Cincinnati State
TECHNICAL AND COMMUNITY COLLEGE

3520 Central Parkway
Cincinnati, Ohio 45223-2690

513-569-1500 tel
www.cincinnatistate.edu

INFORMATION TECHNOLOGY SERVICES

INFORMATION SECURITY GOVERNANCE POLICIES

Revised: 5/21/2014

Table of Contents

01 INFORMATION SECURITY POLICY

Overview:
In order to protect Cincinnati State's information systems and data, an effective security policy framework shall be established, implemented, and enforced.

01.01 Information Security Program

The senior leadership of Cincinnati State recognizes that information security is a management opportunity rather than a technical problem. To this end, full commitment shall be demonstrated by providing a supportive framework that utilizes the college departmental management structure to disseminate this policy and promote a security culture.

01.01.01 Policy Objectives

The information security policy encapsulates the various policies set forth by Cincinnati State for effective information security management. The policies shall address the following areas:
Section 02 Organizational Information Security: The management framework, roles and responsibilities for the initiation and control of information security in the context of core business systems, outsourcing, and third party involvement.
Section 03 Asset Classification and Control: The ownership, control, and protection of major information assets.
Section 04 Personnel Security and User Awareness: The security processes in place to reduce the risks of human error, theft, fraud, or misuse of facilities.
Section 05 Physical and Environment Security: The approach for identifying risks, threats, and vulnerabilities to the physical security of the company's core business systems.
Section 06 Communications and Operations Management: Responsibilities and procedures for the management and operation of core business systems.
Section 07 System and Network Access Control: Definition of business requirements for access to Cincinnati State information assets, user registration, password management, and mobile computing.
Section 08 Systems Development and Maintenance: The design and implementation of business systems plus associated technology with the appropriate levels of security.
Section 09 Business Continuity Management: The measures in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
Section 10 Information Security Compliance: Legislation which needs to be adhered to in order to avoid breaches of any criminal and civil law, stationary, regulatory, or contractual.
Section 11 Acceptable Use: The policies associated with appropriate use for various platforms.

01.01.02 Role of Senior Management

Senior management shall demonstrate their commitment by:

- Reviewing and approving the Information Security Policy documents
- Actively promoting a security culture within the College
- Disseminating the content of this policy through the college departmental management and committee structures
- Using their authority to ensure there are adequate resources to implement and maintain the security policy

01.02 Policy Communication

The College's Information Security Council is responsible to ensure the security policy is communicated in a clear concise manner. The College's Information Security Council shall communicate all policies to the college departments. The policy shall be available for all college personnel and any changes or updates to the policy shall be communicated in a timely fashion to relevant employees.

01.03 Policy Review

The Information Security Council is responsible for reviewing the Information Security Policy to ensure it is accurate, up-to-date, and relevant. The Security Council shall also ensure that changing business requirements and risks are appropriately addressed within the Information Security Policy.

The Information Security Council shall consider the following factors when reviewing the policy:

- The policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents
- Cost and impact of controls on business efficiency
- Effects of changes to technology

02 ORGANIZATIONAL INFORMATION SECURITY

Overview:

Establish the overall framework for the college information security organization; including the infrastructure, roles and responsibilities, authorization process, third party access, security documentation, and outsourcing requirements.

02.01 Information Security Infrastructure, Roles and Responsibilities

The Information Security Council is chaired by the Chief Technology Officer, with representation from all college departments and meets at least 4 times per year.

The role of the Information Security Council is to initiate and control the implementation of information security throughout the College.

Information Security Council acts as special advisor to the Information Security Leader on all information security issues including, but not limited to, the following:

- Policies, standards and guidelines
- Information security architecture
- Incident response
- Strategy and planning
- Security risk assessments

02.02 Authorization Process

Any college department implementing new Information Technology (IT) systems and resources shall ensure that these controls are followed:

- New facilities shall have appropriate user management approval, authorizing their purpose and use. Approval shall also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met.
- Where necessary, hardware and software shall be checked to ensure they are compatible with other system components.

- The use of any personal owned device that can store or process Cincinnati State data may cause new vulnerabilities and is therefore restricted to network segments that filter before granting access to Cincinnati State applications and systems.

02.03 Third Party Access

Access to IT systems and resources by outside organizations and the transfer of data between Cincinnati State and outside organizations is restricted for reasons of security. The Information Security Officer shall receive and consider requests for such access, and gives appropriate advice to management. The list of organizations with access shall be maintained by the Information Security Officer. The Information Security Officer shall serve as a repository for all of this information.
Access to Cincinnati State IT systems and resources by third parties shall be controlled.
Where there is a business need for such third party access, a risk assessment shall be carried out to determine security implications and control requirements. Controls shall be agreed and defined in a contract with the third party.
Third party access may also involve other participants. Contracts conferring third party access shall include allowance for designation of other eligible participants and conditions for their access.
Any third party contracts for information processing shall include at a minimum, bi-directional confidentiality and non-disclosure language, protections for intellectual property and a right to audit clause.
This policy shall be used as a basis for such contracts and when considering the outsourcing of information processing.

02.04 Information Security Documentation

All college departments are required to maintain appropriate information security documentation. All information security documentation shall be marked as college confidential and stored in a secure IT processing area controlled with additional physical security controls such as lock and key.
At a minimum, the following documents shall be maintained:

- Information security architecture diagrams
- Network architecture diagrams
- Information security policies
- User access matrices
- User access request forms
- Confidentiality agreements

02.05 Information Security Requirements for Outsourcing

College departments involved in arranging contracts for outsourcing to application service providers, software developers, or network operations/management companies are required to address the risks, security controls, and procedures for information systems, networks and/or desktop environments in the contract between the parties. The Information Security Officer shall be informed and shall give advice to management.
Any contracts for outsourced information processing shall include a right to audit clause.
Any outsourced software development shall meet the same programming guidelines and standards established for Cincinnati State.
Any outsourced information system or network system shall establish acceptable service levels, downtime agreements, performance measurements, and security requirements.

Any outsourced IT system, resource, network system, or software development shall include a comprehensive confidentiality agreement.
Any outsourced process shall go through an information security risk assessment.

03 ASSET & DATA CLASSIFICATION AND CONTROL

Overview

In order to appropriately protect information systems and the data housed by them, an owner shall be assigned and the data appropriately classified.

03.01 Accountability for Assets

All major information systems assets, including data, shall be accounted for and have a nominated owner and/or custodian. The owner is responsible for ensuring that appropriate security measures are implemented and maintained throughout the life of the asset.

03.02 Inventory of Assets

Inventories of assets help to ensure that effective security protection is maintained, and may be required for other business purposes, such as health and safety, insurance, or financial reasons. An inventory shall be drawn up of the major assets associated with each information system. Each asset, or group of assets, shall be clearly identified and its ownership and security classification agreed and documented. Examples of assets associated with information systems include:

- **Information assets**: Databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements
- **Software assets**: Application software, system software, development tools and utilities
- **Physical assets**: Computer and communications equipment, magnetic media (tapes and disks), digital media (CD-ROM, CD-RW, DVD, DVD-RW), other technical equipment (power supplies, air-conditioning units).
- **Services**: Computing and communications services, other technical services (heating, lighting, power, air-conditioning)

The owner of each information asset is responsible for approving who may have access to it and the type of access they are permitted. All access requests, after approval from the asset owner, shall be forwarded to local security administration for review.

03.03 Information Classification

Information assets vary in sensitivity and criticality. A security classification system shall be used to define an appropriate set of security protection levels, and to communicate the need for special handling measures to users. The use of a common marking system throughout the college ensures that all information exchanged shall receive a common level of protection.

Information Sensitivity Marking Scheme

Confidentiality:

This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. Unauthorized disclosure of this information to people without a

business need for access may be against laws and regulations, or may cause significant problems for the college, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the information Owner. Examples: customer transaction account information and worker performance evaluation records.

Internal Use Only:

This information is intended for use within the college, and in some cases within affiliated organizations. Unauthorized disclosure of this information to outsiders may be against laws and regulations, or may cause problems for college, its customers, or its business partners. This type of information is already widely-distributed within the college, or it could be so distributed within without advance permission from the information Owner. By example: the college telephone book and most internal electronic mail messages.

Public:

This information has been specifically approved for public release by Public Relations Department or Marketing Department managers. Unauthorized disclosure of this information will not cause problems for the college, its customers, or its business partners. Examples: marketing brochures and material posted to the college Internet web page. Disclosure of college information to the public requires the existence of this label, the specific permission of the information owner, or long-standing practice of publicly distributing this information. Actual times associated with each level of availability shall be determined based on

04 PERSONNEL SECURITY & USER AWARENESS

Overview:

Cincinnati State information systems and data are only as secure as the users who are granted access and their understanding of correct information security practices.

04.01 Job Definitions, Roles and Responsibilities

Security roles and responsibilities shall be included in job descriptions where appropriate. These shall include any general responsibilities for implementing or maintaining security policy, as well as any specific responsibilities for the protection of particular assets or the execution of particular security processes or activities.

04.02 Information Security User Awareness

The College's Information Security Council shall determine what is required to make users aware of the need for information security and make appropriate arrangements, including the creation of information systems security guidelines documentation.

All users shall be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

04.03 Personnel Screening

Where allowed by law, adhere to the following personnel screening practices;

- Verification checks on permanent staff shall be carried out at the time of job applications
- Human Resources shall:
    - Verify both business and personal character references
    - Verify the applicant's resume for completeness and accuracy
    - Perform an independent identity check
- The hiring manager and Human Resources shall confirm the applicant's claimed academic and professional qualifications

A similar screening process shall be carried out for contractors and temporary staff. Where these staff personnel are provided through an agency, the contract with the agency shall clearly specify the agency's responsibility for screening and notification procedures they need to follow if screening has not been completed, or if the results give cause for doubt or concern.

04.04 Confidentiality Agreements

All employees shall sign an appropriate confidentiality agreement as part of their initial conditions of employment. Contract personnel and staff not already covered by an existing confidentiality agreement shall also be required to sign the code of conduct prior to being granted access to departmental IT facilities. The agreement shall be reviewed when there are changes to terms of employment or contracts.

04.05 Identifying and Reporting Security Related Incidents

Incidents affecting security shall be reported to the Information Security Council Lead and College Information Security Officer as quickly as possible.

The College Information Security Officer shall develop procedures to facilitate reporting security incidents.

The College Information Security Officer shall establish a College Computer Security Incident Response Team (CSIRT)

All employees and contractors shall know the procedures for reporting the different types of incidents (security breach, threat, weakness or malfunction) that might affect the security of organizational assets. They are required to report any observed or suspected incidents as quickly as possible to the designated contact. College administration in conjunction with Human Resources, shall establish a formal disciplinary process for dealing with employees and students who commit serious breaches. To address incidents properly, evidence may need to be collected as soon as possible after the event. Strict adherence to the formalized chain of custody process, in accordance to local laws, shall be followed.

