



**THOMAS M. HODGSON  
SHERIFF**

**THE COMMONWEALTH OF MASSACHUSETTS**

**OFFICE OF THE  
BRISTOL COUNTY SHERIFF**

**400 Faunce Corner Road  
North Dartmouth, MA 02747**

**TEL: (508) 995-6400  
FAX: (508) 995-3326**

**BRISTOL COUNTY SHERIFF'S OFFICE**

**05.02.00**

**INFORMATION TECHNOLOGY SYSTEMS**

**TABLE OF CONTENTS**

05.02.01	DEFINITIONS	PAGE 2
05.02.02	GENERAL OPERATIONAL PROCEDURES	PAGE 3
05.02.03	INFORMATION TECHNOLOGY (IT) DEPARTMENT	PAGE 4
05.02.04	RULES AND REGULATIONS	PAGE 6
05.02.05	PROHIBITED USE	PAGE 8
05.02.06	NO EXPECTATION OF PRIVACY	PAGE 10
05.02.07	COMPUTER SYSTEMS AND NETWORK SECURITY PROCEDURES	PAGE 10
05.02.08	USE OF THE INTRANET AND INMATE TRACKING SYSTEM	PAGE 14
05.02.09	INTERNET USE	PAGE 15
05.02.10	EMAIL MESSAGES	PAGE 15
05.02.11	USE OF PERSONAL COMPUTERS AND MOBILE DEVICES WHILE ON DUTY	PAGE 16
05.02.12	WEBSITE MANAGEMENT	PAGE 17
05.02.13	ENVIRONMENTAL PROTECTION	PAGE 18
05.02.14	DISCIPLINARY ACTION	PAGE 18
05.02.15	EMPLOYEE TRAINING	PAGE 18

## PURPOSE

The purpose of this policy shall establish general operational procedures regarding the use and management of the Sheriff's Office information technology (IT) systems, including standard rules of conduct for such use. These IT systems shall include, but are not limited to, computers, laptops, tablets, computer software, storage devices, computer files, network(s), electronic mail (email) systems and devices with internet capability.

## 05.02.01 DEFINITIONS

- A. **ADS TECHNOLOGY:** The employee, appointed by the Sheriff, who is responsible for the daily supervision of the Information Technology (IT) Department. The ADS Technology shall be responsible for managing personnel assigned to the IT Department and resolving issues pertaining to Sheriff's Office computers, peripherals, specifications, programming, hardware and software installation and network operations. The ADS Technology shall also oversee mechanical and operational issues regarding the Sheriff's Office MIS system and telephone systems.
- B. **ELECTRONIC COMMUNICATION:** Communication between two or more persons (e.g. email, text, video, etc.) with electronic communication devices and technologies (such as computers, mobile phones, tablets, internet, intranet, etc.)
- C. **EMAIL (Electronic Mail):** Data, in text or other form, sent from one device to one or more other devices using a mail user agent (MUA) program, either externally using the Internet or internally using the Sheriff's Office intranet with LAN (Local Area Network.)
- D. **EMPLOYEE:** For the purpose of this policy and unless otherwise specified, the term shall apply to any full-time, part-time and contractual Sheriff's Office employees. The terms "staff", "staff members" and "personnel" shall be synonymous with one or more employees. For the purpose of this policy, the term shall also apply to volunteers, interns and those individuals employed by a third-party, contracted vendor, unless otherwise noted.
- E. **INFORMATION TECHNOLOGY:** For the purposes of this policy, the term shall apply to any equipment owned or network managed by the Sheriff's Office that is capable of internet connection and/or electronic communications (e.g. computers, tablets or any mobile device facsimile.)
- F. **INFORMATION TECHNOLOGY (IT) DEPARTMENT:** Those employees responsible for the installation and servicing of department computers, peripherals, specifications, programming, hardware and software installation and network operations, etc. Employees assigned to the IT Department shall report directly to the ADS Technology.
- G. **COMPUTER INFORMATION:** Information processed or stored by a computer. This information may be in the form of documents, spreadsheets, images, video, audio clips, software programs or other type of computer data. Computer information is typically processed by the computer's central processing unit (CPU) and stored in files and folders on a computer hard disk, network or other storage device, such as a thumb drive.
- H. **INTEROFFICE COMMUNICATIONS:** The email system - currently accessed via the Microsoft Outlook program- which is part of the Sheriff's Office interoffice communications.



- I. **INMATE TRACKING SYSTEM:** A comprehensive, accurate and real-time computerized network of inmate information that is accessible to authorized staff for decision-making and inmate management issues. Information applicable to an inmate's incarceration, up to and including booking/intake, movement, property, classification, health and program participation information, shall be found within the Inmate Tracking System.
- J. **INTERNET:** The global network of interconnected computers, enabling users to share information along multiple channels. It is the whole assortment of resources that can be accessed using an appropriate browser, providing information, texts, graphics, video and sounds for the user. Only approved users shall have access to the Bristol County Sheriff's Office internet.
- K. **INTRANET (LAN):** The privately maintained information network of the Bristol County Sheriff's Office that can be accessed only by authorized users. The intranet is currently accessed via the Microsoft Outlook program.
- L. **PASSWORD:** A code word(s) used to gain access to a locked computer system.
- M. **STORAGE DEVICE:** Any internal, external or removable device that can temporarily or permanently hold computer information. Examples include, but are not limited to, RAM memory, hard disks, thumb drives and CD/DVD disks.
- N. **TEXT MESSAGING:** The sending/receiving of text messages with devices owned by the Bristol County Sheriff's Office, a contracted vendor, an employee or another person. Also referred to as "texting".
- O. **USER:** One or more persons who have been granted authorization for full or partial use of the Bristol County Sheriff's Office's computer equipment and networks, such as the intranet, the internet and the Inmate Tracking System. For the purposes of this policy, the term may apply to one or more employee (full or part time), contracted vendor, volunteer, guest or other person.

