THE POLICIES AND PROCEDURES INCLUDED IN THIS MANUAL ARE NOT A CONTRACT OF EMPLOYMENT AND SHOULD NOT BE RELIED ON AS SUCH. THESE POLICIES AND PROCEDURES ARE SUBJECT TO AND MAY BE CHANGED AT ANY TIME BY THE DEPARTMENT OF PUBLIC SAFETY, MEDICAL UNIVERSITY OF SOUTH CAROLINA.

A. Overview

The intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to MUSC Department of Public Safety established culture of openness, trust and integrity. MUSC Department of Public Safety’s Security Team is committed to protecting MUSC Department of Public Safety’s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing, File Transfer Protocol, and National Crime Information Center access are the property of the MUSC Department of Public Safety. These systems are to be used for business purposes in serving the interests of the agency in the course of normal operations. Effective security is a team effort involving the participation and support of every MUSC Department of Public Safety employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

B. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at MUSC Department of Public Safety. These rules are in place to protect the employee and MUSC Department of Public Safety. Inappropriate use expose MUSC Department of Public Safety to risk including virus attacks, compromises of the network systems and services, and legal issues.
C. Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at MUSC Department of Public Safety, including all personnel affiliated with NCIC and third parties. This policy applies to all equipment that is owned or leased by MUSC Department of Public Safety.

D. Policy

1. General Use and Ownership

   a. While MUSC Department of Public Safety’s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the Corporate systems remain the property of the MUSC Department of Public Safety. Because of the need to protect MUSC Department of Public Safety’s network, management cannot guarantee the confidentiality of information stored on any network devise belonging to MUSC Department of Public Safety.

   b. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should consult their supervisor or management.

   c. MUSC Department of Public Safety technology section recommends that any information that a user considers sensitive or vulnerable (etc. residual NCIC information on a computer terminal that has access to the internet and CJIS information) be encrypted.

   d. For security and network maintenance purposes, authorized individuals within MUSC Department of Public Safety many monitor equipment, systems and network traffic at any time.

   e. MUSC Department of Public Safety reserves the right to audit the network and systems on a periodic basis to ensure compliance with this policy.

2. Security and Proprietary Information

   a. The user interface for information contained on Internet/intranet/Extranet-related systems should be classified as either confidential or non-confidential as defined by agency confidentiality guidelines. Examples of confidential information include, but are not limited to: NCIC information, state criminal history information, agency personnel data, and etc.
Employees should take all necessary steps to prevent unauthorized access to this information.

b. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

c. All workstations should be secured with password-protected screen savers with and an automation activation feature, set a ten minutes or less or by logging off (control-alt-delete) when the computer is unattended.

d. All devices used by employees that are connected to the MUSC Department of Public Safety Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current database.

e. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs or Trojan horse code.

3. Unacceptable Use

The following activities are, in general, prohibited. Under no circumstances is an employee of MUSC Department of Public Safety authorized to engage in any activity that is illegal under local, state, federal, or international law utilizing MUSC Department of Public Safety owned resources. The list below is by no means exhaustive, but attempts to provide a frame work for activities which fall into the category of unacceptable use.

4. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

a. Unauthorized access, coping, or dissemination of classified or sensitive information (e.g., NCIC information, state criminal information, etc.)

b. Installation of any copyrighted software for which MUSC Department of Public Safety or end user does not have an active license is strictly prohibited.

c. Installation of any software without pre-approval and virus scan is strictly prohibited.

d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, logic bombs, etc.).
e. Revealing your account password to others or allowing use of your account by others.

f. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For the purpose of this policy, “disruption” includes, but is not limited to, network sniffing pinged floods, packet spoofing, denial of service, and forged routing information of malicious purposes.

g. Port scanning or security scanning is expressly prohibited unless prior notification has been given to MUSC Department of Public Safety security administration.

h. Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is a part of the employee’s normal job/duty.

i. Circumventing user authentication or security of any host, network, or account.

j. Interfering with or denying service to any user other than the employee’s host.

k. Using any program/script/command or sending messaged of any kind, with the intent to interfere with or disable a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.

l. Providing information about NCIC or list of MUSC Department of Public Safety employees to parties outside MUSC Department of Public Safety.

5. Unique Identifier

a. The purpose of unique identifier is to ensure accountability of all users that access MUSC Department of Public Safety network and network devices. This section is to define the creation of a unique identifier for individuals that access MUSC Department of Public Safety network, network devices and NCIC information.

b. MUSC Department of Public Safety requires that each employee that has access to MUSC Department of Public Safety network, applications, and/or NCIC for the purpose of storing, processing, and /or transmitting information shall be uniquely identified by use of a unique identifier. A
unique identifier shall also be required for all persons who administer and maintain the system(s) that access agency and NCIC information and/or network. MUSC Department of Public Safety requires users to identify themselves uniquely before the user is allowed to perform any action on the network and/or applications. All user IDs shall belong to currently authorized users. Identification data shall be kept current by adding new users and disabling former users. Employees shall not share their IDs with other employees, supervisors, management, or family members at any time.