05 PHYSICAL & ENVIRONMENTAL SECURITY

Overview:

Information processing facilities shall be provided appropriate physical and environmental security to ensure the confidentiality, integrity, and availability of the data they house.

Critical or sensitive information processing facilities should be housed in secure IT processing areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

05.01 Secure IT Processing Areas

All data processing centers and network wiring closets are considered secure IT processing areas. They are to be kept physically secure through the use of appropriate locks and other security measures. Employees are instructed to keep these areas secure at all times. Any references to Secure IT processing area's in this policy refer to Data Processing Centers and other IT specific area's at the college.

05.01.01 Physical Security Perimeter

Physical security perimeters shall be established to protect all secure IT processing areas.

05.01.02 Physical Entry Controls

Physical entry controls shall be implemented to prevent unauthorized access to secure IT Processing areas.

The type of access control system shall be determined by the nature of risk associated with the area.

Any person granted access to the secured area shall be issued a facility security badge.

- The date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.
- Access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained.
- All contractors, third party users and all visitors are required to wear some form of visible identification. All employees should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification within secure IT processing areas.
- Access rights to secure IT processing areas should be regularly reviewed and updated, and revoked when necessary.

05.01.03 Securing Offices, Rooms and Facilities

Securing offices, rooms and facilities shall take into account the possibility of damage from fire, flood, explosion, civil unrest, and other forms of natural or man-made disaster. Account shall also be taken of relevant health and safety regulations and standards. Consideration shall be given also to any security threats presented by neighboring premises (e.g., leakage of water from other areas).

- Key facilities should be sited to avoid access by the public
- Directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.

05.01.04 Working in Secure IT Processing Areas

The College's Information Security Council shall establish standards and guidelines for working in secure IT processing areas.

05.01.05 Isolated Delivery and Loading Areas

Delivery and loading areas shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. Security requirements for such areas shall be determined by a risk assessment.

05.02 Equipment Security

05.02.01 Equipment Location and Protection

Equipment shall be optimally located or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

05.02.02 Power Supplies

Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications.

05.02.03 Cabling Security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

05.02.04 Equipment Maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity.

05.02.05 Security of Equipment Off-Premises

Regardless of ownership, the use of any equipment outside of Cincinnati State's premises for information processing purposes shall be authorized by management. The security provided shall be equivalent to that for on-site equipment used for the same purpose, taking into account the additional risks of working outside Cincinnati State's premises.

05.02.06 Secure Disposal or Re-Use of Equipment/Media

All items of equipment containing storage media (e.g., fixed hard disks) shall be checked to ensure that any sensitive data and licensed software have been removed or overwritten prior to disposal. Damaged storage devices containing sensitive data may require a risk assessment to determine if the items shall be destroyed, repaired, or discarded.

05.03 General Controls

05.03.01 Removal of Property

Equipment, information assets, or software shall not be taken off-site without authorization. Where necessary and appropriate, equipment shall be logged out and logged back in when returned. Spot checks shall be undertaken to detect unauthorized removal of property. Individuals shall be made aware that spot checks shall take place.

06 COMMUNICATIONS & OPERATIONS MANAGEMENT

Overview

In order to maintain the security of Cincinnati State's IT systems, resources, and data it is necessary to implement policies addressing communications and daily operations requirements.

06.01 Operational Procedures and Responsibilities

The operating procedures identified by the security policy shall be documented and maintained. Operating procedures shall be treated as formal documents and changes authorized by management. The procedures shall specify the instructions for the detailed execution of each job, including:

- Processing and handling of information assets
- Scheduling requirements, including interdependencies with other systems, earliest job start, and latest job completion times
- Instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
- Support contacts in the event of unexpected operational or technical difficulties
- Special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs
- System restart and recovery procedures for use in the event of system failure

Documented procedures shall also be prepared for system housekeeping activities associated with information processing and communication systems, such as computer start-up and shut-down procedures, back-up, equipment maintenance, computer room, and mail handling management and safety.

06.01.02 Operational Change Control

Changes to information processing facilities and systems shall be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, software or procedures. Operational programs shall be subject to strict change control. When programs are changed, an audit log containing all relevant information shall be retained. Changes to the operational environment can impact applications. Wherever practicable, operational and application change control procedures shall be integrated.

System/application administrators shall:

- Identify and record all significant changes
- planning and testing of changes
- Assess and notify management of the potential impact related to any significant change
- Follow the Cincinnati State change control process for any proposed changes
- Communicate the change details to all relevant persons
- Identify back out plans to recover from unsuccessful changes

06.01.03 Incident Response Procedures

The Information Security Council shall establish a Computer Security Incident Response Team (CSIRT). The Information Security Council shall define the makeup and operational procedures and guidelines for the CSIRT.

Procedures shall be established to cover all potential types of security incident, including:

- Information system failures and loss of service
- Denial of service
- Virus outbreaks
- Errors resulting from incomplete or inaccurate business data
- Breaches of confidentiality

In addition to normal contingency plans (designed to recover systems or services as quickly as possible) the procedures shall also cover:

- Analysis and identification of the cause of the incident
- Planning and implementation of remedies to prevent recurrence, if necessary
- Collection of audit trails and similar evidence
- Communication with those affected by or involved with recovery from the incident
- Reporting the action to the appropriate authority
- Coordinating activities with external agencies

Audit trails and similar evidence shall be collected and secured, as appropriate, for:

- Internal problem analysis
- Use as evidence in relation to a potential breach of contract, breach of regulatory requirement or in the event of civil or criminal proceedings (e.g., under computer misuse or data protection legislation). If the evidence is to be used for any legal action, including termination of an employee, only authorized specialist shall manage the process.
- Negotiating for compensation from software and service suppliers

Actions taken to recover from security breaches and correct system failures shall be carefully and formally controlled. The procedures shall ensure that:

- Only clearly identified and authorized staff are allowed access to live systems and data
- All emergency actions taken are documented in detail
- Emergency action is reported to management and reviewed in an orderly manner

- The integrity of business systems and controls is confirmed with minimal delay

06.01.04 Segregation of Duties

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, shall be considered.

Developers/coders shall not have access to modify or change production systems.

Care shall be taken so that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event shall be separated from its authorization.

If there is a danger of collusion of duties, IT shall establish controls so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

Whenever it is not possible to segregate, other controls such as monitoring of activities, audit trails and management supervision shall be used. It is important that security audit remains independent.

06.01.05 Separation of Development & Operational Facilities

Separating development, test, and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status shall be defined and documented. Development and test activities can cause serious problems (e.g., unwanted modification of files or system environment, system failure). The level of separation that is necessary, between operational, test, and development environments, to prevent operational problems shall be considered.

A similar separation shall also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access. Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or operational data. On some systems, this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems.

Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test, and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data.

To ensure this, the following controls shall be implemented:

- Development and operational software shall run on different systems/LPAR, or in different domains or directories.
- Development and testing activities shall be separated as far as possible.
- Compilers, editors and other system utilities shall not be accessible from operational systems when not required.
- Different log-on procedures shall be used for operational and test systems to reduce the risk of error. Users shall be encouraged to use different passwords for these systems, and menus shall display appropriate identification messages.

- Development staff shall only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls shall ensure that such passwords are changed after use.

06.01.06 External Facilities Management

The use of an external contractor to manage information-processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. These risks shall be identified in advance and appropriate controls agreed with the contractor and incorporated into the contract

Particular issues that shall be addressed include:

- Identifying sensitive or critical applications better retained in-house
- Obtaining the approval of business application owners
- Implications for business continuity plans
- Security standards to be specified and the process for measuring compliance
- Allocation of specific responsibilities and procedures to effectively monitor all relevant security activities
- Responsibilities and procedures for reporting and handling security incidents.

06.02 System Planning and Acceptance

06.02.01 Capacity Planning

Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections shall take account of new business and system requirements and current and projected trends in the information processing. Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Managers of all systems shall monitor the utilization of key system resources, including processors, system memory, disk storage, printers, back-up libraries, and other output devices. Network managers shall also be apprised of any possible impact to networks. They shall identify trends in usage, particularly in relation to business applications or management information system tools.

Managers shall use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services, and plan appropriate remedial action.

06.02.02 System Acceptance

Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance. Managers shall ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, tested, and in accordance with all local laws and regulations.

The following controls shall be adhered to:

- Performance and computer capacity requirements

- Error recovery and restart procedures, and contingency plans
- Preparation and testing of routine operating procedures to defined standards
- Agreed set of security controls in place
- Effective manual procedures
- Business continuity arrangements, as required by Information Security Policy 09.01
- Evidence that installation of the new system shall not adversely affect existing systems, particularly at peak processing times, such as month end
- Evidence that consideration has been given to the effect the new system has on the overall security of the organization
- Training in the operation or use of new systems

For major new developments, the operations function and users shall be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests shall be carried out to confirm that all acceptance criteria are fully satisfied.

06.03 Protection Against Malicious Code

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented. Protection against malicious software shall be based on security awareness, appropriate system access, and change management controls. Any attempt to defeat controls is expressly prohibited.

The Information Security Council shall establish a formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software.

The Information Security Council shall establish a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures shall be taken.

All desktop and server systems shall have anti-virus software installation with regular updates scheduled.

System administrators and Information Security shall conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments shall be formally investigated.

Employees shall check any files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use.

All systems shall check any electronic mail attachments and downloads for malicious software before use. This check shall be carried at multiple points of incursion including but not limited to: Electronic mail servers, desktop computers, web proxy servers, FTP proxy servers (It is recommended to employ differing anti-virus solutions at these points to ensure a more effective protection scheme).

Appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements, shall be established.

The Information Security Council shall establish procedures to verify all information relating to malicious software, and ensure that warning bulletins are accurate and informative. Information Security shall ensure that qualified sources (e.g., reputable journals, reliable Internet sites or anti-virus software suppliers) are used to differentiate between hoaxes and real viruses. Employees shall be made aware of the problem of hoaxes and what to do upon receipt of them (Refer to Cincinnati State User Awareness Program).

06.04 Operations

06.04.01 Information Back-Up

Back-up copies of essential business information and software shall be taken regularly. Adequate back-up facilities shall be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of business continuity plans.

All information systems shall have procedures to back-up all business critical information together with accurate and complete records of the back-up copies and documented restoration procedures, to be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Minimum required number of generations or cycles of back-up information shall be determined by the line of business risk assessment.

Back-up information shall be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site shall be extended to cover the back-up site.

Back-up media shall be regularly tested, where practicable, to ensure that it can be relied upon for emergency use when necessary.

Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery. The retention period for essential business information and also any requirement for archive copies to be permanently retained shall be determined.

06.04.02 Operator Logs

Operational staff shall maintain a log of their activities. Logs shall include, as appropriate:

- Application starting and finishing times
- System and application errors and corrective action taken
- System back-up start and finish
- Which account and which administrator or operator was involved

Operator logs shall be subject to regular, independent checks against operating procedures.

