Policy Number:	**700.1**
Policy Title:	**Information Technology Security**
Subject:	**Section 700 – Information Technology**
Date Adopted:	**May 16, 2014**
Date(s) Revised:	
Approved by:	**Daniel J. Bingham** **Dean/CEO** **Helena College University of Montana**

POLICY STATEMENT:

Except as explicitly approved by the Director of Information Technology (IT) Services, IT Services has full responsibility for all wired and wireless telecommunications; electronic information; and computing infrastructure on campus. IT shares responsibilities related to the installation of facilities with the Director of Facility Services; however, IT has sole responsibility for the functional aspects of the campus telecommunication, information, and computing infrastructure. As such, the Director of IT Services, in consultation with the IT Committee, will create procedures to safeguard the telecommunication, information, and computing infrastructure of Helena College. It is the responsibility of all Helena College employees to follow the procedures established under this policy.

In order to fulfill its mission to support instruction, research, and public service, Helena College is committed to provide a secure campus network that protects the integrity and confidentiality of information accessible over the network, and the integrity and operation of services available on that network.

PROCEDURES:

Each member of the campus community is responsible for the security and protection of electronic information resources assigned to his/her control. Resources to be protected include networks, computers and other electronic devices, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized use, unauthorized intrusions, malicious misuse, and inadvertent compromise (e.g., environmental disasters, operator error). Any information technology activity out-sourced to an off-campus entity must comply with the same security requirements applied to in-house activities.

The IT staff has the primary responsibility for the network as a whole, as well as operational control over all components of the network infrastructure and authority over all devices attached to the network. Department-based staff have operational control over devices attached to the network. Both central and department-based staff have responsibilities for identifying and isolating possible threats. This implies that monitoring network activity may be part of their normal job duties. When such activities occur they must be done in accordance with applicable law and policy (see Helena College Policy 700.5).

Insufficient security measures at any level may allow resources to be damaged, stolen, subverted, or otherwise to become a liability to the campus. Therefore, each department that has responsibility for devices attached to the network must assure that its devices meet minimum standards (see Helena College Policy 700.2) and identify a single point of contact for questions or problems associated with those devices (see Helena College Policy 700.3). If/when network threats and/or security problems occur, the IT staff will work with departments to reduce the impact of the problems, which may require aggressive action to be taken (see Helena College Policy 700.4). For example, if a situation is deemed serious enough, a device attached to the campus network that poses a threat to the network or to other attached devices may have its network access blocked (see Helena College Policy 700.4).

ROLES AND RESPONSIBILITIES

Responsibilities range in scope from security controls administration for large systems to the protection of one's own account information (e.g., user name and password). A particular individual often has more than one role.

A campus administrative official must:

- identify the electronic information resources under his/her control;
- define the purpose and function of the resources and ensure that requisite education and documentation are provided to campus users to assure use consistent with this purpose and function;
- establish acceptable levels of security risk for each resource, assessing factors such as the sensitivity of the data (e.g. research data, information protected by law or other policy); the level of criticality or overall importance to the continuing operation of the campus as a whole, individual units, research projects, or other essential activities; how negatively the operations of one or more units would be affected by unavailability or reduced availability of the resource; how likely it is that a resource could be used as a platform for inappropriate actions directed towards other resources; and limits on available technology programmatic needs costs, and staff support.

An electronic information resource provider must:

- become knowledgeable regarding relevant security requirements and guidelines;
- analyze potential threats and the feasibility of various security measures in order to provide recommendations to administrative officials;
- implement security measures that mitigate threats in a manner consistent with the level of acceptable risk established by administrative officials;
- establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- communicate the purpose and appropriate use for the resources under his/her control.

An electronic information resource user must:

- become knowledgeable about relevant security risks, requirements, and guidelines;
- protect the resources under his/her control, such as access passwords, computers and other devices, and data.

Other entities with important responsibilities for electronic information resources include the campus Network Director, the Information Technology Committee (ITC), and the campus IT Director, Leadership team, and CEO/Dean.

KEY SECURITY ELEMENTS

Logical Security. Devices attached to the Campus Network must have the most recently available and appropriate software security patches installed and running, commensurate with the identified level of acceptable risk. For example, a system that provides unrestricted or broad access to resources must be configured with extra care to minimize security risks. Adequate authentication and authorization functions must be used, commensurate with appropriate use and the acceptable level of risk. Attention must be given not only to large central systems but also to smaller systems which if compromised could pose a threat to on- or off-campus resources, including individual computers maintained for use by a small group or individual.

Physical Security. Appropriate controls must be employed to protect physical access to resources commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server systems are located to simple measures taken to protect an individual display when that display is unattended.

PRIVACY AND CONFIDENTIALITY

Programs and user interfaces must be designed and computers must be used so as to protect the privacy and confidentiality of the electronic information they possess, in accordance with applicable laws and policies.

Users authorized to obtain information must ensure that such information is protected to the extent required by applicable laws and policies after they obtain it. For example when sensitive data is transferred from a well-secured central system to a user's desktop computer adequate security measures must be in place for the desktop computer to assure that it protects the data in a manner consistent with the protection provided by the central system.

Technical staff assigned to ensure the proper functioning and security of electronic information resources and services are not permitted to search or monitor the contents of communication or transaction logs except as provided under existing Board of Regents policy, notably 1302 – 1307.

COMPLIANCE WITH LAW AND POLICY

Each campus unit should establish security guidelines, standards, and/or procedures that refine the provisions of this Policy for the specific activities under their purview, in conformance with this Policy and applicable laws and policies.

Policies that apply to all campus electronic information resource security include but are not limited to Board of Regents IT Policies 1300 – 1307. In addition, numerous state and federal laws prohibit theft or abuse of computers and other electronic resources.

The following activities are specifically prohibited under this Policy:

- interfering with, tampering with, or disrupting resources;
- intentionally transmitting any computer virus, worm or other malicious software across the Campus Network to a point inside or outside of the Campus Network;

- attempting to access, actually accessing, or exploiting resources one is not authorized to access or exploit;
- knowingly enabling inappropriate levels of access or exploitation of resources by others;
- downloading sensitive or confidential electronic information to computers that are not adequately configured to protect it from unauthorized access; and/or
- disclosing any electronic information that one does not have a right to disclose.

RESOURCES

Questions about this Policy or other related policies may be directed to the Campus Information Technology Director, Leadership team, or the Dean/CEO.