6-12: Information Technology Security

6-12: Information Technology Security

Issued: 01/2007

TABLE OF CONTENTS

I. PURPOSE

This Policy describes and defines the elements and responsibilities required to create safe and secure Information Systems for all members of the community. The purpose of the Policy is to protect information resources from threats from both inside and outside of the College by setting forth responsibilities, guidelines, and practices that will help the College prevent, deter, detect, respond to, and recover from exploitations of the resources. The Policy is intended to be an enabling mechanism for fostering an environment of secure dissemination of information.

II. AUTHORITY

This Policy was reviewed and approved by the President's Cabinet.

III. SCOPE

These guidelines apply to all students, faculty, visiting faculty, staff, guests, and external individuals or organizations that use computing and electronic communications resources, and computing equipment owned, leased or rented by Fort Lewis College. Computing equipment includes, but is not limited to, dialup modems, terminals and microcomputers in public labs, minicomputers, file servers, and networking equipment used to link these components together and to the Internet.

IV. GENERAL

According to the Federal Critical Infrastructure Assurance Office, an Information System is defined as:

'All electronic and human components involved in the collection, processing, storage, transmission, display, dissemination, and disposition of information. Â http://permanent.access.gpo.gov/websites/www.ciao.gov/ciao_document_library/glossary/i.htm

Fort Lewis College (the 'College'Â) recognizes the extraordinary role information plays in the College's educational, research, operational, and community outreach missions. A safe and secure computing environment is crucial for any institution of higher education. The Information Systems at the College are vital to the welfare of the institution. Information Systems must provide information with the highest possible levels of integrity, availability, and confidentiality. A comprehensive Information Security Policy is a key element of such an environment.

The College utilizes a layered security approach to protect its Information Systems. This Policy includes, but is not limited to, these components:

1. Contingency plan for disaster recovery/business continuity
2. Security safeguards for asset protection
3. Secure architecture design
4. Security awareness and training programs
5. Monitor/audit system

V. ROLES AND RESPONSIBILITIES

All members of the College community share in the responsibility for protecting information resources for which they have access. Responsibilities vary depending upon the role of the user.

A. Roles:

1. Users. All Members of the College community with a computer account are users. Users include faculty, staff, students, authorized volunteers, community members, and visitors. All Stewards, Managers of Users, Information Technology Personnel, and the Information Security Officer are Users. Their responsibilities cover both computerized and non-computerized information and information technology devices that are in their care and possession.

2. Managers of Users. Members of the College community with management or supervisory responsibility, including Vice Presidents, Deans, department chairs, directors, and supervisors are Managers of Users

3. Stewards. Members of the College community who have the primary responsibility for particular information are Stewards. A few examples would be:
a. The Controller is the Steward of the College's financial data.
b. The Registrar is the Steward of student registration data.
c. Faculty members are Stewards of their research and course materials.
d. Students are Stewards of their own work.

4. Information Technology Personnel. Members of the Office of Information Technology manage significant information resources and systems for the purpose of making those resources available to the College community. Information Technology Personnel face more extensive requirements than individuals for information security. Beyond providing access and protecting against unauthorized use and physical threats, they must play a more proactive role in implementing and enforcing security policies and procedures.

5. Information Security Officer. The individual designated in writing by the Vice President of Finance and Administration with the primary responsibility for oversight of information security, networks and systems, security policy, and educating the College community about security responsibilities.

B. Responsibilities (by Role):

1. Users are responsible for:
a. Reading, understanding and complying with the Acceptable Use of Information Technology policy.

2. Managers of Users are responsible for:
a. Ensuring that the people they manage or supervise have access to the information needed to perform their jobs.

b. Requesting access from the Stewards of the information resources.

c. Maintaining, adjusting, and/or requesting removal of access for Users when their job responsibilities change or when their employment is terminated.

d. Ensuring that any specific information security policies and procedures they establish for the people they manage or supervise are consistent with this Policy, as well as with other College Policies, and laws.

3. Stewards are responsible for:
a. Determining the classification of their information as Confidential, Internal Use Only, or Unrestricted as described in the Data Classification Guidelines. Labeling of both physical and electronic information is encouraged where possible, to clearly identify the classification,

b. Determining who is authorized to have access to their information. Directing the Office of Information Technology to grant or remove access for users. Ensuring that those with access have a need to know the information to perform their job. Informing users of the classification of the data they have access to and the security requirements for that data.

c. Collaborating with the Office of Information Technology to establish specific information security policies and procedures for the information resources they manage, including procedures related to the creation, retention, distribution, and disposal of information. Such policies and procedures must be consistent with this Policy, as well as with other College Policies and any applicable laws.