06.04.03 Fault Logging

Faults shall be reported and corrective action taken. Faults reported by users regarding problems with information processing or network systems shall be logged. There shall be clear rules for handling reported faults, including:

- Review of fault logs to ensure that faults have been satisfactorily resolved
- Appropriate escalation procedures for various faults
- Review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized

06.05 Network Management

06.05.01 Network Controls

A range of controls is required to achieve and maintain security in computer networks.

Network managers shall implement controls to ensure the security of data in networks, and the protection of connected services from unauthorized access.

- Operational responsibility for networks shall be separated from computer operations where possible
- Operational responsibility for security systems shall be separated from network and computer operations where possible
- Administration of Information Security equipment shall be separated from network management equipment.
- The Information Security Council shall establish standards and guidelines for the management of remote equipment.
- The Information Security Council shall establish standards and guidelines to safeguard the confidentiality and integrity of data passing over public networks and to protect the connected systems. Special standards and guidelines shall also address controls necessary to the availability of the network services and computers connected.
- Network management activities shall be closely coordinated both to optimize the service to the business and to ensure that controls are consistently applied across the information processing infrastructure (e.g., implementing a new service on a server, setting up the new router access control list, setting up the new firewall rules, setting up new intrusion detection rules, etc.).

06.06 Media Handling

06.06.01 Management of Removable Computer Media

There shall be procedures for the management of removable computer media, such as tapes, disks, CD-ROMs, USB storage devices and printed reports.

The following controls shall be implemented:

- If no longer required, the previous contents of any re-usable media that are to be removed from the organization shall be erased with an approved data deletion tool or the media shall be appropriately destroyed.
- Authorization is required for any media removed from the organization and a record of all such removals (to maintain an audit trail) shall be kept

- All media shall be stored in a safe, secure environment, in accordance with manufacturers' specifications.

All procedures and authorization levels shall be clearly documented.

06.06.02 Disposal of Media

Media shall be disposed of securely and safely when no longer required. Sensitive information could be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media shall be established to minimize this risk.

At a minimum the following controls shall be implemented:

Media containing sensitive information shall be stored and disposed of securely and safely (e.g., by incineration, shredding, overwritten with an approved data deletion tool).

The following list identifies items that might require secure disposal:

- Paper documents
- Voice or other recordings
- Output reports
- Internal hard drives
- Magnetic tapes
- Removable disks
- Removable memory devices
- Optical storage media (all forms, and including all manufacturer software distribution media)
- Program listings
- Test data
- Network or system documentation

Shredders shall be available to all employees to dispose of sensitive paper documentation.

Disposal of sensitive items shall be logged where possible in order to maintain an audit trail.

When accumulating media for disposal, consideration shall be given to the aggregation effect, which may cause a large quantity of unclassified information to become more sensitive than a small quantity of classified information.

06.06.03 Information Handling Procedures

Procedures for the handling and storage of information assets shall be established in order to protect it from unauthorized disclosure or misuse. Procedures shall be drawn up for handling information consistent with its classification in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of fax machines and any other sensitive items.

The following controls shall be implemented:

- Computer operations, with direction from The Information Security Council, shall establish procedures for handling and labeling of all media
- Access restrictions to identify unauthorized personnel
- Maintenance of a formal record of the authorized recipients of data
- Ensuring that input data is complete, that processing is properly completed, and that output validation is applied
- Protection of spooled data awaiting output to a level consistent with its sensitivity
- Storage of media in an environment that accords with manufacturers' specifications
- Keeping the distribution of data limited to those who need it specifically for their job
- Clear marking of all copies of data for the attention of the authorized recipient
- Review of distribution lists and lists of authorized recipients at regular intervals

06.06.04 Security of System Documentation

System documentation may contain a range of sensitive information (e.g., descriptions of applications, processes, procedures, data structures, authorization processes).

The following controls shall be implemented to protect system documentation from unauthorized access:

- System documentation shall be stored securely
- The access list for system documentation shall be kept to a minimum and authorized by the application owner
- System documentation held on a public network, or supplied via a public network, shall be appropriately protected

06.07 Information and Software Exchange

06.07.01 Information and Software Exchange Agreements

Exchange of information with other organizations shall be based on a formal agreement that specifies the conditions for handling the information, such as non-disclosure agreements. The agreement shall exist whether the information is in electronic or physical form. The content of the agreement shall vary depending on the reason for the exchange.

The agreement, at a minimum, shall address the following:

- Management responsibilities for controlling and notifying of transmission, dispatch and receipt
- Procedures for notifying sender of transmission, dispatch, and receipt
- Minimum technical standards for packaging and transmission
- Courier identification standards
- Responsibilities and liabilities in the event of loss of data

- Use of an agreed labeling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected
- Information and software ownership and responsibilities for data protection, software copyright compliance, and similar considerations
- Technical standards for recording and reading information and software
- Any special controls that may be required to protect sensitive items, such as cryptographic keys

06.07.02 Security of Media in Transit

Information can be vulnerable to unauthorized access, misuse, or corruption during physical transport; for instance, when sending media via the postal service or via courier.

The following controls shall be applied as necessary to safeguard computer media being transported between sites:

- Reliable transport or couriers shall be used. A list of authorized couriers shall be agreed with management and a procedure to check the identification of couriers implemented.
- Packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
- Special controls shall be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification. Examples include:
    - Use of locked containers
    - Delivery by hand
    - Tamper-evident packaging (which reveals any attempt to gain access)
    - In exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes
    - Use of digital signatures and data encryption

06.07.03 Electronic Commerce Security

Electronic commerce can involve the use of Electronic Data Interchange (EDI), electronic mail and online transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats, which may result in fraudulent activity, contract dispute, and disclosure or modification of information. Controls shall be applied to protect electronic commerce from such threats.

Security for electronic commence shall include the following controls:

- **Authentication**: What level of confidence shall the customer and trader require in each other's claimed identity?
- **Authorization**: Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?
- **Contract and tendering processes**: What are the requirements for confidentiality, integrity, proof of dispatch, receipt of key documents, and the non-repudiation of contracts?
- **Pricing information**: What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?

- **Order transactions**: How is the confidentiality and integrity of order, payment, and delivery address details and confirmation of receipt provided?
- **Vetting**: What degree of vetting is appropriate to check payment information supplied by the customer?
- **Settlement**: What is the most appropriate form of payment to guard against fraud?
- **Ordering**: What protection is required to maintain the confidentiality and integrity of order information, and to avoid the loss or duplication of transactions?
- **Liability**: Who carries the risk for any fraudulent transactions?

Many of the above considerations shall be addressed by the application of encryption outlined in Section 08.03, taking into account compliance with legal requirements.

Electronic commerce arrangements between trading partners shall be supported by a documented agreement that commits both parties to the agreed terms of trading, including details of authorization (see **Authorization** bullet above).

Other agreements with information service and value added network providers may be necessary.

Public trading systems shall publicize their terms of business to customers.

Consideration shall be given to the resilience to attack of the host used for electronic commerce, and the security implications of any network interconnection required for its implementation.

06.07.04 Security of Electronic Mail

06.07.04.01 Security Risks

Electronic mail is being used for business communications, supplementing traditional forms of communication such as faxes and letters. Electronic mail differs from traditional forms of business communications (e.g., its speed, message structure, degree of informality, vulnerability to unauthorized actions).

Information Security Officer, in conjunction with the Information Security Council, shall establish and implement standards and guidelines to address the security risks associated with electronic mail.

Security risks include:

- Vulnerability of messages to unauthorized access or modification or denial of service
- Vulnerability to error (e.g., incorrect addressing or misdirection, general reliability and availability of the service)
- Impact of a change of communication media on business processes (e.g., the effect of increased speed of dispatch, the effect of sending formal messages from person to person rather than company to company)
- Legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance
- Implications of publishing externally accessible staff lists
- Controlling remote user access to electronic mail accounts

06.07.04.02 Policy on Electronic Mail

The Information Security Council shall establish and implement standards and guidelines that address the following electronic mail issues:

- Attacks on electronic mail (e.g., viruses, interception)
- Protection of electronic mail attachments
- Appropriate use of electronic mail
- Employee responsibility not to compromise the college (e.g., sending defamatory electronic mail, use for harassment, unauthorized purchasing)
- Use of cryptographic techniques to protect the confidentiality and integrity of electronic messages
- Retention of messages which, if stored, could be discovered in case of litigation
- Additional controls for validating messages that cannot be authenticated.

All employees shall comply with acceptable use policies for e-mail.

06.07.05 Security of Electronic Office Systems

The Information Security Council shall establish and implement standards and guidelines to control the business and security risks associated with electronic office systems. These provide opportunities for faster dissemination and sharing of business information using a combination of documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and fax machines.

The following issues shall be addressed by the standards and guidelines:

- Vulnerabilities of information in office systems (e.g., recording phone calls or conference calls, confidentiality of calls, storage of faxes, opening mail, distribution of mail)
- Policy and appropriate controls to manage information sharing (e.g., the use of corporate electronic bulletin boards)
- Excluding categories of sensitive business information if the system does not provide an appropriate level of protection
- Restricting access to diary information relating to selected individuals (e.g., staff working on sensitive projects)
- The suitability, or otherwise, of the system to support business applications, such as communicating orders or authorizations
- Categories of staff, contractors or business partners allowed to use the system and the locations from which it may be accessed
- Restricting selected facilities to specific categories of user
- Identifying the status of users (e.g., employees of the organization, contractors in directories for the benefit of other users)
- Retention and back-up of information held on the system

- Fallback requirements and arrangements

06.07.06 Publicly Available Systems

Care shall be taken to protect the integrity of electronically published information to prevent unauthorized modification that could harm the reputation of the college. Information on a publicly available system (e.g., information on a web server accessible via the Internet) shall comply with laws, rules and regulations in the jurisdiction in which the system is located or where the transaction is taking place, in addition to college policies and procedures. There shall be a formal authorization process before information is made publicly available.

Software, data and other information requiring a high level of integrity, made available on a publicly available system, shall be protected by appropriate mechanisms (e.g., digital signatures). Electronic publishing systems, especially those that permit feedback and direct entering of information, shall be carefully controlled so that:

- Information is obtained in compliance with any data protection legislation
- Information input to, and processed by, the publishing system shall be processed completely and accurately in a timely manner
- Sensitive information shall be protected during the collection process and when stored
- Access to the publishing system does not allow unintended access to networks to which it is connected

All publicly available systems shall be protected by the following security measures, at a minimum:

- Router based access control list (ACL) that restricts access to only the necessary services on the system
- Firewall demilitarized zone (DMZ) to segregate publicly available systems from internal servers
- Firewall rules to limit access from publicly available systems to only necessary services on internal servers
- Restrict log-on access to authorized systems from the internal network
- Limit log-on access to production support team members only
- Intrusion prevention systems (IPS) shall monitor all publicly available systems

06.07.07 Other Forms of Information Exchange

The Information Security Council shall establish and implement standards and guidelines to protect the exchange of information through the use of voice, facsimile and video communications facilities. Information could be compromised due to lack of awareness, policy or procedures on the use of such facilities (e.g., being overheard on a mobile phone in a public place, answering machines being overheard, unauthorized access to dial-in voice-mail systems, accidentally sending facsimiles to the wrong person using facsimile equipment).

