Policy Number:	**700.5**
Policy Title:	**Guidelines for Use of Network Data Reports**
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:

Helena College shall protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of information to authorized users. For an effective approach to information security, the participation and support are required of all Helena College staff, students, and other authorized users of its information technology systems. Monitoring and logging of Helena College systems may be carried out in order to help protect the safety of the user community and to preserve the confidentiality, integrity, and availability of the data held upon Helena College information systems.

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 may need to monitor and analyze network activity in order to isolate, identify, and respond to threats that have the potential to pose a serious risk to the Campus Network, resources attached to the Campus Network, or external networks. Care must be taken to assure that this analysis is consistent with the processes and limitations defined in Board of Regents policies 1301 – 1307.

As part of their assigned job duties IT staff may normally maintain and access logs of network activity, but only at the least invasive level necessary to do their jobs. In response to reported or perceived threats, IT staff may initiate more detailed and/or special logs as required to determine if an actual threat is present, and if so, to help isolate and identify the nature of the threat.

If at any point the activity of a particular person or persons (vs. activity associated with a device) becomes suspect, the IT staff member must follow Board of Regents policies 1301 – 1307 to gain specific approval to monitor the activity of that person or persons.

Logs may be routinely created centrally or within a unit to collect activity, load, or transaction data required to assist in the management of the corresponding resources. Data collected centrally may be shared with a unit; data collected within a unit may be shared with central staff. However, in all aspects of data collection and sharing care must be taken to not impinge on the expectations of privacy afforded in Board of Regents policies 1301 – 1307, and in the event that potential misuses of resources are detected, to follow the specific processes outline in those policies.