / Compliance Officer:** Issues and lifts Litigation Holds, reviews MPIA record requests, and conducts legal compliance audits.
- **Internal Affairs Commander:** Maintains complaint files, ensures 7-year complaint retention, and transfers sustained files to permanent personnel records.
- **Chief Information Officer (CIO):** Manages DEMS server storage, enforces digital retention parameters, and applies automated litigation hold locks.

7.0 COMPLIANCE & ENFORCEMENT

Unlawful destruction, concealment, spoliation, or improper release of agency records is strictly forbidden under Maryland law and MATCOM policy. Employees violating this SOP face immediate termination, civil sanctions, and criminal prosecution under MD Criminal Law Code Ann. § 8-606.

8.0 DOCUMENTATION & ANNUAL AUDIT

The Records Management Division shall undergo an annual audit every November to verify retention schedule compliance, audit evidence vault chain-of-custody logs, and inspect active litigation hold files.

9.0 EFFECTIVE DATE & EXECUTIVE APPROVAL

This policy takes effect on **August 13, 2026**, and is subject to annual review on or before **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental
Affairs
Matcom Office of Public Safety
LLC

Date: August 13, 2026

MD License: 24PLU-SGPD4620

Status: Active & Binding



MATCOM OFFICE OF PUBLIC SAFETY LLC

GOVERNMENT & COMMERCIAL SECURITY OPERATIONS

6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD
21207 | 24/7 Dispatch: 1-855-715-9911

OFFICIAL STANDARD OPERATING PROCEDURE

MD License: 24PLU-SGPD4620
NAICS: 561612 | HQ:
701-809-9911

POLICY NUMBER	SOP-PUB-40		
TITLE	SOP-PUB-40 — Public Accountability Annual Report		
EFFECTIVE DATE	August 13, 2026	REVISION DATE	August 13, 2026
APPROVING AUTHORITY	Dr. Brian C. Askew, CEO	RESPONSIBLE DIVISION	Office of Governmental Affairs / Executive Leadership
CLASSIFICATION	Public	SUPERSEDES	None (Initial Issue)
REVIEW DATE	August 13, 2027	LEGAL BASIS	MD Police Accountability Act / COMAR 12.10.01

STANDARD OPERATING PROCEDURE: PUBLIC ACCOUNTABILITY ANNUAL REPORT

Mandatory Protocols Governing the Compilation, Verification, Executive Sign-off, and Public Issuance of MATCOM's Annual Performance, Complaint, Use-of-Force, and Regulatory Compliance Report

1.0 PURPOSE & SCOPE

1.1 Purpose

This Standard Operating Procedure establishes a formal mandate requiring Matcom Office of Public Safety LLC (MATCOM) to publish an annual, unedited Public Accountability Report. The objective is to demonstrate institutional accountability, publish verified operational metrics, report complaint dispositions, disclose use-of-force statistics, outline training enhancements, and highlight community safety initiatives for public inspection.

1.2 Scope

This SOP applies to all operational divisions, administrative offices, field commands, internal audit teams, and executive leadership within MATCOM. It governs the annual data aggregation cycle covering all operations conducted within the State of Maryland during each calendar year (January 1 through December 31).

2.0 STATUTORY & ADMINISTRATIVE AUTHORITY

This procedure is issued under executive authorization and incorporates state transparency standards:

- **Maryland Police Accountability Act of 2022** (Chapter 59, Acts of 2021), establishing gold-standard public reporting guidelines for law enforcement and private public safety entities operating in Maryland.
- **Maryland Public Information Act (MPIA)**, Maryland Code, State Government Article § 4-101 et seq., establishing public disclosure mandates for statistical and performance metrics.
- **COMAR Title 12, Subtitle 10** (COMAR 12.10.01 & 12.10.02), requiring licensed security guard agencies to maintain complete records of agency operations, guard deployments, and citizen complaints.
- **Maryland Business Regulation Article, Title 12, Subtitle 1**, regulating corporate governance and licensing compliance.
- **State Government Article § 10-608 et seq.**, governing public record archival and retention of annual agency reports.

3.0 KEY DEFINITIONS

- **Public Accountability Annual Report:** An official, comprehensive public document published annually by MATCOM detailing agency performance metrics, complaint statistics, use-of-force incidents, training hours, and policy reforms.
- **Calls for Service (CFS) Metrics:** The total aggregated count of emergency, routine, dispatch-initiated, and field-initiated security responses logged in the CAD database during the reporting year.
- **Complaint Disposition Categories:** Standardized legal classifications for administrative complaint outcomes:
 - Sustained: Investigation disclosed sufficient evidence to prove the allegation.
 - Unsustained: Investigation failed to disclose sufficient evidence to prove or disprove the allegation.
 - Exonerated: The incident occurred, but the officer's actions were lawful, proper, and policy-compliant.
 - Unfounded: Allegation was demonstrably false or factual evidence proved the incident did not occur.
- **Use-of-Force Incident:** Any operational event where a security officer applied physical control techniques, chemical agents (OC spray), conducted energy weapons (CEW), or firearms in the line of duty.
- **Average Investigation Completion Time:** The mean number of calendar days elapsed from initial complaint intake to final executive disposition.

