



Information Security Manual

Prepared by the IIPS Security Standards Committee

IIPS Approval Date:

July 19, 2017

Enterprise Security and Risk Management Office

Pending

Publication Date: July 31, 2017

This page intentionally left blank

TABLE OF CONTENTS

INTRODUCTION.....	1
CHAPTER 1 – CLASSIFYING DATA AND LEGAL REQUIREMENTS.....	3
CHAPTER 2 – SECURING THE END USER	9
CHAPTER 3 – SECURING THE NETWORK	21
CHAPTER 4 – SECURING SYSTEMS.....	49
CHAPTER 5 – PHYSICAL SECURITY	103
CHAPTER 6 – CYBER SECURITY INCIDENT RESPONSE.....	109
CHAPTER 7 – BUSINESS CONTINUITY AND RISK MANAGEMENT	117

This page intentionally left blank

Introduction for Information Security Manual

The Information Security Manual is the foundation for information technology security in North Carolina Community Colleges. It is used to establish a set of standards for information technology security to maximize the functionality, security, and interoperability of the Colleges' distributed information technology assets.

The Manual is based on industry best practices and follows the International Organization for Standardization Standard 27002 (ISO 27002) for information technology security framework, and incorporates references to the National Institute of Standards and Technology (NIST) and other relevant standards. These security standards have been extensively reviewed by representatives of the North Carolina Community Colleges.

The Information Security Manual sets forth the basic information technology security requirements for the College. Standing alone, it provides each College with a basic information security manual. Some Colleges may need to supplement the manual with more detailed policies and standards that relate to their operations and any applicable statutory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), the Internal Revenue Code and the Payment Card Industry Data Security Standard (PCI DSS).

The term "State Network" is defined as the College's off campus Wide Area Network (WAN) connectivity.

Guidance for Colleges

While this Manual is based on the foundation of the State of North Carolina Information Security Manual simply adopting these standards will not provide a comprehensive security program. College management should emphasize the importance of information security throughout their institution with applicable College specific security policies, ongoing training and sufficient personnel, resources and support. When considering the specific controls that are to be used to comply with the security standards, Colleges should refer to the security practices related to information technology implementation as described in the NC Statewide Technical Architecture. The architecture is the means by which College's achieve compliance to the statewide information security standards. Colleges opting to deviate from these standards may be required to provide justification to explain any deviation.

These standards should be followed by College personnel and their computing devices used for administrative computing purposes. It is noted that individual Colleges are academic institutions and classroom instruction (especially in Information Technology curriculums) may be hindered if all standards in this manual are followed. Therefore, classroom computing devices used for instructional purposes (*i.e.*, instructional labs, classroom computers, classroom instructor workstations, presenter workstations) are exempt from certain standards and guidelines defined in this manual. These standards, as outlined in this manual, are to be subject to the individual College's instructional needs and requirements.

IMPLEMENTATION AND MANAGEMENT

Each college should designate a local Chief Information Officer (CIO) to enforce the standards and guidelines as defined in this manual. College administration should also consider periodic internal and external reviews of their information security program. The reviews may be staggered but should collectively include technical security controls, such as devices and networks, and non-technical security controls, which include policies, processes, and self-reviews. Independent information security reviews should also be considered when there are significant changes to the College information security posture because of a technology overhaul, significant change in business case or information protection needs.

ISO 27002 REFERENCES

- 6.1.1 Management commitment to information security
- 6.1.2 Information security coordination
- 6.1.3 Allocation of information security responsibilities
- 6.1.8 Independent review of information security

Chapter 1 – Classifying Data and Legal Requirements

Section 01 *Classifying and Storing Information*

010101 Classifying Information

Purpose: To properly classify the College's information.

STANDARD

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any agency of State government. The State's information shall be handled in a manner that protects the information from unauthorized or accidental disclosure, modification or loss.

