Connecticut State University System

Information Security Standards

Version 1.0

May 2007

TABLE OF CONTENTS

Connecticut State University System
Information Security Standards Committee

The following individuals participated in the development of the CSUS Information Security Standards outlined in this document:

CSUS Institution	Committee Members
Central Connecticut State University	David Orschel, Interim Director of Technical Services Robert Quast, Server Support Specialist Roy Temple, Interim CIO
Eastern Connecticut State University	Walter Zincavage, Director, Information Technology Services
Southern Connecticut State University	Ray Kellogg, Director - Network Telecom Services & Help Desk John Young, Director, Administrative Computing
Western Connecticut State University	Muhammad Ismail, Network Security Specialist Richard Parmalee, Director of Network & Telecommunications
CSU System Office	James Brislin, Associate Executive Officer for IT Security Peter Carey, Network Security Specialist Diane Gilligan, Technical Communications Coordinator Debora Romano-Connors, Associate Executive Officer for IT Planning

PREFACE

The Connecticut State University System consists of Central, Eastern, Southern and Western Connecticut State Universities and a System Office that serves each university and the CSU Board of Trustees.

In January 2006, the CSU Board of Trustees passed a resolution regarding the Connecticut State University System Information Technology Policy. **Board Resolution 06-10** calls for the establishment of an information security program that will ensure the security and integrity of CSU System's tangible and intangible information resources.

Additionally, the resolution calls for the development of clear and consistent standards, procedures and guidelines to assist the entire CSU System in the implementation and execution of the information security program.

1. INTRODUCTION

The Connecticut State University System (CSUS) oversees and supports a broad range of academic and administrative information resources. These resources must be protected and preserved: (1) to achieve the CSUS mission and strategic goals, (2) to support and sustain quality technology services and (3) to ensure legislative and regulatory compliance.

CSUS is committed to securing its information resources by establishing an information security program that addresses the administrative, technical and physical safeguards needed to attain the following:

Confidentiality - Comply with all federal and state laws and regulations as well as CSUS Policies by protecting our information resources against accidental or unauthorized access or disclosure.

Integrity - Maintain the viability and accuracy of CSUS Information Resources by preventing its intentional or accidental corruption, modification or destruction.

Availability - Ensure the availability of CSUS data, information systems and related services through preventive measures such as risk analysis, monitoring, and contingency planning.

1.1 Document Purpose

The purpose of this document is to establish a broad framework for information security within the Connecticut State University System. It is specifically intended to provide baseline standards that will assist each CSUS institution in developing the procedures and guidelines necessary to implement and maintain our information security program.

While this document was initially developed with an emphasis on information security from an Information Technology perspective, it is intended to be dynamic in nature and will gradually expand to encompass the entire CSUS community.

1.2 Document Scope

The CSUS Information Security Standards outlined in this document apply to:

- **CSUS Users:** All employees, faculty, staff, students, and third parties including vendors, contractors, visitors and all others who utilize the electronic and non-electronic information resources of the Connecticut State University System.
- **CSUS Information Resources:** All data created stored, maintained, processed or transmitted by CSUS as well as all internal and external networks, computing platforms, systems, software, hardware, equipment and facilities either owned or leased by the Connecticut State University System.

1.3. Document Development

The standards in this document are intended to adhere to all CSUS policies as well as all federal and state laws and to reflect generally accepted information security practices. Each individual standard is the product of a broad range of research and discussion.

ISO/IEC International Standard 17799 2005(E) and the National Institute of Standards and Technology (NIST) Special Publication 800-53 served as baseline models and primary resources in the development of this document. However, a number of additional resources provided valuable information and perspective including the Commonwealth of Virginia Information Technology Agency (VITA) and the State of New York Office of Technology, as well as various institutions of higher education.

1.4 Document Terms & Acronyms

The following terms and acronyms appear throughout this document and are defined as follows:

TERM	DEFINITION
Board of Trustees (BOT)	The Board of Trustees of the Connecticut State University System
Chancellor	The Chancellor of the Connecticut State University System.
Council on Information Technology (CIT)	University and System Office Chief Information Officers of the Connecticut State University System.
Council of Presidents (COP)	The CSUS Chancellor and the Presidents of Central, Eastern, Southern and Western Connecticut State Universities.
CSUS	The Connecticut State University System - Central, Eastern, Southern and Western Connecticut State Universities and the System Office.
CSUS Information Resources	All data created stored, maintained, processed or transmitted by CSUS as well as all internal and external networks, computing platforms, systems, software, hardware, equipment and facilities either owned or leased by the Connecticut State University System.
Mission Critical	CSUS Information resources that are essential to the academic and administrative operations of the Connecticut State University System.
CSUS Users	All employees, students, and third parties including vendors, contractors, visitors and all others who utilize the electronic and non-electronic information resources of the Connecticut State University System.

1.5 Document Structure

This document is divided into the following sections:

SECTION	TOPIC/STANDARD	PURPOSE
Section 1.	**Introduction**	To outline the purpose, scope, development and organization of this document.
Section 2.	**Governance**	To provide a framework and guide implementation of an effective security program at all levels of the Connecticut State University System.
Section 3.	**Asset & Risk Assessment**	To ensure that Information Resources are identified and classified with respect to risk.
Section 4.	**Personnel Security**	To ensure that all users understand their responsibilities regarding information security and that individuals seeking employment meet the information security criteria for the desired position.
Section 5.	**Physical & Environmental Security**	To secure Information Resources by safeguarding the physical environment and infrastructure supporting those resources.
Section 6.	**LOGICAL SECURITY**	
Section 6.1	**Access Control**	To secure Information Resources through the development and implementation of well-defined access control processes and procedures.
Section 6.2	**Data Security**	To ensure that data is secured during all phases of the data life cycle, i.e. usage, transmission, storage and disposal.
Section 6.3	**Network Security**	To ensure that electronic data is appropriately secured during all phases of the data transport life cycle.
Section 6.4	**Host & OS Security**	To prevent unauthorized access to and maintain maximum availability of host and/or operating systems.
Section 6.5	**Application Security**	To ensure that applications are appropriately secured throughout the life of the application.
Section 7.	**OPERATIONAL SECURITY**	
Section 7.1	**Disaster Recovery & Contingency Planning**	To counteract interruptions to business activities, protect mission critical processes from the effects of major failures of information systems or disasters and ensure their timely resumption.
Section 7.2	**Backup, Storage & Recovery**	To secure electronic data by protecting it from loss or corruption due to events such as natural or man-made disasters, system or hardware failures and human error.
Section 7.3	**Security Monitoring**	To ensure that information security policies, procedures and controls are being followed and are effective in securing Information Resources.
Section 7.4	**Incident Management**	To ensure that the identification, management and reporting of information security incidents occur in a consistent and timely manner.
Section 7.5	**Change Management**	To establish a change management process that will prevent or minimize adverse consequences caused by changes to Information Resources.
APPENDICES		

2.0 GOVERNANCE

Purpose: To provide a framework and guide implementation of an effective security program at all levels of the Connecticut State University System. Security governance ensures that risks are identified and appropriately managed.

The primary objectives of CSUS Information Security Governance are:

1. Develop administrative policies and approve standards to protect CSUS Information Resources consistent with CSUS Board policy statements and resolutions.

2. Develop policies and standards that comply with federal and state information security regulations.

3. Ensure that an ongoing Information Security Program is implemented to meet the prescribed policies and standards.

4. Ensure that the roles and responsibilities for implementing the Information Security Program are defined and assigned.

5. Ensure that security metrics reports are reviewed regularly. Such reports will be based on data derived from controls implemented to meet prescribed policies and standards.

6. Use periodic audits of asset management to control software licensing.

7. Develop an audit program to ensure that regulatory compliance and effective controls are in place.

8. Identify and authorize exceptions to standards specified in this document using a defined Exception Process.

Standards:

2.1 Policies and Standards

For the purposes of this document the following definitions apply:

Term	Definition
Policy	RFC 2196, *The Site Security Handbook*, defines a security policy as "a formal statement of rules by which people who are given access to an organization's technology and information assets must abide." Less formally, they are high-level management statements of security objectives, responsibilities, ethics and requirements. Policies define where the organization is heading.
Standard	Standards are specific, mandatory requirements that support the high-level policies. They will be identified in this document with such words as *will*, *must*, and *required*. Standards define what an organization **WILL** do to achieve the policies.
Guideline	Guidelines are voluntary practices that support the high-level policies. Guidelines are optional. They will be identified in this document with such words as *should*, *may*, and *requested*. Guidelines define what an organization **SHOULD** do to achieve the policies.
Procedures	Detailed instructions outlining how to meet the criteria identified in the Standards. Procedures define how the organization will meet the requirements specified in the standards.

The Board of Trustees establishes policies. The CSUS Chancellor submits policy recommendations to the Board of Trustees (BOT) for review, approval and publication. Senior management, including the CIO's, recommends any additions or changes to policy through the Presidents to the Chancellor. The standards in this document are intended to adhere to all CSUS policies.

1. The CSUS Security Standards Committee **will** draft security standards. The CIT and appropriate departments **will** review these standards. The draft **will** then be submitted to the COP for approval and publication. Modifications to standards **will** be processed through the same review procedure.

2. The CSUS Security Standards Committee may incorporate guidelines as appropriate to provide additional direction.

3. Each University and the System Office **will** document and maintain a set of security procedures that addresses the criteria defined in the standards. Consistency is encouraged but not required.

2.2 Compliance

1. The CSUS **will** develop and follow policies, standards and procedures to comply with state and federal information security regulations.
2. The CSUS Information Security Officer (ISO) **will** keep informed of legislative and regulatory changes that affect security with the cooperation of CSUS Security Standards Committee.
3. If such legislative or regulatory changes are recognized to affect CSUS compliance, they **will** be brought to the attention of the COP and incorporated into the Security Standards when appropriate.

2.3 Information Security Program

The Information Security Program is an action plan with a component of continuous improvement designed to both monitor and to mitigate risk to a level acceptable to management.

