


Atlanta Police Department Policy Manual		Standard Operating Procedure
Effective Date March 2, 2021		APD.SOP.6050 Department Employees' Duties with Regard to Information Technology
Applicable To: All employees		Review Due: 2025
Approval Authority: Chief Rodney Bryant		
Signature: RB		Date Signed: 3/2/2021

Table of Content

1.	PURPOSE	1	4.5	Internet and Electronic Mail	5
2.	POLICY	1	4.6	Internet and Intranet Website Content	7
3.	RESPONSIBILITIES	1	4.7	Computer Access Codes	11
4.	ACTION	2	5.	DEFINITIONS	13
4.1	Personal computers	2	6.	CANCELLATIONS	15
4.2	Technical Support	3	7.	REFERENCES	15
4.3	Budget Support Provided:	4	8.	SIGNIFICANT CHANGES	15
4.4	Network Management	4			

1. PURPOSE

To document the cooperative relationship between the Atlanta Police Department (APD) functions performed by the City of Atlanta Information Management (AIM), and APD employee's duties regarding information technology.

2. POLICY

The APD shall manage personal computers for maximum effectiveness in a secure environment. The APD shall provide current technologies that shall enable users to effectively and efficiently support its operations and aid in the suppression of crime. The APD shall 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 shall apply to on-duty or off-duty employees using Department hardware or software.

3. RESPONSIBILITIES

3.1 AIM shall coordinate the Department's policies and procedures on non-tactical computers, networks, and computerized information systems.

3.1.1 Support Services Division (SSD) and Strategy & Special Projects (SSP) shall be responsible for the acquisition, installation and support of computer hardware, networks, and software for the Department. These divisions shall advise the command staff and unit commanders in evaluating and recommending computer hardware, networks, and software.
(CALEA 6th ed. standard 11.4.4)

3.1.2 The Program Management Director shall be responsible for acquiring and managing all personal computers, network devices, and related equipment for the Department;



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- 3.1.3 Information Technology Liaison is responsible for maintaining and support of computer hardware, networks, and software as well as addressing computer issues within the Department.
- 3.1.4 Information Services Section (ISS) will be responsible for maintaining an inventory of CPUs and other serial-numbered; computer-related equipment owned by the APD.
- 3.1.5 The Technology Coordinator within SSP shall be responsible for:
 - 1. Evaluating the Department's need for new technology and making recommendations to the command staff for the acquisition of new technology; and
 - 2. Assist in arranging demonstrations, vendor's presentations, and product evaluations.
- 3.2 The SSD & SSP Commander shall monitor the implementation of this directive.
- 3.3 Division, section, and unit commanders shall cooperate with AIM, SSD, and SSP in planning, implementing, and maintaining computer hardware, network, and software.
- 3.3.1 Commanders are responsible for the physical security of personal computers, software, and related equipment assigned to their respective commands.
- 3.3.2 Commanders shall limit access to those who are suitably trained and whose job requires personal computers and/or related equipment use.
- 3.4 An approved city contractor shall maintain all tactical computers within the APD that are not maintained by AIM.
- 3.5 The Training Section shall train the Department's employees on the use of its personal computer hardware and software.
- 3.6 Employees shall follow the guidelines in this directive and keep their passwords secret.
- 3.7 Supervisors shall ensure their employees comply with this directive.
- 4. ACTION
- 4.1 Personal computers
- 4.1.1 The AIM Help-site, <https://aimatlanta.service-now.com/>, shall be the first line of response for users to diagnose problems with hardware, software, the network and other technical and access problems.
- 4.1.2 AIM shall support the Department's personal computers by:
 - 1. Configuring the network parameters and adding the personal computer to the APD's local area network (LAN);
 - 2. Ensuring that the operating system has all the current patches recommended by the vendor;
 - 3. Installing the Department's standard anti-virus software and updating the virus signature file; (CALEA 6th ed. standard 11.4.4)



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



4. Verifying that all necessary software is installed and functional;
5. Once installed at the user's location, testing that the user is able to connect with the network and is able to print;
6. Making a surge protector available for each computer. Users shall not remove or circumvent the surge protector; and
7. Ensure that CD or diskettes introduced to the system are automatically scanned for virus prior to execution of the files. (CALEA 6th. ed. standard 11.4.5b)

4.1.3 Personal computer users will:
(GLECP 5th ed. Standard 1.28)

1. Keep their data files in a designated location on the network, where AIM shall 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 assistance of AIM, if necessary; (CALEA 6th. ed. standard 11.4.4) and
5. Not disable or circumvent the anti-virus software function. 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)

4.2 Technical Support

4.2.1 AIM shall determine whether to purchase software for use on Departmental personal computers. The approved software shall also follow AIM standards. The purchase and acquisition of other software shall be justified and approved by AIM.