1. All College information and data shall be classified as to its confidentiality, its value and its criticality.
2. Colleges shall establish procedures for evaluating information and data to ensure that they are classified appropriately. College custodians of data and their designees are responsible for agency data and shall establish procedures for appropriate data handling.
3. All college data shall be labeled to reflect its confidentiality, its value, and its criticality. All data must be clearly labeled so that all users are aware of the custodian, classification and value of the data.
4. Confidentiality is to be determined in accordance with N.C.G.S. Chapter 132 - Public Records Law - and all other applicable legal and regulatory requirements. Data, files, and software shall be clearly marked in such a way that identifies the process by which such information is to be made available or accessible.
5. All colleges shall maintain a comprehensive and up-to-date inventory of their information assets and periodically review the inventory to ensure that it is complete and accurate.
6. All colleges are required to protect and secure the information assets under their control. The basic information requirements include but are not limited to, the following:
 - Determine the vulnerability, risk level, and organizational value of information assets to the college and the business processes they support.
 - Provide the level of protection for information assets the College deems appropriate in accordance with applicable laws and standards based upon their vulnerability, risk level, and organizational value.
 - Comply with applicable federal and state laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all applicable standards, such as the Payment Card Industry Data Security Standard (PCI DSS), and the Department of Homeland Security (DHS) Protective Critical Infrastructure Information (PCII).

ISO 27002 REFERENCES

- 7.1.1 Inventory of assets
- 7.1.2 Ownership of assets
- 7.2 Information classification
 - 7.2.1 Classification guidelines
 - 7.2.2 Information labeling and handling

010102 Storing and Handling Information

Purpose: To protect the College's information through the establishment of proper controls.

STANDARD

The College's information, data and documents shall be handled in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss. All information, data and documents must be processed and stored in accordance with the classification levels assigned to those data in order to protect their integrity, availability, and confidentiality. The degree of protection required shall be commensurate with the nature of the information, the operating environment, and the potential exposures resulting from loss, misuse or unauthorized access to or modification of the data.

1. If information includes both confidential data and non-confidential data, the classification level shall default to confidential.
2. Electronic media brought into or removed from College-maintained premises shall be appropriately controlled.
3. Storage areas and facilities for media containing confidential data shall be secured. Filing cabinets used for the storage of confidential information shall have locking devices.
4. When confidential information is shipped, the agency shall determine the steps necessary to ensure the delivery is verified. If technically possible, confidential data shall be encrypted according to the minimum requirements for encrypting data in STANDARD 030501 - Using Encryption Techniques.
5. A college that obtains confidential information from another college shall observe and maintain all confidentiality conditions imposed by the providing agency. Special protection and handling shall be provided for information that is covered by statutes that address, for example, the confidentiality of financial records, taxpayer information, and personally identifiable information (PII).
6. The College CIO, along with data owners, shall manage and protect confidential information. Records including confidential information submitted to the State CIO or OITS shall be labeled. Such records that include information technology security features shall be labeled by affixing the following statement on each page of the document: "Confidential per N.C.G.S. §132-6.1(c)."
7. Confidential information shall be provided only to agencies and their designated representatives when necessary to perform their job functions.
8. Confidential information shall not be transmitted electronically over public¹ networks, such as FTP or electronic mail, unless encrypted while in transit. See STANDARD 030501 - Using Encryption Techniques for the minimum requirement for encrypting data.
9. All College data, confidential and non-confidential, shall be encrypted when stored on a laptop. Confidential data shall be encrypted when stored on other mobile computing devices and portable storage devices, including non-State owned devices authorized for use. See STANDARD 030501 - Using Encryption Techniques for the minimum requirement for encrypting data.
10. Federally protected confidential data shall not be stored on non-State owned/managed devices without proper approval.
11. Colleges shall ensure that legal and business risks associated with contractors' access are determined, assessed, and appropriate measures are taken such as through non-disclosure agreements, contracts, and indemnities.