**05.02.02 GENERAL OPERATIONAL PROCEDURES**

- A. The Bristol County Sheriff's Office shall:
  - 1. Maintain an Information Technology (IT) Department to manage the security and integrity of the Sheriff's Office information technology systems, hardware, software, computer information and related technologies;
  - 2. Provide a fully functional, ongoing computer networking system that provides users with up-to-date information for timely decision making within the Sheriff's Office, other agencies, etc.;
  - 3. Provide computers, laptops, tablets, mobile devices and other related equipment for official purposes. Such equipment may be accessible to the internet and intranet system, as well as provide texting, video, email capabilities;
  - 4. Provide general information to users before granted access to the Sheriff's Office computer networking system and equipment;
  - 5. Replace, as much as practicable, traditional paper based documentation with electronic communications.
- B. The Bristol County Sheriff's Office expects all users to comply with the general operational procedures of this policy, include the following:
  - 1. Sheriff's Office computer equipment or technologies shall be used for official purposes, as specified within this policy;

2. Users should expect no right of privacy or confidentiality regarding any document, communication or information created or stored with Sheriff's Office computer equipment or technologies;
  3. Users should be aware that electronic communications with Sheriff's Office equipment may be subject to disclosure under the Freedom of Information Act;
  4. Users should be aware that the Sheriff's Office (or its designative representative) maintains the right and ability to enter its computer system and review any information;
  5. Users shall exercise proper care in the treatment and use of Sheriff's Office computers, hardware, software, and related equipment. Users should be mindful of eating or drinking near their workstations. Keyboards or other equipment should not be propped up in precarious places. Equipment should not be damaged, dropped or mishandled;
  6. Users should not alter, remove or add hardware configuration of computer equipment, its location, wiring, connections, or software configurations unless proper notice and consent has been granted by the ADS Technology. Users should never provide or use any of their own hardware, software or storage devices;
  7. Users shall report all technical problems regarding any aspect of a computer's hardware, software or location to the IT Department in a timely manner.
- C. This policy shall apply to all employees and other users who have been granted access to the Sheriff's Office computer network, including the user of a personally owned computer or similar device that has been connected remotely to the computer network of the Bristol County Sheriff's Office.
- D. The Sheriff's Office encourages its employees to communicate with each other person-to-person or by telephone whenever possible and as appropriate to the situation.

#### **05.02.03 INFORMATION TECHNOLOGY (IT) DEPARTMENT**

- A. The Sheriff's Office shall maintain an Information Technology (IT) Department which shall be responsible for the management of the agency's overall computer networking system, its hardware, software, computer information and related equipment/ technologies.
- B. The responsibilities of the IT Department shall include, but shall not be limited to, the following:
1. Providing analytical and technical support for system users, including resolving equipment malfunctions, installing new equipment and addressing soft/hardware problems;
  2. Performing regularly scheduled checks of operating systems, applications and user files, as well as system checks to prohibit system failures or any other event which could cause the loss of important data;
  3. Conducting installations, repairs and replacement of computers, printers and other electronic devices, as necessary;
  4. Maintain and monitor a data backup system to protect all departmental computer programs and information and provide an off-site duplication of that information;
  5. Coordinating the relocation of employee computers, printers and other electronic devices to new work locations with appropriate supervisors.
- C. The ADS Technology shall manage the IT Department, whose duties shall include the following:
1. Coordinating with IT Department personnel and others on the installation, testing and operation of Sheriff's Office computer hardware and software, particularly in areas that are required to maintain information, vital documentation or automated informational management resources;



2. Consulting and providing analytical/technical support regarding new soft/hardware, routine maintenance, software problems or for enhancing existing systems currently in operation;
  3. Coordinating and advising the Training Division with employee training on new or existing aspects of the Sheriff's Office computer network and systems;
  4. Resolving questions/concerns regarding the Sheriff's Office information technology systems;
  5. Coordinating periodic system shutdowns and schedule soft/hardware maintenance and upgrades;
  6. Coordinating routine checks of operational systems, applications and user files for system protection;
  7. Ensuring that new users sign a Computer User Accountability Form before they have access to a Sheriff's Office computer, mobile device, etc.;
  8. Reporting to the Chief Financial Officer other administrators regarding funding, infrastructure or security concerns relative to the Sheriff's Office information technology systems.
- D. The ADS Technology or designee shall be responsible for providing recommendations to the Sheriff and/or the Chief Financial Officer regarding the selection, purchase or acquisition of new equipment or hard/software within the Sheriff's Office information technology systems. Such action shall comply with the purchasing laws of the Commonwealth of Massachusetts (MGL c. 30B) and Sheriff's Office policy. The ADS Technology or designee will coordinate the delivery and installation of any new equipment or system with appropriate personnel so that security and environmental precautions are followed.
- E. Users should not troubleshoot technical computer problems nor attempt to reinstall hardware, wiring, connections or software configurations, etc. Instead, they shall direct questions or work requests relative to the information technology system to the IT Department in a timely manner. Work requests shall be submitted to the IT Department by email at IT Support ([ITSUPPORT@BCSO-MA.ORG](mailto:ITSUPPORT@BCSO-MA.ORG)) or by telephone (if a computer is inoperable). The IT Department must certify all facility computer relocations and reconfigurations. Sheriff's Office employees may be disciplined for attempting to resolve equipment problems without first contacting the IT Department.
- F. The Superintendent or other senior-level administrators may direct the IT Department to conduct security checks of Sheriff's Office computer hardware and/or software, which may include the following:
1. Inspection of computer, printers, etc. for contraband;
  2. Inspection of computer software for potential security threats;
  3. Inspections for unauthorized software, hardware or other related systems within the facilities;
  4. Inspections for illegal activities or policy violations conducted by users; and
  5. Inspection of upgrades to existing computer hardware, software or related equipment.
- G. The IT Department shall ensure that each Local Area Network (LAN) server and connectivity equipment are maintained in a secured area with controlled access, posing minimal threat of damage to the Sheriff's Office computer networking system and prevention plans.
- H. The IT Department shall notify the Sheriff or his designee whenever an actual or possible security breach has been detected within the agency's computer networking/information technology system. If there is a possibility of imminent harm to the system or its data, the IT Department shall take steps necessary to secure the system and its data, including terminating system access. The Sheriff or his designee shall be notified immediately if such steps are taken. The Sheriff or his designee may order an investigation to be conducted regarding a potential or actualized security breach.



