

Policy and Procedure

Policy Number: 701R1

Date: 9/19/2000

Revision Date: 10/28/2013

Division/Department: Information Systems

Author(s): Ken Ries
R1; Ken Ries

Subject: Information Security

Authorities: MnSCU Policy 5.23 Security and Privacy of Information Resources, Policy 5.22 Acceptable Use of Computers and Information Technology Resources, and Procedure 5.22.1 Acceptable Use of Computers and Information Technology Resources.

Purpose: Authentication and access control systems are in place to protect the interests of all users of College information technology resources and ensure compliance with applicable law and policy. The purpose of this policy is to define essential roles and responsibilities for those responsible for granting, and revoking access to information technology resources.

Policy: It is the policy of the College to protect the security and privacy of its information resources and to make information accessible as required by law. The College shall maintain the confidentiality, integrity and availability of information resources; ensure continuity of operations; prevent, control and minimize the impact of security incidents; and manage risks to those resources regardless of the storage medium, transmission or disposal methods.

Procedure: Every College managed information technology systems requiring authentication must have a clearly defined process for requesting, approving, granting, and revoking access to resources contained within the system.

The following elements must be included in each procedure:

1. The process for requesting, approving, granting, and revoking access to resources contained within the system
2. The roles and responsibilities for each individual involved in the process
3. The method of documenting compliance with this policy

Defined processes are included in Appendix 1, Information Security Process.

Responsibilities:

It is the responsibility of every individual involved in approving or revoking access to information technology systems to define a process in compliance with this policy. Changes to Appendix 1 should be submitted to the helpdesk via email. It is the responsibility of all users to comply with this policy and the processes defined in Appendix 1.

Dissemination: All employees

Reviewed by Campus Roundtable: 09/25/2000, 10/28/2013

Approved: 09/25/2000, 10/28/2013

Approved: _____ **Date:** _____
Robert L. Musgrove, President