6. Password

   a. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of MUSC Department of Public Safety’s entire network. As such, all MUSC Department of Public Safety employees (including contractors and vendors with access to MUSC Department of Public Safety systems) are responsible for taking the appropriate steps to select and secure their password.

   b. The purpose of this section is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change. The scope of this section includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any MUSC Department of Public Safety facility, has access to the MUSC Department of Public Safety network and or NCIC network, or stores any non-public MUSC Department of Public Safety information. The general use of passwords creations, protections and frequency change are as followed:

       • All production system-level passwords must be part of the Information Security administrated global password management database.

       • All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days.
• User accounts with access to NCIC privileges must have a unique password from all other accounts held by that user.

• Passwords must not be inserted into email messages or other forms of electronic communication.

• All user-level, system-level, and NCIC access level passwords must conform to the guidelines described below.

c. General Password Construction- Passwords are used for various purposes at MUSC Department of Public Safety. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., Dynamic passwords which are used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

• The password contains less than eight characters.
• The passwords is a word found in a dictionary (English or foreign).
• The password is a common usage word such as:
  ➢ Name of family, pets, friends, co-workers, fantasy characters, etc.
  ➢ Computer terms and names, commands, sites companies, hardware, software.
  ➢ The words “MUSC,” “WVSP,” “HPD,” “CKSFP” or any derivation.
  ➢ Birthdays and other personal information such as addresses and phone numbers.
  ➢ Word or number patterns like aaabbb, 111222, zyxvwts, 4654321, etc.
  ➢ Any of the above spelled backward like nhoj, yrrehckcalb, yffulf, etc.
  ➢ Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

• Contain both upper and lower case characters (e.g., a-z, A-Z)
• Have digits and punctuation characters as well as letter, (e.g., 0-9, !@#$%&*(_+{}[]:"<>/?)
• Are at least eight alphanumeric characters long.
• Are not a word within any language, slang, dialect, jargon, etc.
• Are not based on personal information, names of family, etc.
• Passwords based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way to Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation. **NOTE: Do not use either of these examples as passwords.**

d. Password Deletion- All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to the following:

- When a user retires, quits, is reassigned, released, dismissed, etc.
- Default passwords shall be changed immediately on all equipment.
- Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed:

- Employee should notify his or her immediate supervisor
- Supervisor should fill out a password deletion form and send it to Agency’s POC
- Agency’s POC will then delete the user’s password and delete or suspend the user’s account
- A second individual from the department will check to ensure that the password has been deleted and user account was deleted or suspended.
- The password deletion form will be filed in a secure filing system.

e. Password Protection Standards- Do not use your user id as your password. Do not use the same password for MUSC Department of Public Safety accounts as for NCIC accounts. For example, select one password for your Windows account login and a different one for your NCIC account login. Do not share MUSC Department of Public Safety passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential MUSC Department of Public Safety information.

f. Here is a list of “do not’s”

- Don’t reveal a password over the phone to anyone
- Don’t reveal a password in a mail message
- Don’t reveal a password to the boss
- Don’t talk about a password in front of others
- Don’t hint at the format of a password (e.g., “my family name”)
- Don’t reveal a password on questionnaires of security form
- Don’t share a password with family members
• Don’t reveal a password to a co-worker while on vacation
• Don’t use the “Remember Password” feature of applications
• Don’t write passwords down and store them anywhere in your office
• Don’t store passwords in a file on ANY computer system without encryption.

7. Virtual Private Network (VPN)

This section applies to implementation of “VPN” that allows direct access to the SLED network through the internet.

a. Non-SLED employees and authorized third parties may not store any information obtained while connected to the SLED Network via VPN technology unless granted an exclusive waiver to do so by the Assistant Director for Information Services or his/her designee.

b. All computers connected to SLED networks via VPN or any other technology must use the most up-to-date anti-virus and anti-spyware software. Additionally, all relevant security patches must be installed in a timely manner.

c. Users of computers that are not SLED-owned equipment must configure the equipment to comply with SLED’s VPN and Network technical policies. These policies could be obtained from the SLED CJIS Information Technology Department

8. Media Protection

The intent of this section is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data) or is purged or destroyed in accordance with applicable record retention rules.