- I. The IT Department shall maintain an accurate inventory of Sheriff's Office computerized equipment, where they are located, and, if applicable, who has been issued such equipment. Inventory reviews shall be conducted annually for accuracy. The relocation of computer equipment owned by the Sheriff's Office shall be coordinated between the IT Department and appropriate personnel. To adjust inventory control lists, the IT Department shall inform the Inventory Control Officer when new equipment is purchased, where situated and/or when existing equipment has been relocated.
- J. The IT Department shall coordinate with the Maintenance Division and other personnel when electrical maintenance work is to be performed on the Sheriff's Office computer system, which may affect the power supply and all automated information systems.

**05.02.04 RULES AND REGULATIONS**

- A. The Sheriff's Office has implemented the following general rules and regulations regarding its electronic communication and information technology systems. These rules and regulations are not exhaustive, but should provide users with a general framework regarding the application of such technologies with Sheriff's Office computers, electronic devices and peripheral equipment:
  - 1. Computers and peripheral equipment, such as monitors and printers, will be placed in approved locations. Mobile equipment (e.g. laptops, cellular phones, tablets) will be issued to authorized users for official use. Approved computer, mobile phones and other equipment will have intranet and internet access. The purpose of these devices will be to help manage and enhance productivity, communication, decision-making, etc. within the workplace.
  - 2. Computers and other electronic devices shall be used appropriately. Users should not willingly transmit, receive, submit, disclose, FAX or publish any information that has been deemed confidential in nature, CORI protected, or protected under the provisions of attorney/client privilege, unless specifically authorized by their Immediate Supervisor to do so. This includes sending confidential information by email, CD, DVD, thumb drive, FAX or any other means (electronic or hardcopy) to another party without prior authorization.
  - 3. Users of mobile computers (e.g. laptops, notebooks, tablets) will be responsible for the protection of the computer and the computer information that is stored on it. Any confidential computer information should be stored on and accessed from a password protected storage device, not the computer's internal hard drive.
  - 4. Computers and other electronic devices may be used for incidental, personal purposes - but only when so authorized by an Immediate Supervisor. The personal use of such devices shall be done sparingly and must not interfere with the user's job responsibilities. (For instance, a user may send/receive an email and text message for a personal reason on a Sheriff's Office computer and mobile device, provided that this privilege has been approved by their supervisor and is not abused.)
  - 5. Computers, other electronic devices and the information technology system shall be used appropriately and handled with care. The internet and intranet shall only be used for reasonable time period and for justifiable purposes. Computer and the information technology system shall not be used for illegal purposes under federal, state or international law. Users shall not harass others with this technology, infiltrate other computers without authorization or damage/alter software components of another computer or networking system. Supervisors shall monitor employee use of these devices and technologies. Employees may be disciplined for using these



devices and technologies inappropriately and may have their access to these networks suspended or removed, after review.

6. Computer hardware or software shall be authorized by the ADS Technology prior to being developed, downloaded, installed or used, following a written request. The Director shall determine if such use would be in the best interest of the Sheriff's Office and reserves the right to review/inspect any hardware, software or related technology before/after approval has been granted. The intentional development, downloading or use of hardware or software programs not authorized by the Director is prohibited.
7. The deliberate tampering, destroying, interfering or circumvention any security measure or firewall that has been designed to protect the integrity of the Sheriff's Office electronic communication system is prohibited.
8. The willing transmission, receiving, submitting, disclosing or publishing of any information deemed confidential, CORI protected or protected by attorney/client privilege is prohibited - unless such action is specifically authorized by a supervisor or according to job assignment. This includes email, CD's, DVD's, thumb drives, storage devices, FAX or any other means of electronic or non-electronic communication.
9. The opening or forwarding of suspicious emails, text messages and/or attachments from unknown parties is prohibited until the sender's identity can be confirmed. This is to prevent the spread of possible viruses and/or otherwise violate the conditions of this policy.
10. Good judgment and personal accountability is expected by users when sending electronic communications on department equipment. Such communications should be written professionally and courteously. Emails, audio/video and text messages sent or received with the Sheriff's Office email address shall be considered the equivalent of correspondence sent on official letterhead. Users should remember that electronic postings sent or received on the Sheriff's intranet or internet can be stored and may be forwarded to Sheriff's Office officials for investigative purposes.
11. Users shall assume the risks associated with obtaining information via the internet with Sheriff's Office equipment. Prohibited material opened, downloaded, emailed, saved or recorded from the internet with Sheriff's Office equipment shall be subject to inspection and review. (Prohibited material shall include material that is defamatory, inaccurate, abusive, obscene, profane, sexually orientated, pornographic, threatening, culturally/racially offensive, illegal, or which may compromise the safety and security of the Sheriff's Office, its employees, inmates or others.) While it may be impossible to preview the content of all online material, users should make every effort possible to view only suitable and appropriate internet sites. Users who discover, either by accident or design, unsuitable or otherwise prohibited internet material should immediately remove themselves from that website. The user should report the matter to the IT Department for review. Unless credible evidence exists to the contrary, the Sheriff's Office will assume that the opening of the file by the user was intentional and the file was read. The prohibited use of the internet shall be subject to disciplinary action, up to and including termination and possible criminal prosecution.
12. Placing inappropriate, unauthorized, unprofessional or illegal information onto the internet or intranet with Sheriff's Office equipment is prohibited. Users shall not engage in or subscribe to online chat rooms, blogs, social media sites or bulletin board activities with Sheriff's Office equipment, unless explicitly authorized to do so for specific work related purposes.



