CSU
SYSTEM
Connecticut State University System
Developing a State of Minds

BR#06-10

RESOLUTION

concerning

THE CONNECTICUT STATE UNIVERSITY SYSTEM INFORMATION TECHNOLOGY SECURITY POLICY

January 27, 2006

WHEREAS, The Board of Trustees for the Connecticut State University System recognizes that unauthorized disclosure of certain personal information is prohibited by various state and federal statutes, and

WHEREAS, The Board wishes to ensure that the security and integrity of tangible and non-tangible technology and information resources – including but not limited to hardware, software, communications equipment, peripheral devices, data and information assets – are protected and safeguarded, and

WHEREAS, It is desirable that information technology services should be available to the members of the university community with as little interruption as is practicable, and

WHEREAS, Best practice requires that procedures should be established to provide coherent, consistent rules for access to information resources, and to provide coherent, consistent, orderly methods for conducting business using information technology, and

WHEREAS, Knowledge of such procedures should be disseminated in an easily accessible form to all personnel who use CSU's information resources, therefore be it

RESOLVED, That all employees, students, contractors and others who utilize the electronic and non-electronic resources of the Connecticut State University System shall adhere to federal, state and other applicable laws, rules, and regulations which provide for the protection of the security and integrity of information contained in CSU information files, and be it

RESOLVED, That all employees, students, contractors and others who utilize the electronic and non-electronic resources of the Connecticut State University System shall adhere to the provisions of applicable contracts and licenses, and be it

RESOLVED, That the Chancellor is authorized to establish an implementation plan to provide for the development and promulgation of standards, procedures and guidelines that provide rules for access to information resources and rules for conducting business using information technology, and be it

RESOLVED, That security procedures – including managerial, operational and technical controls – shall be consistent with national standards, and be it

RESOLVED, That privacy procedures and guidelines protecting information shall be consistent with state and federal laws, including but not limited to FERPA and GLBA, and be it

RESOLVED, That such procedures and guidelines shall include but not be limited to matters related to computer crimes, libel, privacy, copyright, and trademark, and be it

RESOLVED, That the procedures and guidelines shall be reviewed and updated on a regular basis, but no less than once a year, and be it

RESOLVED, That all employees, students, contractors and others who utilize the electronic and non-electronic resources of the Connecticut State University System shall adhere to the standards, procedures and guidelines developed as provided in the implementation plan established by the Chancellor, and prior to that time, shall adhere to the initial set of procedures and guidelines contained in the attached document, "General Guidelines to Improving Information Security Practices within the CSU System."

A Certified True Copy:

Lawrence D. McHugh
Chairman

General Guidelines to Improving Information Security Practices within the Connecticut State University System

Important Note: Although internal language in this document refers to this document as a "Security Policy," and this language has been left in place for expediency, it is primarily intended to serve in an interim role until standards, procedures and guidelines are developed (target date: July 1, 2006) pursuant to the CSU Information Technology Security Policy's Implementation Plan. That implementation plan also refers to this document as a "template" for those future developments. During this interim period, Board Resolution # 06-yy provides that all individuals utilizing the electronic and non-electronic resources of the CSU System shall adhere to the provisions of this document.

Preface

The Connecticut State University System (CSU) is made up of Central, Eastern, Southern and Western Connecticut State Universities, and an executive staff serving the universities and the Board of Trustees. According to Connecticut General Statutes Section 10a-89, the CSU Board of Trustees is responsible for establishing policies for the system and the individual institutions under its jurisdiction. Reference to CSU or the CSU System accordingly includes the universities that are part of the System.

Information and information system resources are essential assets of all of the parts of the Connecticut State University System, including its universities. Much information is also an essential personal asset of individual students and staff members, protected by various privacy and other statutes.

The entire community of the CSU System (students, faculty, staff) is responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical and lawful manner. This Security Policy is provided to all members of the CSU community to provide proper guidelines on each individual's responsibility to protect CSU information. Every individual should understand his or her obligations relating to the policy statements described herein.

CSU staff responsible for planning, acquisition, configuration, deployment, management, and auditing of information systems should apply sound risk management practices when selecting security controls. This would include identifying what information is intended to be protected, what are the threats to that information or information system resources, and the proper cost-effective safeguards that need to be applied to adequately protect the information.

Reasons for this policy

This Information Security Policy provides a set of comprehensive security guidelines to ensure that CSU information and information system resources are properly and consistently protected. This Information Security Policy outlines student, faculty, and staff responsibilities in supporting the CSU security program and compliance with this Security Policy.

The objectives of this policy are to:

i) Protect personal and institutional information from disclosure to unauthorized parties

ii) Provide for uninterrupted services to the CSU community

iii) Safeguard the integrity and availability of the CSU data networks through appropriate controls

iv) Protect CSU's computing and communication assets including data, software and hardware

v) Prevent computers anywhere within the CSU System from being used to attack other organizations, bringing liability and disrepute to CSU

vi) Protect CSU, including its universities, against the loss or misuse of any information

vii) Define responsibility and accountability to maintain protection of CSU information

viii) Preserve and support audit and legal compliance.

Conclusion

An organization's information security policy is the set of guidelines that will help protect its environment from damage, mischief, impairment, or havoc. The policy document becomes the cornerstone of an effective Information System Security Program for any successful business operation.

This Policy Statement is a living document and periodic modification will need to be made to the policies aligned with technological evolution; new service offerings; new vendor/supplier/partner relationships; modifications of network architecture; changes in operations; staff organization; and the multitude of actual and perceived threats and vulnerabilities tied to infrastructure, application architecture and human behavior.

CSU believes that information security is the responsibility of all users affiliated with CSU, whatever their status: students, faculty or staff. Every person handling information or using CSU information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at CSU.

Contents

Terms

This document will use the following terms:

Pertaining to the Connecticut State University System:

CSU	for Connecticut State University or the Connecticut State University System
Systemic Security Operations	for CSU Systemic Security Operations Office
System CIO	for CSU Chief Information Officer
PMO	for the CSU Program Management Office
SO	for the CSU System Office
University	for any or all of the CSU Universities

Pertaining to the CSU Security Program:

Security Program

The collection of Security Policies, Standards, and Procedures that together constitute the rules that aim to protect security and manage risk within the CSU information technology environment. This collection will be published in the CSU Systemic Security Manual, after Security standards and Security procedures are developed to implement the Security Policy contained in this document.

Security Policy

A set of statements that articulates the overall intention and direction of the CSU Security Program as determined by the Board of Trustees. The policies as specified are technology- neutral and represent an ideal state. (e.g. we will use strong passwords…) Some statements may apply primarily to users, some may apply mainly to staff members with responsibility for technology, and some may apply to both.

Security Standards — A specific statement of the desired state of affairs in a specific technology environment pursuant to a Security Policy. (e.g. For Windows systems, passwords will be at least 8 characters, contain at least one numeric or special character, not be based on an dictionary word, or proper name…)

Security Procedures — A specification of actions to be followed related to a specific activity. (e.g. a password change procedure…)

Terms included in the Glossary are italicized throughout the document.

In the following text, language referring to either the masculine or feminine gender is intended to include the feminine or masculine gender.

1 Introduction

The provisions of the Security Policy presented in this document will guide System Office, University, business associates and, where appropriate, student resources, will facilitate secure *business continuity*, and enable the development of security standards and procedures.

This Security Policy will provide for management of the security of CSU *information assets* and maintenance of *accountability* for the appropriate use of CSU information systems. This Policy defines the general appropriate and authorized behavior for use of the CSU systems and *information assets*. It provides the framework upon which all subsequent security efforts will be based, i.e., the continuing evolution of security policies, standards and procedures for the CSU system.

Systemic Security Operations, working under the supervision of the CIO or her designee, is charged with developing and documenting specific CSU security standards and procedures as a guide to secure CSU for business operations, both local and via the Internet.

The CSU Security Policy is designed to be immediately functional for implementation of specific actions to secure the CSU environment until more comprehensive standards and procedures are developed and promulgated in a CSU Systemic Security Manual. The System CIO, with the approval of the Chancellor, may take action on the basis of the provisions of this policy to protect against threats to the security of CSU information. The System CIO may also take action to communicate the to users, administrators, faculty, students, contractors and others their obligatory responsibility for protecting CSU technology and information assets pursuant to the provisions of this Policy.

Finally, this Security Policy is specifically designed to be flexible enough to support scalability, growth in user capacity and requirements, and the growing range of CSU services.

1.1 Document Organization

This security policy was developed using International Standards Organization (ISO) 7498 Security Architecture Part 2, security service model: Data Confidentiality Services; Authentication Services, Data Integrity Services; and Access Control Services. It also addresses Communication Availability and Operational aspects of CSU in terms of Internet Engineering Task Force Request for Comment (IETF RFC) 2196, "Site Security Handbook." It is recommended that revisions to this policy adhere to ISO/IEC 17799:2005 (Information technology – Security techniques – Code of practice for information security management), published in 2005, and successor documents developed within the family of Information Security Management System International Standards by ISO/IEC JTC 1/SC 27.

In developing specific policies, standards and procedures it is recommended that for best practices CSU use the Corporate Information Security Working Group, Report of the Best Practices and Metrics Teams developed by the Government Reform Committee, United States House of Representatives, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. The goal of the document is "... to develop a resource that would help Board Members, managers and technical staff establish their own comprehensive structure of principles, policies, process controls, and performance metrics to support the people, process and technology aspects of information security."

The policy is organized into eight major policy sections and appendices. Each section is further divided into policy categories that may contain several more levels. Finally, categories are separated into "Required," "Prohibited," and "Reporting " activities that contain the security policy statements. Major sections of this document are:

- Section 1 Introduction
- Section 2 Governance
- Section 3 Roles and Responsibilities
- Section 4 General Security Policy
- Section 5 Hardware Security Policy
- Section 6 Software Security Policy
- Section 7 Operational Security Policy
- Section 8 Exception Process
- Appendices

Security policy statements are numbered for clarity but not necessarily in precedence order. The reader should assume that each policy statement has equal priority and authority.

1.2 *Policy Goals and Objectives*

The goal of this Security Policy is to set the overall approach and define the overall rules, process and structure for use of CSU information and service delivery resources. The policy should inform the users of the compulsory rules for protecting CSU's technology and information assets. These rules define what is and what is not allowed, and provide guidance to ensure a safe computing environment. This Policy must be supplemented with standards and procedures and other written guidance.

In order for this security policy to be viable for the long term, it requires flexibility based upon an architectural security concept. It should remain (as much as possible) independent from specific hardware and software situations, as specific systems tend to be enhanced, replaced, renamed, or moved. Mechanisms for updating the security policy, standards and procedures shall be clearly spelled out. This shall include the process, the people involved, the management staff who must sign off on the changes, and the methodology for informing personnel of new security policies and/or procedures.

The CSU Security Policy represents a commitment to implement secure practices and procedures. This living document also provides direction to CSU in terms of security architecture for CSU business and academic support activities. This document will be used as the basis for making other lower level information security decisions. High-level security policy should not need to be changed frequently.