The scope of this policy applies to any electronic or physical media containing FBI/SLED Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the MUSC Public Safety Department. This policy applies to any authorized person who accesses, stores, and transports electronic or physical media. Transporting CJI outside the agency’s assigned physical secure area must be monitored and controlled. Authorized MUSC Public Safety Department personnel shall protect and control electronic and physical CJI while at rest and transit. The MUSC Public Safety Department will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent
or inappropriate CJI disclosure and / or use will be reported to the MUSC Public Safety Department Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

9. Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored or actively being accessed. “Electronic media” includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives or digital memory card. “Physical media” includes printed documents and imagery that contain CJI.

To protect CJI, the MUSC Public Safety Department personnel shall:

a. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

b. Restrict access to electronic and physical media to authorized individuals.

c. Ensure that only authorized users remove printed form or digital media from the CJI.

d. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.

e. Do not use personally owned information system to access, process, store, or transmit CJI unless the MUSC Public Safety Department has established and documented the specific terms and conditions for personally owned information system usage.

f. Do not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

g. Store all hardcopy CJI printouts maintained by the MUSC Public Safety Department in a secure area accessible to only those employees whose job functions require them to handle such documents.

h. Safeguard all CJI by the MUSC Public Safety Department against possible misuse by complying with policies.
i. Take appropriate action when in possession of CJI while not in a secure area:
   o CJI must not leave the employee’s immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
   o Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and / or privacy screens. CJI shall not be lift in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
   o When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
   o When encryption is employed, the cryptographic module used shall be certified to meet standards.

j. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.

k. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

10. Media Transport:
Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media, including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, kexternal hard drives, or digital memory card.

a. Dissemination to another agency is authorized if:

   1) The other agency is an Authorized Recipient of such information is being serviced by the accessing agency, or

   2) The other agency is performing personnel and appointment functions for criminal justice employment applicants.
b. The MUSC Public Safety Department personnel shall:

   1) Protect and control electronic and physical media during transport outside of controlled areas.

   2) Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

c. The MUSC Public Safety Department personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

   1) Use of privacy statements in electronic and paper documents

   2) Limiting the collection, disclosure, sharing and use of CJI

   3) Following the least privilege and role based rules for allowing access.

   4) Limit access to CJI to only those people or roles that require access.

   5) Securing hand carried confidential electronic and paper documents by:

      a) Storing CJI in a locked briefcase or lockbox

      b) Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

      c) For hard copy printouts or CJI documents:

         i. Package hard copy printouts in such a way as to not have any CJI viewable

         ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.
6) Do not take CJI home or when traveling unless authorized by MUSC Public Safety Department LASO. When disposing confidential documents, use a shredder.

11. Electronic Media Sanitization and Disposal:

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agency shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

12. Breach Notification and Incident Reporting:

The agency shall promptly report incident information to appropriate authorities. Information security events and weakness associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring and user/administrator reports.

13. Roles and Responsibilities:

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

a. MUSC Public Safety Department personnel shall notify his/her supervisor or LASO, and an incident report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident and steps taken / to be taken in response to the incident. (Agency Discretion).

b. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.

c. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.

d. The CSA ISO will:
1) Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

2) Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCS within their area.

3) Act as a single POC for their jurisdictional area for requesting incident response assistance.

14. Disposal of Media

The purpose of this section is to outline the proper disposal of media (physical or electronic) at MUSC Public Safety Department. These rules are in place to protect sensitive and classified information, employees and MUSC Public Safety Department. Inappropriate disposal of MUSC Public Safety Department and FBI Criminal Justice Information (CJI) and media may put employees, MUSC Public Safety Department and the FBI at risk. It applies to all MUSC Public Safety Department employees, contractors, temporary staff, and other workers at MUSC Public Safety Department, with access to FBI CJIS system and/or data, sensitive and classified data, and media. This policy applies to all equipment that process, stores, and transmits FBI CJI and classified and sensitive data that is owned or leased by MUSC Public Safety Department.

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by MUSC Public Safety Department.

Physical media (print-outs and other physical media) shall be disposed by one of the following methods:

a. Shredding using MUSC Public Safety Department issued shredders.

b. Incineration using MUSC incinerators or witnessed by MUSC Public Safety Department personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copiers hard-drives, etc.) shall be disposed of by one of MUSC Public Safety Department methods:

POLICY AND PROCEDURE # 108 NCIC Security
a. Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.

b. Degaussing – a method a magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.

c. Destruction- a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from MUSC Public Safety Department control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

15. Enforcement

Violations of this policy include, but are not limited to: accessing data to which the individual has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a way that violates applicable policy, procedures, or relevant regulations or law; inappropriately modifying or destroying data; inadequately protecting restricted data. Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, civil or criminal prosecution, and termination of employment.