Business operations could be disrupted and information could be compromised if communications facilities fail, are overloaded, or interrupted.

Information could also be compromised if it is accessed by unauthorized users.

Information Security shall establish standards and guidelines that shall address the following issues:

- Reminding staff that they shall take appropriate precautions not to reveal sensitive information, so as to avoid being overheard or intercepted when making a phone call by:
    - People in their immediate vicinity particularly when using mobile phones
    - Wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers when using analog mobile phones
    - People at the recipient's end
- Reminding staff that they shall not have confidential conversations in public places or open offices and meeting places with thin walls
- Not leaving sensitive messages on answering machines since these may be replayed by unauthorized persons, stored on communal systems, or stored incorrectly as a result of misdialing
- Reminding staff about the problems of using facsimile machines, namely:
    - Unauthorized access to built-in message stores to retrieve messages
    - Deliberate or accidental programming of machines to send messages to specific numbers
    - Sending documents and messages to the wrong number either by misdialing or using the wrong stored number

07 SYSTEM and NETWORK ACCESS CONTROL

Overview

System and network access control are a cornerstone in the foundation of information security. They provide the first line of defense for all information systems and data.

07.01 Business Requirement for Access Control

07.01.01 Access Control

07.01.01.01 Policy and Business Requirements

Business requirements for access control shall be defined and documented. Access control rules and rights for each user or group of users shall be clearly stated in an access policy statement. Users and service providers shall be given a clear statement of the business requirements to be met by access controls.

The policy takes account of the following:

- Security requirements of individual business applications
- Identification of all information assets related to the business applications
- Policies for information dissemination and authorization (e.g., the need-to-know principle, security levels and classification of information assets)

- Consistency between the access control and information classification policies of different systems and networks
- Relevant legislation and any contractual obligations regarding protection of access to data or services
- Standard user access profiles for common categories of job
- Management of access rights in a distributed and networked environment that recognizes all types of connections available

07.01.01.02 Access Control Rules

In specifying the access control rules, care shall be taken to consider the following:

- Differentiating between rules that shall always be enforced and rules that are optional or conditional
- Establishing rules based on the premise, "what shall be generally forbidden unless expressly permitted"
- Changes in information labels that are initiated automatically by information processing facilities and those initiated at the discretion of a user
- Changes in user permissions that are initiated automatically by the information system and those initiated by an administrator
- Rules that require administrator or other approval before enactment and those that do not

07.02 User Access Management

The Information Security Council shall establish procedures to control the allocation of access rights to information systems and services. The procedures shall cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention shall be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. Information Security is responsible for ensuring compliance with this control.

07.02.01 User Registration

There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services. Access to multi-user information services shall be controlled through a formal user registration process that shall include:

- All systems shall use unique user IDs to ensure accountability
- All user access shall be approved by the user's direct manager and the system/application owner
- The system/application administrator responsible for granting access shall ensure access is commensurate with business needs
- All users shall sign the access request form that shall detail the conditions of their access and signify their understanding of the conditions for access

- System/application administrator shall not grant access to any user without an approved access request form
- All access rights for users who have been terminated shall be immediately removed
- All access rights for users who have changed jobs and no longer require access shall be immediately removed
- System/application administrators shall review all user accounts for redundant IDs semi-annually. Any redundant IDs shall be removed immediately
- System/application administrators shall review all user accounts for terminated users semi-annually. Any terminated user account shall have their access rights revoked immediately

07.02.02 Privilege Management

The allocation and use of privileged accounts and utilities shall be restricted and controlled.

The system manager of multi-user systems that require protection against unauthorized access shall have all allocation of privileges controlled through a formal authorization process.

The system and application owner shall identify the privileges associated with each system product (e.g., operating system, database management system, and each application) and the categories of staff that shall be granted access to them.

- Privileges shall be allocated to individuals on a need-to-use basis and on an event-by-event basis (i.e., the minimum requirement for their functional role only when needed)
- System/application owners shall maintain a record of all privileges allocated

07.02.03 User Password Management

Passwords are a common means of validating a user's identity to access an information system or service. The allocation of passwords shall be controlled through a formal management process, the approach shall be:

- All users shall sign a statement to keep personal passwords confidential
- Where users are required to maintain their own passwords, system/application administrators shall provide them with a secure initial temporary password, which they are forced to change immediately. Temporary passwords provided when users forget their password shall only be supplied following positive identification of the user
- Temporary passwords shall be given to users in a secure manner. The use of third parties or unprotected (clear text) electronic mail messages shall be avoided. Users shall acknowledge receipt of passwords
- Passwords shall never be stored on computer system in an unprotected form

07.02.04 Review of User Access Rights

To maintain effective control over access to data and information services, management shall conduct a formal process at regular intervals to review users' access rights:

- System/application administrators shall review all user access rights on a semi-annual basis

- System/application administrators shall review all privileged access rights on a semi-annual basis.

07.03 User Responsibilities

07.03.01 Password Use

Users shall follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services.

- All employees shall keep passwords confidential
- Employees shall not keep a paper record of passwords
- All employees shall change passwords whenever there is any indication of possible system or password compromise
- All users shall comply with the password standards for length and composition
- Users shall not e-mail passwords
- Users shall not store their passwords in any automated log-on process except where authorized by the college
- Users shall not share passwords
- User shall change any temporary/default passwords at the first login

07.03.02 Unattended User Equipment

Users shall ensure that unattended equipment has appropriate protection. Equipment installed in user areas (e.g., workstations or file servers) may require specific protection from unauthorized access when left unattended for an extended period. All users and contractors shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

- All users shall terminate any active sessions when leaving their system unattended unless they can be secured by an appropriate locking mechanism (e.g., password protected screen saver)
- All users shall follow appropriate log-off procedures when necessary, when processing is complete, or when leaving for the day
- Secure PCs or terminals from unauthorized use with an appropriate locking mechanism (e.g., password access) when not in use

07.04 Network Access Control

Access to both internal and external networked services shall be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services. Adhere to the following:

- Any connectivity between networks and public or business partner networks shall be controlled through the use of firewalls, access control lists (ACLs), and intrusion detection or intrusion prevention systems (IDS/IPS)
- Any users or systems connecting to networks shall be appropriately authenticated

07.04.01 Use of Network Services

Insecure connections to network services can affect the whole organization. Users shall only be provided with direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications, or to users in high-risk locations (e.g., public or external areas that are outside the organization's security management and control).

Standards shall be formulated concerning the use of networks and network services. This shall cover:

- The networks and network services that are allowed to be accessed
- Authorization procedures for determining who is allowed to access which networks and networked services
- Management controls and procedures to protect the access to network connections and network services

These standards shall be consistent with the business access control policy.

07.04.02 Enforced Path

The path from the user terminal to the computer service may need to be controlled. Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to business applications, or unauthorized use of information facilities. Incorporating controls that restrict the route between a user terminal and the computer services its user is authorized to access (i.e., creating an enforced path) can reduce such risks.

The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorized to access. This usually requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices.

Examples of this are as follows:

- Allocating dedicated lines or telephone numbers
- Automatically connecting ports to specified application systems or security gateways
- Limiting menu and submenu options for individual users
- Preventing unlimited network roaming
- Enforcing the use of specified application systems and/or security gateways for external network users
- Actively controlling allowed source to destination communications via security gateways (e.g., firewalls)

- Restricting network access by setting up separate logical domains (e.g., virtual private networks) for user groups within the organization

The requirements for an enforced path shall be based on the business access control policy.

07.04.03 User Authentication for External Connections

External connections provide a potential for unauthorized access to college information (e.g., access by dial-up methods). Therefore, access by remote users shall be authenticated. There are different types of authentication methods; some of these provide a greater level of protection than others (e.g., methods based on the use of cryptographic techniques can provide strong authentication). It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

Authentication of remote users can be achieved, for example, using a cryptographic based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines or a network user address checking facility can also be used to provide assurance of the source of connections.

07.04.04 Node Authentication

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems shall therefore be authenticated. This is especially important if the connection uses a network that is outside the control of the organization's security management.

Node authentication serves as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility

07.04.05 Remote Diagnostic Port Protection

Access to diagnostic ports shall be securely controlled. Many computers and communication systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers.

All access to diagnostics ports on systems shall be controlled by the system administrator.

All dial-in access modem ports shall be disconnected until such time that the support team requires access.

Upon completion of any diagnostic/maintenance activity the diagnostic port shall be disabled immediately.

Any access to diagnostic ports shall be logged, where possible.

07.04.06 Segregation in Networks

As networks become increasingly complex and more interconnected between business units and external business partners, it is necessary to segregate the flow of traffic between those networks.

All connections between networks and business partners shall be through the use of firewalls, VLANs (virtual local area networks) and access control lists (ACLs).

All connection between lines of business shall be controlled by VLANs and access control lists. If a line of business has any unsecured connections then a firewall between lines of business shall also be used.

07.04.07 Network Connection Control

Access control policy requirements for shared networks, especially those extending to external business partners, require the incorporation of controls to restrict the connection capability of the users. Such controls can be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied shall be based on the access policy and requirements of the business applications, and shall be maintained and updated accordingly.

Examples of applications to which restrictions shall be applied are:

- Electronic mail
- One-way file transfer
- Both-ways file transfer
- Interactive access
- Network access linked to time of day or date

07.04.08 Network Routing Control

Shared networks, especially those extending to external business partners require the incorporation of routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Routing controls shall be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware.

07.04.09 Security of Network Services

A wide range of public or private network services is available, some of which offer value-added services. Network services may have unique or complex security characteristics. Any line of business using third party network services shall ensure that a clear description of the security attributes of all services used is provided.

07.05 Operating System Access Control

Security facilities at the operating system level shall be used to restrict access to computer resources. Including the following:

- Identifying and verifying the identity, and if necessary, the terminal or location of each authorized user
- Recording successful and failed system accesses
- Providing appropriate means for authentication; if a password management system is used, it shall ensure quality passwords.
- Where appropriate, restricting the connection times of users

Other access control methods, such as multi-factor authentication, are available if these are justified based on business risk.

07.05.01 Automatic Terminal Identification

When possible, all systems shall only allow direct access to privileged system accounts (e.g., root on UNIX and Linux, Sec Officer on AS/400) from a system console.

07.05.02 Terminal Log-on Procedures

Access to information services shall be attainable via a secure log-on process. The procedure for logging into a computer system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure shall therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with unnecessary assistance.