Once this policy has been established it should be clearly communicated to users, staff, and management. A CSU Systemic Security Manual must be developed, probably with separate sections providing security policies, standards, and procedures for users, and security policies, standards and procedures for staff responsible for information technology. All personnel must sign a statement indicating that they have read, understood, and agreed to abide by the policies, standards and procedures.

This policy should be reviewed in its entirety on a yearly schedule by the CIO and her staff to determine if it is successfully supporting and implementing CSU's evolving security needs. Specific security policies, standards and procedures need to be reviewed on a semi-annual schedule.

1.3 *Scope of Effort*

The CSU security policy, standards and procedures, as set out in the CSU Systemic Security Manual, will address the identification and authentication of users and their appropriate use of the technology and information system assets of CSU in terms of security services, i.e., identification, authentication, confidentiality and data integrity. In particular, the Manual will include resources, services and access for users as well as the rules that will provide protection of CSU resources from destruction, havoc and disorder caused by those users (both external and internal, both accidental and malicious).

1.3.1 Limitations

This document pertains to CSU business and academic support operations and any and all networks directly currently connected to the CSU network infrastructure.

The collection of all security policies, standards and procedures, as subsequently developed pursuant to this Security Policy, will be published as the CSU Systemic Security Manual.

The developers of the CSU Systemic Security Manual may find it appropriate to provide separate sections applicable to users, on the one hand, and to staff members with responsibility for technology, on the other. Further refinement may be necessary, such as dividing the user classification further into Staff, Faculty, Students and Resident Students.

The CSU Systemic Security Manual in its entirety will be available for all stakeholders, including appropriate executive staff, administrators and users. This document is to be published internally and made available to appropriate personnel via the Intranet and as a hard-copy reference.

1.4 *Requirements*

CSU's security policies, standards and procedures must address CSU business and academic support requirements. In so doing, they must cover access control mechanisms; means of user identification and authentication; monitoring and alarm conditions of the network; incident response; a change management system for control and validation of network configuration; a communications structure for all security activities; and a security training program for users and administrators.

Those requirements are:

- To provide a highly reliable, secure, and scalable infrastructure and network operations.
- To provide end-to-end production performance management with guaranteed levels of service to end-users.
- To leverage highly specialized technical resource teams and scalable operating environments.

1.5 *Position Statement*

CSU has adopted a security philosophy that articulates its commitment to secure its network and information system assets. That philosophy is as follows:

EACH USER SHALL BE INDIVIDUALLY RESPONSIBLE AND ACCOUNTABLE FOR HIS OR HER ACTIVITIES AND COMPLIANCE WITH CSU INFORMATION TECHNOLOGY SECURITY POLICIES, STANDARDS AND PROCEDURES

THERE IS ZERO TOLERANCE FOR SECURITY VIOLATIONS OF THE CSU SECURITY POLICIES, STANDARDS AND PROCEDURES.

VIOLATORS OF THE CSU SECURITY POLICIES, STANDARDS AND PROCEDURES WILL BE SUBJECT TO DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION, AND PROSECUTED WHEN APPLICABLE.

ALL EXTERNAL CONNECTIONS TO CSU THAT ARE NOT SECURED END-TO-END BY CSU ARE CONSIDERED TO BE HOSTILE.

1.6 *Applicability*

This security policy applies to all users (external and internal) of CSU and its information system assets, at the System Office, at Systemic Security Operations and at the Universities.

1.7 *Compliance*

Users of the CSU information technology systems or services must be notified of this security policy and sign an "Appropriate Use Agreement" after reading and reviewing the published CSU Systemic Security Manual. Human Resources will provide all employees with an "Appropriate Use Agreement" form. An "Appropriate Use Agreement" will also be included in the student registration materials.

2 Governance

2.1 *Overview*

It is vital that CSU maintain an environment which provides its constituents a secure and protected technology environment, and policies, standards and procedures that are updated regularly. Changes to the CSU environment would potentially introduce new security risks. It is important; therefore, that any changes in the technology environment be reviewed for information security impact before significant effort is undertaken in the acquisition or implementation of that change.

In this context, a "change" can be one of the following:

- any modification to federal, state laws that affect the CSU System.
- any change in CSU polices that require modification of security policies, standards, procedures. (e.g. the voluntary compliance with SOX)
- any change in the overall security environment that requires new measures to be deployed to keep the CSU environment secure. (e.g. virus protection no longer being effective using signature based systems)
- the acquisition of a new software utility or application providing access to or from the Internet or WAN.
- the acquisition of a new software utility or application providing access to a data repository where protected data is maintained.
- the acquisition of any component of network infrastructure, hardware or software including the acquisition of any "network appliance" serving any role.
- any modification to existing network infrastructure including transmission, encryption, management or monitoring of the network.
- any modification of application or network configuration of components used in the transmission of protected information.
- any modification of application or network configuration of components used in the protection of protected information at rest.

2.2 *Policy, Standards, Procedures, Approval Process*

The CSU Board of Trustees must approve changes to the CSU Security Policy. The changes would be reviewed by the Chancellor or his designee(s) and presented to the Board of Trustees for its action.

The Chancellor of the CSU System must approve specific security standards and procedures. The System CIO will develop a mechanism for developing or modifying specific security standards and procedures for presentation to the Chancellor for his review.

2.3 *Policy, Standards, Procedures, Communication Process*

Upon approval of Policies, Standards, and Procedures the following will occur:

- The change will be posted on the CSU intranet with the date of the revision
- Users will be notified of changes via e-mail with a link to the change
- A hard copy will be updated and kept in the HR office, and Security Office of the System Office and Universities

2.4 *System(s) and Infrastructure Change, Approval Process*

The Associate Executive Officer for Security, and the Executive Officer for Information Technology must approve the proposed change as part of the candidate selection for new products or as part of change control for configuration changes. Such approval will be provided in writing and maintained as an artifact in the project files or change control files, as appropriate.

Changes to existing applications or network implementation or configuration must be presented to the Enterprise Change Control Board for review and approval.

The acquisition of new applications and network components, either hardware or software, must be presented to an Architectural Review Board as part of the project initiation process.

In support of this, the Associate Executive Officer for Security and the Executive Officer for Information Technology or his/her designee will be a standing member of any Change Control Board and Architectural Review Board at the Enterprise level. Projects at the University level that include one of the attributes listed above must be presented to the Enterprise Change Control Board or Enterprise Architectural Review Board as appropriate.

The Director of Security, Executive Officer for Technology, and Enterprise CIO are empowered to order the termination or removal of any application, device, network component, or circuit connection from any CSU Enterprise or University environment if they feel it exposes CSU to an unacceptable degree if risk.

3 Roles and Responsibilities

3.1 *Overview*

The roles and responsibilities section establishes the responsibilities for each staff member's role in the overall CSU Security Program. Each role may have certain required activities, prohibited activities, and reporting activities.

3.2 *Security Infrastructure Activities*

1. The Board of Trustees reviews and approves the CSU Security Policy and all changes to that policy.
2. The CSU Chancellor reviews and approves security standards and procedures.
3. The CSU System CIO and her staff develops and reviews modifications to the security policy, standards and procedures, and recommends action to the Chancellor.
4. Management of the *Information System Security Program* is delegated to the CSU Associate Executive Officer for Security and his or her designee, as appropriate.

Prohibited Activities

1. No user of the CSU network may circumvent this security policy structure.

Reporting Activities

1. All security issues relating to the CSU will be reported to Systemic Security Operations for incident response, triage, and change control.

3.3 *Owner Activities*

An owner is defined as the designated individual responsible for the business use of the CSU *information assets*. The owner assigns value to the specified information set; authorizes access to that information; specifies protective measures to the custodian and users of the information; and determines retention and privacy of the information.

Required Activities

1. Systemic Security Operations is the designated owner of the management and maintenance of CSU security policy.

Prohibited Activities

1. The designated owner of any portion of CSU information assets may not circumvent security policies, standards and procedures without consultation with the System CIO or her designee. If the System CIO or her designee cannot be reached during an incident response situation where immediate action is required to protect, defend, and assure critical infrastructure and data integrity, or the safety and security of personnel, the ranking manager on site may assume responsibility.

Reporting Activities

1. On a regular interval, assessment and audit of practices will be performed to document the level of policy compliance.

3.4 Custodian Activities

A custodian is defined as the individual tasked to process, store, and protect the information, as specified by the owner. This responsibility includes establishing physical, technical, and procedural guidelines and safeguards to protect CSU information assets.

1. The System CIO or her designee is the custodian for all CSU operational security.

2. All Systemic Security Operations personnel will be delineated in the CSU Organizational Chart. The reporting structure will be defined in the CSU Systemic Security Manual.

Prohibited Activities

1. Custodians are prohibited from denying CSU Systemic Security Operations any security information affecting CSU's information resources.

Reporting Activities

1. All custodians report directly to their designated organizational supervisor.

2. Custodians must inform CSU Systemic Security Operations of any known security issues or security incidents as soon as they become aware of any such incidents, or suspect such incidents.

3.5 User

A User is defined as an individual Staff, Faculty, Student, or consultant who uses CSU information resources and services. Each user is responsible for maintaining the overall security of the CSU system. (FBI statistics have security incidents being twice as likely from internal staff then external and 90% of the internal events are from negligence as opposed to malicious activity.) It is critical that the user community understands their role to protect CSU. The user community includes the following:

- Staff who support CSU business and academic operations.
- Faculty and Staff who support the academic mission of the CSU system.
- Students, whether on campus or off site, who access CSU systems and services in an academic role.
- Students, whether on campus or off site, who access CSU systems and services in a staff-support or intern role.
- Contractors/Vendors/Suppliers who provide goods and services to CSU. Although they have little or extremely short-lived contact with the CSU, they should always be attended by a CSU employee, with exceptions where there has been authority given to perform functions without escort.
- Affiliates and Partners of CSU who may have special access privileges for a short period of time or as needed for maintenance. These users will have limited privileges on the CSU network and will always be monitored by CSU employees. Examples of partners are:
    - Researchers accessing CSU resources outside of a CSU academic program or management support function.
    - Auditors, Financial, Public Account, etc.

Required Activities

1. It is mandatory that members of the CSU user community adhere to all security policies, standards and procedures.
2. It is mandatory that all members of the CSU user community sign an Acceptable Use Agreement, indicating acceptance, compliance with all security policies, and that they have received security training for use of CSU information resources. Users are individually responsible for understanding and respecting the security policies of the systems and computers they are using.
3. Users are individually accountable for their own behavior.
4. Users are responsible for employing available security mechanisms and procedures to protect their own data. They are also responsible for assisting in the protection of the systems they use.
5. Users are expected to handle account privileges responsibly, and to follow procedures for the security of their data as well as that of the system.

6. All users must wear authorized identification (i.e., badges etc.) while in any CSU information technology operating facility, as appropriate.
7. Information on or about CSU system or information system assets should be conveyed to the user community on a *"need to know"* basis.
8. Users must comply with physical security controls and access control measures.

Prohibited Activities

1. No user may intentionally exploit known weaknesses in the security of a system on the CSU network. Weaknesses are not a license to penetrate or abuse a system.
2. Only designated individuals will be allowed to run software "hacking" tools to assess risk of vulnerability on CSU networks or systems.