1. Each University and the System Office **will** develop, document, implement and maintain an information security program.
2. Each Security program **will** include:
    a. Periodic risk assessment (*See **Asset & Risk Management**.*)
    b. Procedures and controls that reduce information security risks to an acceptable level.
    c. Periodic evaluation of procedures and controls.
    d. Procedures that ensure information security is addressed throughout the life cycle of each information system.
    e. Procedures that ensure compliance with the policies, standards of this document, and any applicable legal, regulatory, or contractual requirements.
    f. Procedures for detecting, reporting, and responding to security incidents, including timely risk mitigation, and the set up of a proper notification / communication plan. (*See **Incident Management**.*)
    g. A process for the remediation of program deficiencies.
    h. Plans and procedures to ensure the continuity of the information technology infrastructure that supports CSUS operations. (*See **Disaster Recovery/Contingency Planning**.*)

2.4 Governance Roles and Responsibilities

The tables below outline the key roles and associated responsibilities supporting information security governance for the following:

1. CSUS Board of Trustees (BOT)
2. CSUS Council of Presidents (COP)
3. CSUS Council on Information Technology (CIT)
4. CSUS Administration
5. CSUS Security Standards Committee
6. CSUS Information Security Officer (ISO)
7. University Information Security Officer
8. Information Stewards, Custodians and Administrators

Role (2.4.1)	**CSUS Board of Trustees**
Key Security Responsibilities	a) Issue Information Security Policies. b) Endorse the Development and Implementation of a Comprehensive Information Security Program. c) Oversee the security of all CSUS Information Resources.

Role (2.4.2)	**CSUS Council of Presidents**
Members	Chancellor and Presidents with the advice and counsel of their Cabinets
Key Security Responsibilities	a. Implement and maintain an Information Security Program ensuring compliance with appropriate federal and state regulations. b. Ensure appropriate budgetary, staffing and training resources are established for the program. c. Review and approve CSUS Information Security Standards. d. Ensure that procedures are developed, documented, implemented and maintained to address the criteria defined in the CSUS Information Security Standards. e. Assign individuals to participate on the CSUS Security Standards Committee. f. Designate Stewards responsible for CSUS Information Resources. g. Ensure Business Continuity.

2.4 Governance Roles and Responsibilities *(Cont.)*

Role (2.4.3)	**CSUS Council on Information Technology**
Members	University and System Office Chief Information Officers
Key Security Responsibilities	a) Identify key business objectives to be supported by the Information Security Program. b) Ensure that CSUS Information Security processes are integrated with University Strategic and Operational Planning Processes. c) Provide controls commensurate with the Information Steward's assessment of acceptable risk.

Role (2.4.4)	**CSUS Administration**
Members	▪ Academic Chairs ▪ Department Heads ▪ Deans and Vice Presidents ▪ Senior Management ▪ Supervisors
Key Security Responsibilities	a) Understand their role and responsibilities in the preparation and execution of their unit's Business Continuity Plan. b) Ensure that computer access rights are accurate and up-to-date for their staff members. c) Notify Information Administrators (i.e., the individuals or organizational units responsible for implementing amendments to user access rights) of changes affecting access rights such as changes in staff roles/responsibilities, terminations, transfers, extended leaves of absence, etc. in accordance with established procedures. d) Ensure that staff members within the unit are trained and understand their security responsibilities.

2.4 Governance Roles and Responsibilities *(Cont.)*

Role (2.4.5)	**CSUS Security Standards Committee**
Members	The University Presidents or the Chancellor will appoint members with representation from each CSUS university and the System Office. The initial team will consist of the University/SO Information Security Officers and University/SO IT Security experts appointed by the CIO's. The composition of this team may evolve over time.
Key Security Responsibilities	a) Members will meet quarterly to review the impact of new technologies on existing standards and to share concerns and draft new or revised standards as appropriate. b) The committee will present new or revised standards to the CIT for their review and subsequent presentation to the COP and Chancellor as part of the review process.

Role (2.4.6)	**CSUS Information Security Officer**
Members	An individual assigned the role of CSUS Information Security Officer responsible for the oversight of the CSUS Information Security Program overall and the management of the SO Information Security Program.
Key Security Responsibilities	Coordinate security program activities and reporting processes in support of policy and associated standards. a) Act as consultant for all Information Security matters between CSUS units. b) Act as consultant for all Information Security matters between CSUS and external agencies. c) Provide audit and compliance oversight of the CSUS Information Security Program. d) Represent the University/System Office in all Information Security matters. e) Coordinate and oversees the University/System Office security program activities and reporting processes in support of policy, standards, and procedures. f) Act as Liaison for all Information Security matters between University/ System Office units. g) Act as Liaison for Information Security matters between University/System Office and external agencies. h) Maintain overall University/System Office responsibility for ensuring the implementation, enhancement, monitoring and enforcement of policy and associated standards. i) Due to concerns regarding segregation of duties, will not have IT operational responsibilities.

2.4 Governance Roles and Responsibilities *(Cont.)*

Role (2.4.7)	**University Information Security Officer**
Members	Individuals assigned the role of University Information Security Officer who are responsible for the oversight and management of the University Security Program. Each CSUS institution will designate an individual to fulfill this role.
Key Security Responsibilities	a) Represent the University/System Office in all Information Security matters. b) Coordinate and oversee the University/System Office security program activities and reporting processes in support of policy, standards, and procedures. c) Act as Liaison for all Information Security matters between University/ System Office units. d) Act as Liaison for Information Security matters between University/System Office and external agencies. e) Maintain overall University/System Office responsibility for ensuring the implementation, enhancement, monitoring and enforcement of policy and associated standards. f) Due to concerns regarding segregation of duties, should not have IT operational responsibilities.

Role (2.4.8)	**Information Steward**
Members	Any individual assigned responsibility for a CSUS Information Resource.
Key Security Responsibilities	a) Classify information assets with respect to confidentiality, integrity and availability. b) Determine who should have access to information resources within their jurisdiction, and what those access privileges should be (e.g., to read, to update, to print). Such access will be consistent with the Access Control and Data Security sections. c) Ensure that a backup and recovery process is in place for the information asset. d) Perform a risk assessment on assigned information assets. e) Implement the appropriate policies, standards and procedures based on the risk assessment. The Information Steward may choose to delegate some of these responsibilities to an Information Custodian.
Example	The Vice President for Finance could be designated as Steward for data held in the Banner Finance module.

2.4 Governance Roles and Responsibilities *(Cont.)*

Role (2.4.9)	**Information Custodian**
Members	Any individual to whom Information Steward responsibilities have been delegated.
Key Security Responsibilities	a) Execute whatever responsibilities the Information Steward has chosen to delegate.
Example	The Director of Accounting Services could be designated by the Steward as responsible for Accounts Payable data held in the Banner Finance module.

Role (2.4.10)	**Information Administrator**
Members	Individual assigned Administrator responsibilities by an Information Steward.
Key Security Responsibilities	a) Know their role and responsibilities in the preparation and execution of an IT Disaster Recovery Plan for the site/facility. b) Implement a program to backup and recover the information asset sufficient to restore applications, data and any system software/middleware. c) Grant access to the asset as authorized by Steward or Custodian. d) Ensure computer/communications equipment is housed in locations with suitable physical and environmental controls. e) Formalize and document operating procedures (e.g., permitting an ID, handling backup media).
Example	A Data Base Administrator could act as Information Administrator with responsibility for granting access to authorized Banner data.

2.5 Reports on Security Metrics

1. Reports capturing security metrics **will** be created and reviewed regularly.

2.6 Software Licensing

1. Only properly licensed software **will** be installed on CSUS Information Resources.
2. Periodic platform audits **will** be conducted to confirm compliance.

2.7 Security Compliance Audit

1. Regular review of compliance with existing information security policies, standards and procedures **will** be performed.
2. Audit requirements on mission critical systems **will** be carefully planned to minimize the disruption of business processes.
3. Resources for performing these audits **will** be identified and available.
4. Audit recommendations **will** be addressed in a timely manner.

2.8 Exceptions to Standards

The Chancellor, University Presidents or their designee may classify an information resource as an exception to a relevant Standard.

Exceptions **will** require:

1. Documented risk assessment using a specific form from the requestor identifying:
    a. vulnerabilities
    b. threats
    c. likelihood of event
    d. mitigating controls implemented to lessen the assessed risk
    e. potential impact of event assessed in monetary, temporal, legal and intangible terms
2. Documented signoff by a President or the Chancellor on the determined risk.
3. Commitment by the President or Chancellor to annually:
    a. Review the risk assessment and mitigating controls.
    b. Renew the exception for another year with a signoff.

See **Appendix D** for a sample Information Security Exception form.

3. ASSET & RISK MANAGEMENT

Purpose: The purpose of **Asset Management** is to ensure that CSUS Information Resources are identified, assigned a Steward, and classified. The purpose of **Risk Management** is to ensure that appropriate controls and countermeasures have been implemented to reduce risk to CSUS Information Resources to a level acceptable to management.

Term	Definition
Information Asset	For the purposes of this document the term "Information Asset" is used synonymously with "CSUS Information Resource." Assets are resources that have value to an institution and must be protected. Assets include file servers, routers operating systems, and student and financial records. Information Assets pertain to data (i.e., information) and the resources used to manage it during the data life cycle, i.e. usage, transmission, storage and disposal. Note: Information assets should not be confused with the financial term for "Fixed assets".

Standards:

3.1 Asset Identification

1. Each University and the System Office **will** conduct a survey of mission critical information assets and their supporting resources *(e.g., data, applications, servers, network, service provider).*

   Phase 1 of the inventory process should focus on mission critical assets. The asset inventory should eventually encompass all CSUS Information Resources.

3.2 Asset Inventory

1. Management and IT staff **will** create an inventory of mission critical CSUS Information Resources identifying each with appropriate information. Such identifying information may include:

   a) product/platform name
   b) vendor name
   c) release, when relevant
   d) data location, i.e. server(s) or PC(s)
   e) hardware location in building
   f) serial number or bar code tag
   g) designation as production or non-production

3.3 Information Steward

1. The Information Steward is responsible for ensuring that the asset classification and risk assessment of CSU Information Resources are completed. (*See **Governance** for Steward role and responsibilities.)*

3.4 Asset Classification

1. Information Stewards **will** classify assigned CSUS Information Resources as production or non-production. **Note:** Class A Data will require Class A Data controls even in a non-production environment. *(See **Data Security Section 6.2.1**.)*
2. Information Stewards **will** classify assigned CSUS Information Resources as Class A, B or C according to the classification guidelines listed below. The Information Steward **will** consider confidentiality, integrity and availability in assigning the appropriate classification.