4.0 GENERAL POLICY

MATCOM shall publish its official Public Accountability Annual Report no later than **March 31** for the preceding calendar year. The report shall be posted in downloadable PDF format on MATCOM's website and Public Transparency Portal. Data reported must be complete, verified by Internal Audit, and approved by the CEO without suppression of negative statistics.

5.0 PROCEDURES & REPORT STRUCTURE

5.1 Required Annual Report Data Sections

Every Annual Public Accountability Report published by MATCOM must contain the following ten (10) mandatory data sections:

Section #	Report Module Title	Required Data Parameters & Metrics
Module 1	Executive Summary & Overview	Message from CEO Dr. Brian C. Askew; agency mission; licensing verification; workforce headcount.
Module 2	Calls for Service (CFS) Metrics	Total dispatch CAD volume; emergency vs. routine response times; calls broken down by client sector and jurisdiction.
Module 3	Citizen Complaints & Internal Affairs	Total complaints received; breakdown by category (misconduct, rudeness, procedure, excessive force); complaint sources.
Module 4	Complaint Dispositions & Timelines	Dispositions breakdown (Sustained, Unsustained, Exonerated, Unfounded); average investigation completion time (target: <30 days).
Module 5	Officer Commendations & Awards	Total public commendations; life-saving awards; merit citations issued to MATCOM personnel.
Module 6	Use-of-Force Analysis	Total force incidents; level of force applied (hard hand, OC, baton, CEW, firearm); suspect injury count; officer injury count; policy compliance rate.
Module 7	Policy Reforms & SOP Updates	Summary of newly issued or revised Standard Operating Procedures (e.g., SOP-PUB-36 through 40).
Module 8	Training Standards & MPCTC Alignment	Total instruction hours completed; mandatory de-escalation training hours; firearms qualification pass rates; implicit bias training.
Module 9	Community Engagement & Liaison	Public meetings attended; youth outreach programs; crime prevention seminars; joint operations with local LEOs.
Module 10	Corrective Action Plans & Goals	Administrative corrective actions implemented; equipment upgrades; strategic goals for the upcoming year.

5.2 Data Collection & Compilation Timeline

To guarantee timely publication by March 31, all divisions shall observe the following production schedule:

1. **January 15:** Internal Audit, CAD Dispatch, and Internal Affairs submit raw yearly datasets to the Office of Governmental Affairs.
2. **February 15:** The Communications Division completes the initial draft of the Annual Report and submits it to Internal Audit for statistical verification.
3. **March 1:** Internal Audit certifies data accuracy and submits the audited draft to Legal Counsel for regulatory compliance review.
4. **March 15:** Executive Leadership conducts final review; CEO Dr. Brian C. Askeew signs the formal Authorization Page.
5. **March 31:** Official public release on the Transparency Portal and distribution to the Maryland State Police Licensing Division and municipal stakeholders.

5.3 Public Accessibility & Distribution

The Annual Report shall be permanently hosted at www.matcomops.org/transparency/annual-reports. Free physical printed copies shall be made available upon request at MATCOM Headquarters (6340 Security Blvd., Suite 100-1071, Gwynn Oak, MD 21207).

6.0 ROLES & RESPONSIBILITIES

- **Chief Executive Officer:** Retains final approving authority and issues the annual executive statement.
- **Office of Governmental Affairs:** Coordinates data collection, drafts report modules, manages graphic design, and executes distribution.
- **Director of Internal Audit:** Cross-verifies raw CAD and IA datasets to ensure 100% statistical accuracy.
- **Internal Affairs Division:** Compiles complaint numbers, investigation timelines, disposition summaries, and use-of-force statistics.

7.0 COMPLIANCE & ENFORCEMENT

Data falsification, intentional omission of complaint figures, or failure to publish the Annual Report by the March 31 deadline constitutes a violation of

executive policy. Supervisors responsible for data tampering face immediate termination and licensing disciplinary referral.

8.0 RECORDS RETENTION

Published Annual Reports, raw underlying data files, audit working papers, and signed authorization sheets shall be retained permanently in the MATCOM Executive Vault pursuant to State Government Article § 10-608 et seq. and SOP-PUB-39.

9.0 EFFECTIVE DATE, ANNUAL REVIEW & EXECUTIVE AUTHORIZATION

This SOP takes effect on **August 13, 2026**, and shall undergo annual review on or before **August 13, 2027**.

Brian C. Askew, Ph.D.

Dr. Brian C. Askew

Chief Executive Officer / Approving Authority
Matcom Office of Public Safety LLC

Daune Simpkins

Daune Simpkins

Deputy Director, Governmental
Affairs
Matcom Office of Public Safety
LLC

Date: August 13, 2026

MD License: 24PLU-SGPD4620

Status: Active & Binding