Atlanta Police Department – Standard Operating Procedure			
APD.SOP.6050 – Information Technology (IT) and Data Sharing Effective Date: April 30th, 2026			
Chief Darin Schierbaum	Signature by: DS	Date Signed: 4/30/2026	Expires:2030

SIGNIFICANT CHANGES

APD Staff,

The Policy and Standards Section is dedicated to providing the department, and its employees, with accurate, understandable and transparent policies. In order to publish policies that reflect the most up-to-date standards, the Policy and Standard Section regularly reviews all policies to ensure that they are reflective of the current mission and objectives of the Atlanta Police Department.

This policy has been completely rewritten to reflect modern operations of the Department and updated computer technological advances. We ask that you please read the policy in its entirety so that you understand:

- **When and how to contact AIM.**
- **When it is appropriate to "Reply All".**
- **What to do in the event your computer stops working, physically breaks, or is lost/stolen.**
- **When it's appropriate to use Artificial Intelligence.**
- **That your emails, messages and computer use is subject to Open Records.**

This policy's name has been changed from : Department Employees Duties with Regard to Information Technology

Thank you and stay informed!

Policy and Standards Section
Planning, Research, and Accreditation Unit

TABLE OF CONTENTS

1. PURPOSE

This Policy establishes guidelines for the proper, secure, and professional use of Atlanta Police Department (APD) information technology systems and resources. The purpose of this policy is to ensure the integrity, availability, and security of Department systems and data while providing employees with clear standards for daily technology use in support of law enforcement operations.

2. POLICY

The APD will manage personal computers for maximum effectiveness in a secure environment. The APD will provide current technologies that enable users to effectively and efficiently support its operations and aid in the suppression of crime. The APD will provide use of the Internet, Department's website, and e-mail as a means of sharing information while staying within the constraints of official Departmental business.

This policy will apply to on-duty or off-duty employees using Department hardware or software.

3. RESPONSIBILITIES

3.1 Technology and Information Services (TIS) and AIM will be responsible for the acquisition, installation and support of computer hardware, networks, and software for the Department, as well as for ensuring that all software programs are properly licensed and being used for their intended application. (CALEA 6th Edition 11.4.4)

3.2 The Chief Technology Officer will be responsible for monitoring the implementation of this directive as well as, but not limited to:

1. Acquiring and managing all computers, network devices, and related equipment for the Department.
2. Evaluating the Department's need for new technology and making recommendations to the command staff for the acquisition of new technology; and
3. Assist in arranging demonstrations, vendor's presentations, and product evaluations.

3.3 AIM will be responsible for maintaining an inventory of computers and other computer-related equipment serial-numbered and owned by the APD.

3.4 Division, section, and unit commanders will cooperate with TIS and AIM in planning, implementing, and maintaining computer hardware, network, and software.

3.5 Commanders are responsible for the physical security of ~~personal~~ computers, software, and related equipment assigned under their respective commands.

3.6 The Training Section is responsible for training the Department's employees on the use of its hardware and software.

3.7 Employees will follow the guidelines in this directive and keep their passwords secret.

3.8 Supervisors will ensure their employees comply with this directive.

4. ACTION

4.1 GENERAL

4.1.1 The mission of the Department of Atlanta Information Management (AIM) is to advance Atlanta by consistently delivering innovative, reliable, secure, and user-focused technology solutions. Technology is the nucleus of city government, and through its effective and forward-thinking application, we enhance the experience of every resident, visitor, and stakeholder touched by city services.

4.1.2 This policy covers all hardware and software owned and/or operated by the city of Atlanta, to include, but not limited to: Desktops, Laptops, Email, Intranet, Apps and Platforms, Evidence Systems, and Department Software.

4.1.3 **Privacy Disclosure:** Users should have no expectation of privacy regarding personal or business-related data stored on Department systems. The Department reserves the right to monitor, intercept, and review all internet activity, electronic communications, and data stored on its network to ensure security and policy compliance.

