Colby College Information Systems and Data Security Policy

Information Technology Services

Purpose

To foster an environment where Colby's information systems, resources and data are available to those who need them, secured commensurate with their value, and in which both the data administrators and individuals who use those data understand their roles and responsibilities as stewards of this information.

General Policy

Each member of the Colby community is responsible for the security of electronic resources under his or her control. These resources include computers, networks, software and data in various physical and electronic forms. The security and integrity of these resources must be protected against compromise and any unauthorized use or misuse. Any use of college data by off-campus entities (auditors, consultants, investigators, etc.) must adhere to the same security policies and guidelines as on-campus individuals and departments.

Roles and Responsibilities

The Director of Information Security, in collaboration with the Information Systems and Data Security (ISDS) working group, ITS staff and College officers and staff having legal and policy expertise and authority regarding information management at Colby:

- Recommend policies with regard to the security and integrity of college information systems, resources and data.
- Define, document and implement approved information security technology, practices and procedures.
- Facilitate communication and training on security policies and procedures.
- Ensure available support to members of the College community for all information security policies, procedures and related technology.
- Meet on a regular basis to review policies and procedures and assess the effectiveness of security awareness education programs on campus.
- Report annually in May to the President on the status of information systems and data security at Colby.

Colby President and Senior Staff:

- Review and approve, as appropriate, the Information Systems and Data Security Policy (this document) and any other policies and procedures.
- Review annually the Information Systems and Data Security report from the Director for Information Security.

Division and Department Heads, as well as Other College Officers:

- Maintain awareness of procedures for the creation, management and use of sensitive data within departments that report to them.
- Participate in information security training for supervisors and those in senior leadership positions.
- Ensure that appropriate information security policies and procedures are applied within departments that report to them.
- ITS recommends that senior department heads include a review of information security procedures, goals and accomplishments in the performance appraisals of any employee having significant administrative responsibility for or access to sensitive data.

Information Managers and Users of Sensitive Information (including faculty members, due to their access to student information):

- Become knowledgeable regarding relevant security policies and procedures.
- Participate in periodic information security awareness and procedure training, as well as reading information distributed by ITS.
- Implement required security procedures that mitigate threats to information security.
- Take an active role in reviewing potential information security threats in one's own work environment and the feasibility of using various security measures to enhance information security.
- Immediately report any perceived data compromise or threat of compromise to the supervisor, department head and the ISDS Group.
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with access agreements
- ITS recommends that during the annual performance review of employees with administrative access to sensitive information, the College's requirements for information security maintenance be reiterated and any performance issues in this area be addressed

Other Members of the Colby Community having access only to their own personal, sensitive information.

- Be knowledgeable of relevant campus information security guidelines for protection one's own sensitive information to avoid identity theft and maintain financial account security.
- Protect the resources under one's control, such as passwords, computers and data accessible by virtue of membership in the campus community (for example, directory listings).

Key Information Security Elements

Physical Security: Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room or facility where server machines are located, to simple measures taken to protect the information on a User's display screen and workspace security.

System/Computer Security: All college-owned computers used to access sensitive data must have the most recently available and appropriate software and operating system security patches, commensurate with the identified level of acceptable risk. All systems should require user authentication with appropriate restrictions on access to files from other accounts. Any systems that allow unrestricted access must be configured with extra care to minimize security risks.

Sensitive Information: Defined *as a*ny information for which loss, alteration, misuse or disclosure could adversely affect the interests of the College or its administration, faculty, staff, students, applicants or relations therein. For further definition, refer to IT policy document 'Definition of Sensitive Information.'

Privacy and Confidentiality: Users and administrators of campus information technology resources are required to adhere to the Code of Ethics for Information Technology and other College policies. Network and system administrators are expected to treat the contents of electronic files and network communications as private and confidential. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable U.S. and Maine laws and by College policies.

Resources - Related Documents and Links:

Colby College IT policy page

- http://www.colby.edu/administration_cs/its/policies

Questions about:

- **Information security policy** should be directed to Dan Siff, Director of Information Security.
- **IT procedures and technology** should be directed to the appropriate ITS support desk – support@colby.edu for Faculty and Staff, scshelp@colby.edu for Students (Lovejoy 120).

Physical workplace security questions should be directed to Colby's Security office, security@colby.edu.