

EMPLOYEE RESPONSIBILITIES 6-1010

Computer and Data Security 6-1010.1

Employees are responsible for the security of their assigned Department resources and the information under their control. The following steps are to be taken to protect computer equipment from theft, unauthorized use, and to ensure that Department systems and information privacy and security are not inadvertently compromised:

1. Employees shall use Department information and resources only for Department business purposes.
2. Employees accessing Department information assets shall use due care to preserve data integrity and confidentiality. Please refer to HAM Section 6-1050.
3. Employees shall not possess, or attempt to obtain, a network protocol analyzer, or similar device (including software) for capturing, and/or reading electronic signals from the State's computer network, without prior approval from the Information Security Officer (ISO).
4. Employees shall not possess, or attempt to obtain, password-breaking software (e.g., crack) used to guess employee passwords without prior approval from the ISO.
5. Employees shall not intentionally destroy, modify, or release computer programs or data, or introduce malicious code (such as a computer virus).
6. Desktop systems shall be kept in secure areas (i.e., a secure building or room) or shall be physically attached to a desk or table.
7. The use of surge protectors is required.
8. Unattended Personal Computer (PC) shall be protected with a password protected screen saver.
9. Employees are not authorized to turn off or disable virus-checking systems. Employees shall scan all diskettes or other media for viruses prior to use.
10. Employees shall complete annual training about the Department's information privacy and security policies and sign acknowledgments of their privacy and security responsibilities. (See HAM Section 6-1000.4 and 6-1000.6)
11. During normal work hours, personal, confidential, or sensitive information shall not be left unattended. If the area will be unattended, even for a few minutes, confidential information shall be locked up in a file cabinet, file room, desk, or office. Unattended means that information is not being observed by an employee authorized to access the information.
12. Visitors to secure areas shall be escorted, and personal, confidential, or sensitive information shall be kept out of sight while visitors are in the area.
13. During non-working hours, personal, sensitive, and confidential information shall be kept in a locked office, desk, file, or cabinet, even if the building is secured.
14. Once personal, confidential, and sensitive information has met designated retention periods, it shall be disposed of through confidential means (shredded, pulverized, etc.) with the destruction being witnessed by a state employee. Personal, confidential, and sensitive information ready for destruction shall not be stored in boxes in employee's cubicles or offices. Such information shall be deposited in locked, confidential, destruct bins or shredded on-site.

Passwords 6-1010.2

Employees are responsible for the confidentiality and security of their passwords. The following password protection requirements shall be met to secure data from unauthorized access:

1. Passwords are not to be shared.
2. Select an unusual combination of eight characters or more for a secure password. Avoid words with personal associations, such as names of family members or pets, favorite hobbies, sports, or vacation spots. Non-dictionary words are even more secure.
3. Keep passwords confidential, including passwords used for dial-up access. They are not to be written down, posted where they may be accessed, or included in a data file, log-on script, or macro.
4. Passwords are to be changed immediately if revealed or compromised.
5. Passwords are to be changed every 60 days.
6. Any suspected unauthorized use of a user identification (ID) or password is to be reported to one's supervisor and the ISO upon discovery.

Mobile Computing and Removable Storage Devices 6-1010.3

Purpose/Scope

For the purposes of this Policy, mobile, and removable storage devices are defined as any portable device, such as laptops, Personal Digital Assistant (PDA), Blackberries, tablet Personal Computer, or removable storage, such as compact disk (CD), Universal Serial Bus (USB) drive, diskette, or other devices that have the ability to store information.

Mobile computing has become an inherent part of doing business at the Department. Most mobile and removable storage devices have the capacity to store Department information. Because data can be portable, the Department shall ensure due diligence is taken to protect data appropriately. Employees shall take reasonable precautions for both the security of their devices and the information they contain.

1. The employee's Branch Chief and ISO shall approve all non-Department mobile and removable storage devices and such devices shall meet all of the requirements set forth in this Policy regarding mobile and removable storage devices.
2. All mobile and removable storage devices used for Department business purposes are subject to inspection and possible forensic analysis by Internal Audits, the Information Technology (IT) Division or the ISO at any time.
3. Please refer to HAM Section 6-1050 for handling and protection of confidential information.
4. All mobile devices shall meet Department software and hardware standards, including data encryption.
5. Mobile devices shall be configured with the approved IT Division build unless an exception has been granted by the Chief Information Officer (CIO) and ISO.

Allocation

1. All mobile devices issued to employees remain the property of the Department.
2. Upon termination of Department employment, the individual shall return the Department mobile device(s) to his or her LAN Administrator or supervisor.

Physical Security

1. Mobile devices shall not be left unattended at the worksite at any time. When taken off the worksite premises, mobile devices shall not be separated from employees at airports, automobiles, or hotel rooms.
2. Mobile devices used at an assigned workstation shall be cable-locked to an immovable surface, or removed from a docking station and placed in lockable storage whenever the user leaves the workstation.
3. Users shall take precautions to ensure other persons cannot view on-screen data in public locations.
4. The identification number of the mobile device shall be recorded and kept separately in a safe place. It shall not be stored with the mobile device or in the carrying case.

Access Control/Authentication

1. Mobile devices shall be protected by a power-on password.
2. All non-Department mobile devices (i.e., devices belonging to contractors or other entities) connecting to the network shall meet the following criteria:
 - a. Must be approved by the ISO and the employee's Branch Chief.
 - b. Connections are only permitted via approved communication paths.
3. At a minimum, all access shall be authenticated locally.
4. A disk drive lock is to be installed with the mobile device.
5. Laptop computers shall employ an ISO approved software firewall.