CSUS Data Classifications

Classification	Description
Class A Data	• Confidential/Private • Availability of data is critical to operations (e.g., redundant systems with mirrored data) • High confidentiality, high integrity, medium to high availability • For example, social security numbers, configuration files, system logs
Class B Data	• Proprietary/Sensitive • Availability of data is important to operations (e.g., system/data restoration within 7 days of outage) • Medium confidentiality, high integrity, medium availability • For example, employee time logs, student transcripts, CSU System developed applications
Class C Data	• Non-Proprietary/Public • Availability of data is not needed for operations (e.g., system/data restoration within 30 days of outage) • Low confidentiality, medium integrity, low availability • For example, class schedules, official announcements, press releases

3.5 Risk Assessment

The Information Steward defines acceptable risk for a given asset. Although total risk elimination is impossible, particular risks can be eliminated, reduced/mitigated, transferred *(e.g., insurance)* or accepted by management.

1. Information Stewards **will** work with the University/SO ISO to perform a risk assessment on assigned CSUS Information Resources.
2. Information Stewards **will** implement security controls as documented in the risk mitigation plan and as approved by management.

4. PERSONNEL SECURITY

Purpose: The standards in this section are intended to ensure that all CSUS users understand their responsibilities regarding information security and that individuals seeking employment within the CSUS meet the information security criteria for the desired position.

Personnel security practices include: (a) identification, documentation and communication of CSUS users' roles and responsibilities with regard to information security; (b) processes and procedures to address changes in users' employment status and (c) implementation of appropriate and ongoing security awareness information, training and education.

Standards:

4.1 Users of CSUS Information Resources and Facilities

1. All users, including the public using CSUS Information Resources, **will** be required to adhere to established security policies and procedures.
2. Where possible, appropriate security policies and procedures **will** be made available for access.

4.2 Guests

1. As part of the terms and conditions for the use of CSUS Information Resources, Guests should agree to and sign acknowledgment of their responsibilities in accordance with established security policies and procedures.

4.3 Students & Alumni

1. As part of the terms and conditions for the use of CSUS Information Resources, Students and Alumni **will** agree to and sign acknowledgment of their responsibilities in accordance with established security policies and procedures.
2. Students and Alumni **will** be provided with notification and access to updates in security policies and procedures relevant to their roles and responsibilities.

4.4 CSUS Employees (Faculty, Staff, Student Workers, University Assistants, etc.)

1. An Employee's security roles and responsibilities **will** be defined, documented and communicated prior to employment.
2. Pre-employment background investigations **will** be conducted on all individuals for whom employment is to be offered.
3. As part of the terms and conditions for the use of CSUS Information Resources, Employees **will** agree to and sign an acknowledgment of their responsibilities in accordance with established security CSUS policies and procedures.

4. Employees **will** agree to and sign the terms and conditions of their employment, which **will** state their role and responsibilities regarding CSUS information security.
5. Processes **will** be in place to provide Employees with notification of and access to updates in security policies and procedures relevant to their roles and responsibilities.

4.5 Contractors and Third Party Vendors

1. Security roles and responsibilities of Contractors and Third Party Vendors **will** be defined, documented and communicated prior to employment.
2. Pre-Employment background investigations **will** be conducted on all Contractors and Third Party Vendors prior to the awarding of contracts.
3. As part of the terms and conditions for the use of CSUS Information Resources, Contractors and Third Party Vendors **will** agree to and sign an acknowledgment of their responsibilities in accordance with established CSUS information security policies and procedures.
4. As part of their contractual obligation, Contractors and Third Party Vendors **will** agree to and sign the terms and conditions of their employment, which **will** state their role and responsibilities regarding CSUS information security.
5. Processes **will** be in place to provide Contractors and Third Party Vendors with notification of and access to updates in security policies and procedures relevant to their roles and responsibilities.

4.6 Changes in Employment Status

Changes in employment status such as promotions, transfers, voluntary and involuntary terminations, demotions, and role changes require that the affected individual's access rights be evaluated and adjusted accordingly.

1. Processes and procedures **will** be defined and documented to address changes of employment.
2. The responsibility for performing employment termination or change of employment processes and procedures **will** be clearly defined, assigned and documented.
3. Upon change of employment, an employee's access rights to CSUS Information Resources **will** be removed or adjusted accordingly.
4. Upon termination of employment or contract agreement, all employees **will** return any CSUS assets in their possession.

4.7 Security Awareness, Training, and Education

Security awareness plays a critical role in safeguarding CSUS Information Resources. To be successful, Security Awareness initiatives must be ongoing and tailored to the user's role and responsibilities within the CSUS community.

1. A Security Awareness program **will** be defined and documented.
2. The Security Awareness program **will** be reviewed regularly and updated accordingly.
3. Users **will** receive the appropriate level of security awareness information, education and/or training based upon their roles and responsibilities within the CSUS community.
4. Individuals with roles and responsibilities specific to CSUS information security **will** be provided the requisite training and education to meet those responsibilities.
5. Security Awareness initiatives **will** be ongoing and accessible to all CSUS users.
6. Where appropriate, documented security training requirements for Employees, Contractors, and Third Party Vendors with roles and responsibilities related to CSUS Information Resources **will** be in place and reviewed regularly.
7. Where appropriate, documented security education requirements for Employees, Contractors, and Third Party Vendors with roles and responsibilities specific to CSUS information security **will** be in place.

Security Awareness
"Awareness **is not training**. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly."

Security Training
"The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties **other than IT security** (e.g., management, systems design and development, acquisition, auditing)."

Security Education
"The 'Education' level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce **IT security specialists** and professionals capable of vision and pro-active response."

NIST Special Publication 800-16

4.8 Disciplinary Process

1. There **will** be documented processes in place to address information security policy violations.

5. PHYSICAL & ENVIRONMENTAL SECURITY

Purpose: The standards in this section are intended to protect the confidentiality, integrity and availability of CSUS Information Resources by safeguarding the physical environment and infrastructure supporting those resources. Facilities that contain or transport Class A and Class B information assets must be protected from unauthorized physical access, natural or man-made disaster, theft and compromise.

Note: *Risk assessments should be made with respect to the value of CSUS information assets and the resources and efforts needed to protect those assets. While it is understood that there will be budgetary and time constraints, the value of these assets with respect to CSUS' ability to conduct normal university business should be strongly considered.*

Standards:

Unless stated otherwise, the standards in this section refer to areas normally managed by Information Technology departments, e.g. data centers, network distribution facilities, which process, store, and/or transport critical or sensitive information.

5.1 Securing the Physical Perimeter – *IT Facilities, e.g., data centers, network distribution facilities, etc.*

1. Perimeters of a building or site containing CSUS Information Resources **will** be physically sound, all external walls **will** be of solid construction and all external doors **will** be appropriately protected against unauthorized access.
2. Doors and windows **will** be locked when unattended and additional external protection should be considered for windows, particularly at ground level.
3. Suitable intruder detection systems *(e.g., secure video surveillance system, remote or local alarm systems)* should be installed on all external doors and accessible windows and tested regularly.
4. Intrusion detection systems in unoccupied areas should be activated at all times.

5.2 Physical Entry/Access - *IT Facilities*

1. Auditable security should be enforced. All entry and exit from facilities containing or processing CSUS Information Resources should be logged.
2. Access to facilities **will** be guided by the principles of least privilege. Where possible, entry and exit should be monitored *(e.g., with a secure video surveillance system and/or secure door access control system incorporating remote and/or local alarms)*;
3. Advance notification to local IT management/staff **will** be required prior to granting support personnel access to IT facilities.
4. Third party support personnel **will** be granted restricted access to secure areas or sensitive information processing facilities only when required; this access **will** be authorized and logged and should be monitored as appropriate.
5. Access rights to secure areas should be regularly reviewed, updated and revoked when necessary.

5.3 Protecting Against External and Environmental Threats – *IT Facilities*

1. Facilities **will** be located in a manner that reduces the risk of environmental and/or man-made damage.
2. Hazardous or combustible materials **will** be stored at a safe distance from a secure area.
3. Bulk supplies or other non-secure area related supplies *(e.g., custodial or maintenance supplies)* **will** NOT be stored within a secure area.
4. Non-secure area related services *(e.g., water mains, heating pipes, etc.)* **will** NOT be located within or require access through the secure area.
5. Facilities should have regularly scheduled environmental inspections and cleanings performed.
6. Environmental control systems **will** be installed and periodically checked and maintained for proper function. Depending on the established level of risk, the following environmental control systems **will** be in place:

    - Water and moisture detection systems.
    - A fire suppression system that meets current regulations.

7. Environmental control systems **will** have the electronic notification capability *(e.g., via email, page, text message,)* to alert appropriate personnel of a potential or actual system failure.

5.4 Supporting Utilities – *IT Facilities*

1. Supporting utility control systems **will** be installed and periodically checked and maintained for proper function. Depending on the established level of risk, the following supporting utility control systems should be present:

    a. An uninterrupted power supply system (UPS) capable of maintaining critical load.
    b. A backup generator capable of handling all necessary power requirements in the event of a power outage along with an adequate and regularly maintained supply of fuel.
    c. Air conditioning with temperature and humidity controls capable of handling the requirements of all equipment in the facility. When possible, such controls **will** be configured for failover to the backup generator system.

2. Supporting utility control systems should have notification *(e.g., email, page, text message)* of a failure or potential failure of the system.
3. Emergency power off switches should be located near emergency exits to facilitate rapid power down in an emergency.
4. Emergency lighting in critical areas **will** be provided and connected to a generator or emergency lighting system for the building.

5.5 Public Access – *Non-IT Areas*

Areas that are accessible to the public or vulnerable to unauthorized entry should be isolated from information processing facilities.

5.6 Securing Offices, Rooms, and Facilities – *IT and Non-IT Areas*

Offices, rooms, and facilities that process, store, print or transport critical, sensitive or confidential information should be evaluated in terms of physical and environmental security and the proper safeguards should be put in place. (See Data Security Section 6.2)

5.7 Equipment Re-use & Disposal

1. All equipment containing storage media **will** be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to reuse or disposal.
2. Devices containing sensitive data **will** be deleted or overwritten using techniques to make the original information non-retrievable *(e.g., DOD compliant wipe/delete)* rather than using the standard delete or format function. (*See "CSU System Procedure Disposal of Surplus Property."*
3. Procedures **will** be established to address reuse and re-deployment of PCs and servers.

5.8 Equipment Location & Protection

1. Guidelines addressing the location of equipment that processes sensitive data should be established *(e.g., positioning in relation to viewing angle by unauthorized persons).*
2. Equipment requiring special protection should be isolated to reduce the level of protection required.
3. Controls **will** be adopted to minimize the risk of potential physical threats, (*e.g., fire, smoke, water, dust, electrical supply interference, theft and vandalism.)*
4. Guidelines for eating, drinking and smoking near information processing facilities should be established.