1. Employees shall not make unauthorized copies of the Department's software.
2. AIM shall coordinate the installation of all software and operating system upgrades and patches for the Department's personal computers.
3. AIM shall maintain the original software media in a secure location. Software documentation shall be assigned out to the user as circumstances dictate.

4.2.2 AIM shall 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 shall also maintain firewalls, virus protection, intrusion detection, and other measures to secure the network from outside sources.

4.2.3 AIM shall maintain the APD's inventory of computer hardware and software, including licenses, in cooperation with the Property Control Unit. Software installed on Department computers shall maintain compliance with all applicable licensing agreements.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- 4.2.4 AIM shall identify and resolve problems with mainframe communications and applications.
- 4.3 Budget Support Provided:
 - 4.3.1 As part of the yearly budget process, the manager of AIM shall provide the Chief of Police with a report that identifies and prioritizes the computer and technology needs of the Department.
 - 1. AIM shall assist division, section, and unit commanders in determining their IT related needs, and insure that requests for technology are in compliance with Departmental standards and fit into the Department's ITSP.
 - 2. AIM shall advise the units on replacement of outdated hardware and software equipment.
 - 3. AIM shall develop and maintain a four-year hardware replacement plan for the Department.
 - 4. AIM shall identify and evaluate emerging technologies that may prove useful for the Department, and brief appropriate Department employees.
 - 5. AIM shall coordinate the upgrading to newer versions of software.
- 4.4 Network Management
 - 4.4.1 The Network Administrator shall monitor and ensure that all aspects of network security are adhered to and that the Local Area Network (LAN) is maintained and operated in accordance with Department and AIM directives. The Network Administrator shall brief Department commanders, as necessary, when issues with LAN security arise. (CALEA 6th ed., 11.4.5)
 - 4.4.2 Local Area Network (LAN) Equipment
 - 1. The Network Administrator shall determine and enforce any and all aspects of LAN security
 - 3. Unit commanders who supervise units where LAN's are being utilized shall determine and enforce which employees within the unit are authorized to use the equipment.
 - 4.4.3 Passwords
 - 1. The Network Administrator shall create the initial password and ensure that employees using LAN equipment are aware of their responsibility to change the initial password to a personal password.
 - 2. Employees using LAN equipment shall remember and keep private their personal password.
 - 4.4.4 LAN Cables and Communications Lines
 - 1. The Network Administrator shall be responsible for any LAN cabling changes to networks.
 - 2. No changes or additions to cabling shall take place without the prior approval of the Network Administrator.
 - 3. Only unit commanders are authorized to request cabling changes. The unit commander shall forward his or her request in email form to the AIM manager. If approved, AIM shall coordinate carrying out the request.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



4.4.5 Hardware Changes and Equipment Relocation

1. The Network Administrator shall coordinate any changes or additions to personal computer hardware on all LAN's. This shall include back-up hardware, network interface cards, uninterruptible power units, and any other network related hardware.
2. The unit commander at the location of a LAN shall notify AIM before any equipment movements, transfers, or relocations. Equipment is defined here as personal computers on the LAN (nodes), file servers, uninterruptible power supply units, and any other LAN related equipment.

4.4.6 The Network Administrator is responsible for conducting regular data back-ups on the LAN. (CALEA 6th ed., 11.4.5)

4.5 Internet and Electronic Mail

4.5.1 Internet access is permitted for the following uses:

1. To transmit or receive electronic mail (e-mail).
2. File transmissions, uploads, or downloads of electronic data through the Internet for the purpose of Department related business that falls within the guidelines of this policy.