1. Right to Inspect: The Department maintains the authority to inspect all files, software, and hardware on any device owned, leased, or controlled by the organization at any time.

2. Supervisory and Investigative Audits: While supervisors may conduct routine inspections to ensure policy compliance, audits involving sensitive or ongoing investigations must follow specific protocols to maintain evidentiary integrity:

    a. The inspecting party must consult with the immediate supervisor and provide formal notification to the Section Commander; or

    b. The inspection must be conducted directly by the Office of Professional Standards (OPS).

4.1.4 Department email, documents, electronic communications, and data created, transmitted, or stored on Atlanta Police Department systems or devices are the property of the Department and are not private. Such records may be subject to disclosure in accordance with the Georgia Open Records Act (O.C.G.A. § 50-18-70 et seq.) and applicable Department policies. Users will conduct all electronic communications with the understanding that content may be reviewed, retained, or released as required by law.

4.1.5 In addition to this directly, Employees should be aware of the City of Atlanta Policies pertaining to Information Technology and the usage of City of Atlanta owned Equipment. Additional City of Atlanta Information Management policies such as, but not limited to, the following can be found here.

- Access Control
- Sensitive & Confidential Data Handling Policy
- Privacy Policy
- Artificial Intelligence
- Clear Desk and Clear Screen Policy
- International Travel with COA Equipment
- Vulnerability and Patch Management

4.2 USER ACCOUNTS AND ACCESS

4.2.1 Upon hire with the Department, the Human Resources Unit will generate a Unique ID for each individual. This number cannot be reused or reissued, even when then original employes assigned to the number is no longer employed by the Department.

4.2.2 The Human Resources Unit will send a list of employee identification numbers to the required departments in order to grant the individual with access to the necessary systems.

4.2.3 The Human Resources Unit will forward copies of all personnel orders to Central Records, Communications Section, and to AIM.

4.2.4 Passwords are to be created and maintained in accordance with Department and City IT standards and to be safeguarded and not written, stored, or transmitted in an unsecured manner.

4.2.5 All documents containing password information are considered confidential and must be handled accordingly.

4.2.6 For access to Criminal History, the Communications Section will administer a user ID for Datamaxx and Omnixx.

4.2.7 All departments within the City of Atlanta government, including APD utilize AtlCloud/Oracle as the financial management system. Access to this system is authorized and given by AIM, based on active employment status provided by City of Atlanta Human Resources. For new employees access is requested as a part of Oracle/TALEO. Additional provisioning is approved during the onboarding process.

4.2.8 Central Records Database Repository (CALEA 6th. ed., standard 82.1.6)

1. Access to the database, Image Director, will be given to those employees whose job functions require retrieval or research of incidents and accidents.

2. The Central Records Unit (CRU) will establish a user ID upon receiving a signed written request or Departmental email from the user's commander justifying the need to access the information.

4.2.9 Police Central System

1. Access to Police Central System will be granted to those employees whose job functions require retrieval or research of mug shots.

2. AIM will establish a user ID upon receiving a signed request from the user's commander justifying the need to access the information.

3. Requests for user ID's from outside the Department will be authorized by the Identification Unit commander and established by AIM.

4. AIM will deactivate the ID's of separated employees and those transferred to assignments where access is not required.

1. AIM will audit IDs on an annual basis and deactivate those no longer in use. Copies of the annual audit will be forwarded to the Planning, Research, and Accreditation Unit. (CALEA 6th. ed. standard 82.1.6)

4.2.10 Workstation access is granted only to staff with a documented operational requirement to fulfill their duties. Employees will not release information such as passwords, access codes, or other confidential information that could compromise the security of data, files or software stored on any APD device.