Reporting Activities

1. Users must inform the CSU Systemic Security Operations of any known security weaknesses or security issues or security incidents as soon as they become aware of or suspect any such weaknesses, issues, or incidents.
2. Users are required to cooperate with any security related process or procedure necessary to keep the CSU system secured.

3.6 Policy, Standards and Procedures Reviews

As the requirements for security change constantly, regular reviews of security policies, standards and procedures are required to ensure the CSU environment is kept secure. The added complexity of added Federal and State legislation regarding security requires a periodic review to ensure that the security policies, standards and procedures address current legal requirements.

Required Activities

1. Systemic Security Operations will review the security policy, standards and procedures for completeness and effectiveness as deemed necessary. Ideally, this review should be performed each semester.
2. The Security Policy must be kept current with the changes in the CSU environment.
3. All suggestions, comments, and questions from the user community should be directed to Systemic Security Operations.

4. Systemic Security Operations should maintain an Issues Log to track incidents or threats for which the Security policies, standards, or procedures are deemed to be inadequate or which require clarification or modification.
5. Systemic Security Operations should maintain an Incident Log detailing, to the extent possible, the details of each incident including known or suspected means of exploit, defensive actions taken, remedial actions taken, current status and any appropriate planning associated with the incident or its remediation.

Prohibited Activities

1. The provisions of this document may not be abandoned until officially replaced.
2. Amendments and modifications to the policy must not prohibit any legitimate constituency, academic program, or business activity. Determination of "legitimacy" is the province of the Chancellor, upon recommendation of the System CIO or her designee. All such determinations are reviewable by the Board of Trustees.

Reporting Activities

1. Systemic Security Operations will report its findings directly to the System CIO or her designee.

4 General Security Policy

The General Security Policy covers the basic security functions that apply to all user and technical areas of CSU security. The policies apply across all areas of security within CSU.

4.1 *Communication and Usage Responsibilities*

This Communication and Usage Responsibilities section applies to the communication of data both within CSU and outside of CSU. The communication processes used are critical to make sure data are secure during communication and use.

Required Activities

1. All data communication to the CSU network must traverse a gateway and/or network authorized by Systemic Security Operations.
2. Classification and release of CSU information will be in accordance with standards and procedures specified in the CSU Systemic Security Manual. The manual will provide for a classification of information based on ISO 17799:2005 data classification standards. Until the CSU Systemic Security Manual is complete, data will be classified in the following categories:

   - Restricted Data: Data protected by legal requirements such as FERPA and GLBA
   - Sensitive Data: Data protected by contractual obligation, such as details of research, information covered by non-disclosure agreements, or financial transactions not considered restricted data
   - Public Data: Data protected at the discretion of the owner, such as general university information, campus maps, or directory data

   All release of information must comply with Federal and State Laws.

3. All information assets owned by CSU are the property of CSU and will be used in strict compliance with the standards and procedures established by the CSU Systemic Security Manual.
4. CSU information assets are subject to monitoring at all times by authorized personnel, such as security and authorized network staff. Use of CSU information assets constitutes acceptance of the monitoring policy.
5. In the event of emergency, there may be a need to handle certain network security, performance or integrity issues via incident response. The CSU Systemic Security Manual will establish standards and procedures for incident response, to be implemented by Systemic Security Operations.

6. Any user, regardless of exception status, may have his or her account disabled by Systemic Security Operations if it is interfering with the security, performance and/or integrity of the CSU network or service, as defined by the CSU Systemic Security Manual.

7. CSU business information that is deemed "sensitive" must be discussed, recorded, documented, or presented to individuals strictly on a need-to-know basis. Definition of need-to-know will be documented in Information Classification policy, standards and procedures, which Systemic Security Operations must develop and implement.

8. Users will protect the confidentiality of information deemed sensitive and proper control of that information will be enforced per CSU security policies, standards and procedures.

9. Confidential or sensitive information must be properly disposed of according to procedures to be specified in the CSU Systemic Security Manual. Disposal must comply with federal and state laws.

10. Appropriate restricted access to the "non-production" information infrastructure of CSU, such as lab or development environments, may be given to such users as non-Operations or non–Networks personnel and contractors. If the environment contains protected data, the system will be considered "production" from a security point of view.

Prohibited Activities

1. Any attempt to evade or circumvent security policies and procedures specified in the CSU Systemic Security Manual is strictly prohibited (e.g., disconnecting a security device, or "tunneling a protocol" through a gateway that provides "incoming connections from untrusted networks").

2. Unauthorized use, destruction, modification, or distribution of CSU *information assets* is prohibited.

3. Joining of any network (internal and/or external) to the CSU network without authorization is expressly forbidden. The CSU network can be accessed using only devices and processes authorized by Systemic Security Operations in conjunction with the System CIO or her designee. This includes any network media including wireless, alternative carrier (e.g. power line or telephone line) and inductive technologies not authorized by Systemic Security Operations.

4. CSU information assets will not be used in a manner that adversely affects CSU operations.

5. Use of any CSU *information assets* or dissemination of any information in a manner bringing disrepute, damage, or ill will against CSU is prohibited.

6. Users will not attach computers or other network devices to the CSU network in a manner that could cause disruption of production services without prior approval of Systemic Security Operations.
7. Users may not mount any system scans, exploits, vulnerability assessments, or any penetration-type attack against the CSU system or any other supporting CSU system.

If any above outlined procedures are required to be mounted in the course of fulfilling projects by any Operations or Network staff, approval by Systemic Security Operations is required prior to any such course of action.

Reporting Activities

1. Security irregularities, *security incidents*, emergency conditions (alarms), alerts, and system failures, facility security breaches and any other security-related occurrences that in any manner affect CSU *information assets* will be reported to Systemic Security Operations and all other appropriate management immediately.
2. All policies will be formally reviewed at least annually, preferably quarterly. Updates to the Systemic Security Manual will be effected, via appropriate channels and reporting, on an emergency basis as is required.
3. CSU will cooperate with law enforcement authorities regarding *information security* and related incidents through the Systemic Security Operations chain of command.

4.3 *Information Assets*

The Information Assets section covers the ability to access an information asset within the CSU network. The section specifies how information assets will be accessed, maintained for security, and updated.

Required Activities

1. Individual access to the CSU network and CSU information assets will comply with the User Identification and Password Management provisions of the CSU Systemic Security Manual.
2. Whenever connecting to the CSU network, systems will employ a "least privilege" access control configuration, i.e., it will offer only the minimum services and access required to get the job done, and to satisfy any need-to-know requirements, as outlined in the CSU Systemic Security Manual.
3. Users will utilize a screen lock or password protected screen saver to secure their workstation whenever they leave their computer workstations, as outlined in the CSU Systemic Security Manual.

4. All sensitive files will be backed up periodically (daily backup is recommended for any files that have changed). All backups will be in compliance with Connecticut State law. All sensitive files will be stored (both on- and off-site) in compliance with the CSU Disaster Recovery and Business Resumption policy, as specified in the CSU Systemic Security Manual.
5. Users will secure all printed material and other electronic media, containing protected data, associated with their use of CSU information assets.
6. Approved and updated versions of virus management software and anti-spyware software must be installed and operational on all workstations as outlined in the CSU Systemic Security Manual.
7. The current version of patches and embedded features approved by Systemic Security Operations must be installed and enabled on all systems as outlined in the CSU Systemic Security Manual.

Prohibited Activities

1. All users of the CSU are prohibited from attempting to access files, databases, and other information to which they are not granted access.
2. Users will not conduct any illegal activities, nor any activities that will discredit, inhibit, impair, or disrupt authorized users of the CSU service.
3. Desktop resources will not be used to compromise, harm, destroy, or modify any other services or resources (internal or external) of the CSU service.
4. Users of desktop resources are prohibited from intermixing sensitive and non-sensitive information, such as using a floppy to deliver a trivial file when that floppy also contains a copy of a sensitive file.

Reporting Activities

1. The CSU user community must report any suspicious activity that might constitute a CSU security incident to Systemic Security Operations. An example of a security incident could be a router configuration file carelessly left lying about.

4.4 Documentation

The Documentation section covers the documentation of security program and the reporting of security events.

Required Activities

1. The CSU Systemic Security Manual shall include security procedures and security practices for every section of this document.
2. Documentation for the CSU network should be developed using a methodology outlined by Systemic Security Operations. Network schematics must be sufficiently detailed, and kept up-to-date. Systemic Security Operations shall formally review them on a regular schedule.
3. Security procedures and guidelines on the use of security mechanisms and how they interact and interface with other CSU components should be available to the appropriate user community.
4. All developed software, whether in-house or through a contractor, must have its security features and mechanisms documented and available to the appropriate personnel.
5. Security Report Matrices should be a fundamental part of the reporting function of Systemic Security Operations.

   At minimum, these security matrix reports should be submitted by Systemic Security Operations to the System CIO or her designee on a monthly basis.

   The security report matrix reports should include tests and results for testing for all security-oriented deliverables as set forth by the System CIO or her designee.

   Security Report Matrices must include a clear and visual charting function to plot the achievement of goals and achievements, improvements in cost reduction, and all other business deliverable security functions of Systemic Security Operations.
6. A *certification* test plan, test methods (*functional testing* and *penetration testing*), and the test results will be developed so as to enable Systemic Security Operations to submit scheduled Security Report Matrices.

Prohibited Activities

1. Failure to secure or dispose of electronic documents mentioned above is prohibited.
2. Leaving critical electronic documents on desks or stored in unlocked file cabinets is prohibited.

Reporting Activities

1. Appropriate members of the user community should report areas of the network or application documentation that are either incorrect or need additional documentation.

4.5 Password Management

Currently, CSU uses passwords as one of its *authentication* schemes. Reusable passwords represent one of the more vulnerable aspects of information security. Ensuring that passwords are not misused is critical to securing information resources.

Required Activities

1. Users must follow appropriate strength-level recommendations for password creation. Password strength needs to be set for each application depending on the user level and documented as required by the CSU Systemic Security Manual.
2. Where possible, user credentials and passwords should be synchronized across all technology platforms.
3. Passwords must be protected as CSU "Sensitive," in accordance with the CSU Systemic Security Manual.
4. User and system passwords must be changed periodically. The change interval will be set for each application depending on user level and documented as required by the CSU Systemic Security Manual.
5. Systemic Security Operations will enforce a mandatory user password change when various security events occur, e.g., employee relocation, intrusion attempts, or employee termination. It is recommended that user accounts be blocked, rather than terminated, to support any forensic or investigative activity.
6. Systemic Security Operations will enforce mandatory password changes on administrative accounts (e.g. root, oracle, sysadmin, administrator, etc.) when various security events occur (staff changes in the administrative team, certain security incidents, etc.).
7. Individual users are responsible for maintaining the confidentiality of their passwords.
8. Where possible, the use of strong authentication via challenge/response is recommended (as opposed to user-id/password).
9. It is mandatory that access to the password on all *hosts* of the CSU should be tightly restricted. This includes the utilization of pseudo, directory-based pluggable authentication modules (PAMs), Radius servers, or other appropriate centrally-managed password authentication management software. Ideally, there should be one centrally managed, highly available authentication capability.
10. If a user posts notice of resignation, quits his or her position by default or abandonment, or is terminated, immediate action must be taken to freeze all documents, user IDs, passwords, all appropriate access control devices, and access

to sensitive areas or systems, unless contravened by Systemic Security Operations for operational reasons.