13. Taking photos and/or audio-video recordings of Sheriff's Office activities, inmates, facilities or systems is only permitted for official purposes, when so authorized. Such photos and/or audio-video recordings shall be Sheriff's Office property. For security and safety purposes, these photos and/or audio-video recordings shall not be copied, shared, or placed onto the internet or intranet without explicit authorization from the Sheriff or his designee to do so.
14. Streaming media (audio and/or visual) shall only be used for official, work related purposes. Streaming media may be used for approved purposes, such as internet instruction, training, research, watching security/law enforcement events or other official purposes. Streaming media shall not be used illegally, for political purposes, personal or private gain, personal entertainment or other activities not approved by the Sheriff's Office.
15. Employees belonging to a Collective Bargaining Unit may use Sheriff's Office computers and printers to write and produce documentation relative to official union business, such as grievances. They may not, however, use the internet with Sheriff's Office computers or other electronic devices to conduct union related business or research.
16. Users must sign a Computer User Accountability Form before granted access to the Sheriff's Office information technology system, its computers, peripheral equipment, networking systems, etc. The form shall verify an understanding of the rules regarding this technology and equipment. (See 05.02.07 A)
17. Users who knowingly access a Sheriff's Office computer and/or network system without proper authorization shall be subject to disciplinary action, up to including punishment by imprisonment for no more than 30 days or by a fine not more than \$1,000 or both (MGL c. 266 s. 120 F). The same procedure and penalties shall apply to any person who, after gaining access to a computer/networking system by any means, knows that such access is not authorized and fails to terminate such access.

#### **05.02.05 PROHIBITED USE**

- A. The Sheriff's Office prohibits the use of its electronic communication system for the following purposes:
1. For personal gain, commercial use or to conduct personal business. (Designated employees may use the internet to purchase materials for the Sheriff's Office, but such transactions must comply with Sheriff's Office policy and MA state law);
  2. To commit or further any illegal act, including the violation of any criminal or civil laws or regulations;
  3. To access or send threatening or harassing messages or images, sexual or others, to one or more persons;
  4. To access or share sexually explicit, pornographic, obscene or otherwise inappropriate or offensive material, messages, video, images, etc.;
  5. To use language that is abusive, harassing, unprofessional, unethical or contrary to the generally accepted rules of professional etiquette;
  6. To access or send discriminatory, defamatory, inaccurate, abusive, threatening or offensive or illegal language or images to one or more persons, including racially, ethnically or sexual offensive material;
  7. To solicit or proselytize others for religious causes;
  8. To solicit participation in outside organizations or activities (unless so approved by the Sheriff or designee);
  9. To communicate electronically incidental personal memos, announcements, advertisements, etc. (unless so approved by the Sheriff or designee);
  10. To infringe any intellectual property rights;



11. For political purposes;
12. For inmate access to any Sheriff's Office computer, network device or system for any purpose, including the use of the intranet or internet;
13. To gain, or attempt to gain, unauthorized access (hacking) into any computer, file or network to which the employee has not been granted authorization or access;
14. To deliberately crash, retard, interfere, deny or disrupt service of any computer network or resource, including the propagation of a computer virus, security breaches or other harmful programs (worms, Trojan horses, email bombs, etc.);
15. To intercept communications intended for other persons (unless so authorized);
16. To make copies of another employee's user file without their knowledge or consent;
17. To willingly disclose confidential material, CORI protected information or other classified material accessible on a Sheriff's Office computer, unless so authorized within the scope of the employee's duties or as expressly authorized;
18. To misrepresent the Sheriff's Office or the role of any employee, vendor or volunteer;
19. To download or use an unauthorized computer system, program upgrade or "app" without prior authorization from the ADS Technology or designee to do so;
20. To "stream" audio or video materials via the internet for unauthorized purposes;
21. To distribute chain letters;
22. To gamble or to access online gambling sites;
23. To libel or otherwise defame any person;
24. To violate any local, state, federal or international law or regulation;
25. To violate any provision of a Collective Bargaining Agreement;
26. To jeopardize the safety and security of a correctional facility, law enforcement/public safety agency, Homeland Security or other governmental operation;
27. To subscribe to websites, blogs, chat-rooms, social media sites, etc. unless so authorized and related to their job functions;
28. To violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, including the installation of pirated software;
29. To copy copyrighted materials without authorization, including digitization and distribution of photos from magazines, books, music, videos or other copyrighted sources for which the Sheriff's Office or the end user does not have an active license for its use;
30. To export software, technical information, encryption software or technologies in violation of export control laws;
31. To swap files and/or file share software on a computer, server, tablet, Personal Digital Assistant or other device connected with a local area network (LAN) in any fashion, including for wireless connections;
32. To reveal an individual's employees personal password or account to other person, unless so authorized to do so, including the individual's family or others when work is being conducted at home;
33. To make fraudulent offers of products, items or services originating from a Sheriff's Office account;
34. To circumvent user authorization or security of any host, network or account;
35. To use a proxy server of any type (other than an approved internal proxy server);
36. To steal, vandalize or obstruct the use of the Sheriff's Office computer equipment, network systems or computer information;
37. To send text messages while driving;
38. To violate any other Sheriff's Office rule or procedure, especially with regards to the Code of Ethics, security matters or state law.



- A. There shall be no expectation of privacy relative to the use of the Sheriff's Office electronic communications system. Any person logging onto the system shall be consenting to the possibility that the Sheriff's Office (or its designated representative) may monitor and/or inspect any data, message or content created or received on the system, as well as any website accessed. Electronic communications sent/received within the system may also be subject to disclosure under the Freedom of Information Act. Sheriff's Office computers, mobile phones and peripheral devices are the property of the Sheriff's Office and shall be used according to this policy and state/federal law.

A. **ACCESS TO SHERIFF'S OFFICE ELECTRONIC COMMUNICATION SYSTEM**

1. Access to the electronic communication system shall be based on job assignment and need. A user's level of access (full or partial) to the system shall be determined by the Sheriff's Office, such as their access to the Inmate Tracking System and/or the internet. The Sheriff's Office reserves the right to suspend or terminate any user's access to its electronic communication system, if necessary.
2. The Computer Use Accountability Form shall be completed and submitted for approval before a user may access to the Sheriff's Office electronic communication system. Supervisors shall ensure that new users complete the form prior to access. Original, completed forms shall be sent to the IT Department and forwarded to the Communications Department for preservation. Copies of the form shall be provided upon user request. Employees assigned as liaisons between the Sheriff's Office and a contacted vendor shall ensure that this procedure is completed accordingly.
3. Access into the Criminal Justice Information System (CJIS) or other networks established by the Commonwealth of MA (MMARS, CAMIS) may be provided. The Sheriff's Office shall determine which users will have such access. Users shall follow the official policies/procedures for that network. They may also be required to sign a user agreement before having access to these systems. User agreements shall be signed and maintained with the Communications Department and/or other Sheriff's Office departments. The Sheriff's Office reserves the right to suspend or terminate any user's access to these networks at any time. Users may also be disciplined for violating network procedures, up to and including termination. (The enforcement of user access to the CJIS network shall be the responsibility of the Communication Division.)

