Policy Number:	**700.2**
Policy Title:	**Minimum Security Standards for Networked Devices**
Subject:	**Section 700 – Information Technology**
Date Adopted:	**May 16, 2014**
Date(s) Revised:	**February 9, 2023**
Approved by:	**Sandra J. Bauman** **Dean/CEO** **Helena College University of Montana**

POLICY STATEMENT:

Except as explicitly approved by the Chief Information Officer (CIO), IT Services has full oversight and discretion for all wired and wireless telecommunications, electronic information, and computing devices attached to the College's network infrastructure. As such, the CIO, 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, students, and guests to follow the procedures established under this policy.

The Helena College's ability to provide a campus network that protects the integrity of accessible information and services depends to a very large degree on the level of security maintained for each device connected to that network, so it is reasonable and prudent to define minimum standards each device must meet if it is to be attached to the network.

Helena College policies shall adhere to and be consistent with relevant federal and state laws, rules, and regulations, and with the Board of Regents' policies and procedures.

PROCEDURES:

Access to and use of campus network services are privileges accorded at the discretion of Helena College, regulated in large part by existing Board of Regents, Montana University System, and University of Montana policies. Each device connected to the Helena College campus network must comply with minimum security standards, listed in Appendix A, as established by the Information Technology Committee (ITC), Helena College's CIO. Devices that host particular systems or data may be subject to additional, more rigorous standards (e.g. the Banner system and its data, data associated with research projects for which there are special or externally defined security constraints). A campus unit may develop stricter standards that apply to devices under its control, but may not adopt standards that are less strict or in conflict with central standards defined in this policy. Devices that do not meet minimum standards may not be connected to the campus network, except for temporary connection of legacy devices as outlined in Appendix A.

Mandatory compliance with minimum security standards helps protect individual devices, other devices attached to the network, and campus resources as a whole. The Helena College encourages the use of its network in support of instruction, research, and public service, but because this resource is limited and vulnerable to attack, Helena College reserves the right to deny access to the network by devices that do not meet its standards for security.

The policy applies to all devices connected by wired or wireless connections to the network, independent of whether those devices are connected behind a local firewall, network address translation (NAT) system, or any other device designed to logically isolate a subnetwork from the main campus network.

RESPONSIBILITIES:

The following responsibilities are assigned to various members of the campus community for compliance with the policy.

Each campus administrative official must ensure that devices connected to the network by his/her unit comply with the standards and are supported by an administrator or user with the ability to ascertain and maintain minimum security standards.

Each system administrator (or user functioning as his/her own device administrator) must ensure compliance with minimum security standards for devices under his/her control.

The Information Technology Committee:

(a) provides direction, planning, and guidance about information security;
(b) develops and reviews campus-wide information security policy and procedures;
(c) develops and maintains minimum security standards for networked devices; and
(d) makes recommendations to the CIO and/or Dean's Cabinet concerning any requests to waive or grant an exception to any part of the minimum-security standards.

The Chief Information Officer

(a) works with the campus community to protect computers and the campus network from attack;
(b) works with units responsible for systems and information subject to additional special security guidelines to assist in protecting those systems and data, as well as to meet any special compliance requirements; and
(c) when necessary, approves the logical disconnection of a device from the Network (see Helena College Policy 700.4).

Each unit and individual user must:

(a) Use only those network-attached devices that comply with the minimum-security standards; and
(b) Accept responsibility as the system administrator in the absence of an assigned system administrator.

STANDARDS:

Minimum security standards for devices attached to the Helena College Network are specified in Appendix A: Minimum Device Standards. These standards change periodically; the most recently adopted standards will be published online on the College's IT Office website. Network device administrators and users must consult the online version frequently to make sure they are working with the newest version of the standards. Implementation guidelines for each of the specific standards in Appendix A are linked point by point online, and collected in Appendix B: Implementation Guidelines for Minimum Device Standards.

A unit with an existing (legacy) device/system that is unable to comply with the minimum security standards but wishes to continue to connect to the Network must request a temporary waiver from the CIO. Such a request must address the particular compliance problem and outline a plan to upgrade or replace the device/system to become compliant. Requests should be sent to the CIO, who will make a recommendation for review by the IT Committee and a final decision by the CIO and/or Leadership team. Unless and until such a waiver is granted, non-compliant legacy devices/systems must be disconnected.

A unit wishing to connect a new non-compliant device/system to the Network must request a waiver from the CIO before connecting the device/system. This request should address the same points described above, and again be sent to the CIO for final decision by the IT Committee.

Decisions by the CIO may be appealed by either the requesting unit or the IT committee to the Dean/CEO. The Dean/CEO's decision will be final.

Revisions to the minimum standards (i.e., revisions to Appendix A) will be periodically considered and approved by the CIO. Both proposed and approved revisions will be posted on the College's IT Office website, and those who have expressed a prior interest in being notified of pending or approved changes will be notified by some appropriate means (e.g., email or something comparable). It is the responsibility of the CIO and ITSC to post these notices and alert those who have expressed interest in new postings. It is the responsibility of administrative officials, systems administrators, and users to check periodically for revisions and maintain compliance when the standards change.