4.5.2 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.

4.5.3 Restrictions

1. It is expressly prohibited to use the internet or electronic mail on any APD computer or any other computer while conducting departmental business while on or off-duty, or by any other presentation of being on departmental business, to view, upload, download, copy, retain, transfer, or otherwise deal with any images, files or programs that contain any of the following:
 - 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.
 - d. Exceptions are listed in sections 4.5.9 and 4.5.11.
2. Employees are responsible for purging any images or files that violate section 4.5.3 from APD computers.
3. Employees shall not allow non-employees to use the Internet or e-mail through the use of Department hardware or software other than for conducting Department business.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



4. No APD computer shall 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.

4.5.4 Electronic Mail (E-Mail)

1. E-mail is not a private or protected form of communication. E-mail shall be used for business purposes and the following restrictions apply:
 - a. The message cannot contain language that would be considered offensive due to sexual or graphic content by any reasonable member of the public or employee of the Department.
 - b. The message content shall not bring discredit to any employee or the APD as a whole.
 - c. Transmitted mail must not contain attached files that would violate any part of this policy.
 - d. Employees shall not transmit chain email or similar messages through the City's mail server.
 - e. It is the user's responsibility to purge materials that violate this policy.
 - f. Messages must be written in a professional, business-like manner.

4.5.6 Employees shall 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 computer.

4.5.7 Employees shall not in any way disable data protective software; exceptions shall be made for PSITD employees for maintenance, upgrades, or other necessary purposes.

4.5.8 Employees shall not intentionally interfere with a Departmental computer system, such that Departmental data is lost, stolen, falsified, forged, compromised, or deleted.

4.5.9 In order to properly investigate criminal activity, it may be necessary to upload, download, or transfer certain files that are prohibited within this policy.

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



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



notified of this exception and the file name, location of the storage, and the reason for the exception.

- 4.5.10 It may become necessary during the course of a criminal investigation to establish a communicative link between a Department computer and a remote system involved in criminal activity.
1. This link shall be established only for the purpose of conducting a legitimate investigation and may continue only while the investigation is active.
 2. This link shall only be established 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.
- 4.5.11 Any other exceptions not in this policy must be pre-authorized by the CID commander.
- 4.5.12 The APD has the right to inspect the files, programs, hardware, or software of any computer owned, leased, or otherwise controlled by the Department. The Department may electronically monitor internet activity or e-mail.
- 4.5.13 Employees do not have a right to privacy regarding any personal or business-related information stored on a Department computer system.
- 4.5.14 The use of encryption software, unless authorized by the CID commander, is in violation of this policy. In all cases, the key to the encryption must be provided to the CID commander.
- 4.5.15 The use of encryption software to prevent the inspection of any files is forbidden.
- 4.5.16 A computer owned, leased, or otherwise controlled by the Department may be inspected at any time by a supervisor to check for full compliance with Department policies. In the case of sensitive investigations and in order not to compromise ongoing investigations, an inspection of a computer containing such an investigation must be done either:
1. After consultation with the immediate supervisor. The section commander must then be notified of this inspection; or
 2. By the Office of Professional Standards (OPS).
- 4.6 Internet and Intranet Website Content
- 4.6.1 Information on the Intranet and Internet websites shall be timely, accurate, up-to-date, and Department related.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- 4.6.2 The Horizon Intranet is authorized for access only by APD employees and shall 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.
- 4.6.3 The Departments Internet website (www.Atlantapd.org) is for public use. Data used on this website must be approved for public viewing.
1. All information that was prepared for another purpose and shall be posted to the website must follow the guidelines set forth in this directive.
 2. All internal and external links must be verified prior to being published to the website.
- 4.6.4 Personal information such as telephone numbers or address, date of birth, social security number, etc., shall not be published.
- 4.6.5 Crime Statistics and Investigations
1. Authorized information that may be posted:
 - a. Official Uniform Crime Report data;
 - b. Management data crime maps;
 - c. Wanted persons and notification of arrests of wanted persons;
 - d. Missing persons and notification when missing persons are located;
 - e. Suspect and vehicle lookouts; and
 - f. Information on rewards.
 2. Information requiring approval by the Chief of Police prior to posting:
 - a. Neighborhood-level crime data other than online crime maps;
 - b. Demographic data on crime or arrests;
 - c. Information on open investigations other than specified in paragraph one (1), particularly any information that could hinder an investigation or prosecution;
 - d. Information received from other law enforcement agencies, GCIC, or NCIC;
 - e. Official crime scene photographs;
 - f. The identity or location of victims of sex offenses, in particular rape or attempted rape;
 - g. Any information concerning the identity of individuals under the age of 17 who are taken into custody;
 - h. The prior criminal record, character, or reputation of a suspect;