B. **USE AND CARE**

1. Electronic communication equipment (e.g. computers, printers, mobile devices, etc.) should be generally cleaned, maintained and treated with care. Users should take care when eating or drinking when near such equipment and protect such equipment from possible physical damage.
2. Electronic communication equipment should not be left unattended once activated, particularly within a secured perimeter. Users should remain close to activated equipment, especially within a secured perimeter.
3. Electronic communication equipment should be logged off at the end of the work day, unless the computer is assigned to a 24 hour post. Users should also log off such equipment when away from their workstation for a reasonable time period. When away for a brief time period, user should lock their computers by pressing the Ctrl-Alt-Del key sequence on their keyboard and press "Enter" or click the "Lock Computer" button. Users should



not turn off electronic communication equipment, especially computers, while logged in or while running an application, unless instructed by the IT Department to do so.

4. Electronic communication equipment shall be charged and operational at all times, as applicable;
5. Electronic communication equipment, such as computers, printers, keyboards, etc. should not have objects placed near them in a manner which might compromise proper ventilation, the protection of equipment or possible heat damage.
6. Computer equipment, hardware configurations, wiring, connections or installed software should not be removed, installed or adjusted without the consent of the ADS Technology or designee.
7. The IT Department should be contacted to resolve issues with office computers, printers, or other electrical devices and/or operating software.

#### **C. INSTALLING COMPUTER RELATED HARDWARE**

1. The introduction or installation of unauthorized software, hardware or related technology is prohibited. Hardware, such as wireless access points, storage devices, etc. may present a security risk or impede established operations. New software or software packages shall be brought to the IT Department before use for virus inspection and network compatibility. All copyright laws and licensing rules shall be followed.

#### **D. SOFTWARE**

##### **1. PIRACY CONCERNS**

- a. The installing of software into a computer without the legal right to do so ("pirating") is prohibited. The ADS Technology, with proper approval, must purchase a software program from a reputable source in accordance with c.30B and possess the license/software to use the program. The posting or uploading of copyrighted material without the permission of the owner of such material shall also be prohibited. Disciplinary and/or legal action may be taken against a user who illegally uses or copies computer software without meeting these criteria.

##### **2. INSTALLING AND/OR DOWNLOADING SOFTWARE**

- a. The installing or downloading of new software onto computers or onto the computer network is prohibited. The ADS Technology or designee shall authorize such actions. Users who wish to use new software should contact the Director, in writing, with specifics about the program. Permission must be obtained before downloading or purchasing the software. Should an employee require the use of software not owned by the Sheriff's Office, they must arrange to purchase the software through routine purchasing procedures. Such purchases shall also be pre-approved by the ADS Technology and other appropriate supervisors. (Software includes, but is not limited to, scripts and commands.)

#### **E. SECURITY OF INFORMATION**

1. The IT Department shall be primarily responsible for the security and integrity of the Sheriff's Office information technology system, including all related hardware, software, related technology and equipment. Security breaches shall be considered a serious matter. Users shall not tamper with, destroy, interfere or circumvent any security measure or firewall that is designed to protect the integrity of the Sheriff's Office information technology system. Whoever knowingly accesses a computer and/or network system without proper authorization shall be subject to disciplinary action, up to including punishment by imprisonment for no more than 30 days or by a fine not more than \$1,000 or both (MGL c. 266 s. 120 F) The same procedure and penalties shall apply to any person who, after gaining access to a computer/networking system by any means, knows that such access is not authorized and fails to terminate such access.
2. All computer information is the property of the Sheriff's Office. Employees will only access computer information that is part of their job assignment and to which access permission has been granted.
3. Questionable computer files, discs, storage devices, or questionable images, videos or emails downloaded from the internet shall be brought to the attention of the IT Department for scanning. Scanning shall attempt to prevent the threat of possible computer viruses. Under no circumstance should an employee download a suspicious/questionable file unless it has been previous checked by the IT Department using updated anti-virus software. Under no circumstance should files be downloaded regularly or automatically from external servers without the explicit consent of the IT Department. Adherence to these guidelines will avoid the use of excessive amounts of space on a PC or network hard drive and prevent serious stress to the Sheriff's Office internet connection.
4. Inmates shall not have access to a computer or peripherals connected to the Sheriff's Office computer network. The only exception shall be inmate access to the Legal Computer Workstations. Inmate access to the Sheriff's Office intranet or internet systems is prohibited. Inmates shall not send or receive emails, text messages, video messages, etc.

#### **F. COMPUTER VIRUSES**

1. Sheriff's Office computers are not immune from computer viruses. The threat of a virus infection is real and can occur from downloading files from the Internet, loading data into a computer from an infected diskette or other storage device or from running an infected email attachment. Questionable files, diskettes, storage devices or emails should be scanned for viruses by the IT Department before use.
2. Executable files should not be downloaded off the Internet since viruses presently exist in executable files (those files with the .EXE or .COM extensions). Newer generation of viruses, however, can live in documents as well. Therefore, without exception, if there is a need to download a file(s) from the Internet, the IT Department should be contacted for assistance. Under no circumstances should any file be downloaded unless the file has been checked for viruses using an updated version of anti-virus software used by the Sheriff's Office. Under no circumstances should files be downloaded regularly or automatically from external servers without the explicit consent of the IT Department. Adherence to these guidelines will avoid the use of excessive amount of space on a PC or network hard drive and prevent serious stress to the Sheriff's Office Internet connection.