5.9 Cabling

1. Power and telecommunications cabling carrying CSUS data should be protected from interception and/or damage. *Refer to CSUS Telecommunication wiring standards document.*

5.10 Equipment Maintenance

1. Maintenance should be followed in accordance with the supplier's recommended service intervals and specifications.
2. Only authorized maintenance personnel or trained personnel should carry out repairs and service.

5.10 Equipment Maintenance *(Cont.)*

3. Detailed records should be kept of all suspected or actual faults along with the preventive and corrective maintenance performed.

5.11 Removal of Property

1. CSUS equipment, information or software **will** not be taken off-site without prior authorization.
2. Employees, contractors and third party users who have authority to permit off-site removal of assets **will** be clearly identified.
3. Removal time period **will** be established upfront and compliance checks in place for returns.
4. For inventory audit purposes, a record **will** be kept when equipment is removed and when it is returned.

5.12 Off Premises

1. To lessen the risk of theft, equipment and media taken off premises **will** not be left unattended in public places or an automobile.
2. Control for working remotely should be determined by a risk assessment and suitable controls applied *(e.g., lockable storage or filing cabinets*).
3. Appropriate access controls for secure communications back to the office should be implemented.
4. Adequate insurance and warranty coverage should be in place to protect critical equipment off site.

6. LOGICAL SECURITY

This section of the document outlines Information Security Standards for the following:

6.1 ACCESS CONTROL

Purpose: The standards in this section are intended to ensure the confidentiality, integrity and availability of CSUS Information Resources through the development and implementation of well-defined access control processes and procedures.

Standards:

6.1.1 Access Control Process

The access control process is based on the established rules and procedures for granting, managing and removing user rights to access CSUS Information Resources.

1. The access control process **will** be defined and documented.
2. The access control process **will** be based on the premise that access to CSUS Information Resources is prohibited unless expressly granted.
3. Where possible, standard access profiles for types of CSUS users and/or roles **will** be developed.
4. Access control rules and rights for various types of CSUS users **will** be developed and reviewed regularly.
5. Responsibility for granting, documenting and periodically reviewing individual access rights **will** be clearly identified.
6. Responsibility for changing or removing access rights **will** be clearly identified.
7. Provision for auditing the access control process **will** be included.
8. Provision for reviewing and modifying the access control process **will** be included.

6.1.2 Authorizing Access

Authorization is the process of granting an individual access rights to specific systems, information or resources.

1. Access to CSUS Information Resources **will** be driven by pedagogical and business requirements.
2. Procedures used to grant, document, review, modify, delete and audit access rights to confidential and sensitive information **will** be clearly defined and documented.
3. The procedure used to grant and change access rights **will** include approval by one level of management and review by a second level of management for confidential and/or sensitive information.
4. Users with access to confidential and/or sensitive material **will** be provided with a written statement of their access rights.
5. ID's used to access CSUS Information Resources **will** be unique and auditable. Exceptions may be permitted where there is justification based on pedagogical or business needs. The need for such exceptions **will** be documented and frequently reviewed.
6. Users of CSUS Information Resources **will** agree to all conditions of access.

6.1.3 Managing Privileged Access

Privileged access to systems includes access beyond the normal scope such as the ability to change or modify operating system and application processes, root access and the ability to configure network devices. When systems require or permit the assignment of privileged activity to individual users, the following standards **will** apply:

1. Privileges **will** be granted to individuals based on the minimum required to fulfill their job responsibilities and only for the period of time they are needed.
2. The procedures used to grant, document, review, modify, delete and audit privileges **will** be clearly documented.
3. The procedure used to grant and change privileges **will** include approval by one level of management and review by a second level of management.

6.1.4 Authenticating Users

Authentication is the process of verifying a user's identity. One method of doing so is to base that identification on something the user knows such as a password or personal identification number.

1. Assuming that single factor authentication based on passwords is the method currently used to authenticate users, the access control process **will** specify techniques and strategies for maintaining password integrity.

6.1.4 Authenticating Users *(Cont.)*

2. An acknowledgement or agreement to keep passwords confidential **will** be signed by the user and retained. Exceptions may be permitted when justified based on pedagogical or business needs. The need for such exceptions **will** be documented and frequently reviewed.

3. Passwords **will** be constructed to meet the current industry standard for strong passwords such as minimum number of characters, incorporation of special characters, prohibition of reuse of passwords, minimum age requirements, and password expiration.

   Recommended password guidelines for privileged and system level passwords include:

   - minimum of eight characters
   - upper and lower case characters
   - at least one punctuation character and one numeral
   - random sequence of characters (not a word or name
   - expiration quarterly or more frequently

   Recommended password guidelines for user level passwords include:

   - minimum of six to eight characters
   - upper and lower case characters
   - at least one punctuation character and one numeral
   - random sequence of characters (not a word or name)
   - expiration every four to six months

4. Procedures to identify a user before making a password change or providing a new password **will** be in place.
5. Procedures to educate users regarding the creation and maintenance of secure and confidential passwords **will** be included in the Security Awareness Training.
6. Procedures to assign and maintain secure, temporary passwords and to insure their immediate replacement by the user **will** be documented and implemented.

6.1.5 Critical System Access Control

The most widely used authentication method within the CSUS is a single factor process based upon a user's confidential knowledge of a password. For sensitive and critical systems and equipment a stronger authentication process is warranted. Additional practices, although they may not meet the full requirements of multi-factor authentication, can provide effective safeguards

1. Procedures used to identify CSUS Information Resources that require a stronger access control process **will** be documented and implemented.

6.1.5 Critical System Access Control *(Cont.)*

2. Once implemented, a stronger authentication process at the network, system and user levels **will** be documented. The following practices should be considered for adoption:

    a. Access control lists
    b. Kerberos or other secure authentication systems such as TACACS+
    c. Requirement that management of a device be performed from a specific, restricted physical location or station.
    d. Authentication token devices
    e. A multi-single factor method

6.1.6 Network Access

Openness and ease of access to multiple resources are important requirements of a productive, engaging learning environment. Additionally, the mission of CSUS institutions requires that local networked information and resources via the web be accessible to individuals with no formal relationship with those institutions. As a result, access control to networked resources is especially challenging.

The access control standards identified in this section are directly related to network infrastructure and architecture. At the same time, the technologies used in the network infrastructure and those used to access the network, locally and remotely, are related to access control standards.

1. Procedures used to identify groups of users of networked resources, based on the nature of their relationship to the institution *(e.g. formal - student, faculty, staff, vendor, etc. versus informal - local or remote visitor)* **will** be defined, documented and implemented.

2. Procedures used to determine the networked information and resources to which each type of user is granted access **will** be defined, documented and implemented.

3. Authentication process and requirements for each type of user **will** be defined, documented and implemented.

4. Access control procedures and requirements for various technologies used to access the campus network **will** be defined, documented and implemented.

6.2 DATA SECURITY

Purpose: Standards in this section are intended to ensure that CSUS data is secured with respect to confidentiality, integrity and availability during all phases of the data life cycle, i.e. usage, transmission, storage and disposal.

Data security practices are designed to protect information regardless of its form *(e.g., electronic, viewable on monitors, print).* The more critical data is to CSUS operations, the greater the need for its protection. Thus, a key aspect of data security is the classification of data with respect to CSUS operations.

Standards:

6.2.1 General Data Standards

1. The Classification standards previously defined in the **Asset & Risk Management** section of this document **will** be applied when classifying data. *See table below*:

CSUS Data Classifications

Classification	Description
Class **A** Data	• Confidential/Private • Availability of data is critical to operations (e.g., redundant systems with mirrored data) • High confidentiality, high integrity, medium to high availability • For example, social security numbers, configuration files, system logs
Class **B** Data	• Proprietary/Sensitive • Availability of data is important to operations (e.g., system/data restoration within 7 days of outage) • Medium confidentiality, high integrity, medium availability • For example, employee time logs, student transcripts, CSU System developed applications
Class **C** Data	• Non-Proprietary/Public • Availability of data is not needed for operations (e.g., system/data restoration within 30 days of outage) • Low confidentiality, medium integrity, low availability • For example, class schedules, official announcements, press releases

2. Unclassified data **will** be assigned a Class B Data status by default.

3. Supporting IT resources **will** be configured with controls consistent with the requirements of the most restrictive Data Class using the resource. Therefore, Class A Data will require Class A Data controls even in a non-production environment.
4. Copies of data **will** conform to controls at least as strong as the designated official source for confidentiality purposes.
5. Copies of data should be refreshed appropriately to remain consistent with the data in the **System of Record** for integrity purposes. See below:

Term	Definition
SYSTEM OF RECORD	The repository of record for data as identified by the Steward. **Example:** The Steward may designate CoreCT as the System of Record for employee information. If a university maintains a copy of that information in the Banner Human Resources System, the copy should be protected with controls at least as good as those found in CoreCT. Similarly, if an individual downloads a copy of the employee information to their workstation or a flash drive, the copy should be protected with comparable controls.

6. The following data encryption standards **will** be applied:
    a. Unauthorized encryption of CSUS data **will** be prohibited.
    b. Only authorized encryption tools with keys managed by the University/System Office Information Security Officers **will** be applied to CSUS data.
    c. All encryption keys **will** be maintained in a protected area with documented auditable access.
    d. Two-party access, such as IT and Finance, **will** be required to make an encryption key available.
    e. Custodian **will** maintain tools to make data available when needed *(e.g., key to decrypt certificate recognized as trusted*).

6.2.2 Data Standards Specific to Class A Data:

1. Whenever possible, Class A Data **will** be encrypted when stored locally, off the server, to prevent unauthorized access of stored data. This includes:
    - desktop systems (remote and in the office),
    - mobile systems, e.g., laptops, PDA's and
    - portable storage devices, e.g., floppies, CDs, USB flash drives.

6.2.2 Data Standards Specific to Class A Data *(Cont.)*

2. Class A Data in print or written form **will** be physically protected, *(e.g., stored in a locked room or file cabinet*).
3. Whenever possible, the integrity of stored Class A Data **will** be secured by a host-based intrusion detection system.
4. Hash totals **will** be used to validate the integrity of system configuration files associated with Class A Data
5. Class A Data in print or written form **will** be properly destroyed *(e.g., via shredder, incineration).*
6. When an email is transmitted over an untrusted public network, any attachments containing Class A Data **will** be appropriately encrypted.

