Policy No: 814
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures Responsibilities for Establishing a Secure Information Environment

INTRODUCTION:

In order to fulfill its mission of teaching, research, and public service, the University is committed to providing a secure environment that protects the integrity and confidentiality of information while maintaining its accessibility.

PHILOSOPHY

Each member of the CSU community shall be responsible for the security and protection of information resources over which he or she utilizes or for which they have responsibility. Resources to be protected include, but are not limited to, networks, computers, software, data, medical records, financial information, identification information, and personal information. The confidentiality, integrity and availability of these resources must be protected against physical and digital threats including, but not limited to, unauthorized intrusion, malicious misuse, inadvertent compromise, *force majeure*, theft, errors, omissions, or loss of custody and control. Activities outsourced to corporate or other entities must comply with the same security requirements and meet CIO approval.

ROLES

Responsibilities range in scope from administration of security controls for an enterprise system to the protection of one's own password. Any individual may have more than one role.

Administrative Officials - Individuals with administrative responsibilities for campus organizational units or individuals having functional responsibility for data. Information may be distributed to individuals, but overall responsibility for data is controlled by supervisors at the unit level.

Responsibilities include:

- Become knowledgeable regarding relevant security requirements and guidelines;

- Identify the information resources within areas for which they have responsibility;
- Define the purpose and function of the resources and ensure that requisite education and documentation are provided to the campus as needed;
- Establish acceptable levels of risk for resources by assessing factors such as:
    - How sensitive the data is, such as research data or information protected by law or policy,
    - The level of criticality or overall importance to the business continuity of the University as a whole, individual departments, research projects, or other essential activities;
    - How negatively the operations of one or more units would be affected by unavailability or reduced availability of the resources,
    - How likely it is that a resource could be used as a platform for inappropriate acts toward other entities,
    - Limits of available technology, programmatic needs, cost, and staff support;
- For systems in support of university business processes, ensure compliance with relevant provisions of all federal, state, and local laws;
- Ensure that requisite security measures are implemented for the resources;

Providers - Individuals who design, manage, and operate campus electronic information resources e.g. project managers, system designers, application programmers, or system administrators must:

- Become knowledgeable regarding relevant security requirements and guidelines;
- Analyze potential threats and evaluate the feasibility of various security measures in order to provide recommendations to the Administrative Officials;
- Implement security measures that mitigate threats, consistent with the level of Acceptable risk established by administrative officials;
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements;
- Communicate the purpose and appropriate use for the resources for which they are responsible.

Users - Individuals who access and use campus electronic information resources must:

- Become knowledgeable about relevant security requirements and guidelines;
- Protect the critical resources for which they are responsible, including but not limited to, access passwords, computers, and data in their possession.

KEY SECURITY ELEMENTS

The following elements are considered the basic foundation for a secure environment:

Digital Security

Computers must have the most recent software security patches, commensurate with the identified level of acceptable risk.

Adequate authentication and authorization functions must be maintained, commensurate with appropriate use and the acceptable level of risk.

Compliance with procedure and policies must include consideration of both large systems and also smaller computers. Which if compromised, could constitute a threat to campus or off-campus resources.

Physical Security

Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. This 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 a User's display screen.

Privacy and Confidentiality

Applications must be designed and computers must be used so as to protect the privacy and confidentiality of the various types of electronic data they process, in accordance with applicable laws and policies.

Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy.

Approved technical staff assigned to ensure the proper functioning and security of University electronic information resources and services are prohibited from searching the contents of electronic communications or related transactional information except as provided by the CSU Electronic Communications Policy.

Compliance with Law and Policy

Campus departments, units, or groups shall recommend security guidelines, standards, or procedures that enhance the provisions of appropriate policies for specific activities under their purview, in conformance with these operational procedures and other applicable policies and laws.

In addition to any possible legal sanctions, violators of any policy or law may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to GCSU policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the University. Recourse to such actions shall be as provided for under the provisions of those instruments.

RISK ASSESSMENT & RESPONSIBILITES

It shall be the responsibility of the CIO or designee of the CIO to conduct an annual risk assessment of the University. Assessments may be more frequent as warranted by the CIO. The

CIO designee shall provide a report of findings to the Chief Information Officer (CIO) and the President of the University to make them aware of potential threat or compliance issues. It is the responsibility of each unit of the University to cooperate with the assessment and to participate in any necessary remediation

SUMMARY

The University and its administration recognize that information security is an important issue and has established all associated policies and guidelines that are reasonable and prudent. The University will continue to evaluate its compliance with these and all policies as a means to protect the information of its students, faculty, and staff. The University will continue to monitor the evolution of information security and revise its policies and procedures appropriately.

RESOURCES

Questions about this or any information security policy or procedure may be directed to the Chief Information Officer at cio@csu.edu.