## G. PASSWORDS

1. Individualized user passwords shall be established for access to the Sheriff's Office computer network, operational systems and devices. User passwords should be a combination of letters, numbers and symbols. The passwords should be revised every three months or as necessary.
2. Individualized passwords shall remain confidential. Users should not disclose their passwords to others, unless so ordered by their Immediate Supervisor, a senior level supervisor or the IT Department. Unauthorized requests to obtain a user's password should be documented and reported to the ADS Technology or designee.
3. Users should not gain, or attempt to gain, access to a Sheriff's Office computer or electronic device with another person's password - unless so ordered to do so. The Sheriff's Office shall investigate allegations of such action occurring. Users who believe that another person has unofficially gained access to their computer should change their password immediately and then contact the IT Department.

## H. STORAGE DEVICES

1. Storage devices may be used for electronically transferring computer information from a computer or the system network. Users must receive authorization from their immediate Supervisor to use a storage device. The immediate Supervisor may grant permission per request or may allow continuous use as part of the user's duties. Only authorized storage devices, issued by the Sheriff's Office, shall be used. Users may not under any circumstances use any type of storage device not issued by the Sheriff's Office.
2. Users shall be held responsible for the safety and security of content stored onto a storage device. Password protection must be maintained at all times for all storage devices. Unless so authorized, no confidential material, emergency plan, official record or information pertaining to one or more specific inmates shall be stored onto a storage device. CORI laws and other state/federal privacy rights shall be followed. Users found in violation of this rule may face disciplinary action, up to and including termination.
3. Lost storage devices must be verbally reported to an immediate Supervisor and the IT Department as soon as possible, followed by an Incident Report. Employees may be disciplined for losing an issued storage device.

## I. REMOTE COMPUTER ACCESS

1. Remote access to the Sheriff's Office computer network may be provided, if authorized by the Sheriff or his designee. The Director of Computer Operation shall facilitate such access, once authorized. Devices to be used for remote access must meet the requirements of the Sheriff's Office. Remote access to the Sheriff's Office network with a personal computer, laptop, mobile phone, etc. must be approved in advance by the ADS Technology or designee.
2. The same security considerations and procedures established within this policy shall apply once a user has been approved remote computer access. Remote computer access must be secured and strictly controlled. Individualized passwords and email accounts shall be implemented for remote computer access, which shall be confidential. Users shall ensure that their personal computer is not simultaneously connected to another network when connected to the Sheriff's Office network, with the exception of personal networks that are under the complete control of the user.
3. Users shall have an authorized email account or other external resource to conduct official business.

4. Users who are finished with their use of the Sheriff's Office network via remote access should promptly disconnect from the network.
5. Hosts that are connected remotely to the Sheriff's Office computer network should use the most current anti-virus protection software available, approved by the ADS Technology or designee. This includes with personal computers, laptops, etc. The anti-virus program must be running at all times when using the Sheriff's Office computer network.
6. The Sheriff's Office reserves the right to deny or remove a user's remote access privileges at any time.

**J. GAMES AND ENTERTAINMENT**

1. Users are prohibited from using Sheriff's Office computers for entertainment purposes (games, non-work related DVDs and/or internet game play). Musical CDs are not permitted at security computer workstations.

**05.02.08 USE OF THE INTRANET NETWORK AND INMATE TRACKING SYSTEM**

- A. An intranet communication system has been established that is available to users via the Microsoft Windows Network for e-mail use and for disseminating documentation electronically to persons linked to the system. The intranet system allows users to create folders/files onto the "Shared on Dartmouth" folder within the Window's program. An Inmate Tracking System has also been established, which shall provide a comprehensive, accurate and real-time electronic accounting system on inmate admittance, processing, movement, release and other classification activities.
- B. Permanent folders on the intranet can be established on the "Shared on Dartmouth" file. Users who wish to establish a permanent folder shall contact the ADS Technology. The ADS Technology shall verify the need for such a folder with the employee's senior level supervisor. If approved, the IT Department shall establish the folder. The employee who requested the folder shall be responsible for the validity and accuracy of its content – NOT the IT Department. The employee shall be responsible for monitoring folder content periodically –not the IT Department. The placement of inaccurate, unauthorized or inappropriate material into a permanent folder shall be investigated.
- C. Immediate Supervisors shall contact the ADS Technology when a new employee is to have access to the intranet system and the Inmate Tracking System. Prior to such access, the user shall complete a Computer Use Accountability Form, verifying their understanding of facility rules. The ADS Technology may confer with senior-level administrators regarding the new employee's access to the intranet or Inmate Tracking System.
- D. Unauthorized persons, especially inmates, shall not have access to the intranet network or Inmate Tracking System for any purpose. Inmates shall not have access to any personal or professional email account via the intranet.
- E. The intranet and Inmate Tracking System shall only be used for reasonable and justifiable purposes. Excessive or unofficial use is prohibited. The intranet or Inmate Tracking System shall be closed when no longer in use.
- F. Users shall comply with the requirements of this policy regarding the use of the Sheriff's Office intranet and Inmate Tracking System, particularly 05.02.05 "Prohibited Use".



**05.02.09****INTERNET USE**

- A. The Sheriff's Office may provide user access to the internet via its computers, mobile phones, etc. Internet access is available via the BCSO SOPHOS Astaro firewall. The Sheriff or his designee shall approve which users may have access to the internet via Sheriff's Office equipment. Requests procedures are established in 05.02.07 (A). Inmates are prohibited from access to the internet for any purpose.
- B. Internet access and use through the Sheriff's Office internet shall only be for official purposes, in compliance with this policy. Supervisors should monitor employee use of the internet during work hours. Employees found using the internet for extended or unofficial purposes will be investigated and their internet access may be suspended or removed, after review.
- C. Audio-video watching in real-time via the internet ("streaming") shall only be used for official purposes, such as for training, research or instruction purposes or when a major event occurs. Streaming media, however, shall not be used for purposes that violate this policy and the law, such as for political campaigning, personal gain, personal entertainment or other unauthorized activities. Employees found streaming via the internet for unofficial/inappropriate reasons will be investigated and their internet access may be suspended or removed, after review.
- D. Content downloaded from the internet with Sheriff's Office equipment shall be subject to inspection and review. The IT Department is authorized to conduct periodic reviews of sites visited by employees online with department equipment.
- E. Only authorized personnel shall develop, download or use operational systems, programs or "apps" from the internet for official use.
- F. Sheriff's Office employees who belong to a Collective Bargaining Unit shall not use agency equipment to conduct union business and research via the internet. They may, however, use the internet with agency equipment for producing documents relative to official union business, such as grievances.
- G. The unauthorized use of file swapping and/or file sharing software on any Sheriff's Office PC, server, tablet, Personal Digital Assistant (PDA), mobile phone or any other device connected to a local area network (LAN) in any fashion, including wireless connections, is strictly prohibited.
- H. Chat rooms, on-line chat, blogs, bulletin boards, etc. with Sheriff's Office equipment are prohibited, unless specifically related to a job assignment and approved by the Immediate Supervisor for official work purposes.