All systems shall adhere to the following:

- Display a general notice warning that the computer shall only be accessed by authorized users
- Not display system or application identifiers until the log-on process has been successfully completed
- Not provide help messages during the log-on procedure that would aid an unauthorized user
- Validate the log-on information only on completion of all input data. If an error condition arises, the system shall not indicate which part of the data is correct or incorrect
- Limit the number of unsuccessful log-on attempts allowed
- Record unsuccessful attempts
- Forcing a time delay before further log-on attempts after a failed log-on
- Limit the number of failed login attempts
- Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system shall terminate the log-on
- Display the following information upon completion of a successful log-on:
    - Date and time of the previous successful log-on
    - (Where possible) Details of any unsuccessful log-on attempts since the last successful log-on

07.05.03 User Identification and Authentication

All users, including technical support staff, such as operators, network administrators, system programmers and database administrators shall have a unique identifier (user ID) for their personal and sole use so that activities can subsequently be traced to the responsible individual. User IDs shall not give any indication of the user's privilege level (e.g., manager, supervisor). In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management shall be documented for such cases. Where shared accounts shall be used, ultimate accountability shall be assigned to a specific employee.

There are various authentication procedures that can be used to substantiate the claimed identity of a user. Passwords are a very common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols.

Objects such as memory tokens or smart cards that users possess can also be used for identification and authentication. A combination of technologies and mechanisms securely linked shall result in stronger authentication.

07.05.04 Password Management System

Passwords are one of the principal means of validating a user's authority to access a computer service. Password management systems shall provide an effective, interactive facility that ensures quality passwords.

A good password management system shall:

- Enforce the use of individual passwords to maintain accountability
- Where appropriate, allow users to select and change their own passwords and include a confirmation procedure to allow for input errors
- Enforce a choice of quality passwords that meet Standards
- Where users maintain their own passwords, enforce password changes as described in Information Security Standards
- Force users to change temporary passwords at the first log-on
- Maintain a record of previous user passwords and prevent re-use
- Not display passwords on the screen when being entered
- Store password files separately from application system data
- Store passwords in encrypted form using a one-way encryption algorithm
- Alter default vendor passwords following installation of software

07.05.05 Use of System Utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled. The following controls shall be used when possible:

- Use of authentication procedures for system utilities
- Segregation of system utilities from applications software
- Limitation of the use of system utilities to the minimum practical number of trusted, authorized users
- Authorization for ad hoc use of systems utilities
- Limitation of the availability of system utilities (e.g., for the duration of an authorized change)
- Logging of all use of system utilities
- Defining and documenting of authorization levels for system utilities
- Removal of all unnecessary software based utilities and system software

07.05.06 Terminal Time-Out

Inactive terminals in high-risk locations (e.g., public or external areas outside's security management) or serving high risk systems, shall shut down after a defined period of inactivity to prevent access by unauthorized persons. This time-out facility shall clear the terminal screen and close both application and network sessions after a defined period of inactivity. The time-out delay shall reflect the security risks of the area and the users of the terminal.

A limited form of terminal time-out facility shall be provided for some PCs (e.g., password protected screen saver), which clears the screen and prevents unauthorized access but does not close down the application or network sessions.

07.05.07 Limitation of Connection Time

Restrictions on connection times provide additional security for high-risk applications. Limiting the period during which terminal connections are allowed to computer services reduces the window of opportunity for unauthorized access. Such a control shall be considered for sensitive computer applications, especially those with terminals installed in high-risk locations (e.g., public or external areas that are outside security management). Any such connections shall use the following controls, where possible:

- Using predetermined time slots for batch file transmissions or regular interactive sessions of short duration
- Restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation.

07.06 Application Access Control

Security facilities shall be used to restrict access within application systems. Logical access to software and information shall be restricted to authorized users. Application systems shall:

- Control user access to information and application system functions, in accordance with a defined business needs
- Provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls
- Not compromise the security of other systems with which information resources are shared
- Be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users

07.06.01 Information Access Restriction

Users of application systems, including support staff, shall be provided with access to information and application system functions in accordance with the access control policies. The following controls shall be used in order to support access restriction requirements:

- Providing menus to control access to application system functions
- Restricting users' knowledge of information or application system functions which they are not authorized to access, with appropriate editing of user documentation

- Controlling the access rights of users (e.g., read, write, delete, execute)
- Ensuring that outputs from application systems handling sensitive information contain only the information that are relevant to the use of the output, and are sent only to authorized terminals and locations, including periodic review of such outputs to ensure that redundant information is removed

07.07 Monitoring System Access and Use

Systems shall be monitored to detect deviation from access control policy and record events to provide evidence in case of security incidents. System monitoring allows the effectiveness of adopted controls to be checked and conformity to the access policy verified.

07.07.01 Event Logging

Audit logs recording exceptions and other security-relevant events shall be produced and retained for a specified time, based on the line of business risk assessment, to assist in future investigations and access control monitoring. Audit logs shall also include:

- User IDs
- Dates and times for log-on and log-off
- Terminal identity or location if possible
- Records of successful and rejected system access attempts
- Records of successful and rejected data and other resource access attempts

Certain audit logs are required to be archived as part of the record retention policy or because of requirements to collect evidence.

07.07.02 Monitoring System Use

07.07.02.01 Procedures and Areas of Risk

Information Security shall establish and assist with implementing procedures for monitoring the use of IT systems and resources. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities shall be determined by a risk assessment. Areas that shall be considered include:

- Authorized access, including detail such as:
    - The user ID
    - The date and time of key events
    - The types of events
    - The files accessed
    - The program/utilities used
    - All privileged operations, such as:
    - Use of supervisor account
    - System start-up and stop
    - Input/output device attachment/detachment

- Unauthorized access attempts, such as:
  - Failed attempts
  - Access policy violations and notifications for network gateways and firewalls
  - Alerts from proprietary intrusion detection systems
- System alerts or failures such as:
  - Console alerts or messages
  - System log exceptions
  - Network management alarms

07.07.02.02 Risk Factors

The result of the monitoring activities shall be reviewed regularly. The frequency of the review shall depend on the risks involved. Risk factors that shall be considered include:

- The criticality of the application processes
- The value, sensitivity, or criticality of the information involved
- The past experience of system infiltration and misuse
- The extent of system interconnection (particularly public networks)

07.07.02.03 Logging and Reviewing Events

System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation shall be considered.

When allocating the responsibility for log review, a separation of roles shall be considered between the person(s) undertaking the review and those whose activities are being monitored.

Particular attention shall be given to the security of the logging facility because if tampered with it can provide a false sense of security.

Procedures shall be implemented to protect against unauthorized changes and operational problems including:

- The logging facility being de-activated
- Alterations to the message types that are recorded
- Log files being edited or deleted
- Log file media becoming exhausted, and either failing to record events or overwriting itself

07.07.03 Clock Synchronization

The correct setting of computer and network systems clocks is important to ensure the accuracy of audit logs which may be required for investigations, or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

Where a computer or communications device has the capability to operate a real-time clock, it shall be set to an agreed standard (e.g., universal coordinated time (UCT), local standard time). As some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.

07.08 Mobile Computing and Teleworking

The protection required shall be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment shall be considered and appropriate protection applied. In the case of teleworking, the organization shall apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

07.08.01 Mobile Computing

When using mobile computing facilities (e.g., notebooks, palmtops, laptops and mobile phones), special care should be taken to ensure that business information is not compromised.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities (e.g., using cryptographic techniques).

It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, for example, theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place.

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference center and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

Training should be arranged for staff using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

07.08.02 Teleworking

Teleworking uses communications technology to enable staff to work remotely from a fixed location outside of their organization. Suitable protection of the teleworking site shall be in place against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, and misuse of facilities.

The following controls shall be adhered to:

- Any system connecting to networks shall have appropriate up to date anti-virus software.
- Any system connecting to networks shall have appropriate personal firewall that prevents split tunneling.

- All access by teleworkers shall be monitored for inappropriate activities.
- Any teleworker connecting to networks via public networks (e.g., the Internet) shall do so utilizing an approved VPN.
- The employee's direct manager and Information Security shall approve all access to networks by teleworkers.

08 INFORMATION SYSTEM DEVELOPMENT & MAINTENANCE

Overview

The development of new systems and the maintenance of current systems shall be completed with an awareness of information security, accepted best practices, and development standards.

08.01 Security Requirements of Information Systems

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

08.01.01 Security Requirements Analysis and Specification

Statements of business requirements for new systems (developed in-house/outsourced/or purchased package) or enhancements to existing systems shall specify the requirements for security controls. Such specifications shall consider the automated controls to be incorporated in the system and the need for supporting manual controls.

Security requirements and controls shall equal the business value of the information assets involved and the potential business damage, which might result from a failure or absence of security.

All new systems shall be reviewed utilizing the information security risk assessment process.

08.02 Correct Processing in Applications

Appropriate controls shall be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

08.02.01 Input Data Validation

All data input to applications shall be validated to ensure that this data is correct and appropriate.

Checks shall be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables. The following guidelines shall be considered:

- Verified input or other input checks to detect the following errors:
  - Out-of-range values
  - Invalid characters in data fields
  - Missing or incomplete data
  - Exceeding upper and lower data volume limits
  - Unauthorized or inconsistent control data
- Periodic review of the content of control data files to confirm their validity and integrity
- Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents shall be authorized)
- Procedures for responding to validation errors
- Procedures for testing the plausibility of the input data
- Defining the responsibilities of all personnel involved in the data input process

08.02.02 Control of Internal Processing

Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. The design and implementation of applications shall ensure that the risks of processing failures leading to a loss of integrity are minimized. Specific areas to consider include:

- the use of add, modify, and delete functions to implement changes to data
- the procedures to prevent programs running in the wrong order or running after failure of prior processing
- the use of appropriate programs to recover from failures to ensure the correct processing of data

An appropriate checklist of applications shall be prepared, activities documented, and the results kept secure. The validation checks required will depend on the nature of the application and the business impact of any corruption of data.

08.02.03 Message Integrity

Message authentication shall be considered for applications where there is a security requirement to protect the integrity of the message content (e.g., electronic funds transfers, EDI transactions, personnel information, financial data) with high importance or other similar electronic data exchanges. An assessment of security risks shall be carried out to determine if message integrity is required, and to identify the most appropriate method of implementation.

Message integrity is not designed to protect the contents of a message from unauthorized disclosure. Cryptographic techniques can be used as an appropriate means of implementing message authentication.

08.02.04 Data Output Validation

Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances. Checks shall be applied to the output of all business transactions.

Output validation may include:

- Plausibility checks to test whether the output data is reasonable
- Reconciliation control counts to ensure processing of all data
- Providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information
- Procedures for responding to output validation tests
- Defining the responsibilities of all personnel involved in the data output process

08.03 Cryptographic Controls

The objective of cryptographic controls is to protect the confidentiality, authenticity or integrity of information by cryptographic means.

08.03.01 Use of Cryptographic Controls

Any use of cryptographic controls shall be based on a determination from an information security risk assessment. The assessment shall be used to determine whether a cryptographic control is appropriate, what type of control shall be applied and for what purpose and business processes.

Cryptographic controls shall be used on all confidential or sensitive data that shall traverse any public network. Information Security shall identify the appropriate encryption levels for such data.

Information Security shall be responsible for all cryptographic key management.

Information Security shall be responsible for advising all Information Technology Services departments on implementing cryptographic controls.