6.2.3 Data Standards Specific to Class A & B Data:

1. Class A or B data **will** NOT be stored on a computer or printed on paper in an unattended public access area such as a computer laboratory.
2. Class A or B data should be encrypted before being transmitted over an untrusted public network.
3. Class A or B data **will** be protected from unauthorized viewing *(e.g., via screen covers, private fax machines and printers).*
4. Access to Class A or B data **will** be granted only to accountable ID's, i.e., unique ID's with authentication and audit.
5. Class A or B data stored electronically on optical or magnetic media such as CD, DVD, floppies, tape **will** be destroyed appropriately for the medium *(e.g., shred, incinerate, overwrite as described below).*
6. Data stored electronically on computer equipment **will** be destroyed in accordance with Board Resolution #96-28 "*CSU System Procedure Disposal of Surplus Property.*" (*See **Physical & Environmental** Security.)*

6.2.4 Data Standards for all CSUS Data:

1. Users **will** lock or log off their computers when they are not present.
2. A service level agreement specifying expected availability for all data **will** be in place.

6.2.5 Summary of Data Class Standards

The following grid summarizes the data security standards outlined in this section:

Data Security Standard	**Class A** (Confidential/ Private)	**Class B** (Proprietary/ Sensitive)	**Class C** (Non-Proprietary/ Public)
1. If unclassified, set to Class B	x	x	x
2. IT resource controls will be consistent with Data Class	x	x	x
3. Copies will conform to controls as strong as source; updated for consistency with source.	x	x	x
4. Encryption rules for data stored locally	x		
5. Encrypt on PCs with multiple users	x		
6. Store print data in locked area	x		
7. Utilize host-based intrusion detection to detect change	x		
8. Utilize hash totals for system configuration files	x		
9. Shred data on paper	x		
10. Protect from public access/viewing	x	x	
11. Encrypt data before untrusted transmission	x	x	
12. Protect from unauthorized viewing	x	x	
13. Grant access only to accountable IDs	x	x	
14. Destroy computers/devices with storage	x	x	
15. Lock or log off when not present.	x	x	x
16. SLA specifying availability	x	x	x

6.3 NETWORK SECURITY

Purpose: Standards in this section are intended to ensure that CSUS electronic data is appropriately secured with respect to confidentiality, integrity and availability during all phases of the data transport life cycle. It is essential that protection of information and the supporting infrastructure used for delivery be built into the Connecticut State University System network. *(ISO/IEC 17799 2005 Sec 10.6)*

Standards:

6.3.1 Secure Network Services

1. Security parameters, service levels and management requirements for public network services (T-1's, broadband) and university owned network services **will** be defined and documented in any in-house network services agreements as well as those with outside network service providers.
2. Managed network access control systems such as intrusion detection / prevention systems and firewalls **will** be in place.
3. Validation of minimum security standards (such as through Cisco Clean Access) for all network and system devices **will** be required before access to CSUS network services are made available.
4. Secure remote connections such as Virtual Private Networks (VPN) and Secure Sockets Layer (SSL) **will** be implemented for access to all CSUS information deemed confidential and sensitive. Guidelines and restrictions on the effective use of such connections should be included in any remote access policies and procedures.
5. Wireless access to CSUS network services **will** be through a CSUS managed gateway that controls access based on user role.
6. Wireless access should include effective monitoring controls such as logging of user id's and dates, times, and duration of access.

6.3.2 Network Access Control

1. Network authentication, access and accounting mechanisms **will** be applied for users and equipment *(ISO/IEC 17799 2005 Sec 11.4)*
   Note: *Authentication* identifies a user; *Authorization* determines what that user can do; and *Accounting* monitors the network usage time for logging, record and security purposes.
2. Policies and procedures **will** be in place to limit, control, remove and authorize access to network services (*See **Access Control.***)
3. User access to network services **will** be based on level of authorized use.

4. Systems and networks responsible for the processing and transmission of CSUS information deemed confidential and sensitive **will** be separated from all other networks and systems resident on the University-owned network, i.e., segregation of networks.

   Network and System tools that can provide such segregation include:
   - Virtual Local Area Networks (VLAN)
   - Access Control Lists (ACL)
   - Virtual Private Networks (VPN)
   - Unique Internet Protocol (IP) addressing schemes such as non-routable subnets.

5. Development, test, and pre-production systems **will** be installed on a network separate from the operational, i.e., production network.

6. Critical safeguards such as VLAN's, ACL's, VPN's and non-routable subnets should be implemented to enable effective securing of the CSUS network.

6.3.3 Network Management & Control

1. Privileged access to network devices and servers **will** be separated based on roles and responsibilities. (*See **Governance**.)*
2. Secure remote management of network equipment **will** be conducted on a network separate from the university production network. This may be accomplished via a separate management VLAN. (*ISO/IEC 17799 2005(E) Sec. 10.6.1 b)*
3. Network management and monitoring (status, alarms, logs, reporting) **will** be sufficiently applied to ensure the CSUS network remains secure and operates efficiently and cost effectively. Such management **will** include:
   a. **Configuration** - track system and network configuration changes and resulting effects on the network.
   b. **Accounting** - measure network utilization parameters so one group does not consume excessive bandwidth.
   c. **Fault** - detect, log, and notify users of network problems.
   d. **Security** - control access to network resources to prevent accidental or intentional sabotage and unauthorized access to confidential and sensitive CSUS information.
   e. **Performance** – monitor bandwidth usage and associated trunk statistics to maintain optimal application performance over the CSUS network.

4. Secure Protocols such as SSH and HTTPS **will** be employed for confidential and sensitive CSUS information such as online financial transactions via secure server.
5. Basic identity management mechanisms (authentication, authorization, access control) for access **will** be implemented and regularly reviewed. This includes in-house, remote, and third party access.
6. A bandwidth management system (such as Packetshaper) **will** be used to monitor and control bandwidth usage. Quality of Service (QOS) should be implemented for mission critical applications such as an Enterprise Resource Planning (ERP) system.

6.4 HOST & OPERATING SYSTEM SECURITY

Purpose: Standards in this section are intended to prevent unauthorized access to and maintain maximum availability of host and/or operating systems.

Standards:

6.4.1 Host and Operating System Installation and Deployment

1. A designated individual or group will be clearly identified to administer and maintain the host and operating system throughout its lifecycle.
2. A process to identify, assess, approve and install software on CSUS owned equipment **will** be defined and documented.
3. Software **will** be installed and used in accordance with license agreements.
4. Wherever possible, a standard image or process **will** be developed to ensure a consistent installation occurs.
5. Periodic review of the host and/or OS image **will** be performed.
6. Wherever possible, hosts and/or operating systems **will** be installed in a segregated network, a logically-independent network that isolates new hosts and operating systems from the production network.
7. Vulnerability assessment and mitigation **will** be performed prior to use in the production network

6.4.2 Protection against Malicious Software

Securing systems against the introduction of malicious software will require proper system controls, security awareness training, and change management procedures. Malicious software includes but is not limited to computer viruses, computer spyware, network worms, Trojan Horses, and denial of service attacks. *(ISO/IEC 17799 2005 Sec 10.4)*

1. Use of unauthorized software **will** be prohibited.
2. Only services deemed required **will** be available, e.g. SMTP, telnet, http.
3. The software and data content of mission-critical systems **will** be reviewed periodically to detect the presence of unauthorized files, either executable or data. *(ISO/IEC 17799 2005(E) Sec 10.4.1 c).*
4. Files from unknown sources **will** be reviewed before use.
5. Whenever possible, application level firewalls **will** be installed on all hosts or operating systems.

6.4.2 Protection against Malicious Software *(Cont.)*

6. Whenever possible, intrusion detection/prevention software **will** be installed on all hosts or operating systems.
7. Whenever possible, anti-virus software **will** be installed and updated on all hosts or operating systems as necessary.
8. Whenever possible, anti-spy ware software should be installed and updated on all hosts or operating systems as necessary.
9. Malicious software warnings and bulletins distributed to the CSUS community **will** be accurate, timely and informative.

6.4.3 Vulnerability Assessment and Mitigation

Vulnerability assessment and mitigation is the process of identifying and quantifying vulnerabilities in a system and the process by which they are corrected.

1. Assessments **will** be performed regularly as well as prior to any new system gaining access to the network.
2. Vulnerabilities **will** be categorized into appropriate risk levels.
3. Mitigation practices **will** be established and implemented for each risk level whenever possible.

6.4.4 Patch Management

Patch management includes procedures for identifying, evaluating, approving, testing, installing, and documenting patches.

1. Patches **will** be divided into the following three categories:
    a. **Critical** - Patches that directly address a security threat that has the potential to impact computer or network resources.
    b. **Non-Critical Hotfixes** - Patches that have minimal or no security implications.
    c. **Service Packs** – A single update package containing many individual patches.
2. The designated administrator(s) will evaluate, assess and implement patch management for the hosts and operating systems in their control.
3. Procedures for identifying software vulnerabilities and patch information **will** be established.
4. Prior to installing a patch, an evaluation to assess the technical, business, and security implications **will** be performed.
5. All patches that are NOT installed should be documented.
6. Whenever possible all patches **will** be tested in a proper test environment.
7. Prior to installation, proper backup and back out procedures **will** be created.
8. Patches **will** be applied in a timely manner to prevent exploitation of the host or operating system.

6.4.5 Upgrade Management

Upgrade management includes procedures for identifying, evaluating, approving, testing, installing, and documenting upgrades. Upgrades can offer improved features and correct errors in existing code. Operating Systems should only be upgraded when there is a requirement to do so.

1. The designated administrator(s) will evaluate, assess and implement patch management for the hosts and operating systems in their control.
2. Prior to installing an upgrade, an evaluation to assess the technical, business, and security implications and needs **will** be performed.
3. Whenever possible all upgrades **will** be tested in a proper test environment.
4. Prior to installation, proper backup and back out procedures **will** be created.
5. Vendor supplied software used in operational systems should be maintained at a level supported by the supplier.

6.4.6 System Monitoring

System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to security standards. The CSUS will comply with all relevant legal requirements applicable to its monitoring activities. *(ISO/IEC 17799 2005 Sec 10.10)*

1. Hosts and operating systems **will** be monitored and security events **will** be recorded.
2. Where possible and relevant, logs should include:
    a. User ID's
    b. Dates, times and details of key events
    c. Terminal identity or location
    d. Records of successful and rejected system access attempts
    e. Changes to system configurations
    f. Use of privileges
    g. Use of system utilities and applications
    h. Network addresses and protocols
    i. Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.
    j. Origin of fault
3. A process to maintain and retain critical log files **will** be developed.
4. Log files **will** be secured to prevent unauthorized alterations.
5. A separate log on a separate server **will** be created for critical **Class A** Data.
6. A process and/or system should be developed to review log files.