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- i. Any opinion of an APD employee regarding the guilt or innocence of a suspect;
- j. Any opinion of an APD employee regarding the merits of a case or quality of evidence gathered;
- k. 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
- l. The identity, testimony, or credibility of any prospective witness.

4.6.6 Social Networking Site(s) Regulation(s)

1. Department employees shall conduct themselves in a manner which does not bring discredit upon department employees, the APD, the City of Atlanta, or the community when utilizing social networking sites on and off duty.
 - a. It is the policy of the Department to acknowledge that employees have a right to maintain personal web pages or sites and to encourage employees to exercise that right to the extent possible without causing a decline in public confidence and respect for the Department or the employee as a member of the Department. As such, the APD shall impose restrictions and oversight, when direct or indirect references to the Department or its employees are made within social networking forums, not to include legitimate and professional web pages or sites that are primarily used for posting, viewing, and submitting a Department employee's résumé. It shall be the policy of the Department that all employees shall adhere to the procedures and guidelines outlined in this policy.
 - b. Department employees shall not post any material that is violent, sexually explicit, racially or ethnically derogatory; that discredits or tarnishes the image of the Department, Department employees, the City of Atlanta, the community, or show a negative bias to one gender. This restriction shall not prohibit any posting of material that is a legitimate public speech involving a matter of genuine public concern.
2. Off-Duty Conduct
 - a. Social Networking Sites

Employees of the Atlanta Police Department are held to the highest ethical standard, which is an inherent part of the law enforcement profession. An officer's conduct, both on and off duty, is the means by which the officer and the Department's reputation are measured. Sworn personnel must maintain high standards of professional and personal conduct at all times. Department employees utilizing, posting pictures, audio, video, commenting, or creating a social networking site(s), blogs, and comment oriented websites must conduct themselves at all times in a manner so as to not bring embarrassment, disgrace, or doubt to their credibility as an impartial police officer or employee of the Atlanta Police Department, or does not bring discredit upon individuals, the Department, the City of Atlanta, or the community.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



b. Working Environment

Employees of the Atlanta Police Department, while on or off duty, shall never utilize digital technology, blogs, or social networking sites to harass, belittle, or criticize an employee or another person in any manner. The posting of any digital technology to a social networking site or forwarding or sending an email(s) that criticizes, ridicules, or otherwise may potentially embarrass or disgrace another employee or person is prohibited. This also includes the altering and/or editing of digital technology that harasses, belittles, or criticizes an employee in any manner.

c. Privacy

Department employees should be aware that they may be jeopardizing their personal confidentiality and/or that of other employees by posting photographs or personal information about themselves or other members of the City of Atlanta and/or the Atlanta Police Department. In addition, the Department employee(s) may be jeopardizing their safety, the safety of their family, their co-workers, and on-going or future investigations. Department employees are advised that in the event information has been posted on a social networking site identifying themselves as a police officer, the posting could make them ineligible for specialized assignments where anonymity is required.