4.3 CORRESPONDENCE (EMAIL, TEAMS, SHAREPOINT) AND DATA SHARING

4.3.1 E-mail, collaboration platforms, and messaging apps authorized by the Department for communication and file sharing, such as TEAMS, SharePoint, Whiteboard, etc, are intended for official City business. All communications conducted within these platforms is considered official records and may be subject to supervisory review, audit, retention requirements, and the Georgia Open Records Act, therefore employees will maintain professionalism, accuracy, and compliance in all communications conducted through the platforms.

4.3.2 When using collaboration platforms, e-mail and messenger, the following restrictions will apply:

1. Communication must be written in a professional, business-like manner and not contain language that would be considered offensive in nature (including sexual or graphic content) by any reasonable member of the public or employee of the Department.

2. The message content will not bring discredit to any employee or the APD as a whole.

3. Transmission of confidential, criminal justice, or personally identifiable information is prohibited unless done in accordance with CJIS security standards and departmental data protection policies.

4. Employees will make every attempt to limit the use of "Reply All" in department email communications and should respond only to recipients who require the information for official duties, in order to prevent unnecessary distribution, mailbox congestion, and disruption of operations.

5. No outside email accounts, including personal, business, and/or government accounts, are permitted to be automatically forwarded to the employee's department email address.

6. It is prohibited to view, upload, download, copy, retain, transfer, or otherwise deal with any images, files or programs that contain any of the following, unless part of a criminal investigation and approved by the unit commander:

    a. Images or files that display nudity, obscenity, or sexually explicit material.

    b. Images or files that would be considered offensive due to sexual or graphic content by any reasonable member of the public or any employee of the Atlanta Police Department.

    c. Images or files that would bring discredit to any employee or to the Atlanta Police Department as a whole.

    Employees are responsible for purging any images or files that violate this policy.

4.3.3 With the exception of a supervisor-monitored criminal investigation, no APD computer or device is to be used to communicate with or establish a link with another computer if the remote computer is reasonably believed to be engaged in activities that violate any Department policies or city, state, or federal Laws.

4.3.4 In order to properly investigate criminal activity, it may be necessary to upload, download, or transfer certain files that are prohibited above and/or establish a communicative link between a Department computer and a remote system involved in criminal activity.

1. These files may be temporarily stored on Department computers during the course of an active criminal investigation or if the storage of such files on removable media might hinder the prosecution of a criminal investigation. As soon as possible, these images or files are to be removed from the computers and either deleted or transferred to external storage media after the criminal investigation has been completed. The storage media will then be maintained under the evidentiary policies of the Department per APD.SOP.6030 "Property and Evidence Control".

2. A supervisor directly involved in or supervising the investigation must approve this exception. In all cases, the unit commander, the section commander, and the division commander will be notified of this exception and the file name, location of the storage, and the reason for the exception.

3. Any links established with remote systems may be done so for the purpose of conducting a legitimate investigation and may continue only while the investigation is active under the supervision of technical personnel designated by the Criminal Investigations Division (CID) commander, in consultation with AIM and the Cyber Crimes Unit.

    a. It is vital that no link be established that could compromise the security of the Department's computer network.

    b. Links of this type must be established by a "stand-alone" computer in all cases. This link may not be established with a computer directly connected via network to any Department server.

4.3.5 Information provided through the Intranet, Internet, and social media websites operated by the Atlanta Police Department will be accurate, up-to-date, and Department related. All internal and external links must be verified prior to being published to the website

4.3.6 The Horizon Intranet is authorized for access only by APD employees and will be accessible only from computers on the Department's network. The Intranet is not secure from unauthorized access; material on the Intranet may be subject to open records requirements.

4.3.7 The Departments Internet website (www.Atlantapd.org) is for public use. Data used on this website must be approved for public viewing by the Public Affairs Unit.

4.3.8 When utilizing the department's websites and/or social media for the use of providing the public with Crime Statistics and Investigations, the following information is authorized to be posted:

1. NIBRS.
2. Management data crime maps.
3. Wanted persons and notification of arrests of wanted persons.
4. Missing people and notification when missing persons are located.
5. Suspect and vehicle lookouts; and
6. Information on rewards.