**05.02.10****EMAIL MESSAGES**

- A. Employees may be issued Sheriff's Office mobile devices with emailing capabilities, as well as internet access. Good judgment and personal accountability is expected when using these devices. Emails sent from a Sheriff's Office device should be written in a professional and courteous manner. Emails sent/received with the Sheriff's Office e-mail address (Username @bcso-ma.org) shall be considered equivalent to correspondence sent on official letterhead. Unauthorized, unprofessional, illegal or prohibited content, pictures, videos, etc. shall not be sent via email from a Sheriff's Office device.
- B. Subject to certain exceptions in the law, any email composed or received on Sheriff's Office equipment shall be considered public record and copies of which may be requested by any member of the public. Such emails are also



considered a public record for the purposes of the Freedom of Information Act and MGL c.4, §7, cl.26. Unless protected under an applicable exemption or privilege as determined by the keeper of records, all emails are subject to litigation discovery, subpoena, Freedom of Information Act requests, audits and investigations. Emails that are public record shall be saved by the custodian or keeper of that public record to a permanent electronic record and preserved in accordance with the MA records retention schedule. (It should be noted that even deleted messages might be subject to disclosure because they may still exist on backup tape.)

- C. Employees composing or receiving emails on Sheriff's Office device should not consider these communications as private conversations between two or more people. In accordance with state laws and the Electronic Communications Privacy Act (Title 18 US Code, §§2501, et. seq. and 2701, et. seq.), the Sheriff's Office reserves the right to monitor emails composed or received on Sheriff's Office devices. The ADS Technology, the Communications Division and others, when so authorized by the Sheriff or his designee, shall have access to these records to detect possible abuses to the system. It is possible that emails sent from the Sheriff's Office system can be intercepted on the local system and on the internet; therefore, users should not expect any degree of privacy regarding emails. Emails on Sheriff's Office devices that were deleted by a user may be retrievable from the archive, backup system or the receiving or sending system.
- D. Upon receipt of a litigation hold letter placing a Sheriff's Office employee on notice that litigation is or may be forthcoming, the employee shall comply with the terms of the letter and shall:
  - 1. Suspend the deletion, overwriting or any other destruction of email and/or other electronic records and/or paper records relevant to the subject matter of said litigation, even if in the normal course of operations said records could be destroyed pursuant to the MA records retention schedule. The records subject to the requirement herein cover all electronic information wherever it is stored, including work computers, laptops or home computer if utilized for work. Such records include all forms of electronic communication (e.g. email, word processing, calendars, voice messages, video, photographs and information stored on a personal data storage device (PDA). Such records must be preserved in its original electronic form, available for inspection.
  - 2. Notify the Sheriff's Office Legal Services Division if he/she is aware, or becomes aware, that any email relevant to the subject matter of said litigation has been destroyed or deleted.
- E. Person-to-person conversations should occur when possible, particularly if discussing sensitive matters between employees.
- F. Emails (or texting) should not be sent or read with Sheriff's Office equipment while driving. The laws of the Commonwealth shall apply.
- G. The Sheriff's Office may revoke a user's ability to send/receive emails with department equipment.

#### **05.02.11 USE OF PERSONAL COMPUTERS AND MOBILE DEVICES WHILE ON DUTY**

- A. Personal mobile devices (cellular phones, laptops) may be used by an employee at their workstation during work hours, if so authorized by the employee's Immediate Supervisor. The following rules shall apply:
  - 1. Such employees may send/receive a justifiable amount of personal telephone calls, emails and text messages while on duty. They may also be able to use the internet from their personal device, if possible.



2. Such employees shall not photograph, videotape or record any activity with their personal mobile devices, unless so authorized to do so. For safety and security purposes, the placement of such photographs, videotapes or recordings onto any media site without proper authorization is strictly prohibited.
  3. Such employees should place such their personal mobile devices on either "silent", "vibrate" or minimize the volume of incoming alerts to a respectable level. This is to not disturb other employees. With a secured perimeter, the use of personnel cellular phones in/around inmates should be limited and only when necessary.
  4. Such employees job duties should not be compromised or suffer due to the excessive or improper use of such devices at their work station.
- B. Employees performing inmate security duties, such as Correctional Officers performing a hospital detail or a Law Enforcement Deputy Sheriff on a work detail, shall not use their personal mobile devices while on duty, except during official break periods or to communicate with proper officials during an emergency situation.
  - C. Employees who are not authorized to keep a personal mobile device at their work station shall store such items inside their motor vehicle or employee locker during work hours. These employees may be able to view and use the devices during approved breaks, time permitting.
  - D. The Sheriff's Office reserves the right to prohibit any employee from carrying their personal mobile device at their work station for security reasons or rule violation. This includes work stations outside a secured perimeter. Violators of this policy shall be disciplined accordingly.
  - E. The Superintendent shall approve the carrying of personal mobile devices inside a secured perimeter. An approved listing shall be maintained at Security Reception posts.