GUIDELINES

1. An appropriate set of policies and procedures should be defined for information labeling and handling in accordance with the classification scheme adopted by the college. The procedures should cover information assets in both physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information-processing activity:
 - Copying
 - Storage
 - Transmission by post, fax, and electronic mail
 - Transmission by spoken word, including mobile phone, voice mail, and answering machines
2. Where appropriate, physical assets should be labeled. Some information assets, such as documents in electronic form, cannot be physically labeled and electronic means of labeling need to be used. In other cases, such as with tapes, a physical label is appropriate for the outside of the tape in addition to electronic labeling of documents contained on the tape.
3. Documents that contain confidential information should be restricted to authorized personnel using controls such as passwords to augment other technical and administrative controls. Any person who prints or photocopies confidential data should label and control the original and copied document in accordance with all applicable policies, statutes and regulations. Proper retention, archive and disposal procedures for such documents should be observed. College employees should consider using document headers and footers to notify readers of files classified as confidential.

ISO 27002 REFERENCES

- 7.2.2 Information labeling and handling
- 10.7.3 Information handling procedures
- 11.6.2 Sensitive system isolation
- 15.1 Compliance with legal requirements

Section 02 *Complying with Legal Obligations*

010201 Being Aware of Legal Obligations

Purpose: To ensure that employees are familiar with the laws that govern use of information technology systems and the data contained within those systems and that agencies comply with such laws.

STANDARD

Colleges are subject to Federal, State and local laws governing the use of information technology systems and the data contained in those systems.

1. Colleges shall comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems.
2. Colleges shall ensure that all employees and contractors are aware of legal and regulatory requirements that address the use of information technology systems and the data that reside on those systems.
3. Colleges shall ensure that each public employee and other State Network user is provided with a summary of the legal and regulatory requirements.

Examples of laws that affect computer and telecommunications use in North Carolina are as follows:

- **Federal**
 - 18 U.S.C. §1030. Fraud and related activity in connection with computers.

- 18 U.S.C. §2701 et seq. Stored Communications Act.
- 17 U.S.C. §§ 500 and 506. Copyright infringements and remedies.
- **North Carolina**
 - N.C.G.S. §114-15.1. Department heads to report possible misuse of state property to the SBI.
 - N.C.G.S. §14-196. Using profane, indecent or threatening language to any person over the telephone; annoying or harassing by repeated telephoning or making false statements over telephone. The statute includes the sending by computer modem of any false language concerning death, injury, illness, disfigurement, indecent conduct or criminal conduct of the person receiving the information or any close family member.
 - N.C.G.S. §14-454. Accessing computers.
 - N.C.G.S. §14-455. Damaging computers, computer systems, computer networks, and resources.
 - N.C.G.S. §14-458. Computer trespass; penalty.
 - N.C.G.S. §14-155. Unauthorized connections with telephone or telegraph.

Examples of laws that affect data residing on State information technology systems are as follows:

- **Federal**
 - 26 U.S.C. §§6103, 7213, 7213A, 7431, Internal Revenue Code.
 - Public Law 104-191, 104th Congress, Health Insurance Portability and Accountability Act of 1996.
 - 5 U.S.C. §552a, as amended. Privacy Act of 1974.
- **North Carolina**
 - N.C.G.S. Chapter 132. Public records law.
 - N.C.G.S. §105-259. Secrecy required of officials (tax information).
 - N.C.G.S. §122C-52. Client rights to confidentiality (disability clients).

Laws that relate to confidential records held by North Carolina government are summarized in the following document:

http://www.records.ncdcr.gov/guides/confidential_publicrec_2009.pdf

ISO 27002 REFERENCES

- 8.1.3 Terms and conditions of employment
- 15.1.1 Identification of applicable legislation
- 15.1.4 Data protection and privacy of personal information

010202 Complying with General Copyright Laws

Purpose: To ensure that Colleges comply with laws that address copyright protection.

STANDARD

1. Colleges shall provide employees, contractors and other third parties with guidelines for obeying software licensing agreements and shall not permit the installation of unauthorized copies of software on technology devices that connect to the State Network. The guidelines shall inform employees, contractors and other third parties of the following:
 - Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.
 - Employees, contractors and other third parties shall obey licensing agreements and shall not

- install unauthorized copies of software on State agency technology devices.
 - Employees, contractors and other third parties who make, acquire or use unauthorized copies of software shall be disciplined as appropriate. Such discipline may include termination.
2. Colleges shall inform their users of any proprietary rights in databases or similar compilations and the appropriate use of such data.
 3. Colleges shall inform users of any sanctions that may arise from inappropriate use of databases or similar compilations.
 4. Colleges shall define policies and procedures to comply with legal and regulatory requirements in regards to the protection of intellectual property.
 5. Each College shall establish procedures for software use, distribution and removal within the college to ensure that college use of software meets all copyright and licensing requirements. The procedures shall include the development of internal controls to monitor the number of licenses available and the number of copies in use.

