

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.8	Information Security	Revised:	February 2012
Policy 5.8.12	Portable Computing Policy	Responsibility:	Chief Information Security Officer

PORTABLE COMPUTING POLICY

Overview

The purpose of this policy is to establish the rules for the use of mobile computing devices and their connections to the University's network. These rules are necessary to preserve the integrity, availability, and confidentiality of sensitive and/or confidential information. This policy applies to any portable device used to access or store sensitive/confidential information and/or to conduct business for both institutional and privately owned/funded devices.

Policy

Only approved portable computing devices may be used to access the Health Science Center's information resources and computer network. See the *Handbook of Operating Procedures* (HOP), [Section 5.8.7](#), "Network Access Policy".

As a general practice, sensitive/confidential information must only be stored on servers located in an approved data center. Data owners must carefully evaluate the risk of lost or stolen data against efficiencies related to mobile computing before approving the storage of sensitive information on portable computing devices.

All laptops and tablet PCs purchased with University funds or grants must be encrypted with the University's enterprise-wide whole disk encryption solution regardless of the device's intended usage. All other portable devices, including but not limited to, USB drives, external hard drives, personal digital assistants (PDAs), smart phones, iPads and personally owned laptops that are used to conduct University business must, at a minimum, encrypt sensitive/confidential data using techniques approved by the Chief Information Security Officer (CISO).

Data owners and data custodians are responsible for ensuring the availability of data created and/or stored on a portable computing device using appropriate back-up processes and supported back-up devices. In the event of loss, damage, or theft, appropriate steps must be taken to ensure recoverability. Various methods may be used to meet this requirement, including but not limited to:

- Use of a Health Science Center approved server or approved central storage as the primary repository for data accessed, created, updated, and stored on mobile devices.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.8	Information Security	Revised:	February 2012
Policy 5.8.12	Portable Computing Policy	Responsibility:	Chief Information Security Officer

-
- Use of an enterprise supported encryption solution that provides emergency access to facilitate recovery.
 - For other encryption technologies, the encryption key must be escrowed with a trusted party, preferably the departmental administrator.
 - Use of other methods approved by the CISO.

Users of portable computing devices who access and log onto the Health Science Center's network are required to use the institution's approved secure remote access methods, such as Virtual Private Network (VPN) or Secure Sockets Layer (SSL).

All reasonable precautions to prevent data compromise should be taken when using portable computing devices, such as ensuring the screen is shielded from passive viewing, that the system is not left unattended and logged in, and that a password protected screen saver is deployed.

Physical Security

Unattended portable computing devices must be physically secure. The device should be locked in an office, locked in a desk drawer or filing cabinet, or attached to a desk or cabinet via a cable lock system. In an automobile, secure the laptop in a non-visible location.

While traveling, do not leave the portable computing device unattended. If staying in a hotel, use a cable-lock system when the portable computing device is in not use. It is recommended that the portable computing device be stored in a hotel lock box, if the user intends to leave it in the hotel room for an extended period of time.

Portable computing devices that are Health Science Center property must follow appropriate property guidelines when taking them to and from campus. Rules for "Property Removal" can be found in [Section 6.3.8](#), "Property Removal Permit", of the HOP.

Reporting

Missing or stolen Health Science Center portable computing devices must be reported by the person responsible for the device to University Police, IT Security and the Office of Regulatory Affairs & Compliance as soon as practical. When reporting, the user should know the type,

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.8	Information Security	Revised:	February 2012
Policy 5.8.12	Portable Computing Policy	Responsibility:	Chief Information Security Officer

classification, and amount of information that resided on the device, and be prepared to estimate the impact of the loss against the institution's mission. The IMS Service Desk must also be contacted so that access can be denied to anyone trying to use the device on the institution's network.

Data compromise, in any form, should be directed to the department Technical Support Representative (TSR) or [IMS Service Desk](#) using the incident reporting process. A lost or stolen non-Health Science Center device containing Health Science Center sensitive information is considered a reportable data compromise.

Exceptions

To address a specific circumstance or business need, the CISO may grant an exception to the encryption requirements for portable devices. An exception request requires written justification from the data owner, as well as documentation of compensating controls. The data owner must have the approval of their Dean, Director or Department Chair prior to seeking the CISO's approval. An individual cannot approve an exception without a supervisor's approval.

Accountability

Departmental

Deans, Chairs, and Directors are accountable for ensuring their department remains in compliance with all applicable local, state, and federal information security policies as described in [Section 4.9.2](#) of the HOP, "Management's Responsibilities". If the Health Science Center network, systems, data, or mission are placed at risk due to a willful or negligent lack of compliance with information security policies, Information Management and Services (IMS) personnel are authorized to terminate service as appropriate to mitigate the risk. Additionally, IMS is authorized to assess the department a service fee for security remediation and/or reconnection of services. The service fee will be charged to the department's state funds account.

Individual

Violations of this policy are subject to disciplinary action as described in [Section 2.1.2](#), "*Handbook of Operating Procedures*", of the HOP.