



**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) 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.