6.4.7 Capacity Management

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. *(ISO/IEC 17799 2005 Sec 10.3)*

1. Projections of future capacity requirements **will** be performed regularly to reduce the risk of system overload.
2. The operational requirements of new systems **will** be established, documented, and tested prior to their acceptance and use.
3. Monitoring and assessing of critical system resources should be performed regularly.

6.4.8 Clock Synchronization

1. The clocks of all managed hosts and operating systems **will** be synchronized with an agreed accurate time source where possible. *(ISO/IEC 17799 2005 Sec 10.10.6)*
2. A procedure should be created that checks and corrects any drift in time.

   Example: One internal host or operating system should be set to synchronize with an external trusted time source, e.g. pool.ntp.org, and all internal clients should point to the dedicated internal host.

6.5 APPLICATION SECURITY

Purpose: Standards in this section are intended to ensure that applications are appropriately secured with respect to confidentiality, integrity and availability throughout the life of the application. Appropriate protection is a function of Application Classification. The more critical an application is to CSUS operations, the greater the need for protection. Mission critical applications are defined as enterprise software whose failure impacts the business operations of the CSUS.

Standards:

6.5.1 Application Classification

1. Applications **will** be classified and appropriate security controls **will** be applied based on risk assessment.
2. Applications **will** be classified considering employing the following criteria:

Class Type	Description
Class A Applications:	• The entire (or a large portion of the) organization cannot function when failed • High Utilization • Encompassing data is of high value • Availability and integrity is critical • Examples: ERP applications - the CSU Banner system, email
Class B Applications:	• Numerous individuals cannot function without • Active or infrequent utilization • Medium to high value data • Availability and integrity is important
Class C Applications:	• Low utilization • Availability and integrity is desired • For example, test and non-production systems

6.5.2 Application Availability

1. Application availability **will** be ensured through hardware and software redundancy and designated/dedicated administration of the application system as appropriate based on application classification.

6.5.2 Application Availability *(Cont.)*

2. The following infrastructure recommendations **will** be in place to support Class A and Class B application availability:
    a. A designated individual(s) **will** be assigned for Class A and Class B application administration
    b. Administrative tasks **will** be defined and documented
3. Hardware and software architectures should be designed to maximize the availability of applications. This availability can be achieved by:

Recommended Hardware Architecture:

- Raid storage
- Error correction memory
- Multiple network pathways
- Failover hardware

Recommended Software Architecture:

- Multi-Tiered software design model
- Replication of data

Backup/recovery of data: (*See **Backup, Storage & Recovery**.)*

6.5.3 Application Provisioning and Maintenance

1. Capacity planning **will** take place for Class A applications.
2. Resource planning, security requirements and controls for new Class A applications **will** be addressed as part of the project planning process.
3. The operational requirements of new Class A applications **will** be established, documented and tested prior to their acceptance and use.
4. A Service Level Agreement **will** be defined and documented.
5. The planning and management of the application's lifecycle on organization security **will** be defined, documented and regularly reviewed.

6.5.4 Application Development & Configuration

1. Where possible and appropriate, applications **will** require secure authentication.
2. Based on data class, encryption requirements should be evaluated and implemented accordingly. (*See **Data Security.***)
3. Appropriate controls should be designed into applications to ensure correct processing, including validation of input data, internal processing, and output data. *(ISO/IEC 17799:2005(E) 12.2)*

6.5.4 Application Development & Configuration *(Cont.)*

4. The use of Class A information for testing purposes should be avoided. If used, controls allowing access to the information in the non-production environment **will** be the same as the controls used to access the information in the production environment.
5. Access to program source code **will** be restricted.*(ISO/IEC 17799:2005(E) 12.4.3)*
6. Before any changes to the operating system are implemented, Class A applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. *(ISO/IEC 17799:2005(E) 12.5.2)*
7. All modifications such as patches, upgrades and enhancements, when required, **will** follow an established Change Management Process. *(See **Change Management**.)*

7. OPERATIONAL SECURITY

This section of the document outlines Information Security Standards for the following:

7.1 Disaster Recovery & Contingency Planning
7.2 Backup, Storage & Recovery
7.3 Security Monitoring
7.4 Incident Management
7.5 Change Management

7.1 DISASTER RECOVERY & CONTINGENCY PLANNING

Purpose: The standards in this section are intended to counteract interruptions to business activities, to protect mission critical processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. *(ISO/IEC 17799:2005(E) section 14.1)*

Disaster Recovery and Contingency Planning are necessary to mitigate the effects of a natural or man-made disaster, accident, equipment or resource failure. Such plans must provide an organized, collaborative and well-rehearsed response to such events in order to recover all services necessary for the institution to function in a timely manner.

Disaster Recovery and Contingency Planning is the responsibility of ALL administrative and academic units of the CSUS. The IT Disaster Recovery/Business Resumption Plan is an integral part of, and will be incorporated in, any overall University/System Office Crisis Management Plan. Because the activities in the various phases of Contingency Management are so tightly linked, it is important to provide consistent governance and oversight of the entire contingency planning process. The following standards are intended to ensure this consistency and produce a contingency planning process that enables institutions to recover mission critical information technology resources.

*** Note:** *Disaster recovery and business resumption planning should be made with respect to the value of CSUS information assets/resources and their importance in conducting normal business of the institution. While it is understood that there will be budgetary and time constraints, it should be recognized that in the event of a disaster or emergency, the institution's ability to resume critical and non-critical levels of service will be directly related to the effort and resources spent on this process.*

Standards:

7.1.1 Information Technology Business Risk and Impact Analysis

1. Business resumption planning by Universities and System Office **will** include an IT Business Risk assessment and Impact Analysis. The purpose of this activity is to correlate academic and administrative functions with specific IT functions and services.
2. The analysis by each business area within each CSU institution **will** identify and prioritize mission critical functions should operations be partially or completely shut down. Prioritization **will** be based on the impact of the disruption of such a service.
3. The analysis **will** identify financial, organizational, technical, and environmental resources needed to recover mission critical services. It may include analysis and recommendations for optional methods of providing services, such as alternate data center sites, third party recovery services and insurance options.

7.1.2 Information Technology Business Continuity/Service Recovery (BC/SR) Plan

Standards in this section strictly address the Information Technology component of Business Continuity/Service Recovery planning. It is recognized that strategies in this plan may be altered depending on the severity, circumstances and impact of a given disaster or accident.

1. Based on the results of the institution-wide Business Impact Analysis, a detailed and structured IT BC/SR Plan **will** be developed with input from all business units of the institutions.
2. The IT BC/SR Plan **will** be documented and should be included as part of a larger crisis management plan for the institution.
3. After initial development, the IT BC/SR Plan **will** be reviewed on an annual basis.
4. The BC/SR Plan **will** be developed with the following assumptions:
    a. Personal safety **will** always take precedence over recovery of equipment and/or services.
    b. A recovery strategy for every service that is defined as critical in the Business Impact Analysis **will** be developed and documented.
    c. The corresponding financial, organizational, technical, and environmental resources of each recovery strategy used **will** be identified.
    d. Response and recovery teams, including membership and contact information **will** be identified.
    e. Roles, responsibilities, and basic tasks of each team, including coordination mechanisms and procedures, **will** be identified.
    f. Timelines and milestones **will** be developed for the recovery of all mission critical services.
    g. A communications plan **will** be developed and documented.
    h. Within reasonable limits of funding, time, and resources, the plan **will** be tested on an annual basis. Results of such testing **will** be reported to management.
    i. To the extent possible, the Universities and the System Office should work cooperatively to provide temporary alternate resources (e.g. data center space, used equipment, manpower) to each other in the event of a disaster or emergency.

7.2 BACKUP, STORAGE & RECOVERY

Purpose: The standards in this section are intended to ensure the integrity and availability of CSUS electronic data by protecting it from loss or corruption due to events such as natural or man-made disasters, system or hardware failures and human error.

Standards:

7.2.1 Backup Process & Procedures

1. Procedures for backing up mission critical information **will** be defined and documented.
2. Procedures for identifying non-critical but essential system and information to be backed up **will** be defined and documented.
3. Users and administrators of a Desktop/laptop PC's **will** be responsible for making and keeping backups of their own local hard drives. Only network drives provided by the University **will** be backed up.
4. A record of all backup processes performed, including verification of their success, **will** be maintained.
5. All CSUS production information **will** be backed up on a regular basis.
6. A system backup **will** be performed before and after major changes to any operating system, system software or applications.
7. To avoid loss of data changes between scheduled backups, a manual, unscheduled backup process **will** be defined for protecting production data.
8. All network backup procedures **will** ONLY be performed on CSUS owned or the trusted network.
9. To streamline the backup and recovery process, a centralized backup strategy should be considered at each institution.
10. The extent *(i.e. full or differential backup***)* and frequency of backups **will** be determined by some or all of the following factors:
    a. Business risks/requirements of the organization (e.g. value of data)
    b. The criticality of the information to continuity of CSUS operations.
    c. The security requirement(s) associated with the data.
    d. Effort required to re-create the information if lost.
    e. Frequency with which the information changes (e.g. data/software/configurations).

*** Note:** A ***Full backup***, also known as a master backup, includes every file on a particular system regardless of whether any changes have occurred. *A* ***Differential backup*** includes every file on a system that has changed since the last full backup. Each consecutive differential backup compounds the changes from the previous one, allowing the last differential to contain all of the changes since the last master.

7.2.2 Testing

1. Backup media **will** be tested regularly to ensure that it is reliable, complete and efficient.
2. Regular tests of mission critical systems backup data should be performed in a safe environment to verify that the system can be recovered from backups.
3. Precautions **will** be taken when upgrading hardware, software, operating systems, applications and other technologies to ensure that backup data is readable in the new environment.

7.2.3 Onsite and Offsite Storage

1. An onsite backup storage process **will** be developed to ensure current data is readily available in machine-readable form in the production area should operating data be lost, damaged, or corrupted.
2. An off-site backup storage process **will** be developed for data requiring longer-term protection in a controlled environment and data that requires less frequent updating.
3. The offsite storage location **will** be at a distance sufficient to avoid damage from a disaster at the main site.
4. The security controls (i.e. logical and physical security) applied to the onsite and offsite backup information and resources **will** be at least as strong as the primary resource.
5. Service level agreements **will** be required for any contract with an external vendor that provides off-site storage of data *(e.g., response time*). Backup media **will** be retrievable within a procedurally defined period of time. All recovery requests should be documented.