3. Restrictions

- a. No pictures, video, artwork, comments or other reference depicting violent, sexual, racial, or ethnically derogatory material may be posted or associated with an Atlanta Police Department employee.
- b. Department employees shall not post or be associated with any material on the internet that brings discredit to or may adversely affect the efficiency or integrity of the Department or the City of Atlanta.
- c. Department employees shall not post on any Social Networking site, Blog, or any other type of web platform, any opinions, articles, post, pictures, audio or any other material that has the potential to or has caused a lack of trust with any members of the public regardless of their geographical location.
- d. Department employees shall not post on any Social Networking site, Blog, or any other type of web platform, any opinions, articles, post, pictures, audio, or any other material that directly or indirectly disrupts or may potentially disrupt the operations of this Department or the City of Atlanta.
- e. Department employees shall not use the Department's computer systems to access, download, or contribute to any social networking site unless he or she is lawfully doing so as a part of their regular duties or as a part of an investigation requiring access to a social networking site.
- f. Department employees may not upload any audio, or video files captured on devices owned by the Atlanta Police Department.
- g. Department employees should consider the possible adverse consequences of internet postings with regards to future employment and cross-examination in criminal cases.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- h. Department employees shall seek the guidance of supervisors regarding any posting that may adversely reflect upon either the Department or upon the professionalism or integrity of the employee.
- i. Photographs of equipment and vehicles which would reveal or compromise the investigative capabilities of the department.

4. Restrictions – Disciplinary Action

- a. Department employees found to be in violation of any restrictions of this directive (Section 4.6.6, Number 3, a – i) will be subject to disciplinary action.
- b. The disciplinary range of the violation may be from Category A – D in accordance with APD.SOP.2020 Disciplinary Process depending on the egregiousness of the material in question posted on any Social Networking site, Blog, or any other type of web platform, any opinions, articles, post, pictures, or audio.

4.7 Computer Access Codes

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

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

4.7.3 Employee Unique Identification Number

- 1. The Human Resources Unit shall generate a unique ID number for each Department employee at the time of hire. The employee ID number is unique, and it cannot be reused or reissued, even when the person is no longer employed by the Department.
- 2. The Human Resources Unit shall send a list of employee identification numbers to the Training Academy when each recruit class is formed.
- 3. Prior to graduation, the Training Academy commander shall forward an updated roster of recruits' identification numbers to AIM, Central Records, Communications Section and the Human Resources Unit. Prior to field training, all police officer recruits shall choose a confidential password (4-6 alphanumeric characters) for their employee identification number.
- 4. If a civilian employee needs his or her employee ID number, the employee's supervisor shall retrieve that information from the Human Resources Unit.
- 5. The Communications Section shall activate all employee identification numbers for the field reporting software. At the request of an employee, the Communications Section shall reset his or her password. The Communications Section shall also de-authorize the employee identification number for all terminated employees but leave them in the system.
- 6. When writing reports on the field reporting software, officers shall use their employee ID numbers as their electronic keyboard signature.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



4.7.4 Criminal History Access Code

1. Section commanders may request in writing a criminal history access code for employees performing criminal history checks as a part of their assignment.
2. The Terminal Agency Coordinator in Communications shall oversee and authorize the distribution of the criminal history access codes.
3. Upon successful completion of GCIC certification training, the requesting employee must complete a criminal history password request form.
4. The Terminal Agency Coordinator in Communications shall coordinate with GCIC to have the criminal history access code issued.
6. The Communications Section shall maintain a log of all employees with criminal history access codes and deactivate codes no longer necessary. The Communications Section shall also coordinate the resetting of passwords for criminal history access codes at the request of the employee.
7. As part of Criminal History access, the Communications Section shall administer a user ID for Datamaxx and Omnixx.

4.7.5 Other Access Codes

1. An ORI number (originating agency) is GCIC's identifier for a computer terminal authorized to access GCIC databases. These numbers are obtained and assigned by the Communications Section.
2. All departments within the City of Atlanta government, including APD utilize AtICloud/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.

4.7.6 Access to the Atlanta Police Department Network

1. At the request of an employee's supervisor, AIM shall establish the employee's ID on the LAN.
2. The employee shall choose a unique password on first login and shall change it on a regular basis as specified by the system security policy.
3. AIM shall set standards for network ID's and passwords including the length of passwords and the frequency of changes.
4. AIM shall deactivate the ID's of separated employees and those transferred to assignments where access is not required.
5. AIM shall audit network ID's on an annual basis and deactivate those not in use. Copies of the annual audit shall be forwarded to the Planning, Research, and Accreditation Unit. (CALEA 6th. ed., standard 82.1.6)



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



6. Access to a unit's files by persons outside the unit shall be with the approval of the unit commander.

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

1. Access to the database, Image Director, shall be granted to those employees whose job functions require retrieval or research of incidents and accidents.
2. The Central Records Unit (CRU) shall 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.
3. Requests for user ID's from outside the APD shall be authorized by the CRU commander.
4. An employee shall be required to change his or her password at first login and at an interval specified by CRU thereafter. All passwords are to be kept confidential. CRU shall deactivate the ID's of separated employees and those transferred to assignments where access is not required.
5. The CRU shall be the main point of contact with the Unisearch provider for user access and environments.