08.03.02 Encryption

Encryption is a cryptographic technique that can be used to protect the confidentiality of information. It shall be considered for the protection of sensitive or critical information.

Based on an information security risk assessment, the required level of protection shall be identified, taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

Information Security is responsible to ensure that when implementing the organization's cryptographic policy, all the statutory and regulatory requirements are to be met.

Information Security shall identify appropriate key management systems that comply with all local statutory and regulatory requirements.

08.03.03 Digital Signatures

Digital signatures provide a means of protecting the authenticity and integrity of electronic documents. For example, they can be used in electronic commerce where there is a need to verify who signed an electronic document and check whether the contents of the signed document have been changed.

Digital signatures can be applied to any form of document being processed electronically (e.g., electronic payments, funds transfers, contracts, agreements).

Digital signatures can be implemented using a cryptographic technique based on a uniquely related pair of keys where one key is used to create a signature (the private key) and the other to check the signature (the public key).

Care shall be taken to protect the confidentiality of the private key. This key shall be kept secret since anyone having access to this key can sign documents (e.g., payments, contracts) thereby forging the signature of the owner of that key. In addition, protecting the integrity of the public key is important. This protection is provided by the use of a public key certificate.

Consideration needs to be given to the type and quality of the signature algorithm used and the length of keys to be used. Cryptographic keys used for digital signatures shall be different from those used for encryption.

When using digital signatures, consideration shall be given to any relevant legislation that describes the conditions under which a digital signature is legally binding. For example, in the case of electronic commerce, it is important to know the legal standing of digital signatures. It may be necessary to have binding contracts or other agreements to support the use of digital signatures where the legal framework is inadequate. Legal advice shall be sought regarding the laws and regulations that might apply to the organization's intended use of digital signatures.

08.03.04 Non-Repudiation Services

Non-repudiation services shall be used where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action (e.g., a dispute involving the use of a digital signature on an electronic contract or payment). They can help establish evidence to substantiate whether a particular event or action has taken place (e.g., denial of sending a digitally signed instruction using electronic mail). These services are based on the use of encryption and digital signature techniques.

08.03.05 Key Management

08.03.05.01 Protection of Cryptographic Keys

The management of cryptographic keys is essential to the effective use of cryptographic techniques. Any compromise or loss of cryptographic keys may lead to compromise of the confidentiality, authenticity and/or integrity of information.

Information Security shall establish management systems to support the organization's use of the two types of cryptographic techniques; secret key and public key. Any such management system shall comply with any local statutory or regulatory requirements.

- Secret key techniques: Where two or more parties share the same key and this key is used both to encrypt and decrypt information. This key shall be kept secret since anyone having access to

it is able to decrypt all information being encrypted with that key, or to introduce unauthorized information.

- Public key techniques: Where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which shall be kept secret). Public key techniques can be used for encryption and to produce digital signatures.

All keys shall be protected against modification and destruction, and secret and private keys need protection against unauthorized disclosure. Cryptographic techniques can also be used for this purpose. Physical protection shall be used to protect equipment used to generate, store and archive keys.

08.03.05.02 Standards, Procedures and Methods

Any key management system shall be based on an agreed set of standards, procedures and secure methods for:

- Generating keys for different cryptographic systems and different applications
- Generating and obtaining public key certificates
- Distributing keys to intended users, including how keys shall be activated when received
- Storing keys, including how authorized users obtain access to keys
- Changing or updating keys including rules on when keys shall be changed and how this shall be done
- Dealing with compromised keys
- Revoking keys, including how keys shall be withdrawn or deactivated, for example, when keys have been compromised or when a user leaves an organization (in which case keys shall also be archived)
- Recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information)
- Archiving keys (e.g., for information archived or backed up)
- Destroying keys
- Logging and auditing of key management related activities

In order to reduce the likelihood of compromise, keys shall have defined activation and deactivation dates so they can only be used for a limited period of time. The period of time shall be dependent on the circumstances under which the cryptographic control is being used and the determined risk.

Procedures shall be established for handling legal requests for access to cryptographic keys (e.g., encrypted information may need to be made available in an unencrypted form as evidence in a court case).

In order to ensure the protection of public keys, Information Security shall establish a relationship with a recognized certificate authority.

The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g., with a certification authority) shall cover issues of liability, reliability of services and response times for the provision of services.

08.04 Security of System Files

Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

08.04.01 Control of Operational Software

There shall be procedures in place to control the installation of software on operational systems. To minimize the risk of corruption to operational systems, the following shall be guidelines to be considered to control changes:

- The updating of operational software, applications, and program libraries shall only be performed by the authorized systems administrator upon appropriate management authorization.
- When possible, production systems shall not include the source code for any application.
- Executable code shall not be implemented on any operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated.
- An audit log shall be maintained of all updates to operational programs.
- Previous versions of software shall be retained as a contingency measure.
- Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier.
- Software patches shall be applied as soon as possible when they can help to remove or reduce security weaknesses.
- Physical or logical access shall only be given to vendors for support purposes when necessary, and with management approval. The supplier's activities shall be monitored and all changes logged.

08.04.02 Protection of System Test Data

Test data shall be selected carefully, and protected and controlled. System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data. Data owners shall approve anytime production information is copied to a test application systems. These test systems must be controlled to prevent unauthorized accessed.

08.04.03 Access Control to Program Source Code

In order to reduce the potential for corruption of computer programs; strict control shall be maintained over access to program source code as follows:

- Program source libraries shall not be stored on production systems
- Application owners shall identify a custodian for all source code
- Only identified IT support staff shall have unrestricted access to source code

- All source code shall be monitored and maintained through the use of a source code control system
- Any physical listing of application source code shall be maintained securely (e.g., locked file cabinet)
- All maintenance to source code shall follow change control procedures

08.05 Security in Development and Support Processes

The objective of security in development and support processes is to maintain the security of application system software and information.

08.05.01 Change Control Procedures

In order to minimize the corruption of information systems, all employees shall adhere to change control procedures.

08.05.02 Technical Review of Operating System/Application Changes

Periodically it is necessary to change the operating system (e.g., to install a newly supplied software release or patches). When changes occur, the application systems shall be reviewed and tested to ensure that there is no adverse impact on operation or security.

Information Security shall review application controls and integrity procedures to ensure they have not been compromised.

Information Security shall ensure that an annual budget exists to covers vulnerability assessment and penetration tests/tools for all critical systems/applications.

As part of the change control process the Information Security shall review any operating system changes/application changes before implementation.

All changes to operating systems/applications shall be appropriately reflected in the business continuity plan (disaster recovery plan).

08.05.03 Restrictions on Changes to Vendor-Supplied Software Packages

Modifications to vendor-supplied software packages shall be discouraged. As far as possible, and practicable, vendor-supplied software packages shall be used without modification.

When it is deemed essential to modify a software package, these controls shall be followed:

- Information Security shall identify any risk of compromise to built-in controls and integrity processes
- The application owner shall notify management of the vendor's approval/disapproval of any modification
- The application owner shall address the possibility of obtaining the changes from the vendor
- The original software shall be maintained and clearly identified

08.05.04 Covert Channels and Trojan Code

A covert channel can expose information by some indirect and obscure means. It may be activated by changing a parameter accessible by both secure and insecure elements of a computing system, or by embedding information into a data stream.

Trojan code is designed to affect a system in a way that is not authorized and not readily noticed and not required by the recipient or user of the program.

In order to avoid covert code and Trojans, these controls shall be followed:

- Buying programs only from reputable sources
- Buying programs in source code, where possible, so the code may be verified
- Using products evaluated by trusted organizations
- Inspecting all source code before operational use
- Controlling access to, and modification of, code once installed

08.05.05 Outsourced Software Development

Outsourced software development shall be supervised and monitored by the college. Where software development is outsourced, the following points shall be considered:

- Licensing arrangements, code ownership, and intellectual property rights
- Certification of the quality and accuracy of the work carried out
- Escrow arrangements may be required in the event of failure of the third party
- Rights of access for audit of the quality and accuracy of work done
- Contractual requirements for quality and security functionality of code
- Testing before installation to detect malicious and Trojan code

09 BUSINESS CONTINUITY AND DISASTER RECOVERY

Overview

An incomplete or inaccurate disaster recovery plan can result in anything from a slight to catastrophic impact on the organization/or its students. Therefore, it is the policy of Cincinnati State to develop and implement disaster recovery plans that facilitate the backup of all critical computer, network, and telecommunications systems and for their recovery within a timeframe that minimizes disruption and/or cost to the school in the event of a localized or general disruption of service. Disaster recovery plans are a critical and mandatory component of overall business continuity planning.

09.01 Business Continuity Management Process

There shall be a managed process in place for developing and maintaining business continuity throughout the organization. It shall bring together the following key elements of business continuity management:

- Understanding the risks the school is facing in terms of their likelihood and their impact, including identification and prioritization of critical business processes.

- Understanding the impact which interruptions are likely to have on the business (it is important that solutions are found that shall handle smaller incidents, as well as serious incidents that could threaten the viability of the organization) and establishing the business objectives of information processing facilities.
- Considering the purchase of suitable insurance which may form part of the business continuity process.
- Formulating and documenting a business continuity strategy consistent with the agreed business objectives and priorities; formulating and documenting business continuity plans in line with the agreed strategy.
- Regular testing and updating of the plans and processes put in place.
- Integrating the management of business continuity in the organization's processes and structure.

09.02 Business Continuity and Impact Analysis

Business continuity shall begin with a business impact analysis which identifies events that can cause interruptions to business processes (e.g., equipment failure, flood and fire). This shall be followed by a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period). Both of these activities shall be carried out with full involvement from owners of business resources and processes. This assessment shall consider all business processes, and is not limited to the information processing facilities.

Depending on the results of the risk assessment, a strategy plan shall be developed to determine the overall approach to business continuity.

At a minimum, the strategy plan shall address the following:

- Recovery time objective (RTO): Amount of downtime the business before all business processes are re-established
- Recovery point objective (RPO): Establishes how current the data used to restore the business processes shall be
- Disaster recovery plan for information systems recovery: To include network, data process systems, and telecommunications

09.03 Writing and Implementing Continuity Plans

Plans shall be developed to maintain or restore business operations in the required time-frames following interruption to, or failure of, critical business processes. The business continuity planning process shall consider the following:

- Identification and agreement of all responsibilities and emergency procedures
- Implementation of emergency procedures to allow recovery and restoration in required timeframes. Particular attention needs to be given to the assessment of external business dependencies and the contracts in place
- Documentation of agreed procedures and processes

- Appropriate education of staff in the agreed emergency procedures and processes, including crisis management
- Regular testing of the plans
- Routing maintenance of the plans

The planning process shall focus on the required business objectives (i.e., restoring of specific services to customers in an acceptable amount of time). The services and resources that shall enable this to occur shall be considered, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities.

09.04 Business Continuity Planning Framework

A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance. Each business continuity plan shall specify clearly the conditions for its activation, as well as the individuals responsible for executing each component of the plan.

