

**Office of the Chief Information Officer  
Enterprise Policy**

**Policy Number:** CIO-083

**Effective Date:** 01/18/2010

**Subject:** Storage of Confidential Information on Portable Devices and Media

**Policy Statement:** This policy requires all portable computing and storage devices containing confidential data to be encrypted in order to protect the confidentiality, availability, and integrity of the Commonwealth's information technology resources. Portable devices covered by this policy include but are not limited to: laptops, mobile telephones, USB thumb drives and portable hard drives. This policy supports the principles of the Enterprise Security Architecture as expressed in [Enterprise Security Domain 5000](#).

**Applicability:** This policy is to be adhered to by all employees and contractors ('personnel') engaged with agencies within the Executive Branch of state government ('users').

**Responsibility for Compliance:** Each agency is responsible for enforcement of this policy and assuring that personnel within their organizational authority are aware of the provisions of this policy, that compliance by personnel is required, and that intentional, inappropriate use may result in disciplinary action pursuant to [KRS 18A](#), up to and including dismissal.

**Policy Maintenance:** The Commonwealth Office of Technology, Office of the Chief Information Security Officer, has the responsibility for the maintenance of this policy. Agencies may choose to add to this policy as appropriate, in order to enforce more restrictive standards. Therefore, employees are to refer to their agency's internal policy, which may have additional information or clarification of this enterprise policy.

**Policy:**

The Commonwealth discourages the placement (download, copy or input) of confidential data on portable devices. Storage on such devices is permitted only if the following requirements have been satisfied:

- Use is restricted to specific individuals requiring such data to perform their job duties.
- Storage is for a limited, defined period of time as required to perform specific job duties.
- Approval has been obtained by the system/data owner for such
- Information should be abbreviated, if possible, to limit exposure (e.g., last 4 digits of the social security number)
- Sensitive data has been encrypted.

**Unencrypted storage of confidential data on portable devices and/or portable media is strictly prohibited.**

If confidential data is placed on any mobile devices, that device shall have automatic full encryption that does not require user intervention nor allow user choice to implement.

If confidential data is stored on a mobile device, it is the department's responsibility to ensure that the mobile device supports the Commonwealth approved encryption software and that all appropriate information is encrypted that resides on this device.

In the event the mobile device is lost or stolen, the department must be able to recreate the confidential data with 100 percent accuracy and must be able to provide notification to the affected persons/entities, if necessary (see [COT-F107 Data Breach Determination Form](#)).

Any actual or suspected loss or disclosure of confidential data shall be immediately reported to the agency's security organization and the COT Security Administration Branch in the office of the Chief Information Security Officer. In all cases, every attempt must be made to assess the impact of storing, and to mitigate the risk to, confidential data on all mobile devices.

The following points provide additional policy direction that should be followed to reduce the risk of security breach or compromise.

- Only portable computing devices owned or leased by the Commonwealth or being utilized for official business (contractors, employee's personal devices) are to be connected to the Commonwealth's networks, servers and other computers. Exemptions to this policy must be approved by the agency/cabinet chief information officer. Approved Exemptions must comply with this policy.
- Portable computing devices must not be used for Commonwealth business unless they have first been configured with the necessary controls and approved for use by the Agency/Cabinet chief information officer.
- If possible, devices that are lost or stolen should be deactivated immediately by appropriate agency security staff to prevent possible security breach or compromise.
- Portable computing devices connected to the Kentucky Information Highway must comply with all policies and procedures pertaining to that environment.
- Confidential information must not be transmitted to or from a portable computing device unless approved transmission protocols and security technologies are utilized, i.e. encryption, VPN, etc.
- Devices must be password protected. Boot and logon passwords must be employed where feasible. Password usage and composition rules must adhere to the [Enterprise UserID and Password Policy \(CIO-072\)](#).
- Inactivity/timeout settings that automatically lock the device must be enabled where possible. Settings should be configured to comply with [Securing Unattended Workstations Policy \(CIO-081\)](#).
- Portable computing devices are prohibited from being used by anyone other than the user to whom the device was assigned.
- Devices must employ current virus protection software and definition files, where feasible, and adhere to the [Enterprise Anti-Virus Policy \(CIO-073\)](#).
- Devices must be physically secured when not in use by locking them in desk drawers, filing cabinets, or other secure areas.
- Devices that use wireless technologies such as BlueTooth and 802.x should not broadcast their presence or be left enabled when not in use.
- Devices containing confidential data should not be connected to unsecured Wi-Fi 'hotspots'.

#### **Definitions:**

Confidential - Information that is specific and personal in nature that could be used to negatively impact the Commonwealth or individuals through identity theft, fraud, or an invasion of privacy. This information falls under the restrictions of confidential information but may also have additional regulatory compliance standards that shall be met. Unauthorized disclosure of this information is considered very serious and could have a severe adverse impact on the Commonwealth or individual(s). For additional information and other data classifications see: [Enterprise Standard 4080 Data Sensitivity Classification Matrix](#)

Portable Devices: Electronic computing and communication devices designed for mobility, including laptop, desktop, and in-vehicle personal computers, personal data assistants (PDAs), cellular devices, and other devices that have the ability to store data electronically.

Portable Electronic Storage Media (Portable Storage): Includes floppy disks, CDs, DVDs, optical platters, flash memory drives, backup tapes, and other electronic storage media or devices that provide portability or mobility of data.

**References:**

- CIO-072 Enterprise UserID and Password Policy:  
<https://gotsource.ky.gov/dsweb/Get/Document-13212>
- CIO-073 Enterprise Anti-Virus Policy:  
<https://gotsource.ky.gov/dsweb/Get/Document-13213>
- CIO-081 Securing Unattended Workstations Policy:  
<https://gotsource.ky.gov/dsweb/Get/Document-35939>
- COT-F107 Data Breach Determination Form  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-179690>
- Enterprise Standard 4080 Data Sensitivity Classification Matrix:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301107/>
- Enterprise Security Domain 5000:  
<https://gotsource.ky.gov/docushare/dsweb/Get/Document-301110/>
- KRS 18A:  
<http://www.lrc.ky.gov/KRS/018A00/CHAPTER.HTM>