7.2.4 Recovery

1. Restoration procedures **will** be defined, implemented, documented and tested regularly to verify effectiveness and to ensure their completion within the time allotted.
2. Logs of all data recovery processes performed should be maintained to verify that all necessary procedures were followed.

7.2.5 Retention

1. The retention period for back ups containing mission critical information and any requirements for copies to be permanently retained **will** be defined, documented and implemented.
2. A cycle of backup media should be used for all backups *(e.g., daily, weekly, monthly).* At least one copy of each cycle should be stored off-site.
3. A cycle of backup media of all data required to meet CSUS operational, legal or statutory obligations **will** be retained.

7.2.6 Data Archiving

Data archiving is the process of backing up and storing data for an extended period or permanently. Archived data is not affected by rotation of other scheduled backups.

1. Procedures **will** be defined and documented for securely storing and aging archived data.
2. Procedures **will** be defined and documented for the secure disposal of archived data.

7.3 SECURITY MONITORING

Purpose: The standards in this section are intended to ensure that CSUS information security policies, procedures and controls are being followed and are effective in ensuring the confidentiality, integrity and availability of CSUS Information Resources. This is accomplished through security monitoring and intrusion detection processes that are used to identify and document unauthorized activity as well as information faults and exceptions.

Standards:

7.3.1 Security Monitoring

1. Procedures for monitoring use of CSUS Information Resources **will** be established based on risk and **will** be documented.
2. Results of monitoring activities **will** be reviewed regularly by authorized personnel.
3. When possible, notification of monitoring activity **will** be provided.
4. Personnel responsible for security monitoring **will** be designated and their responsibilities **will** be documented.
5. Monitoring requests **will** be authorized and documented.
6. Monitoring **will** only be performed by authorized personnel.
7. Automated processes to detect and alert unauthorized activity regarding CSUS Information Resources **will** be defined and documented.
8. The CSUS **will** comply with all legal requirements applicable to its monitoring activities. (need Legal to comment)

7.3.2 Security Logging

1. Audit logs recording user activities, exceptions, and information security events **will** be produced and kept for a designated period.
2. Where appropriate based on risk assessment, system administrator and system operator activities **will** be logged.
3. System administrators **will** not have permission to erase or disable logs of their own activities.
4. Procedures for reviewing logs **will** be established and reviewed regularly.
5. Logging facilities and log information **will** be protected against tampering and unauthorized access.
6. Where possible, error logging **will** be enabled and the level of logging required **will** be determined by risk.
7. The clocks of all relevant CSU Information Resources **will** be synchronized with an agreed upon accurate time source.

7.4 INCIDENT MANAGEMENT

Purpose: The standards in this section are intended to ensure that the identification, management and reporting of information security incidents occur in a consistent and timely manner. Incident management includes the effective and timely reporting of and response to security incidents and vulnerabilities as well as the evaluation of event data to reduce and/or mitigate future occurrences.

Standards:

7.4.1 Management of Information Security Incidents

1. Processes and procedures for managing information security incidents **will** be defined and documented to ensure such events are managed in a consistent and effective manner.
2. Roles and responsibilities for the management of information security incidents **will** be defined and documented.
3. Mechanisms **will** be in place to identify and quantify the types, frequency, and costs of information security incidents.
4. Information gained from the evaluation of information security incidents should be used to determine whether improved or additional controls are required to reduce or minimize future incidents.

7.4.2 Reporting Information Security Incidents & Vulnerabilities

1. An information security incident reporting procedure **will** be defined and documented and accompanied by an incident response and escalation procedure.
2. A point of contact **will** be established for the reporting of information security incidents and vulnerabilities. This point of contact, along with their designated backup, **will** be clearly communicated to the CSUS user community.
3. All CSUS users **will** be made aware of their responsibility to report any information security incidents or vulnerabilities to the point of contact or their backup.
4. Information security incidents and vulnerabilities **will** be reported through appropriate management channels.
5. CSUS users **will NOT** attempt to prove or exploit a suspected vulnerability. Such action may be interpreted as misuse of CSUS Information Resources.

7.4.4 Collection of Evidence

When an information security incident is first detected, the designated CSUS personnel will act to prevent the intentional or accidental destruction of evidence before the seriousness of an incident can be determined.

1. Processes and procedures for the collection of evidence should be defined and documented.
2. All evidence collection processes and procedures should be in compliance with legal and forensic practices.

7.5 CHANGE MANAGEMENT

Purpose: The standards in this section are intended to ensure the confidentiality, integrity and availability of CSU Information Resources by establishing a change management process that will minimize the adverse consequences caused by changes to CSUS Information Resources.

Change Management is a process that ensures that any change made to an Information Resource is documented, reviewed and approved. It encompasses both larger planned changes such as projects and smaller reactive changes such as software patches and unscheduled server boots. Change Management also encompasses environmental changes *(e.g., HVAC, power and building access that might affect resource availability).*

Change Management will be integrated into the System Development Life Cycle (SDLC). Including security early in the SDLC will usually result in less expensive and more effective security than adding it to an operational system.

Standards:

7.5.1. Change management processes and procedures **will** be developed, documented and implemented for CSUS Information Resources at each University and the System Office.

7.5.2 Management responsibilities and procedures **will** be defined to ensure satisfactory control of all changes to equipment, software, or procedures.

7.5.3 The change management process **will** address:

1. change identification and documentation,
2. change scheduling for individual changes and windows of high availability when changes are not to be scheduled,
3. classification according to risk level or potential impact,
4. areas affected by the change,
5. roles and responsibilities,
6. notification to concerned parties,
7. approval by responsible party,
8. testing,
9. availability for review,
10. signoff on successful implementation, and
11. backout or recovery procedures.

7.5.4 The Change Management process **will** address three categories of change with respect to approval: Scheduled, Unscheduled and Administrative.

1. Scheduled changes **will** require an approval with a prescribed lead-time for review *(e.g., patch).*
2. Unscheduled changes **will** require an approval but it may be issued retroactively *(e.g., emergency boot*).
3. Administrative changes **will** only need to be approved once *(e.g., establish telecom or network drops, create authorized user accounts).*

7.5.5 CSUS Information Resources **will** be grouped into classes/subclasses where appropriate *(e.g., network/firewall, hardware/storage, OS/Unix, database/DBMS, application/Banner, environment/power).* Identification of the change as a System-wide change versus University/SO change **will** also be considered.

1. An Approver and backup(s) **will** be identified for each class of resource.
2. An Approver **will <u>not</u>** approve changes they themselves have implemented.
3. If a change may significantly affect an area outside of the Approver's responsibility, the requestor **will** contact the Approver for that affected area.
4. An escalation procedure for addressing System-wide changes **will** be clearly defined and documented.

7.5.6 Change management processes and procedures **will** be incorporated into System Development Life Cycle procedures. The security aspects of change management are critical for product acquisition and development.

7.5.7 When products being acquired or developed involve CSUS Information Resources, a process to ensure that they conform to IT Security Standards **will** be developed. The process **will**:

1. Identify criteria for determining when a security review of product acquisition or development will be conducted. Criteria that automatically trigger a review by the University/SO Information Security Officer or a delegate include, but are not limited to:
    a. Opening a port in a firewall to allow inbound, unsolicited connection requests
    b. Using Class A data
    c. Providing a service that is critical to University/SO *operations (e.g., access control systems, core routers, environmental control systems, security monitoring systems).*
    d. Changing Directory Services
2. Identify the person(s) responsible for conducting the review

3. Identify major items to be considered as part of the review process *(e.g., access, audit trail)*.
4. Identify responsible parties to insure that the product will be managed and maintained in accordance with IT Security Standards. This identification is critical for turn-key products and applications developed locally but outside of IT.

7.5.8 When a security review is required, the University/SO Information Security Officer or a delegate **will** provide a signoff indicating whether or not the product being acquired or developed conforms to IT Security Standards.

7.5.9 Acquisition/development products that are System-wide in nature **will** be subject to a joint-review and signoff by all University/SO Information Security Officers or a delegate.

7.5.10 When the product acquisition or development security review determines that the product does not conform to IT Security Standards, the product **will <u>not</u>** be acquired or developed as proposed unless an exception review is conducted and the product is granted an exception to IT Security Standards.

APPENDICES

Appendix A: References & Resources

Appendix B: CSUS Board Resolution 06-10

Appendix C: Information Security Governance Core Set of Principles *(National Cyber Security Summit Task Force)*

Appendix D: Sample Request for Security Exception *(University of Texas at Austin)*

Appendix E: Information Security Glossary

Appendix A

References & Resources

References

1. International Standard ISO/IEC 17799(E) Code of Practice for Information Security Management
2. National Institute of Standards and Technology (NIST) - Special Publication 800-53: “Recommended Security Controls for Federal Information Systems – Information Security”
   http://csrc.nist.gov/publications/drafts/800-53-rev1-ipd-clean.pdf
3. National Institute of Standards and Technology (NIST) - Special Publication 800-50:
   “Building an Information Technology Security Awareness and Training Program”
   http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
4. New York State Office for Technology - "Protection of OFT's Information Assets"
   http://www.oft.state.ny.us/policy/p04-003/files/Protection_of_OFTs_Digital_Assets-FINAL.pdf
5. Commonwealth of Virginia Information Technology Security Management Standard
   http://www.ts.vcu.edu/security/SEC501.pdf
   http://www.vita.virginia.gov/docs/psg/SEC2001_01_1_ITSecurityGuid.pdf
6. National Cyber Security Partnership - Corporate Governance Task Force Report
   “Information Security Governance – A Call to Action”
   http://www.cyberpartnership.org/InfoSecGov4_04.pdf
7. State of Texas
   http://www.dir.state.tx.us/security/policies/index.htm
8. Oregon State University
   http://www.ous.edu/its/security/CO_Security_Policy_2003.pdf
9. University System of Georgia
   http://www.usg.edu/acit/docs/security_guide.pdf
10. Solstice backup and Storage Management – A Technical White paper
    http://www.sun.com/software/whitepapers/backup-n-storage/
11. Unitrends: Questions and Answers
    http://unitrends.com/QandA/BackupTypes.aspx
12. Griffith University Information Security Policy – Access & Asset Security Standards and Operational Guidelines
    http://www62.gu.edu.au/policylibrary.nsf/mainsearch/197052c1efb735204a256c710063d4e9?opendocument#backup

General Resources

1. SANS (SysAdmin, Audit, Network, Security) Institute
   http://www.sans.org/
   http://www.sans.org/resources/policies/Policy_Primer.pdf