Prohibited Activities

1. It is prohibited to configure or maintain any CSU computer account that does not have a password that conforms to this policy or to the appropriate standard established by the CSU Systemic Security Manual.
2. Passwords must not be words that are found in the dictionary in any language, must not be made up of only letters or only numbers, must not be the user's name or username, and must comply with best practices for password creation as outlined in the CSU Systemic Security Manual.
3. Sharing of passwords – including the use of operational group passwords – is prohibited. Role-based password assignment is allowed, but only on an individual-as-role basis.
4. Users shall not disclose their passwords to anyone claiming to be authorized. (i.e., to prevent social engineering).
5. Using programs or scripts that include system passwords is prohibited. For example, if a user has automated the login process so that typing in the password and user ID is avoided, an intruder may steal that program and impersonate the user.

Reporting Activities

1. Any suspicious queries regarding a user's password (e.g. an unsolicited inquiry about a password to help diagnose a network problem) will be reported to Systemic Security Operations as a *security incident.*
2. All intrusion attempts, attempted password compromise or unauthorized account access are *security incidents* and must be reported to Systemic Security Operations.
3. Events such as employee relocation or employee termination must be reported to Systemic Security Operations.

4.6 User Identification and Authentication

The purpose of this policy is to ensure that authorized users of the CSU have access to its *information assets.* It is critical that CSU knows all authenticated users and that user has a single identity.

Required Activities

1. Each user shall have a user identifier (ID) that is unique within the CSU environment. Whenever possible, physical verification of the user should be made before assigning a user identifier (ID).
2. Root, administrator, and guest accounts should be removed from all host files where possible.
3. The individual authentication (i.e., password) method should not be shared; this ensures user accountability activity on the system.
4. Authentication should be encrypted. When authentication is entered at a workstation keyboard, it should be encrypted at the workstation before it is transmitted to the host server for verification, where possible.
5. CSU should employ extended user authentication for all hosts on the CSU. In the case of the routers and other net-edge devices, use this feature when available.

Prohibited Activities

1. Users of the CSU network are prohibited from sharing their authentication means unless authorized by Systemic Security Operations. For instance, a group account is permissible in certain cases, but only after authorization by Systemic Security Operations.

Reporting Activities

1. When a user forgets his or her password or loses his or her authentication device of any kind, it must be reported to Systemic Security Operations and a temporary *authentication* means should be provided. Authentication devices may be either physical objects (e.g., badges) or access control devices (e.g., passwords, biometrics, other access authorizations, etc.)

4.7 *Encryption*

Protected data transmitted internally within the CSU network must be secured during transmission and storage. This is critical with the Gramm-Leach-Bliley Act (GLBA) if information assets containing protected data are lost or stolen. If the data is not secured with encryption, GLBA may require notification to all individuals that data has been compromised.

Required Activities

1. *Cryptography* and message *authentication* will be applied to protected and sensitive information transmitted and stored on the CSU network.

2. *Cryptography* will be used on data protected data stored in devices that are removable from a CSU location. (e.g. laptops)
3. Only *encryption* methodologies approved by Systemic Security Operations will be used.
4. Sensitive or proprietary CSU encrypted files will have the *encryption* keys or tokens held in escrow by Systemic Security Operations or its designated representatives.

Prohibited Activities

1. Providing *encryption* technology or methodologies to anyone in any manner that is contrary to the laws and codes of the United States of America is prohibited.
2. Using unauthorized *encryption* technology is prohibited.
3. Denying senior-level management the ability to decrypt files is prohibited.

Reporting Activities

1. Any addition or deletion of encryption technology will be reported to Systemic Security Operations.

4.8 Physical Security

Physical security is essential for the protection of CSU data. If protected data is stored in systems in unsecured locations all electronic security measures can be rendered ineffective through physical access to the system. Systemic Security Operations shall conduct a comprehensive physical security assessment report for all physical security assets.

Required Activities

1. Visitors or employees in operational areas such as the Network Operations Center (NOC) should be challenged to prove identity.
2. Locking and checking procedures will be established, as provided in the CSU Systemic Security Manual.
3. Access to critical system components should be restricted to a small number of individuals (usually the administrator and backup personnel).
4. A backup power source and other line conditioning equipment will be installed to protect network components against power failures, power surges, brownouts, line noise, etc.

5. Network components will be equipped with power bars that have built-in surge protection circuitry to protect against damage that may be caused by sudden and extreme power fluctuations.
6. Critical network components will be located in a locked room to which access is restricted.
7. Signs will be posted near network components to warn housekeeping and maintenance personnel not to unplug the equipment.
8. Users will be provided with locking and anchoring devices for their workstations. This is especially important in areas open to access by contractors or visitors.
9. Wiring closets housing network equipment will be kept locked at all times.

Prohibited Activities

1. Exposing CSU assets to threats as a result of not observing this *security policy* is a violation of this policy.

Reporting Activities

1. The CSU user community should report any suspicious activity on the CSU network, and in physical locations related to the CSU network, to Systemic Security Operations.

5 Hardware Security Policy

This area focuses on the policies governing the network. In many cases, there is a close interaction between the hardware and software policies, especially as they pertain to data communications devices. **5.1 Network Architecture**The CSU network architecture developed by Systemic Security Operations shall be based initially on a three-tier model of core, access, and edge routers. Different standards and procedures may be developed for the business and residential segments of the network covering the needs of the staff and faculty, and student populations, respectively.

Required Activities

1. Hardware architecture standards shall be established in the CSU Systemic Security Manual. The standards will be based on best practices and reviewed regularly to ensure compliance with current standards.
2. Standard templates for the configuration of each class of routers shall be established in the CSU Systemic Security Manual. For example, the edge routers can control traffic entering the CSU network.
3. The CSU network architecture, established in the CSU Systemic Security Manual, shall include: a routing plan, an address scheme, naming services and hierarchy, network and transport protocols, security features, management, and monitoring.
4. All changes to the CSU network architecture should be authorized only through the Change Control Management process.
5. All external data connections must traverse a secured gateway, unless an exception is granted by Systemic Security Operations.
6. Authority for remote management of servers must be assessed and granted by Systemic Security Operations.

Prohibited Activities

1. No modifications to the CSU network architecture are to be performed without the express approval of the System CIO or her designee, following review by Systemic Security Operations.
2. No external connection to any CSU network shall be made without conducting a Change Management process, in which the owner/custodian, all stakeholders, and staff from Systemic Security Operations participate. The System CIO or her designee must approve the results of the process.

Reporting Activities

1. Any Change Management process must be attended by at least one representative of Systemic Security Operations.
2. All external connections will be recorded through the Access Request process and will be controlled by the Change Management process.

5.2 *Network & Server Hardening*

The purpose of this policy is to protect the routers, paging terminals, and gateways that make up the CSU network from susceptibility to attacks. These general hardening mechanisms apply to routers, switches, traffic shaping, load distribution equipment, and gateways and servers.

Required Activities

5.2.1 General Hardening

1. The CSU Systemic Security Manual shall provide a common set of standards and procedures, applicable to all devices on the CSU network, necessary to cover access control, limiting protocols, use of static routing, strong authentication etc., based on current best practices.
2. Implement security monitoring processes to monitor all network devices end to end.
3. Any changes to the established architecture must follow the Change Management procedures.
4. Monitor and comply with vendor and industry security bulletins.
5. To the greatest extent possible, all systems and networks should use a standardized, synchronized time source to aid in reporting, diagnostics and auditing.

5.2.2 CSU Network Hardening

1. CSU should implement IP network defenses within the IP network. The security posture for the business network should be stricter than the residential network and based on best practices.

Prohibited Activities

1. No party, including CSU users, may unduly interfere with operation of the network. Specifically, users are prohibited from doing attacks on the network, such as scanning all IP ports or doing a Denial of Service attack
2. The Change Management process may not be bypassed for the convenience of administrators.

Reporting Activities

1. Configuration change requirements will be reported via the Change Management process. Systemic Security Operations must authorize and document any emergency configuration changes.
2. All non-authorized configuration changes are considered a *security incident* and constitute an "alarm" condition.

6 Software Security Policy

This area focuses on the policies that are driven by software. Network services are primarily driven and controlled by software. Security penetrations most often capitalize on weaknesses in software and the use of information generated by the software. The software security policies that follow are organized into these topic areas:

6.1 *Host Configuration*

Required Activities

1. The CSU Systemic Security Manual shall provide standards and procedures to be followed regarding the limiting of protocols, hardened hosts, static routing, etc., based on best practices.
2. Changes to any host must have prior authorization as required by the Change Management process provided in the CSU Systemic Security Manual.

Prohibited Activities

1. Changes to any *host* without appropriate approvals specified in the Change Management process is prohibited.

Reporting Activities

1. All changes to any *host*, as authorized according to the Change Management process, must be documented and reported as provided in the CSU Systemic Security Manual, subsequent to implementation and validation.

6.2 *Acceptable Use*

The CSU Systemic Security Manual shall provide standards and procedures, based on best practices, for the implementation of software.

Required Activities

1. The standards and procedures for the implementation of software, as delineated in the CSU Systemic Security Manual, must be followed.
2. The implementation of all software that has access to protected data must be approved in advance by CSU Systemic Security Operations.

3. Systemic Security Operations, following the Change Management process, must authorize all software used in the CSU System.
4. Authorized software may only be used as intended.

Prohibited Activities

1. No modifications to CSU software are allowed without proper authorization by Systemic Security Operations.

Reporting Activities

1. Suspicious or unusual activity should be reported to Systemic Security Operations.

6.3 Software Import Control

Required Activities

1. The CSU Systemic Security Manual shall provide standards and procedures to ensure that, prior to introducing any software installation into the operational CSU environment, all files must be scanned for viruses and Trojans, using the latest approved version of malicious code management software, or CRC checks, and programs must be inspected for hostile and/or malicious code.
2. All information systems media, such as disks and CD-ROMs introduced to the CSU environment, will be scanned for malicious code. Code that has been vetted and approved for use in the production environment must be archived on appropriate media, and archived for reference and backup and/or restoration purposes.
3. All software used on the CSU must be used in concert with its license. Software covered by the GNU Public License must be treated as licensed software.
4. All freeware must be assessed and approved by Systemic Security Operations prior to installation on the CSU network.

Prohibited Activities

1. The unauthorized development, transfer, or execution of viruses and hostile and/or malicious code are prohibited.

Reporting Activities

1. All users must report any suspicious occurrences of software (e.g., if a "sniffer" was known to be on the network or if someone had installed unauthorized software) on the CSU network to their supervisor <u>and</u> Systemic Security Operations immediately.