4.3.9 The following information requires the submission of a Media Release Form to Public Affairs and approval by the Chief of Police, or his/her designee, prior to posting:

1. Neighborhood-level crime data other than online crime maps.

2. Demographic data on crime or arrests.
3. Information on open investigations other than specified in paragraph one (1), particularly any information that could hinder an investigation or prosecution.
4. Information received from other law enforcement agencies, GCIC, or NCIC.
5. Official crime scene photographs.
6. The identity or location of victims of sex offenses, in particular rape or attempted rape.
7. Any information concerning the identity of individuals under the age of 17 who are taken into custody.
8. The prior criminal record, character, or reputation of a suspect.
9. Any opinion of an APD employee regarding the guilt or innocence of a suspect.
10. Any opinion of an APD employee regarding the merits of a case or quality of evidence gathered.
11. The existence of any confession, admission of guilt, or statement made by the accused or the failure or refusal by the accused to make a statement; and
12. The identity, testimony, or credibility of any prospective witness.

4.4 USE OF ARTIFICIAL INTELLIGENCE

4.4.1 Law enforcement operations are rapidly evolving, sensitive in nature, and must maintain a certain level of objective reasonableness. Artificial Intelligence does not possess "objective reasonableness" in the human, ethical, or legal sense of having conscious judgment, common sense, or the understanding of right and wrong, therefore operation reliance on artificial intelligence should be avoided.

4.4.2 All reports, investigative decisions, and enforcement actions must be based solely on personal knowledge, cumulative crime stats, training, and human judgment.

4.4.3 Employees are strictly prohibited from using any artificial intelligence platform to automatically create or complete official department documentation. Official department documentation includes, but not limited to:

1. Probably Cause and Reasonable Articulable Suspicion Statements
2. Internal Investigation and Use-of-Force Statements
3. Police Reports and Investigative Narratives
4. Search/Arrest warrants
5. Policies & Directives
6. Public Service Announcements and Information directed for the Public

4.4.4 Employees are permitted to use AI platforms to assist with grammar, sentence structure, research, and as a thesaurus for written documentation, **so long as** it does not include case-sensitive and/or private information, including, but not limited to:

1. Confidential Personnel data regarding police officers and civilian personnel.
2. Personal Identify Information (especially for victims and children).
3. Case-sensitive details of any investigation or call.
4. Security-sensitive information.
5. Department Finances.

4.4.5 When artificial intelligence or automated software tools (such as Grammarly) are utilized, employees must personally review and confirm the accuracy of all information prior to submitting it, to ensure the material reflects their own observations, knowledge, and/or conclusions.

4.4.6 No employee will submit, adopt, or rely upon system-generated content without confirming it is truthful, complete, and articulated in the employee's own words.

4.4.7 Any prohibited usage of Artificial Intelligence for documentation and reporting may result in disciplinary action.

4.5 HARDWARE AND SOFTWARE MAINTENANCE

4.5.1 Employees are prohibited from disabling or modifying data protective software and will not intentionally interfere with a Departmental computer system, such that Departmental data is lost, stolen, falsified, forged, compromised, or deleted.

4.5.2 Employees are prohibited from making unauthorized copies of the Department's software.

4.5.3 The use of encryption software, unless authorized by the CID commander, is prohibited. If using encryption by supervisor approval, the key to the encryption must be provided to the CID commander is required by CJIS, and there for users should work with AIM to ensure encryption is within CJIS regulations.

4.5.4 The loading of software for an Internet Service Provider (ISP) on a Department computer and the creation of a Department ISP account must have the prior approval of AIM. The AIM commander may issue a list of approved ISPs for this purpose.

Employees will not install or use internet connectivity software, remote access applications, VPN services, cloud-storage synchronization tools, or similar programs unless specifically authorized by AIM.