General Resources (*Cont.)*

2. Virginia Alliance for Secure Computing & Networking (VA Scan)
   http://vascan.org/
   http://www.educause.edu/PressReleases/1175&ID=1224
3. Educause http://www.educause.edu/security/
4. Purdue University - CERIAS (Center for Education and Research in Information Assurance and Security) http://www.cerias.purdue.edu
5. Carnegie Mellon (CERT) http://www.cert.org

Reports, White Papers & Surveys

1. UCLA Security Work Group Report
   http://www.csg.oit.ucla.edu/documents/2005_Postings/2005_08_August/Infor_Sec_Workgrp_%20final%20report_2005.pdf
2. Carnegie Mellon-CERT - "Building a Framework for Enterprise-wide Security Management"
   http://www.cert.org/archive/pdf/secureit_esm_allen_may0304.pdf
3. SANS Institute – "A Short Primer for Developing Security Policies"
   http://www.sans.org/resources/policies/Policy_Primer.pdf
4. Tulane University – Gramm-Leach Bliley Questionnaire
   http://www2.tulane.edu/privacy/survey.cfm

Security Awareness, Training and Education

1. CERIAS (Purdue)
   "Information Security in the Workplace: What Every User Should Know
   "http://www.educause.edu/section_params/security/cd/higher_education/manuals/CERIAS-Purdue%20What%20Every%20User%20Should%20Know%20Manual.pdf

   "Training for System Administrators"
   http://www.educause.edu/section_params/security/cd/higher_education/manuals/CERIAS-Purdue%20SysAdmins%20Training%20Manual.pdf

2. Educause Security Awareness Library & Resources
   http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762
   http://www.educause.edu/HigherEducationResources/8767

3. The Information Warfare Site
   http://www.iwar.org.uk/comsec/resources/sa-tools/index.htm

   Effective Security Awareness Communication
   http://www.iwar.org.uk/comsec/resources/sa-tools/Principles-of-Effective-Security-Awareness.pdf

   Benchmarking and Metrics
   http://www.iwar.org.uk/comsec/resources/sa-tools/Security-Awareness-Benchmarking-and-Metrics.pdf
   http://www.iwar.org.uk/comsec/resources/sa-tools/index.htm

   Train the Trainer
   http://www.iwar.org.uk/comsec/resources/sa-tools/Trainers-Notes-for-Security-Awareness-01.pdf

   Quizzes & Scenarios
   http://www.iwar.org.uk/comsec/resources/sa-tools/Monthly-Quizzes.pdf
   http://www.iwar.org.uk/comsec/resources/sa-tools/Scenario-Based-Exercises-for-Security-Awareness.pdf

Appendix B

CSUS Board Resolution 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

Appendix C

Information Security Governance Core Set of Principles *(Excerpted from the National Cyber Security Summit Task Force – Corporate Governance Report)*

The following table, "Information Security Governance Core Set of Principles" is excerpted from the *Corporate Governance Report* published by the National Cyber Security Summit Task Force in April 2004. As the report indicates, this set of principles "is derived from widely recognized information security and IT governance frameworks – International Organization for Standardization (ISO) 17799, Federal Information Security Management Act (FISMA), and Control Objectives for Information and Related Technology (COBIT)…"

Information Security Governance Core Set of Principles

Table 2.

- CEOs should have an annual information security evaluation conducted, review the evaluation results with staff, and report on performance to the board of directors.
- Organizations should conduct periodic risk assessments of information assets as part of a risk management program.
- Organizations should implement policies and procedures based on risk assessments to secure information assets.
- Organizations should establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability.
- Organizations should develop plans and initiate actions to provide adequate information security for networks, facilities, systems and information.
- Organizations should treat information security as an integral part of the system life-cycle.
- Organizations should provide information security awareness, training, and education to personnel.
- Organizations should conduct periodic testing and evaluation of the effectiveness of information security policies and procedures.
- Organizations should create and execute a plan for remedial action to address any information security deficiencies.
- Organizations should develop and implement incident response procedures.
- Organizations should establish plans, procedures, and tests to provide continuity of operations.
- Organizations should use security best practices guidance, such as ISO 17799, to measure information security performance.

Source: Corporate Governance Task Force Report – "Information Security Governance - A Call to Action" (April 2004) http://www.cyberpartnership.org/InfoSecGov4_04.pdf

Appendix D

SAMPLE FORM

(courtesy of the University of Texas at Austin)

REQUEST FOR SECURITY EXCEPTION

Before Submitting an Exception Request

The Security Exception Reporting Process outlines the proper steps to comply with law and policy at The University of Texas at Austin. Before you request what you believe is an exception, please review the Information Technology Resources Security Operations Manual carefully.

If you have read and reviewed all the University Polices and you are unsure about something, please send an e-mail message to the ISO at abuse@utexas.edu.

Security Exception Request Form

IT Custodian's Name:

IT Custodian's Title:

IT Custodian's Phone Number:

IT Custodian's E-mail Address:

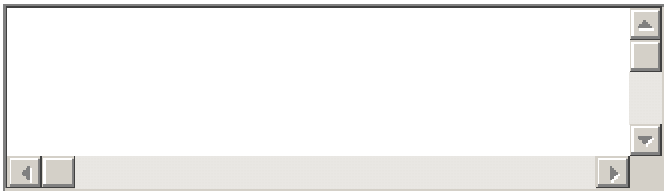
Standard/Policy/Guideline for which an exception is being requested:

SAMPLE FORM *(Cont.)*

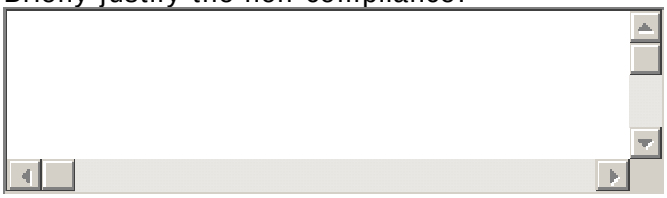
(courtesy of the University of Texas at Austin)

Security Exception Request – courtesy of the University of Texas at Austin

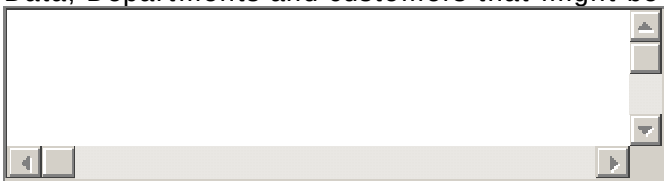
Describe the non-compliance:



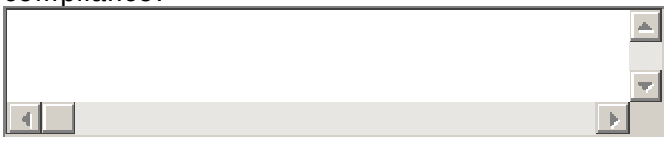
Briefly justify the non-compliance:



Data, Departments and customers that might be put at risk by the exception:



Provide an assessment of the risk (vulnerability, threat, likelihood) associated with non-compliance:



Describe what is being done to mitigate (manage) risk:

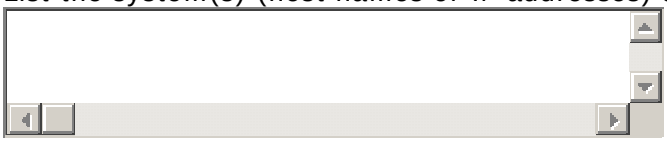
Provide metrics to evaluate the success of risk management:

The college, school, or unit which initially requested the exception:

SAMPLE FORM *(Cont.)*

(courtesy of the University of Texas at Austin)

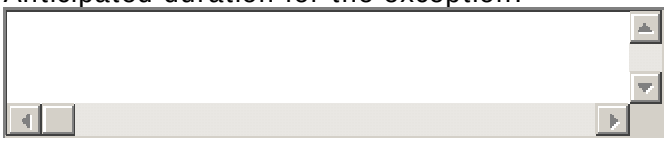
List the system(s) (host names or IP addresses) associated with this report:



Sample Security Exception Request – University of Texas at Austin *(Cont.)*

Data Classification: Category I

Anticipated duration for the exception:



EID for approving IT owner:

Submit Request

Appendix E

Information Security Glossary

ACL (Access Control List) – A set of data associated with a file, directory or other network resource that defines the permissions that users, groups, processes or devices have for accessing that resource.

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 granting or denying access to the resources of a system to authorized persons, programs, processes or other systems.

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.

Asset – See ***CSUS Information Resources***.

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 – 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.

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

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

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.

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.

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.

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.

CSUS - The Connecticut State University System: Central, Eastern, Southern and Western Connecticut State Universities and the System Office.

CSUS Employees - Faculty, staff, student workers, university assistants and all other individuals employed by the Connecticut State University System.

CSUS Information Resources - All data created stored, maintained, processed or transmitted by CSUS as well as all internal and external networks, computing platforms, systems, software, hardware, equipment and facilities either owned or leased by the Connecticut State University System.

CSUS User - All employees, students, and third parties including vendors, contractors, visitors and all others who utilize the electronic and non-electronic information resources of the Connecticut State University System.

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

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

Employees - See ***CSUS Employees***

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.

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) - A version of HTTP used when a secure connection is required such as for credit card transactions.

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.

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 - *See* ***CSUS Information Resources****.*

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

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.

LAN (Local Area Network) – A computer network that covers a small local area, like a home, office, or small group of buildings such as a home, office, or college.

Malicious Software - 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.

Mission Critical - CSUS Information resources that are essential to the academic and administrative operations of the Connecticut State University System.

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.

Non-Production Environment – An environment specifically created for development, testing and/or training purposes.

Operational Readiness – The state of an application, service or device that is ready to be implemented.

Production Environment - An operational environment identified by a Data Steward as the System of Record (i.e. the repository of record for the identified data.)

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.

SDLC (System Development Life Cycle) – A conceptual process or model that describes the various phases of an information system development project from feasibility through maintenance and disposition.

SSH – A security protocol for logging onto a remote server. SSH provides an encrypted session for transferring files and executing server programs.

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 violation or imminent threat of violation of computer security policies, acceptable use policies or standard computer security practices. (SOURCE: NIST SP 800-61).

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

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

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.

VLAN (Virtual Local Area Network) - A network of computers that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN. (SOURCE: webopedia.com)

VPN (Virtual Private Network) - A network that provides remote offices or users with secure access to their organization's network using the Internet or other public telecommunications system. (SOURCE: MS Encarta)

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.

WAN (Wide Area Network) - A computer network that spans a relatively wide geographical area and generally includes two or more local area networks.