6.4 *Software Development Standards*

The CSU Systemic Security Manual shall provide standards and procedures, based on best practices, for software development for both internally and externally developed software.

Required Activities

1. CSU will use the standard "best practice" of a Software Development Life Cycle (SLDC) methodology when appropriate.
2. Before implementation, a code review of all scripts and programs that implement dynamic content must be performed.
3. Changes to any module must be reviewed following a Change Management process to assure that no vulnerability has been introduced into the CSU environment by the change.

Prohibited Activities

1. No software that is developed for CSU may bypass this policy.

Reporting Activities

1. All reporting will follow the procedures established by the CSU Systemic Security Manual.

7 Operational Security Policy

This section focuses on the policies governing operational efforts. While these policies are administered behind the scenes, they are often the most critical.

Network, server and desktop operations staff and administrators are the primary lines of defense against intentional or accidental security breach. The operational security policies for the CSU network appear in the sections that follow, organized into these topic areas:

- Network Monitoring and Alarm/Alert Management
- System and Configuration Backup
- Disaster Recovery
- Audit Trail Analysis and Event Audit Policies
- Change Management
- Remote System Access
- Intrusion Management and Incident Handling
- Security Awareness and Training
- Testing and Certification Standards

7.1 Network Monitoring and Alarm/Alert Management

The CSU's heterogeneous *network architecture* requires more than one type of Network Management System (NMS) and should include intrusion detection systems and host-based auditing systems.

Systemic Security Operations is the owner of the NMS.

Required Activities

7.1.1. General Network Management

1. The CSU Systemic Security Manual pertaining to NMS must at a minimum address access to all mission-critical applications, automatic monitoring, client monitoring, messaging / alert system, and automatic alarming.
2. The CSU System Security Manual's standards and procedures should be developed in line with best practices. As the threat level is continually increasing regular reviews and revision of the standards and procedures is critical.
3. All remote management activities will use some kind of end-to-end *encryption* scheme.

4. The CSU must have controls and protection enforced by network management administration systems. Network management controls must include *resource* accountability, errors and omissions, reporting malfunctions, and preventive maintenance. Network protection controls must address the need for *risk analysis* and security assessments, security awareness, security administration, and *physical security.*

5. Access Request forms need to be signed by the user and the custodian of the data that the user is authorized to access.

6. Network management will maintain a formal inventory of network components and will check the network configuration regularly to ensure that all components attached to the network are authorized.

7. Procedures should require a risk analysis or security assessment to be performed whenever significant changes to the network (e.g., physical facility, hardware, software, or communications) occur.

8. Physical access to the network *hosts* need to be limited to authorized network management personnel and secured. The network server, backup facilities, UPS, network hubs, etc. should be installed in locked areas that are only normally accessible to the Operations organization.

9. The network administrator or some other responsible individual should be present when maintenance work on network components is being performed.

10. All unused network connections should be disabled and physically monitored, or otherwise controlled

7.1.2. Specific Policy for Alarm Conditions

1. The CSU Systemic Security Manual shall establish standards and procedures to implement this policy concerning alarm conditions. The standards and procedures should be developed in line with best practices and regularly reviewed and revised to stay current. The standards and procedures must address, at a minimum, software configuration change, prohibited packets or IP addresses, login failures, and excessive login attempts from the same server etc.

7.1.3. Specific Policy for Alert Conditions

1. The CSU Systemic Security Manual shall establish standards and procedures to implement this policy concerning alert conditions. The standards and procedures should be developed in line with best practices and regularly reviewed and revised to stay current.

2. The standards and procedures must specify the conditions that would create an alert. At a minimum the following must be addressed: failed login attempt,

termination of key personnel, repeated failed login attempts, unauthorized modification of software, and unauthorized attempt to connect to the network.

Prohibited Activities

1. No alarm or alert may be ignored (even if known to be a false alarm, it sould be recorded and annotated for audit purposes).
2. Unauthorized personnel are prohibited from accessing NMS hardware, software, or information.
3. Disabling, tampering with, or modifying any NMS agent logfile is prohibited.

Reporting Activities

1. An alarm condition requires the operator to take immediate action that will generally have the effect of disrupting some or all of CSU's business.
2. An alert condition requires the operator to contact Systemic Security Operations Systemic Security Operations may be contacted to facilitate necessary authorization from the appropriate authority.
3. The NMS must provide message paging and detailed management reporting.
4. All alarms will be recorded and acted upon by authorized personnel only.
5. All security alarms will be reported to Systemic Security Operations.
6. Security related events must be immediately posted to security files, acted on in a timely manner, and reported to Systemic Security Operations.
7. Corrective actions must be documented, and time-stamped.
8. All network malfunctions must be recorded and reported. Malfunction must be matched to the specific report. Solutions to all malfunctions must be permanently retained.
9. Regular preventive maintenance scheduling for all network components must be reported.
10. There must be documented evidence of the time and type of maintenance that was performed on any network component.

7.2 System and Configuration Backup

Required Activities

1. Backup of *host* server files and network infrastructure equipment should be automated and should happen on a regular basis in most cases nightly.

2. Several generations of backup files should be maintained. Backup media should be stored in media safes, preferably off-site.
3. One backup copy should be available on-site in case recovery is necessary. Another copy should be stored at an off-site location in case of a fire or some other contingency.
4. Various backup techniques should be employed, including full backups and incremental backups. Full backups are used for total system recovery. Incremental backups use fewer media and are faster to run. Incremental backups are generally used to recover old versions of files and to restore file integrity when files become corrupted.
1. Backup media must be rotated and checked for working order.
2. Backups are to be regularly checked to verify they are functional to fully restore the system from the backup.
3. New and modified system implementations require verification of backup and recovery before the system can be moved to production.

Prohibited Activities

1. Non-authorized personnel may not perform network backup and recovery functions.

Reporting Activities

1. Authorized system administrator(s) or representatives will report backup/recovery status to Systemic Security Operations on a quarterly basis. Systemic Security Operations will include this data in its scheduled reporting to the System CIO. The status will include instances where backup could not be performed successfully, and restoration attempted, successful or not.
2. Security must be notified of need to restore system or configuration files prior to the recovery activity. All such incidents shall be documented.

7.3 Business Continuity / Disaster Recovery

Business Continuity / Disaster prevention is a technique used to forestall disasters or minimize the effects of a disaster. CSU initially will implement a business resumption plan and evaluate the need for a disaster recovery plan.

Required Activities

1. A *Business Continuity / Disaster Recovery* Plan must be prepared that will enable CSU to provide service to its customers and enable users to continue performing critical business functions while the network is unavailable. The plan should:
   - Prioritize activities,
   - Prepare:
     - Housekeeping procedures,
     - Backup procedures, and
     - Hardware redundancy in case of failure of critical components.
2. The Business Continuity Plan should be exercised at least annually to ensure that in the event of a disaster it can be relied upon for failover.
3. Systemic Security Operations will oversee the exercising of the Business Continuity Plan.
4. The plan should be stratified for different levels of disaster including those isolated to a university location, or a region (e.g. Hartford and New Britain).

Prohibited Activities

1. It is against security policy to neglect Business Continuity / Disaster Recovery planning.

Reporting Activities

1. Results of the exercise will be reported to the System CIO or her designee.

7.4 Audit Events and Audit Trail Analysis Policies

Audit trail analysis is used to detect and deter *penetration* of a computer system and to reveal misuse. Audit event information provides *assurance* that the *security policy* is being enforced. It serves as a *deterrent* to would-be *crackers/hackers* and dishonest employees and students from potentially *browsing* unauthorized areas within the CSU.

Required Activities

1. The *network security architecture* design should include a mechanism to invoke the audit function at the request of Systemic Security Operations. A mechanism should also be included to determine if the event is to be selected for inclusion as an *audit trail* entry.

2. The *audit trail* itself shall be protected from unauthorized access (*read, write, delete, execute* privilege and only the designated personnel may access the audit trail).
3. The audit-event enabling/disabling mechanism shall remain inaccessible to unauthorized users.
4. At a minimum, audit data should be considered to be sensitive.
5. Audit logs should be reviewed regularly by Systemic Security Operations to detect any attempts to breach the security of the network.
6. The audit diagnostic tool should be run on a regular basis and any exceptions uncovered by the tool should be corrected in a timely manner.
7. The audit diagnostic tool should have an "intruder alert" notification and it must remain activated. All alerts should be acted upon. Refer to Alert Management in Section 6.1.

7.4.1 Audit Events

1. Audit events should include identification and *authentication* mechanisms.
2. Audit events should include actions taken by computer operators and system administrators and/or system security administrators.
3. Audit events should include date and time of the event.
4. Audit events should include the unique identifier on whose behalf the subject generating the event was operating
5. Failed logins must be audited: An attempt to log in as a known user ID failed, or an attempt to log in as an unknown user ID was made.
6. Attempts to connect from a non-management system to a paging terminal or router using a management protocol must be audited.

Prohibited Activities

1. Unauthorized access to *audit trails* or audit data is prohibited.
2. Destruction, disabling, or tampering with audit files is prohibited.
3. Proper operational conditions must be maintained for audit files or reports.

Reporting Activities

1. All auditable events will be reported to Systemic Security Operations.
2. If an attempted breach or an actual breach impacts any network systems, notify Systemic Security Operations of the *security incident*.

7.5 *Change Management*

Change Management controls provide for the management process to review and determine changes to hardware, software, operations, or related policy, standards, and procedures for the CSU System.

1. Formal change control procedures are required for all CSU production systems.
2. An approved Emergency Configuration Change Process can be used when changes are required on the fly due to outages, or to restore or ensure operations.
3. A configuration management Change Control Board will be implemented to control and maintain the CSU documentation of the baseline of data, hardware, software, networks, and procedures, records of property control and audits of inventory items.
4. The Change Control Board will develop a process flow for requesting changes. An effective change control procedure will include documenting and approval justification for the change and review of the changed material (code or content).
5. An effective change control procedure should include the following steps:

   Step 1: Document and approve justification for the change.

   Step 2: Review the changed material (code or content) to:

   Step 3: Ensure that the change addresses the justified requirement,

   Step 4: Ensure that unapproved changes are not made,

   Step 5: Establish that all changes are "safe" and do not introduce errors that could compromise the service,

   Step 6: Test the operation of the change in a development or testing environment,

   Step 7: Establish a recovery procedure if the change fails to accomplish its stated goal or causes a disruption of service,

   Step 8: Log the time and date of the change, along with the documentation from steps 1 and 2 above.

Prohibited Activities

1. User installation of software on any system that affects the CSU system is prohibited.
2. Change Management may not unduly interfere with the operation of the network; however, this should not be interpreted as a means to bypass Change Management control for convenience of administrators.

Reporting Activities

1. All changes made through the Emergency Configuration Change Process must be reported to the Change Control Board for configuration control.
2. The Change Control Board will report activity and status periodically to CSU management.
3. Operational issues should be directed to the Change Control Board owner, the System Office Executive Officer for Information Technology, for resolution.
4. All security issues will be directed to Systemic Security Operations.
5. Systemic Security Operations will have the means and the audit trail to evaluate any CSU configuration changes both before implementation by the CSU Change Control process, and after such implementation, in the due diligence Systemic Security Operations routinely performs during regular audits of the network.