When new requirements are identified, established emergency procedures (e.g., evacuation plans or any existing fallback arrangements) shall be amended as appropriate.

A business continuity planning framework shall consider the following:

- The conditions for activating the plans which describe the process to be followed (how to assess the situation, who is to be involved, etc.) before each plan is activated.
- Emergency procedures that describe the actions to be taken following an incident which jeopardizes business operations and/or human life. This shall include arrangements for public relations management and for effective liaison with appropriate public authorities (e.g., police, fire service, local government).
- Fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations and to bring business processes back into operation in the required time frames.
- Resumption procedures that describe the actions to be taken to return to normal business operations.
- A maintenance schedule that specifies how and when the plan shall be tested, and the process for maintaining the plan.
- Awareness and education activities that are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective.
- The responsibilities of the individuals (i.e., describing who is responsible for executing which component of the plan). Alternatives shall be nominated as required.

Each plan shall have a specific owner. Emergency procedures, manual fallback plans and resumption plans shall be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, shall usually be the responsibility of the service providers.

09.05 Testing and Maintaining Business Continuity

Business continuity plans shall be maintained and tested on a schedule prescribed by a risk assessment to ensure their continuing effectiveness. Procedures shall be included within the change management program to ensure that business continuity matters are appropriately addressed.

Responsibility shall be assigned for regular reviews of each business continuity plan; the identification of changes in business arrangements not yet reflected in the business continuity plans shall be followed by an appropriate update of the plan. This formal change control process shall ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

The following situations might necessitate updating plans include the acquisition of new equipment or upgrading of operational systems and changes in:

- Personnel
- Addresses or telephone numbers
- Business strategy
- Location, facilities and resources
- Legislation
- Contractors, suppliers and key customers
- Processes, or new/withdrawn ones
- Risk (operational and financial)

09.06 Corporate Relationships for Business Continuity and Disaster Recovery

Where appropriate Information Security should engage in relationships with other organizations to provide Business Continuity and Disaster Recovery (BCDR) services such as data center hosting space, server co-location, etc. These services can often be non-monetary in nature such as a contractual agreement to provide temporary space in the event of a significant outage affecting either organization. These contracts or agreements shall adhere to all provisions and controls of the Information Security policy sections.

10 COMPLIANCE

Overview

Compliance is a defining factor for information security and mandates or prohibits certain protections.

10.01 Compliance with Legal Requirements

10.01.01 Identification of Applicable Legislation

Every Information Technology Services department shall identify and document all relevant statutory, regulatory, and contractual requirements for each information system.

Every Information Technology Services department shall identify the specific controls and individual responsibilities to meet these requirements.

10.01.02 Intellectual Property Rights (IPR)

10.01.02.01 Copyright

The Information Security Council shall establish and implement standards to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, or trademarks.

All employees shall comply with legislative, regulatory and contractual requirements that place restrictions on the copying of proprietary material.

10.01.02.02 Software Copyright

All employees shall comply with software license agreements that limit the use of products to specific machines and/or limit the creation of copies to back-up copies only.

Every Information Technology Services department shall maintain an appropriate software asset inventory.

Every Information Technology Services department shall maintain proof and evidence of ownership of licenses (e.g., license certificate, master media, and manuals).

The Information Security Council shall ensure the user awareness program addresses software copyright issues.

Every Information Technology Services department shall implement controls to ensure that maximum number of users is not exceeded.

Every Information Technology Services department shall ensure that any business use of publicly available software (e.g., shareware, freeware, open source - including Linux) complies with the software terms of use.

10.01.03 Safeguarding of Organizational Records

Every Information Technology Services department shall implement controls to protect important records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements, as well as to support essential business activities. Examples of this are records that may be required as evidence that an organization operates within statutory or regulatory rules, or to ensure adequate defense against potential civil or criminal action. The time period and data content for information retention may be set by national law or regulation.

Every Information Technology Services department shall, in partnership with business owners, establish a records retention standard that shall categorize record types (e.g., accounting records, database records, transaction logs, audit logs, operational procedures), each with details of retention periods and type of storage media (e.g., paper, microfiche, magnetic, optical). Any related cryptographic keys associated with encrypted archives or digital signatures, shall be kept securely and made available to authorized persons when needed.

Consideration shall be given to the possibility of degradation of media used for storage of records. Storage and handling procedures shall be implemented in accordance with manufacturer's recommendations.

When electronic storage media is chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period shall be included to safeguard against loss due to future technology change.

Data storage systems shall be chosen such that required data can be retrieved in a manner acceptable to a court of law (i.e., all records required can be retrieved in an acceptable timeframe and in an acceptable format).

The system of storage and handling shall ensure clear identification of records and of their statutory or regulatory retention period. It shall also permit appropriate destruction of records after that period if they are not needed by the school.

10.01.04 Data Protection and Privacy of Personal Information

Every Information Technology Services department shall provide necessary controls to ensure they meet all statutory and regulatory requirements on the processing and transmission of personal data.

Such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data.

It is the responsibility of the owner of the data to consult with the legal department about any proposals to keep personal information in a structured file and to ensure awareness of the data protection principles defined in the relevant legislation.

10.01.05 Prevention of Misuse of Information Processing Facilities

The information processing facilities are provided for business purposes. Management shall authorize the use of these facilities. Any use of these facilities for non-business or unauthorized purposes, without management approval, shall be regarded as improper use of the facilities. If such activity is identified by monitoring or other means, it shall be brought to the attention of the individual manager concerned for appropriate disciplinary action, up to and including termination.

Every Information Technology Services department shall ensure that any monitoring of usage complies with any regulatory and statutory requirements in which they operate. Every Information Technology Services department shall consult with the legal department before implementing monitoring procedures.

Every user of an information processing facility shall be notified of the scope of their authorized access.

At log-on, a warning message may be presented on the computer screen indicating that the system being entered is private and that unauthorized access is not permitted. Where possible, the user shall acknowledge and react appropriately to the message on the screen to continue with the log-on process.

10.01.06 Regulation of Cryptographic Controls

Every Information Technology Services department shall ensure that they comply with any statutory or regulatory requirement associated with cryptographic controls.

Such requirements may include the following:

- Import and/or export of computer hardware and software for performing cryptographic functions

- Import and/or export of computer hardware and software which is designed to have cryptographic functions added to it
- Mandatory or discretionary methods of access to information encrypted by hardware or software to provide confidentiality of content

Legal advice shall be sought to ensure compliance with national law.

10.01.07 Collection of Evidence

10.01.07.01 Rules for Evidence

It is necessary to have adequate evidence to support an action against a person or organization. Whenever this action is an internal disciplinary matter, the evidence necessary shall be described by internal procedures.

Where the action involves the law, either civil or criminal, the evidence presented shall conform to the rules for evidence laid down in the relevant law or in the rules of the specific court in which the case shall be heard. In general, these rules cover:

- Admissibility of evidence: Whether or not the evidence can be used in court
- Weight of evidence: The quality and completeness of the evidence
- Adequate evidence that controls have operated correctly and consistently (e.g., process control evidence) throughout the period that the evidence to be recovered was stored and processed by the system

10.01.07.02 Admissibility of Evidence

To achieve admissibility of the evidence, Information Security shall ensure that their forensic processes comply with any published standard or code of practice for the production of admissible evidence.

10.01.07.03 Quality and Completeness of Evidence

To achieve quality and completeness of the evidence, a strong evidence trail is needed.

In general, such a strong trail can be established under the following conditions:

For paper documents: The original is kept securely and it is recorded who found it, where it was found, when it was found and who witnessed the discovery. Any investigation shall ensure that originals are not tampered with.

For digital media: Copies of any removable media, information on hard disks or in memory shall be taken to ensure availability. The log of all actions during the copying process shall be kept and the process shall be witnessed. One copy of the media and the log shall be kept securely. Only a trained computer forensics specialist shall perform these operations.

When an incident is first detected, it may not be obvious that it shall result in possible court action. Therefore, the danger exists that necessary evidence is destroyed accidentally before the seriousness of the incident is realized. For this reason, the Information Security Lead shall be notified immediately.

10.02 Reviews of Security Policy and Technical Compliance

10.02.01 Compliance with Security Policy

Managers shall ensure that all security procedures within their area of responsibility are carried out correctly. In addition, all areas within the organization shall be considered for regular review to ensure compliance with security policies and standards.

These shall include the following:

- Information systems
- Systems providers
- Owners of information and information assets
- Users
- Management

Owners of information systems shall assist in regular reviews of the compliance of their systems with the appropriate security policies, standards and any other security requirements.

10.02.02 Technical Compliance Checking

Information systems shall be regularly checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It shall be performed manually (supported by appropriate software tools, if necessary) by an experienced system engineer or by an automated software package which generates a technical report for subsequent interpretation by a technical specialist.

Compliance checking also covers, for example, penetration testing, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities. Caution shall be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

Any technical compliance check shall only be carried out by, or under the supervision of Information Security.

10.03 System Audit Considerations

10.03.01 System Audit Controls

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed, in order to minimize the risk of disruptions to business processes.

The following shall be observed:

- Audit requirements shall be agreed with appropriate management
- The scope of the checks shall be agreed and controlled
- The checks shall be limited to read-only access to software and data

- Access other than read-only shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed
- IT resources for performing the checks shall be explicitly identified and made available
- Requirements for special or additional processing shall be identified and agreed
- All access shall be monitored and logged to produce a reference trail
- All procedures, requirements, and responsibilities shall be documented

10.03.02 Protection of System Audit Tools

Access to system audit tools (e.g., software or data files) shall be protected to prevent any possible misuse or compromise. Such tools shall be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

Any individuals utilizing system audit tools without appropriate authorization may be subject to disciplinary action, up to and including termination.

11 ACCEPTABLE USE OF TECHNOLOGY

Overview

In order to define what users may or may not do in the process of utilizing Cincinnati State IT systems and resources, acceptable use policies are provided.

11.01 Scope

This policy addresses the use of Cincinnati State communications services and the communication of information among Cincinnati State employees (full & part-time), students, contractors, and vendors.

Cincinnati State reserves the right to modify this policy from time to time at its discretion.

11.02 Policy Statement

Cincinnati State provides communications services for the convenience and efficiency of employees and school-approved business partners for use in the course and scope of conducting business for or with the school. All messages and documents sent or received through these communications services and/or stored on Cincinnati State owned or controlled computers, servers, or other devices are subject to Cincinnati State integrity standards.

11.03 Definitions

“Employees” are individuals classified as full-time, part-time (including adjunct faculty), or temporary employees of Cincinnati State including student workers.

College refers to Cincinnati State and its subsidiaries, divisions and affiliates.

Business Partners are individuals or firms considered customers and suppliers of the College, including contractors and consultants.

Communication Services, for the purposes of this policy, are messages and documents sent or received via letter, memo, telephone, voice-mail, fax, audio/video tape, computer media, file/print servers, electronic mail, on-line computer services (internet, AOL, etc.), instant messaging, wireless message devices or any other means provided by the College or conducted over College resources.