ISO 27002 REFERENCES

- 15.1.1 Identification of applicable legislation
- 15.1.2 Intellectual property rights (IPR)

010203 Legal Safeguards against Computer Misuse

Purpose: To disclose to users of State information systems the legal policy requirements for using State information technology resources as well as any methods an agency may use to monitor usage.

STANDARD

1. Colleges shall provide users of information technology services with the legal policy requirements that apply to use of State information technology systems and, where practical and appropriate, agencies shall provide notice to users of State information technology systems that they are using government computer systems.
2. If a college monitors computer users, it shall provide notice to computer users that their activities on State information technology systems may be monitored and disclosed to third parties. The notice may take many forms, such as a privacy statement on an Internet Web page or a monitoring notice affixed to a computer monitor.
3. Where practical and appropriate, sign-on warning banners shall be posted on State information technology systems to appear just before or just after login on all systems that are connected to the State Network. This gives notice to users that they are accessing State resources and that their actions while using these resources are being monitored and are subject to disclosure to third parties, including law enforcement personnel.

Examples of warning banners:

- **WARNING:** This is a government computer system, which may be accessed and used only for authorized business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil and/or administrative action.
- All information on this computer system may be intercepted, recorded, read, copied and disclosed by and to authorized personnel for official purposes, including criminal investigations. Such information includes data encrypted to comply with confidentiality and privacy requirements. Access or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system.
- **NOTICE:** This system is the property of the State of North Carolina and is for authorized

use only. Unauthorized access is a violation of federal and State law. All software, data transactions and electronic communications are subject to monitoring.

- This is a government system restricted to authorized use and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use or modification being used for criminal prosecution and civil litigation.
- *Notice to Users:* This is a government computer system and is the property of the State of North Carolina. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.
- Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected and disclosed to law enforcement personnel, as well as to authorized officials of other agencies. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of the agency.
- Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

ISO 27002 REFERENCES

15.1.5 Prevention of misuse of information processing facilities

Chapter 2 – Securing the End User

Section 01 Controlling Access to Information and Systems

020101 Managing Access Control Standards

Purpose: To establish requirements for controlling access to College information assets.

STANDARD

Access to College information technology assets shall be controlled and managed to ensure that only authorized devices/persons have appropriate access in accordance with the college's business needs.

1. All computers that are permanently or intermittently connected to the College's network shall have an approved credentials-based access control system. Access shall be controlled by the following:
 - User profiles that define roles and access.
 - Documented review of standard users' rights.
 - Documented review of administrator user accounts every 3 months.
 - Revocation upon termination of employment.
2. Regardless of the network connections, all systems handling the College's confidential data shall employ approved authentication credentials-based access control systems and encryption for data in transit. For the College's encryption standard, see 030501 – Using Encryption Techniques.
3. Only authorized users shall be granted access to the College's information systems, and the principle of least privilege shall be used and enforced.
4. Assignment of privileges shall be based on an individual's job classification, job function, and the person's authority to access information. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.
5. User rights shall be reviewed and approved by data owners at six (6)-month intervals.
6. Default access for systems containing confidential information shall be deny-all.

ISO 27002 REFERENCES

- 11.1.1 Access control policy
- 11.2.4 Review of user access rights
- 11.5.6 Limitation of connection time

020102 Managing User Access

Purpose: To prevent unauthorized access to College networks.

STANDARD

1. Colleges shall establish policies and procedures for managing access rights for use of their networks throughout the life cycle of the user's credentials, such as user IDs, ID cards, tokens, or biometrics.
2. There shall be a documented approval process whereby authorized parties create user accounts and specify required privileges for user access to systems and data.
3. Colleges shall communicate user account policies and procedures including authentication procedures and requirements to all users of an information system.