7.6 Intrusion Management and Incident Handling

1. The primary goal of intrusion management is to prevent or avoid intrusions entirely.

   The following policies will help to implement effective security controls that can achieve that goal:

   - Security Policy
   - Security Standards and Practices
   - Security Awareness
   - Incident Response Planning
   - Business Resumption Planning
   - Training of Operations Personnel
   - Evaluating the Results of a Successful Intrusion ("lessons learned" feedback)
2. Administrators will actively monitor compliance of security policies, standards and procedures through:
   - Security Audits
   - Intrusion Testing
   - Vulnerability Testing
   - Security Reviews
   - Risk Assessments on New Systems

3. Systemic Security Operations will use appropriate tools to test systems for vulnerabilities before system implementation and periodic reviews when in production. Preventive tools will include those that perform initial evaluation and configuration.
4. Systemic Security Operations will use detective tools that are intended to ensure that any change to the configuration is noticed.
5. Systemic Security Operations will use investigative measures when other avoidance measures have failed to prevent an attack. Systemic Security Operations should undertake investigations of security incidents, whether they are successful or simply strong attempts.
6. Systemic Security Operations will monitor traffic on peripheral segments. Early detection of attacks will permit administrators to shut down exposed connections before damage to the network is sustained.

Prohibited Activities

1. Tampering with or modifying intrusion detection software, hardware, or practices is prohibited.

Reporting Activities

1. All security incidents will be reported to Systemic Security Operations. Systemic Security Operations shall be tasked with coordinating with the user organization and CSU Legal if required.

7.7 Security Awareness and Training

The CSU Systemic Security Manual pertaining to standards and procedures for security awareness and training shall require initial training prior to access to the CSU network and systems and refresher awareness training as indicated by Systemic Security Operations. All staff and students should receive training in Security Basics and Awareness. Other faculty and staff should receive additional training as appropriate to their job functions. Security awareness training must comply with meeting Federal and State Requirements.

Required Activities

1. "Security Basics and Awareness Training" should create sensitivity to the *threats* and vulnerabilities, and recognition of the need to protect data, information, and the means of processing them.
2. "Network/System Administrator Security Training" provides the ability to recognize and assess the threats and vulnerabilities to automated information

*resource*s on the network so that the responsible managers/custodians can set security requirements that implement the CSU security policies.

3. "Application Security Training" provides the ability to recognize and assess the threats and vulnerabilities to internally authored code, so that code custodians can achieve code security requirements that implement the CSU security policies.
4. "Security Refresher" will be contingent upon current security conditions, (e.g., security incidents, etc.) which may affect the CSU environment and new security material identified by Systemic Security Operations.
5. This training will be offered in the most efficient and appropriate form, whether that be formal external training, internal classroom training, written curricula, CBT training, conferencing, or other appropriate forms of education via media and/or presentation.

Prohibited Activities

1. The CSU user community is prohibited from access to the CSU infrastructure without completing the required security awareness training as prescribed in this document.

Reporting Activities

1. Systemic Security Operations will report annually the training results (effectiveness) to the System CIO or her designee.

7.8 Testing and Certification Standards

CSU must develop *security testing* and *certification* standards for its environment due to several key factors that have a direct or indirect impact on the security of CSU. These factors are continually changing and include technology changes; integration of systems and networks; internal threats to information; and external threats to information.

Required Activities

1. Systemic Security Operations is responsible for the *security testing* of the CSU network. This is done at regular intervals of *functional testing* and *penetration testing.* Upon successful completion of these two tests, the network will be deemed *certified.*
2. Systemic Security Operations must also take steps to implement the appropriate security mechanisms and controls required to keep the CSU secure.
3. CSU management, systems administrators and the system's custodians must be actively involved in the implications of a changing environment if the CSU security is to remain effective.

4. Indicators for certification testing:

   - *Security incident* - (*penetration, denial-of-service attack, social engineering, intrusion detection, malicious code* identification, etc.). A *security incident* may expose a security weakness or a failure of an existing security mechanism or control.
   - Security monitoring report. On-going systems monitoring is necessary in order to ensure that any attempts, whether successful or unsuccessful, to gain unauthorized access or to make unauthorized changes to a computer system, are identified and investigated in a timely manner.
   - Self-assessment. Network administrator, along with Systemic Security Operations, should conduct a security self-assessment or *Risk Analysis* of the CSU in order to identify any weaknesses in the network's security scheme.
   - Security audit review report. An audit review may result in recommendations for changes to the network environment. Internal audit and Security co-operate in areas of security reviews, inspections, and assessments.
   - New network connection. All requests to attach existing or new networks to a certified network should be reviewed by the owner and Systemic Security Operations. An inspection of the network to be connected should be conducted in order to determine whether the connection would introduce any security weaknesses to the certified network.

Prohibited Activities

1. Once the CSU network has been certified, no changes may be made that will disrupt any security mechanisms that have been put in place without permission from the owner and/or custodian, and without adherence to the Change Management Process.

Reporting Activities

1. Changes to the certified CSU network should be reported to the owner. Following a review of the proposed changes, the owner should determine whether the network *certification* process should be invoked.
2. Changes to the security practices and standards for the CSU may affect the security scheme of the existing network. When changes are made to the network *security policy* and standards, the owner should review the security scheme in order to determine whether the network security *certification* process should be invoked.

8 Exception Process

CSU recognizes that some portions of the Security Policy may have to be bypassed from time-to-time because of technical or business reasons.

Accordingly, exceptions may be made provided:

1. The need for the exception is legitimate and approved by the System CIO.
2. The exception does not disrupt or compromise other portions of the CSU service delivery capability.
3. The implementation of the exception is vetted through the Change Management Process.
4. Systemic Security Operations can establish a monitoring function to assess the operations of the implementation exception.
5. The exception has a defined lifecycle, in that the "retirement" of the exception is scheduled (e.g., "when Release 4.9 is implemented," "at contract termination," etc.)

Required Activities

Exception Request

To request an exception, the CSU Systemic Security Manual should define a process that includes the following items at a minimum.

- Originator Name and Contact Information
- Requested Implementation Plan
- Nature of Exception
- Approved Alternative Exception (if different)
- Expected Retirement Condition
- Expected Exception Retirement Date
- Systemic Security Operations Approval
- Approval by System CIO

The requestor and Systemic Security Operations will define the approved alternative configuration if different than the original proposal of the requestor.

The exception process is NOT an alternative to the Change Control Management process.

Appendix A - Security Training Guidelines (Sample)

Security Administration Training is the introduction to the basic concepts behind industry accepted *network security* practices and the importance of the need to protect the CSU information assets from *vulnerabilities* to known *threats.* Areas to cover include:

- *Network security* planning and management is concerned with *risk analysis*, the determination of security requirements, security training, and the *security infrastructure* to carry out the *network security* function.
- *Network security* policies and procedures looks at network-specific security practices in the areas of physical, personnel software, communications, data, and administrative security.
- Contingency planning covers the concepts of all aspects of *contingency planning*, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all the players involved.
- Systems life cycle management discusses how security is addressed during each phase of a system's life cycle (e.g., system design, development, test and evaluation, implementation and maintenance). It addresses procurement and network *certification.*

Training audiences are groups of employees with similar training needs. They are defined as follows:

- Executives (owners) are those senior managers who are responsible for setting the CSU *security policy*, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the *resource*s and support for the CSU *Information System Security Program.*
- Functional Managers (custodians) are those managers and supervisors who have a program or functional responsibility (not in the area of *network security*) within CSU. They have primary responsibility for the security of that CSU asset within their area of responsibility. This means that they designate the sensitivity and *criticality* of the information asset, assess the risks to those assets, and identify security requirements to the supporting organization, physical facilities personnel, and users of their asset. Functional managers are responsible for assuring the adequacy of all *contingency plan*s relating to the safety and continuing availability of that CSU asset.
- Systemic Security Operations and Audit Personnel are all involved with the daily management of the CSU information *resource*s, including the accuracy, availability, and safety of these *resource*s. As a group these persons issue procedures, guidelines, and standards to implement CSU's policy for *information*

security of the CSU, and to monitor its effectiveness and efficiency. They provide technical assistance to users, Functional Managers, and to the organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

- Network Management Operations and Network Administration Staff are all involved with the daily management and operations of the CSU hardware and processing services. They provide for the protection of the data in their custody and identify security measures to the data owners. The group includes System Administrators, Data Base Administrators, and Network Planning. They provide the technical expertise for implementing security-related controls within the automated environment. They have primary responsibility for all aspects of *contingency planning.*
- Subscribers/Users are persons (as described in the user community section of this document) who have access to the CSU system.

Appendix B - Glossary of Information System Security Terminology

Access – A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Access Control – The process of limiting access to the resources of a system only to authorize persons, programs, processes, or other system (in a network).

Access Control Mechanism – Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in a network.

Access List – A list of users, programs, and/or processes and the specification s of access categories to which each is assigned.

Accountability – The quality or state which enables actions on a network system to be traced to individuals who may then be held responsible. These actions include violations and attempted violations of the security policy, as well as allowed actions.

Administrative Official – An individual with administrative responsibility for university or System organizational units (e.g. unit heads, deans, department chairs, principal investigators, directors, or managers).

Assurance – A measure of confidence that the security features and architecture of the network accurately mediate and enforce the *security policy.*

Availability - The ability of authorized persons or programs to expediently access an information resource.

Audit Trail – A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticate –
(1) To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system.
(2) To verify the integrity of data that have been stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authentication – To establish the validity of a claimed identity. To provide protection against fraudulent transactions by establishing the validity of the individual or system.

Authorization – The granting of access rights to a user, program, or process.

Browsing – The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

Business Continuity - Ongoing, unaffected business operation is the primary goal of information security. It includes responding to incidents and recovering from natural or human initiated disasters.

Category – A restrictive label for identifying data.

Certification - The comprehensive evaluation of a system's technical and non-technical security features, made as part of and in part of the approval/accreditation process, that establishes the extent to which a particular system's design and implementation meet a set of specified security requirements.

Change Control, or Change Management – The process of controlling changes made to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system.

Change Control Board – A group of no more than five information technology personnel, broadly representative of the CSU System, as designated by the Chancellor, which collectively will review proposed changes to hardware, software, firmware or documentation to determine which proposals to approve.

Component – A device or set of devices, consisting of hardware, along with its firmware, and/or software that performs a specific function on a computer communications network. A component is a part of the larger system, and may itself consist of other components. Examples include modems, telecommunications controllers, message switches, technical control devices, host computers, gateways, communications subnets, etc. .

Compromise – A violation of the *security policy* of a system such that unauthorized disclosure of sensitive information may have occurred.

Confidentiality - Ensuring that privacy information or data is protected from unauthorized release or use.

Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Cracker – A person who uses other people's computers for criminal purposes.

Criticality - The degree to which information or information assets are depended upon for business operation. Criticality is based on the impact to operations in the event of denial of service, modification, or destruction of data or software.