4. Information Technology Personnel are responsible for:
a. Providing and maintaining a secure network architecture. Elements of design shall include, but are not limited to firewalls and intrusion detection and prevention devices.

b. Ensuring that the Information Technology infrastructure of the College (including, but not limited to servers, network switches, routers, cables) is physically secured. Power, temperature, water, and fire monitoring devices shall be in place as appropriate. Locks, cameras, alarms, etc. shall be installed in critical areas to discourage and respond to unauthorized access to the electronic or physical components.

c. Backing up College data stored on network servers on a regular schedule. Schedules, retention periods, and storage facilities shall provide for restoration of data following disaster or corruption. Backup processes shall conform to the record keeping requirements as identified by the data Stewards. Frequency of backups will be determined by a risk assessment process, and may range from continuous to no more than weekly. Backup media are to be stored in a secure location. Data on backup media should be encrypted, where possible.

d. Implementing technologies, designs, policies, and procedures that protect the confidentiality, integrity and availability of College information, in general following currently accepted industry best practices. Examples include but are not limited to:

i. Properly configuring operating systems and other software to reduce vulnerabilities to a minimum.
ii. Updating software in a timely fashion to alleviate security vulnerabilities as they arise.
iii. Providing software that detects, removes, and prevents the spread of malware such as viruses, worms, Trojan horses and spyware.
iv. Periodically probing the network for vulnerabilities, using software tools designed for this purpose.
v. Using available software features to require strong passwords, and requiring Users to change initial passwords upon first use. Requiring proper identification before resetting forgotten passwords.

e. Ensuring that College information systems are in compliance with published security standards that the College is legally bound by. Such standards may include but are not limited to FERPA, HIPPA, and credit card acceptance security standards such as CISP and SDP.

f. Periodic Auditing of systems containing confidential data to detect intrusions. This includes monitoring event logs, examining performance data, and using other available tools and procedures to check for any evidence of unauthorized access, the presence of viruses or other malicious code, or any other indicators of confidentiality or integrity loss.

g. Responding to security incidents in an appropriate and timely fashion. This includes but is not limited to:

i. Reporting suspected or known compromises of information resources to the College Information Security Officer
ii. Preserving and protecting evidence and cooperating with authorized investigations
iii. Locking or revoking accounts
iv. Restricting network access for individuals or computing devices
v. Restoring compromised college-owned equipment to a clean, functional, malware-free state. Installing additional security measures where needed to protect against future compromises.
vi. Treating security incidents as "Confidential."

h. Ensuring that all data storage media are electronically sterilized using currently accepted industry standards before disposal. If electronic sterilization methods are not available or practical, such devices will be destroyed in such a method as to prevent retrieval of data.

i. Granting individuals access privileges to information resources. In circumstances where the data being accessed is controlled by a data Steward, such access will not be granted without receipt of written permission from the Steward. In time-critical situations, verbal authorization may be accepted but must be confirmed by a written authorization within a reasonable time period.

j. Providing information security and awareness training for all members of the College community, and informing them of their responsibilities as Users, Stewards, Managers, and Information Technology Personnel.

k. Understanding, agreeing to and complying with the Fort Lewis College Privileged Access Agreement.

5. The Information Security Officer is responsible for:
a. Staying abreast of Federal, State, and local legislation and how it affects security policy and planning. Monitoring activities and best practices relating to security at institutions of higher education.

b. Overseeing all information network and system security. The Information Security Officer has authority for temporary implementations that deviate from this Policy in emergency situations or until the policy can be reviewed.

c. Overseeing all stages of security incident responses. Depending on the nature of the incident, this can involve collecting and analyzing evidence, determining the responsible party, assessing damages, restoring data from backup files, closing security holes, installing stronger security measures, revising security guidelines and procedures, and reporting incidents to law enforcement and the State of Colorado Chief Information Security Officer. The Information Security Officer will coordinate with all other necessary members of the College community.

d. Overseeing the Security Training and Awareness program.

e. Establishing procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements.
f. Contingency Planning. This includes but is not limited to:
i. Creating and maintaining a Disaster Recovery plan that details procedures for the resumption of mission critical business information services following the loss of equipment and/or data. Printed copies of this Internal Use Only document are stored in the office of Information Technology and distributed to internal IT Managers for off-site storage.
ii.Participating in the College business continuity planning process.
iii. Periodic review of procedures for backup and restoration of College data.

VI. POLICY COMPLIANCE AND ENFORCEMENT

A. Policy audit.

The Information Security Officer shall determine whether information is being protected in conformance with this Policy and with other College policies.

B. Enforcement.

The Information Security Officer shall oversee the enforcement of this Policy. Violations shall be handled consistent with College disciplinary procedures. The College may temporarily suspend, block or restrict access to information and network resources if necessary in order to protect the integrity, availability, and/or confidentiality of College information or to protect the College from liability. The College may refer suspected violations of applicable law to appropriate law enforcement agencies.

VII. REVIEW AND REVISION

The Information Security Officer shall assess this Policy annually to determine if revisions are needed to accommodate the fast changing nature of information technology or weaknesses in the Policy.