4.5.5 TIS is responsible for purchasing software for use on Departmental computers and:

1. Coordinate the installation of all software and operating system upgrades and patches for the Department's devices.
2. Maintain the original software media in a secure location. Software documentation will be assigned to the user as circumstances dictate.
3. Ensure the security of the Department's computers and networks by establishing inventories, user accounts, passwords, and access to the various systems they manage. AIM will also maintain firewalls, virus protection, intrusion detection, and other measures to secure the network from outside sources.
4. Maintaining the software installed on Department computers to ensure compliance with all applicable licensing agreements.
5. Identify and resolve problems with mainframe communications and applications.

4.5.6 Unit Commander will advise the TIS and AIM Director regarding the needs to update outdated hardware and software equipment.

4.5.7 Individuals using department hardware and software will:

(GLECP 5th ed. Standard 1.28)

1. Keep their data files in a designated location on the network, where AIM will back it up and provide access security; (CALEA 6th ed. standard 11.4.5d)

2. Be responsible for data integrity and security if data is stored on the local drive; (CALEA 6th ed. standard 11.4.5d)

3. Not share their local drives on the network with other users;

4. Not install additional hardware, devices, or software without the proper anti-virus inspection and approval from AIM or TIS; (CALEA 6th. ed. standard 11.4.4) and

5. If a user becomes aware of a virus or similar problem, call the AIM Help-line (404-330-6474) immediately. (CALEA 6th. ed. standard 11.4.4)

4.6 IT SUPPORT AND SECURITY

4.6.1 Security protocols must be established for all data storage devices or software applications prior to introduction into department computer systems; therefore, AIM will be responsible for installing the Departments standard anti-virus software and updating the virus signature files as needed. (CALEA 6th ed. standard 11.4.4)

4.6.2 Users are to remain alert for suspicious emails, messages, or system activity and report concerns to AIM and their supervisors immediately.

4.6.3 Technical Help:

1. The AIM Help-site, https://aimatlanta.service-now.com will be the first line of response for users to diagnose problems with hardware, software, the network and other technical and access problems.

2. Users experiencing account lockouts or access issues should contact the AIM Help Desk or designated support unit for assistance.

3. Broken or malfunctioning hardware and software need to be reported to to AIM first with a ticket. Anything critical should be escalated to TIS and CTO to work on a resolution with AIM and APD Personnel with the issue.

4.6.4 As part of the yearly budget process, the CTO will provide the Chief of Police with a report that identifies and prioritizes the computer and technology needs of the Department.

5. DEFINITIONS

- APD Network: The Atlanta Police Department in-house network of computers; also known as the LAN (local area network), WAN (wide area network), or Intranet. It is the home of Horizon.

- Chain e-mail: Any e-mail that suggests to the recipient that he forward it to "all your friends and relatives" or anything similar, thus forming a chain between the author of the e-mail and each recipient.

- Criminal History Access Code: A code that allows the user to have access to criminal history information from the Georgia Criminal Information Center (GCIC).

- Employee Identification Number: A unique number assigned to each Atlanta Police Department employee for identification purposes.

- Intranet: An electronic communications network that connects computers or computer networks. Like the Internet, but having access restricted to a limited group of authorized users (such as employees of a company).

- LAN: A system that links together electronic office equipment, such as computers and printers, and forms a network within an office or building.

- Terminal Agency Coordinator (TAC): Designated by the Chief of Police as the Department's official liaison with GCIC.

- Web site: One or more Internet or intranet addresses at which an individual or organization provides information to others often including links to other locations where related information may be found.

6. CANCELLATIONS

APD.SOP.6050 "Department Employees' Duties with Regard to Information Technology", effective October 31, 2019.

7. REFERENCES

APD.SOP.6030 "Property and Evidence Control"
Commission on Accreditation for Law Enforcement Agencies (CALEA) 6th. Edition Standards 11.4.4, 11.4.5, and 82.1.6