Cryptography – The principles, means and methods for rendering information unintelligible and for restoring encrypted information to the intelligible form.

Data safes – Fire-resistant safes specially designed to protect magnetic media from damage caused by magnetism, fire, heat, water and air-borne contaminants such as smoke and dust.

Delete – A fundamental operation that results only in the removal of information of an object by a subject.

Denial of Service – The prevention of authorized access to system assets of services, or the delaying of time critical operations.

Deterrence - The act of discouraging or preventing unauthorized activities associated with information assets.

Disaster Recovery - The attempt to salvage information and/or systems that have been interrupted or destroyed by an environmental or human activity.

End-To-End Encryption – The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

Execute - A fundamental operation that results only in the operation of privileged instructions by a subject.

Extended User Authentication – Should be a challenge response scheme. This is also referred to as "strong authentication" and means that someone can prove knowledge of a secret without revealing it. This is possible with cryptography. This is particularly useful when two computers are trying to communicate over an insecure network.

Firewall – A security filter, which could be implemented in hardware or software, which is logically separated from the remainder for the system to protect the system's integrity.

Functional Testing – The portion of security testing in which the advertised features of a system are tested for correct operation.

Hacker – See cracker. Originally, this meant someone who plays with computers because it's fun vs. how the media uses the term.

Host – Any computer-based system connected to the network and containing the necessary protocol interpreter software to initiate network access and carry out information exchanged across the communications network.

Identification – The process that enables recognition of an entity by a system.

Incident – A computer security incident is any adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.

The definition of an incident may vary for each event depending on many factors. Tthe following categories and examples are the most commonly applicable:

- *Compromise of integrity*, such as when a virus infects a program or the discovery of a serious system vulnerability;
- *Denial of service*, such as when an attacker has disabled a system or a network worm has saturated network bandwidth;
- *Misuse*, such as when an intruder (or insider) makes unauthorized use of an account;
- *Damage*, such as when a virus destroys data; and
- *Intrusions*, such as when an intruder penetrates system security.

Another definition, which relies on the definition of "Threat" is: "an instance of any computer security threat."

Incident Response - The effort to react by isolating, removing and recovering from the results of unauthorized or illegal attacks against an information system. Normally, a team made up of technicians, public affairs, and legal personnel will work to contain the effects of an incident.

Information Assets - Valuable or sensitive information in any form and the systems which pass or store that information.

Information Security - The protection of information systems and the data they contain from unauthorized or prohibited activity.

Information System Security Program – A complete security program that includes a *security policy*, security practices/procedures, security implementation plan, security training and awareness program.

Integrity - The accuracy of data and information systems. The property that data has not been exposed to accidental or malicious alteration or destruction.

Intrusion Detection - The recognition of unauthorized activities or electronic attacks. The process of detection may be automated or performed ad-hoc.

Malicious Code - An unauthorized program intentionally inserted into a system that can compromise, delete, or corrupt information assets. Some examples include a computer virus, a Trojan horse, a trap door and a worm.

Need To Know – Only that information the user must have in order to perform his/her duty or activity.

Network Architecture – The set of layers and protocols, including formats and standards that different hardware and software must comply with to achieve stated objectives, which define a network.

Network Connection – Any logical or physical path from one host to another that makes possible the transmission of information from one host to the other. For example, when a host transmits an IP datagram, in a TCP/IP connection, employing only the services of its "connectionless" IP interpreter it is still considered to be a connection between the source and the destination hosts for this transaction.

Network Security Architecture – A subset of network architecture specifically addressing security-related issues.

Network Security – The protection of networks and their services from unauthorized modification, destruction, or disclosure.

NMS – Network Management System.

Object – A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video display, keyboards, clocks printers, paging devices etc.

Object Reuse – The reassignment of a medium (e.g., page, frame disk sector, and magnetic tape, CD-ROM) that contained one or more objects to some subject. To be securely reassigned, such media must contain no residual data from the previously contained object(s).

Penetration – The successful violation of a protected system.

Penetration Testing – The portion of security testing in which the penetrators attempt to circumvent the security features of a system.

Provider – An individual who designs, manages and/or operates CSU electronic information resources (e.g., project managers, system designers, application programmers or system administrators).

Read – A fundamental operation that results only in the flow of information from an object to a subject.

Reliability – The extent to which a system can be expected to perform its intended function with required precision.

Resource – Anything used or consumed while performing a function.

Risk—The probability that a threat will exploit a vulnerability of an information asset and the resulting loss.

Risk Analysis—A formal examination of an organization' s information *resource*s, controls, and vulnerabilities in both manual and automated systems. Risk analysis predicts potential damage in dollars or other assets by assessing the loss potential for each *resource*, the probability of occurrence, and the burden.

Risk Assessment—Identification and evaluation of types of risks, their probability of occurrence, and the potential adverse impact they could have on an automated information system.

Risk Management—The overall process of identifying, controlling, and eliminating or minimizing potential events that could adversely affect information system *resource*s. It includes reviewing the overall status of the system; analyzing risks; analyzing cost-benefits; and selecting, implementing, and evaluating system safeguards.

Safeguards—Processes, procedures, or features intended to mitigate the effects of risk. Although risk can never be entirely eliminated, safeguards can reduce it to an acceptable level. Some examples of safeguards are hardware and software security features, operational security procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical security structures, areas, and devices.

Security Incident – A security incident is any infraction of the *security policy.* Obvious and overt examples are network penetration, denial-of-service attack, *social engineering*, malicious code, spoofing, tampering, technical attack, virus detection, etc.

Security Infrastructure—The internal organizational structure, functions, and associated responsibilities that provide a framework for the authorization, development, dissemination, enforcement, and evaluation of a security program.

Security policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes its information assets.

Security Posture - The overall security status of an organization. It can be determined by quantifying several specific security aspects into a single, comprehensive, layered evaluation.

Security Testing – A process used to determine that the security features of a system and implemented as designed and that they are adequate for a proposed application environment. This process includes hands-on functional testing, penetration testing, and verification.

Sensitive – A classification for document handling that represents the security level of an object requires special handling in accordance with the corporate document handling guidelines.

Sensitivity - A measure of harm to information or information assets resulting from observation, modification, destruction, or unavailability of information.

Social Engineering - The act of attacking the weakest security link in any computerized network, which is the human being, mainly to obtain passwords. A social engineer may pose as an employee over the phone or in person or, go so far as getting hired by the company as part of an attack. There are many types of *social engineering*, for example: A social engineer gathers information about specific employees so he/she can pose as one of them. The social engineer calls around the company asking innocent questions--acting as a repairperson, perhaps--and discovers that an executive has a new secretary. Posing as the secretary, the attacker calls human *resource*s and makes up an excuse to request the boss's employee identification number. The attacker contacts the help desk in the guise of the executive. Armed with the correct employee identification number, the 'executive' is issued a new password and authorized access is obtained. Experienced social engineers can often gain such access with a few well-placed calls in a day or two. The 'victim' company may never be the wiser. The key to preventing social-engineering success is to create consistent security policies to guard against it. These policies can include a rule in which no critical information is given out over the phone, call-backs are used as a *verification* method when taking requests for passwords or employee identification's, and most importantly employees are empowered to report suspicious activity, without fear of recrimination.

Spoofing – An attempt to gain access to a system by posing as an authorized user.

Statistical Process Control - The approach to decision support that uses statistical evidence to drive evaluations of the effectiveness, efficiency, or other aspects of a particular process.

Strong Authentication – see extended user authentication.

Subject – An active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically a process/domain pair.

System – A collection of hardware, firmware, and software necessary configured to collect, create, communicate, compute, disseminate, process, store, and/or control data and information.

Tampering – An unauthorized modification that alters the proper functioning of a component/equipment of system in a manner that degrades the security of functionality it provides.

Technical Attack – An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

Threat - The catalyst of a potential loss to information assets. Threat can be categorized into two arenas: (1) environmental, and (2) human-initiated. There are internal threats (e.g., human error, disgruntled employee), external threats (e.g., hackers, computer viruses), and natural disasters (e.g., earthquakes, flooding) that can potentially compromise the confidentiality, integrity, and availability of automated information systems.

Trap Door – A hidden software or hardware mechanism that permits system protection mechanisms to be circumvented.

Trojan Horse – A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security. An example would be making blind copies of sensitive information for the creator of the Trojan Horse.

Trusted Functionality – That which is determined to be correct with respect to some criteria such as an established *security policy.* The functionality shall neither fall short of nor exceed the criteria.

User – An individual who accesses and uses CSU electronic information resources.

Validation - A process that substantiates the content of a course or the utility of a particular program.

Verification – The process of comparing two levels of system specifications (e.g., comparing operational files against disaster recovery backups) for proper correspondence. This process may or may not be automated.

Virus - A program that reproduces itself when it is executed. It can corrupt and infect other programs, and spread from one computer to another. A virus usually has hostile intent and corrupts data files or causes other damage.

Vulnerability - Design, administration, or implementation weaknesses in information processing systems that, if exploited, could lead to an unacceptable impact.

Vulnerability Prevalence - A structured procedure to determine the extensiveness of a specific set of vulnerabilities.

Write – A fundamental operation that results only in the flow of information from a subject to an object.

Implementation Plan for Developing Procedures and Guidelines for Information Technology Security

Pursuant to BR # 06-xxx, the following implementation plan is established to provide for the development and promulgation of policies, standards, procedures and guidelines for information technology security in the Connecticut State University System.

The System CIO and the Executive Officers for Information Technology at each university shall develop procedures and guidelines that provide rules for access to information resources and rules for conducting business using information technology.

The System CIO, with the advice of the Council on Information Technology, shall develop such policies, standards, procedures and guidelines for the security of information resources within the responsibility of the System, the System Office, the System Telecommunications enterprise, and the Shared Information Technology Enterprise Services (SITES), as well as minimum standards and procedures for the security of information resources within the responsibility of the universities. As of now, the areas of responsibility within the responsibility of systemwide entities include, but are not limited to, Vista, the network, server administration, Banner, *OnlineCSU*, groupware and SITES management of desktop support.

The Executive Officers for Information Technology at each of the universities shall develop procedures and guidelines for the security of information resources within the responsibility of the universities, subject to the minimum requirements established as noted above. As of now, these areas of responsibility include pedagogy support, instructional design, media services, technology in the classroom, computer labs, research support and university managed desktop support. The standards, procedures and guidelines must be at least as stringent as the minimum standards and procedures developed by the System CIO, and must not contradict the standards and procedures developed by the System CIO.

The document named "General Guideline to Improving Security Practices within the CSU System" shall be utilized as a template by all of those officers responsible for developing their operating procedures and guidelines relating to security.

The operating procedures and guidelines relating to security shall also incorporate the statements and guidelines contained in the following documents, which are attached:

- Connecticut State University System Employee Confidentiality Policy Statement concerning Access to and Usage of Information

- Connecticut State University Policy on Administrative Access to Electronic Data
- Connecticut State University Policy on Responsible Use of Information Technology Resources

The development of these new security procedures and guidelines should be completed by July 1, 2006. The Chancellor shall promulgate and distribute them, in an easily accessible format, upon completion.