4.7.9 Police Central System

1. Access to Police Central System shall be granted to those employees whose job functions require retrieval or research of mug shots.
2. AIM shall 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 shall be authorized by the Identification Unit commander and established by AIM.
4. AIM shall deactivate the ID's of separated employees and those transferred to assignments where access is not required.
4. AIM shall audit IDs on an annual basis and deactivate those no longer in use. Copies of the annual audit shall be forwarded to the Planning, Research, and Accreditation Unit.
(CALEA 6th. ed. standard 82.1.6)

5. DEFINITIONS

- 5.1 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.
- 5.2 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.
- 5.3 Criminal History Access Code: A code that allows the user to have access to criminal history information from the Georgia Criminal Information Center (GCIC).



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



- 5.4 Employee Identification Number: A unique number assigned to each Atlanta Police Department employee for identification purposes.
- 5.5 Internet: An interconnected system of networks that connects computers around the world via the TCP/IP protocol. For the purposes of the directive, in general, it is the electronic connection of any Atlanta Police Department computer to any non-Atlanta Police Department computer, computer system or network. This includes any connection through direct network cable, dial-up modem access, radio frequency modem, proxy servers, or any other similar connection.
- 5.6 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).
- 5.7 ISR: Information System Request form, a City of Atlanta form used to request computer equipment, computer programs and program changes.
- 5.8 LAN: A system that links together electronic office equipment, such as computers and printers, and forms a network within an office or building.
- 5.9 Mainframe: The City's large computer that supports CJIS, MARS-G, and other programs that are available through the network.
- 5.10 Non -Tactical Computer: Computers which are not defined as tactical.
- 5.11 Password: Confidential alphanumeric characters used for entry into various computer software applications.
- 5.12 Personal Computer System: Any desktop or laptop computer, owned, leased or otherwise controlled by the Atlanta Police Department.
- 5.13 Social Networking: A social networking site can be defined as web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system; and/or (b) articulate a list of other users with whom they share a connection; and/or (c) view and traverse their list of connections and those made by others within the system; and/or (d) a site that provides a virtual community for people interested in a particular subject or just to "hang out" together; and/or (e) create their own online "profile" with biographical data, pictures, likes, dislikes and any other information they choose to post; and/or (f) communicate with each other by voice, chat, instant message, videoconference and blogs; and/or (g) the service typically provides a way for members to contact friends of other members. The nature and nomenclature of these connections may vary from site to site. These social networking sites include, but are not limited to Facebook, Twitter, all blogs, etc.
- 5.14 Tactical Computers: Computers which support mission critical applications, and contain highly sensitive information such as Field Reporting, Computer Voice Stress Analysis, and Cyber Crime investigation.
- 5.15 Terminal Agency Coordinator (TAC): Designated by the Chief of Police as the Department's official liaison with GCIC.
- 5.16 Unisearch: The database providing access to the imaged incident, accident, and related reports.



Atlanta Police Department Policy Manual
APD.SOP.6050
Department Employees' Duties with Regard to Information Technology



5.17 Webmaster: A person responsible for the creation or maintenance of a World Wide Web site, especially for a company or organization. The World Wide Web is a part of the Internet designed to allow easier navigation of the network through the use of graphical user interfaces and hypertext links between different addresses.

5.18 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

8. SIGNIFICANT CHANGES

8.1 Revisions

Sections 3.1.1, 3.2, 3.3, 4.1.1, 4.6.6(b), 4.7.5(2), 4.7.7, and 4.7.7(1)

8.2 Additions

Sections 3.1.2, 3.1.3, 3.1.4, 3.1.5, & 4.6.6(d), and 4.6.6 (3i)

8.2 Deletions

Sections 4.6.6 (1b) (2), 4.6.6 (3a&b)