#### **5.02.12 WEBSITE MANAGEMENT**

- A. The Sheriff's Office shall maintain a website, which shall be available to for the general public. The website shall provide the public with pertinent information relative to the activities of the Sheriff's Office, such as media releases, statistical information, departmental forms, telephone numbers, addresses, policies, videos, etc.
- B. The Media Specialist shall be responsible for the overall web development and programming on the Sheriff's Office website. The Media Specialist is authorized for the placement of materials onto the website. Individual supervisors, however, shall be responsible for the content of materials placed onto the website relative to their operations/duties. These supervisors shall be responsible for providing the Media Specialist with updated materials for the website, as needed. It shall be the responsibility of these supervisors to monitor the content or updates of their website materials-not the Media Specialist.
- C. Employees interested in placing materials onto the Sheriff's Office website should complete a Media Request Form, for on the Shared/Dartmouth file within the intranet network. The request shall be reviewed by the Sheriff or his designee for approval and implementation. No employee or other individual is authorized to place materials onto the Sheriff's Office website without complying with these protocols.

#### **05.02.13 ENVIRONMENTAL PROTECTION**

- A. Every effort shall be made to ensure that adequate disaster suppression plans are developed to prevent damage to information technology systems and to detect potential environmental threats (fire, smoke, water and lightning) to the systems. The Sheriff or designee shall approve such plans. The ADS Technology shall ensure that all Local Area Network (LAN) servers and network connectivity equipment are maintained in a secure area with controlled access, which poses minimal threat of damage to the technology systems and has disaster prevention controls in place.
- B. Procedures for the Sheriff's Office network systems to identifying specific off-site storage facilities for LAN server backups should be integrated into the department's Emergency Response Plans.

#### **05.02.14 DISCIPLINARY ACTION**

- A. Employees who violate any aspect of this policy are subject to disciplinary action, up to and including termination and possible criminal prosecution. They may also be temporarily or permanently banned from having access to any issued Sheriff's Office mobile device or computer and/or have internet access on Sheriff's Office equipment. Only the Sheriff, or in his absence, the Special Sheriff has the authority to deny or reinstate an employee's access to such equipment or the internet. When so authorized, such decisions shall be communicated to the ADS Technology for implementation.

#### **05.02.15 EMPLOYEE TRAINING**

- A. Employees shall receive orientation training pertaining to the Sheriff's Office computer/information technology system. Refresher training may be provided routinely to employees during annual in-service, as determined by the Training Division.
- B. Computer/Information Technology training shall provide information on the use of information technology systems and specific applications. Training of computer hardware (computer stations, printers, etc.) should consist of a general overview of its utility, proper function and usage. Training of computer software should consist of a general overview and, when possible, in-depth training of specific software programs.
- C. Users who may use a particular software application will receive, when possible, training in the purpose, function and proper use of the software.
- D. The IT Department may perform an advisory role in the development of curriculum and course content for information systems training. User documentation in the form of a written guide and/or on-line help should assist the user in developing competency in the use of particular software whenever possible. Outside training may be provided as needed to improve competency or to develop basic proficiency in the use of a new or upgraded hardware or software program.
- E. Employees who use Sheriff's Office computers or other piece of technological equipment should familiarize themselves with applications pertinent to their duties. Should any questions arise, employees shall immediately contact their Immediate Supervisor, who shall communicate to the IT Department for clarification. Volunteers, part-time, and contractual, third-party, vendors should contact their Immediate Supervisors if they require computer training to complete their specific job responsibilities.



## REFERENCES

- M.G.L. c. 124, §1 (d) and (q); c. 127 §§ 1A and 1B.
- M.G.L. c. 30B, the Electronic Communications Privacy Act (Title 18 US Code, §§2501, et. seq. and 2701, et. seq.).

## APPLICABILITY

ALL EMPLOYEES

## PUBLIC ACCESS

YES

## LOCATION

The Sheriff's Office Central Policy Files, Policy Manuals and the Shared Policy File of the Sheriff's Office computer network

## RESPONSIBLE STAFF FOR IMPLEMENTATION AND MONITORING OF POLICY

The ADS Technology, the IT Department

## EFFECTIVE DATE

This policy is effective upon the signature of the Sheriff.

## CANCELLATION

This policy cancels all previous policy statements, bulletins, directives, orders, notices, rules and regulations regarding the Sheriff's Office Information Technology Department or systems to the extent that they are inconsistent with the requirements of this policy.

## SERVABILITY CLAUSE

If any article, section, subsection, sentence, clause or phrase of this policy is for any reason held to be unconstitutional, contrary to statute, in excess of the authority of the Sheriff or otherwise inoperative, such decisions shall not affect the validity of any other articles, section, subsection, sentence, clause or phrase of this policy.

## ANNUAL REVIEW DATE

The Sheriff or his designee shall review this policy annually from the effective date. The party or parties conducting the review shall develop a memorandum to the Sheriff with a copy to the Central Policy Files indicating that the review has been completed. Recommendations for revisions, additions or deletions shall be included.

## **EMERGENCY SITUATIONS**

Whenever, in the opinion of the Sheriff, the Superintendent or the Asst. Superintendent of Security, the reporting requirements outlined within this policy may be suspended up to 48 hours. The Sheriff shall approve any suspensions lasting beyond 48 hours of the emergency.

## **SANCTION FOR POLICY VIOLATION**

Employees who knowingly violate, permits the violation of, or who fail to report any violation, or the suspected violation of this policy shall be subjected to disciplinary action, up to and including termination, as well as criminal sanctions.

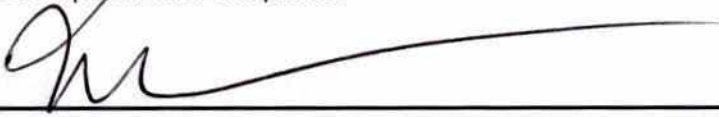


THE FOLLOWING HAVE REVIEWED AND APPROVED THIS POLICY (#05.02.00) AS TO FORM AND CONTENT



Michael F. Foley  
ADS/Policy Development and Compliance

8/4/17  
Date



Robert Novack, Esq.  
Sheriff's Office Legal Services

8-11-17  
Date



Steven J. Souza  
Superintendent

8/7/17  
Date



Thomas M. Hodgson  
Sheriff of Bristol County

08/14/17  
Date