Policy Number:	**700.4**
Policy Title:	**Guidelines and Procedures for Blocking Network Access**
Subject:	**Section 700 – Information Technology**
Date Adopted:	**November 24, 2014**
Date(s) Revised:	
Approved by:	**Daniel J. Bingham** **Dean/CEO** **Helena College University of Montana**

POLICY STATEMENT:

This policy is intended to ensure that the confidentiality, integrity, and availability of the information assets residing in the Helena College infrastructure are preserved. To keep the network secure from viruses, spyware, and malware, device connection to the network requires that certain requirements must be met. Helena College IT reserves the right to suspend services that cause network disruptions, interrupt general resource availability, or are perceived to be a threat to the Helena College network.

All Helena College policies shall adhere to and be consistent with relevant federal and state laws, rules, and regulations; with Board of Regents' policies and procedures; and with The University of Montana's policies and procedures.

PROCEDURES:

IT staff must take immediate action to mitigate threats that have the potential to pose a serious risk to the Campus Network, resources attached to the Campus Network, or external networks. Acceptable actions including logically disconnecting devices attached to the network, AKA by "blocking" those devices, or in extreme circumstances working with appropriate University personnel to physically disconnect a device.

Central campus network and security personnel have the responsibility of evaluating the seriousness and immediacy of any threat campus information system resources or external networks, and the authority to take action to mitigate that threat. Action that is taken must be responsible and prudent, based on the risk associated with the threat and the potential negative impact on the campus mission caused by blocking access to the offending resource(s). Actions also must produce an auditable log, by following the specific procedures outlined below. Examples of threats that are serious enough to invoke these procedures include but are not limited to:

- the level of network activity is sufficiently large as to cause serious degradation of the performance of the network;
- an attack is being or has been launched on another resource or external network;
- confidential, private or proprietary electronic information or communication is being collected or distributed;
- one or more questions about inappropriate activity have been directed to a unit through a security incident report and no response has been received from the unit; and/or
- there is clear indication that system administrative privilege has been acquired by someone not authorized to have it.

If the threat is immediate, the offending resource will be blocked immediately, without prior warning – concurrently a security incident report will be sent to the appropriate security contact explaining that and why blocking has occurred. If there is reason to believe that blocking will affect the contact persons' ability to receive the email notification, attempts should be made to follow up as soon as possible with contact via telephone.

If the threat is not immediate, a security incident report will be sent to the appropriate security contact explaining the threat and the potential for blocking. If an appropriate response is not received within four hours, the offending resource(s) will be blocked.

In either case network personnel will work with system administrators to ensure that the resources in question are properly secured as soon as possible. If a block has been imposed, it will be removed when both unit and central security personnel agree that the problem causing the incident has been sufficiently addressed.

Security incident notification and response logs represent the minimum log for an incident. Any other pertinent email or other exchanges should also be logged in some manner to permit a complete post-incident review.

If a unit feels that one of its resources has been inappropriately blocked it may request a review of the decision by the IT Director or the CEO/Dean. If after review there is still disagreement with the decision it may be further reviewed by the IT Committee and /or Leadership team.