Proposed variations and exceptions from the new security procedures and guidelines shall be reviewed by the System CIO, with the advice of the Council of Information Technology, at appropriate times for possible adoption.

A process to review and update the new security procedures and guidelines, based on systemwide business needs, will be undertaken at least once each year.

The Chancellor, with the advice and assistance of the Council on Information Technology, shall at least annually submit a report to the Board of Trustees regarding the implementation and progress of security and privacy guidelines.

Connecticut State University System

Employee Confidentiality Policy Statement concerning Access to and Usage of Information

Access to all databases, including but not limited to Banner, is granted solely for the purpose that you may perform legitimate, authorized, assigned responsibilities required for the proper operation of the CSU System, and is granted strictly on a "need to know" basis. No employee of the CSU System shall use or distribute State information for other than State business purposes. Any unauthorized or illegitimate use of the Banner system, databases or data may result in disciplinary action up to and including termination of employment, criminal prosecution and/or civil action.

Please be aware that Federal and State laws protect the data to which you have access and that it must be treated with complete confidentiality. You must ensure that such confidential information is shared only with other authorized users. Examples of such confidential data or materials include but are not limited to: written or verbal reports or computer terminal displays containing employee, student, vendor or donor personal data such as education, financial, medical, employment or business history, family or personal relationships, reputation or character which because of name, identifying numbers, mark or description can be readily associated with a particular person.

Please be aware that you may access and/or modify only the data for which you have been given full authorization and have a legitimate purpose in performing your assigned responsibilities. You should further understand that you may not share your account or password with anyone else to gain access to confidential information.

Please be informed that you are not permitted to modify your own records and that your activities may be audited. If you do modify your own records, you will be subject to disciplinary action, up to and including termination of employment, criminal prosecution and/or civil action.

Please be aware that, if you attend or have attended classes in the Connecticut State University System, you will not be permitted to work with your own student records and that your activities may be audited. You should further understand that if you do work with your own student records, you will be subject to disciplinary action, up to and including termination of employment, criminal prosecution and/or civil action, as well as subject to academic disciplinary actions, including dismissal.

You are expected to take all steps reasonably necessary to safeguard the confidential information entrusted to you and to prevent it from falling into the possession of unauthorized persons.

I hereby acknowledge that I have read and understand this confidentiality statement.

Employee Name: ____

Employee Title: ____

____ ____________________

Employee Signature Date

I have discussed and reviewed the confidentiality provisions with the above employee.

____ ____________________

Authorized University Representative Date

c. Employee Personnel File

Connecticut State University Policy on Administrative Access to Electronic Data

Purpose: The purpose of this document is to clarify CSU policy regarding administrative access to electronic data/activity such as electronic mail, word processing files and web browser usage.

Scope: The following guidelines apply to the CSU System employees as well as consultants and vendors contracted by CSU. Individuals who are employed/contracted by or enrolled at CSU's four universities should contact their respective information technology departments for additional information.

For the purposes of this policy, computing and network resources include all software, hardware, internal and external networks, systems, databases, electronic mail, and any other files, data, equipment or facilities either owned or leased by the Connecticut State University System.

Overview: The CSU System is committed to protecting the privacy of every member of the CSU community, subject to the limitations of this policy. As the owner of all CSU computing resources, including any information generated or stored on our network, CSU reserves the right to access those resources. Situations that might necessitate such actions include but are not limited to: (1) business need; (2) system maintenance/ management; (3) suspicion of employee misconduct; and (4) Freedom of Information requests and state or federal laws.

User Guidelines: The following guidelines have been developed to assist in the implementation of this policy:

- When administrative access to electronic data is necessary, every effort shall be made to avoid viewing data beyond that needed to meet the intended purpose.
- Should an employee inadvertently view personal electronic data, such information shall be kept confidential. However, if the individual accidentally uncovers evidence of employee misconduct, he or she must report this information to his/her supervisor or manager.
- Conditions under which administrative access to electronic data shall be permitted include but are not limited to:

Business Need - In an employee's absence, his or her manager/supervisor or other authorized individual may access the necessary CSU documents or files if there is an immediate need for that data. Note: Proper use of file sharing and common directories should be encouraged to eliminate or reduce the need for such access.

System Maintenance/Management - Authorized Information Technology department personnel shall periodically monitor network and system activity to: (a) perform routine maintenance; (b) optimize system and network performance; and (c) preserve the security of the CSU network and its data. Personal electronic data may be viewed in conjunction with these activities and/or to investigate security breaches, bandwidth issues, etc.

Suspicion of Employee Misconduct - If an employee is suspected of misconduct, CSU reserves the right to monitor that individual's electronic activity and review his/her stored data. This is particularly applicable if illegal activity is suspected.

FOI Requests/State or Federal Laws - Documents and files created or received in the course of CSU business are considered public records. If a Freedom of Information request is received, the authorized individual will evaluate that request to determine its validity. If the information meets the legal definition of a public record, the information must be released. CSU is also required to release information in compliance with court orders, subpoenas or other mandates issued by state or federal authorities.

Additional Information/Resources:

State of Connecticut Electronic Monitoring Notice
http://www.das.state.ct.us/HR/Regs/State_Electonic_Monitoring_Notice_11.00.pdf

State of Connecticut Freedom of Information Access to Computerized Public Records
http://www.ct.gov/doit/cwp/view.asp?a=1245&q=253992

Connecticut State University Policy on Responsible Use of Information Technology Resources

Purpose: The purpose of this policy is to establish common standards for the responsible use of information technology resources within the Connecticut State University System.

Scope: This policy applies to all users of the Connecticut State University System's computing and network resources.

For the purposes of this policy, computing and network resources include all software, hardware, internal and external networks, systems, databases, electronic mail, and any other files, data, equipment or facilities either owned or leased by the Connecticut State University System.

Overview: The CSU System provides members of the CSU community with access to a broad range of information technology resources including computers, software, networks, databases, files, electronic mail and the Internet. Members may also have access to confidential data and external networks. Use of these resources is authorized only if users use them responsibly, demonstrating respect for individual privacy, ethical standards, and the law.

User Guidelines: Responsible use of CSU information technology resources means acting in a manner that: (1) respects the confidentiality of CSU data; (2) preserves the security, integrity and performance of our information technology resources and (3) complies with all CSU policies, legal standards and contractual agreements.

1. Respecting the confidentiality of CSU data.

Violations include but are not limited to:

- Intentionally accessing another user's files, e-mail, or other information technology resources without permission.
- Unauthorized monitoring, distribution, duplication or modification of another's data, e-mail, or documents.
- Accessing information beyond the extent necessary to accomplish one's assigned duties.

2. Preserving the security, integrity and performance of CSU's information technology resources.

Violations include but are not limited to:

- Sharing the user's personal password(s) or username with others.
- Using the CSU network to sabotage or cause harm to external resources.
- Limiting system capacity/bandwidth by running programs, computers or servers which may cause excessive network traffic (e.g. Napster).
- Sending/forwarding chain letters, virus hoax messages; letter bombing/spamming, etc.
- Using shared resources excessively (e.g., non-essential printing which might hinder other's workflow, wasting valuable disk space, etc.)
- Installing, changing, or removing software on the user's computer without authorization.

Violators of this policy may be subject to disciplinary action up to, and including, dismissal or expulsion, as may be provided in CSU policies, collective bargaining agreements, codes of conduct, or other instrument governing the individual's relationship with the University. Violators may also be subject to possible legal sanctions.

Employee Guidelines: Users of CSU information technology resources who are CSU employees, or who contract with CSU to provide goods and/or services, must read this policy, and sign the statement below.

I hereby acknowledge that I have read and understand this policy, and agree to comply with its provisions.

Employee Name: ____

Employee Title: ____

Employee Signature: ______________________________ Date: __________

I have discussed and reviewed the provisions of this policy with the above employee.

Authorized CSU Representative: ________________________________

Date: ____________________

STAFF REPORT **FINANCE AND ADMINISTRATION COMMITTEE**

ITEM

Connecticut State University System Information Technology Security Policy

BACKGROUND

As early as 2000, the Management Letter of our Independent Auditors, PriceWaterhouseCoopers (PWC), called attention to the need for information security planning, recommending that

> Management should continue in their efforts to finalize a security plan, which details management's steps for improving information security at CSU. In addition, management should develop an infrastructure that allows for monitoring the adherence to established policies and procedures.

PWC's 2000 Management Letter also called for the establishment of Information Systems Policies and Procedures, as well as Program Change Control Procedures. These comments were repeated in its 2001 Management Letter.

In its 2002 Management Letter, PWC's comments were repeated once again, with the observation that there should be "centralization of security administration" in order to enhance the reliability of computer security.

As recently as PWC's 2004 Management Letter, presented to the Board in the early months of 2005, the auditors noted the continued need to provide for information security, once again repeating earlier comments.

A consultant, ETC Sunstorm, was hired in 2003 to perform an assessment of security within information technology operations throughout the CSU System, encompassing systemwide operations as well as university-specific operations. Its recommendations were presented to the Council of Presidents (COP) in the Fall of 2004, and were refined in several presentations to COP in early 2005. One of the highest priority recommendations was the creation of an information security policy, to be followed by the implementation of information security procedures.

Given the widespread publicity about security breaches nationwide, the necessity for information security has become apparent.

ANALYSIS

The resolution presented for Board consideration recognizes the need to protect against unauthorized disclosure of certain personal information, as provided by state and federal law, and accordingly requires that all employees, students, contractors and others who use information resources of the CSU System and its universities adhere to relevant federal, state and other applicable laws, rules and regulations, as well as to the provisions of applicable contracts and licenses.

In addition, the resolution authorizes the Chancellor to establish an implementation plan which provides for the development and promulgation of standards, procedures and guidelines that provide rules for access to information resources. A copy of the implementation plan that will be established by the Chancellor is attached to the resolution so that the Board will be aware of what it will include. The implementation plan requires the System CIO, with the advice of the Council on Information Technology, which is composed of the Executive Officers for Information Technology within the System, to develop administrative policies, standards, procedures and guidelines for security of information resources within the responsibility of systemwide entities, as well as minimum standards for procedures and guidelines, to be developed by the Executive Officer for Information Technology at each university, to be used for protecting the information resources within the responsibility of the universities. The implementation plan also provides that a lengthy document, "General Guidelines to Improving Security Practices within the CSU System," shall be utilized as a template for these policies, standards, procedures and guidelines. Moreover, three specific statements and administrative policies shall be incorporated into the final set of policies, standards, procedures and guidelines. Those documents, concerning employee confidentiality concerning access to and utilization of information, administrative access to electronic data, and responsible use of information technology resources, are attached to the implementation plan. Overall, a final set of security procedures should be ready for adoption by July 1, 2006.

Finally, the resolution provides that until the promulgation of the final set of security procedures, all employees, students, contractors and others shall adhere to the standards, procedures and guidelines contained in the "General Guidelines to Improving Information Security Practices within the CSU System."

CHANCELLOR'S RECOMMENDATION

That the CSU System Information Technology Security Policy be adopted.