11.04 Controls

11.04.01 Content

Communications Services are provided for the convenience and efficiency of users in the course and scope of performing their duties for the College. Although they sometimes may be intended to be confidential, all communications may become subject to discovery in a civil or criminal proceeding , or to disclosure in response to a valid request for documents under the Ohio Public Records Act. The contents of electronic communications (e-mail, fax, computer files, etc.) and voice mail messages may have the same status as paper records. The following types of messages are strictly prohibited:

- Messages with threatening, harassing, abusive, embarrassing, vulgar, sexual, racially offensive, defamatory, indecent content or implication, or anything else contrary to any Cincinnati State policy.

- Messages proposing any type of commercial transaction, including sales or trades (such as "want ads"), chain letters, betting pools, gambling, political announcements or solicitations, 'junk' e-mail or e-mail posted on a bulk basis to multiple recipients or other solicitations and distributions that are not related to Cincinnati State.
- Messages that violate any law, regulation or Cincinnati State policy, including, for example, copyright or employment laws.
- Messages that disclose any confidential or proprietary information of Cincinnati State to any employee, business partner, or other third party having no business-related need to know the information.
- Messages or communications disclosing sensitive Cincinnati State data (such as posting messages on internet "chat rooms") unless said message are authored by a designated Cincinnati State spokesperson.

Communications between employees must be carefully thought out. The ease of use and instantaneous nature of e-mail sometime lulls the user into making statements that he or she would never have made using written memos. Messages and material downloaded from the Internet and sent by e-mail can give rise to legal action against Cincinnati State and employees. Therefore, no one may put something into an e-mail message that they would not put down on paper, and voice mail may not be appropriate for certain confidential communications. When using e-mail for confidential communication, use caution and make sure that the person to whom you are sending the communication knows that you are sending a confidential message by, for example, putting the word “confidential” in the subject line..

11.04.02 College-wide Message Distribution

In the event an employee (other than system administrators) wishes to use Cincinnati State communications services for distribution of a Cincinnati State-wide message, said message must be approved in advance by the Human Resources Department and/or the Marketing & Communications Department of the highest level that represents the audience to which the information will be sent.

11.04.03 Guidelines for Protection of Confidential Communications

Employees must take appropriate steps to safeguard all sensitive or confidential information regardless of the method of communication. Depending on the circumstances and the nature of the confidential information, appropriate steps may include:

- **Fax**: ensuring that the actual recipient or recipient's designee is present at the receiving fax machine.
- **E-mail**: sending the message via a file attachment that is password-protected or with encryption enabled. Consult with Information Technology Services for further details and requirements on encryption and before you encrypt any data.
- **Voice mail**: avoiding communication via voice mail. Direct telephone contact with the recipient may be necessary. Using speakerphone in public areas, pay phones in high traffic areas such as airports, and analog mobile (vs. digital encrypted) telephone services are usually not appropriate when sensitive or confidential information is to be discussed.
- **Interoffice Mail**: having sensitive or confidential information hand delivered whenever possible. When this is not possible, notify the intended recipient via telephone to expect the mailing and send the information in a solid, sealed container (envelope, box, etc.) labeled “confidential”.

- **Public Mail**: sending with registration, return receipt requested, and/or other means to verify that the intended recipient actually received it. Notify the intended recipient via telephone to expect the mailing.
- **Print**: avoiding the use of printers located in open, generally available areas (e.g., departmental network based printers) when printing sensitive or confidential information unless the person printing the information is present at the printer to ensure privacy.
- **Internet Services**: sensitive or confidential information must not be disclosed via an internet or other online service bulletin board, chat room, usenet news bulletin, or any other messaging service.

Where e-mail messages do contain confidential information, they must be clearly marked “confidential.” They must also incorporate a warning in the event that they reach anyone other than the intended recipient, which must read as follows:

"This transmission is intended only for use by the intended recipient(s). If you are not an intended recipient you must not read, disclose, copy, circulate or in any other way use the information contained in this transmission. The information contained in this transmission may be confidential and/or privileged. If you have received this transmission in error, please notify the sender immediately and delete this transmission, including any attachments."

If you intend to rely on the contents of an e-mail at any future date, a separate hardcopy must be kept on file. The e-mail must not be stored electronically.

11.04.04 Personal Use of Communication Services

Occasional personal use of Cincinnati State communications services is allowed to Cincinnati State employees. The following rules apply to such usage:

- Personal use of Cincinnati State communications services must in no way impact the employee's ability to perform job functions at acceptable levels.
- Personal use of Cincinnati State communications services may in no way conflict with other policies, procedures or guidelines.
- Personal use of Cincinnati State communications services must be confined to the employee's own time (e.g., before/after business hours, during lunch, during breaks as defined by Human Resources policy). Personal use for commercial purposes not related to Cincinnati State business is prohibited.
- Under no circumstances are personal documents, messages, chat room conversations, usenet news bulletins, pictures, or other communications to be posted to an internet or other online service from a Cincinnati State e-mail address, user ID, or server.

11.04.05 Monitoring & Disclosure

It is critical that Cincinnati State be able, for its legitimate business purposes, to access and monitor all Cincinnati State communications services. Legitimate business purpose include (without limitation) such activities as: (a) legal or contractual obligations to produce any communication or audit any communication process; (b) retrieval of data from back-up or archive for system functioning; (c) network and system security; (d) safeguarding of Cincinnati State confidential information; (e) prevention of publicity adverse to Cincinnati State; (f) prevention of sexual harassment and workplace intimidation; (g)

enforcement of Cincinnati State policies (particularly those on authorized use of IT); and (h) management and control of costs and capacity of Cincinnati State IT systems.

Any automated monitoring that might be used by Cincinnati State would be applied to all communications in a particular communication channel and would not be directed at any specific employee. That said, the College may request, through Human Resources and/or Public Safety, monitoring a specific employee for a specific reason. Generally, it is not practical for Cincinnati State to have separate access control and monitoring systems for business and personal use. Accordingly, all users of Cincinnati State communications services must expect that the following can be accessed or monitored for legitimate business purposes.

- Messages sent or received via Cincinnati State-provided internal or external electronic communications services, including e-mail and voice mail
- Data or software stored on Cincinnati State-owned computers, servers, storage media or other devices
- Usage of the internet or Cincinnati State intranets

No facilities are provided or maintained for private or confidential e-mail, voice mail or computer files. Cincinnati State may:

- Authorize security personnel system administrators, and/or supervisors to review and/or monitor electronic or voice mail messages and/or data or software contained on Cincinnati State computers, servers, storage media or other devices on a periodic, random and/or ongoing basis to ensure compliance with this policy, for other purposes authorized by law or as part of an investigation
- Grant access for other staff, for necessary business purposes, to access data or software stored on Cincinnati State equipment

11.04.06 Violations

Any employee found to have violated Cincinnati State policy related to access or use of Cincinnati State communications services will be subject to disciplinary action up to and including termination.

In addition, subject to local, state or federal laws, employees could face criminal charges resulting in a fine or imprisonment.

11.05 Internet Usage

Cincinnati State provides access to public information networks for the convenience and efficiency of employees in the course and scope of conducting business for Cincinnati State. It is the responsibility of each user to closely adhere to the following with respect to his or her use of all public information networks (e.g., the Internet).

11.05.01 Introduction

Cincinnati State provides access to public information networks, such as the Internet, as an information and communications tool. While Cincinnati State recognizes that use of these public networks offers tremendous benefits, these public networks can create exposure to potentially damaging risks, including liability due to careless communication, exposure to computer hackers and viruses, and potential loss of productivity. When using the Internet in the context of their job, users shall be cognizant of the implication of their communications. They shall consider that their communications can create the same

impression as a memo printed on Cincinnati State letterhead. Hence, each user has a responsibility to ensure that when using the Internet on the job that any communications are in accordance with the nature and context of the user's job responsibilities.

11.05.02 Usage

When using Cincinnati State-provided communications services to access the Internet, the following usage rules shall be strictly observed. Any violation of the rules shall subject a user to disciplinary action, up to and including termination. These rules are:

- A user shall adhere to all policies governing written communications. Specifically, the user shall adhere to all IT Control Policies concerning communication services.
- A user may not disclose confidential or proprietary information of Cincinnati State.
- A user is not allowed to post information on any chat rooms, bulletin boards, and/or external discussion groups except for the purposes of technical/professional use or support. Any information that is posted shall conform to the policies of Cincinnati State.
- A user shall not purposely visit any Internet website that contains threatening, harassing, abusive, embarrassing, vulgar, sexual, racial, indecent content or implication, or anything else contrary to any Cincinnati State policy.
- A user shall utilize the public information networks primarily for purposes relating to Cincinnati State, and shall refrain from recreational or idle activity. Incidental and occasional personal use is permissible, but its use is subject to all of the College's policies.
- A user is prohibited from downloading any software which is not approved by their respective Information Services group.
- A user shall strictly observe all license restrictions for software that may be used on the Internet.
- A user may not violate any law or government regulation.
- A user may not send any message that is any way threatening, harassing, abusive, embarrassing, derogatory or vulgar in content or implication.

Finally, if users access the Internet from a Cincinnati State-provided computer, they shall use only authorized internet service providers or other Cincinnati State authorized internet gateways. Using software that has not been approved by Information Technology Services to access the Internet from a Cincinnati State computer is strictly prohibited.

11.05.03 Insider Information

It is the policy of Cincinnati State to comply with all relevant state and federal civil and criminal securities laws which, among other things, prohibit insider trading. An employee may be held liable for violating state and federal civil and criminal laws if they trade in securities while in possession of material, non-public information regarding the business of the College or disclose or tip material, non-public information to another person who subsequently uses that information to his or her profit. These laws are severe. It is imperative that each user of any public information network exercise extreme caution when disclosing information about the college. Dissemination of non-public information over the Internet is strictly prohibited by the college and is grounds for immediate dismissal.

REVISION HISTORY FOR THIS DOCUMENT

The following is a summary of the historical changes to this document.

Date	Changed made by	Change
5/21/2014	Frankie Baker	General formatting (bullets, punctuation, etc.)
5/21/2014	Frankie Baker	Updated section 07.08.02 Teleworking
5/21/2014	Frankie Baker	Updated section 08.04.02 Protection of System Test Data
5/21/2014	Frankie Baker	Updated section 08.05.04 Covert Channels and Trojan Code
5/21/2014	Frankie Baker	Updated section 11.01 Scope
5/21/2014	Frankie Baker	Updated section 11.03 Definitions
5/21/2014	Frankie Baker	Updated section 11.04.01 Content
8/24/2012	Frankie Baker	• Renamed the title of the document to include “governance”
8/21/2012	Frankie Baker	• Minor, non-substantive document edits to update the Acceptable Use of Technology Acceptance Process in Blackboard.
8/2/2012	Frankie Baker	• Added the REVISION HISTORY FOR THIS DOCUMENT section • Minor, non-substantive document edits
11/1/2011	Frankie Baker	Original document creation