Policy Number:	**700.3**
Policy Title:	**Department Security Contact**
Subject:	**Section 700 – Information Technology**
Date Adopted:	**November 24, 2014**
Date(s) Revised:	**January 14, 2021**
Approved by:	**Sandra J. Bauman** **Dean/CEO** **Helena College University of Montana**

POLICY STATEMENT:

The purpose of this policy is to identify a primary and secondary point of contact in each department responsible for electronic devices attached to the network to ensure that departments can be contacted in the event of an incident associated with those devices. The ability to quickly contact responsible departmental personnel and have them take appropriate action can mitigate the negative effects of an incident, both locally in the department and more globally throughout the campus and the Internet.

All 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:

Helena College's ability to provide a Campus Network that protects the integrity of information and services available on that network depends, to a very large degree, on its ability to identify a point of contact for each device connected to that network.

Each unit with electronic information resources under its control (see Helena College Policy 700.1) must appoint a primary security contact person, plus one or more secondary (backup) contacts. Current email addresses and campus phone numbers for both the primary and secondary staff members must be registered with the central IT Office. If/when a question or problem arises involving a particular resource, central IT staff will immediately attempt to contact the designated contact person for that resource via email or by phone if email is not available.

Messages sent to the unit security contact person may be simple questions or notifications, or they may represent clearly labeled security incident reports. Each security contact person (or his/her backup) must respond to a security incident report promptly, or be prepared to forward the message to a technical contact within his/her unit who will respond. That is, the contact person may be a technical person or may simply be responsible for forwarding information to an appropriate technical person within the unit, but either way, the unit has the responsibility to respond. Groups of units may agree to share contact persons to promote efficiency.

Failure for a unit to respond to a security incident report promptly may result in one or more resources under that unit's control being "blocked" from network access (see Helena College Policy 700.4 – Guidelines and Procedures for Blocking Network Access).

Communication associated with security incident reports may utilize email or some other messaging capability, but must be conducted in a manner that assures that both incident reports and responses are logged, and that the log is preserved for post-incident review and analysis.

Procedures related to this Policy are outlined in Appendix A: Procedures Related to Unit Contact Personnel. These include how a unit specifies or changes its unit contact information, and how communication needs to be conducted for security incident reports and responses. If Appendix A is not available, contact the Director of IT Services.