4. Colleges shall identify a backup system administrator to assist with user account management when the primary system administrator is unavailable.
5. Users shall be responsible for maintaining the security of their user authentication credentials.
6. User credentials shall be individually assigned and unique in order to maintain accountability.
7. User credentials shall not be shared but only used by the individual assigned to the account, who is responsible for every action initiated by the account linked to that credential.
8. Where supported, the system shall display (after successful login) the date and time of last use of the individual's account so that unauthorized use may be detected.
9. Default/generic credentials shall be disabled or changed prior to a system being put into production.
10. User credentials shall be disabled immediately upon the account owner's termination from work for the College or when the account owner no longer needs access to the system or application.
11. Access rights of users in the form of read, write and execute shall be controlled appropriately and the outputs of those rights shall be seen only by authorized individuals.
12. The default access method for files and documents is role-based access control (RBAC), however, other methods to securely access files and documents may be used.
13. Access to confidential information shall be restricted to authorized individuals who require access to the information as part of their job responsibilities.
14. Colleges may change, restrict or eliminate user access privileges at any time.
15. Colleges shall modify an individual's access to a College information technology asset upon a change of employment or change in authorization, such as termination, a leave of absence or temporary reassignment.
16. Where possible, an information system shall limit unsuccessful logon attempts to three (3) before the user's account is disabled. The locked out duration shall be at least thirty (30) minutes, unless the end user successfully unlocks the account through a challenge question scenario or an administrator re-enables the user's account.
17. User credentials that are inactive for a maximum of ninety (90) days must be disabled, except as specifically exempted by the security administrator.
18. All accounts that have been disabled for greater than 365 days shall be deleted.
19. Only authorized system or security administrators or an authorized service desk staff shall be allowed to enable or re-enable a user credential except in situations where a user can do so automatically through challenge/response questions or other user self-service mechanisms.
20. All user credential creation, deletion and change activity performed by system administrators and others with privileged access shall be securely logged and reviewed on a regular basis.
21. For those systems and applications that enforce a maximum number of concurrent connections for an individual user credential, the number of concurrent connections must be set to two (2).
22. User credentials established for a non-employee/contractor must have a specified expiration date unless a user credential without a specified expiration date is approved in writing by the College security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.
23. Access control may need to be modified in response to the confidentiality, integrity or availability of information stored on the system, if existing access controls pose a risk to that information.
24. In order to facilitate intrusion detection, information shall be retained on all logon attempts until the College determines the information is no longer valuable, or as required by law or the standards of this Security Manual.

ISO 27002 REFERENCES

- 11.2 User access management
- 11.2.4 Review of user access rights
- 11.6.1 Information access restriction
- 11.1.1 Access control policy

020103 Securing Unattended Work Stations

Purpose: To prevent unauthorized system access.

STANDARD

Machines that access a College system shall be safeguarded from unauthorized access — especially when left unattended. Colleges shall inform personnel of the risks involved in leaving confidential work on their computer screens while away from their desks.

1. Each college shall be responsible for configuring all workstations to require a password-protected screen saver after a maximum of thirty (30) minutes of inactivity.
2. Users shall not disable the password-protected configuration established by their college.
3. Users shall lock their workstations when leaving them unattended.
4. When not in use for an extended period of time, as defined by the college, users shall log off from their workstation(s).
5. Personnel shall load only software, including screen savers, which have been approved by their college. Colleges shall train their employees on the risks of acquiring malware such as viruses, spyware and Trojan horses by downloading and installing unauthorized software.
6. Personnel shall transmit confidential data to printers residing in common areas only when there is a person authorized to receive the information present to protect the confidentiality of the printed material. Personnel shall clear all printers and fax machines of confidential printouts.

GUIDELINES

Colleges should consider requiring all personnel to shutdown/power off computers when they are not in use for an extended period of time, as defined by the college.

ISO 27002 REFERENCES

- 10.7 Media handling
- 11.2 User management
- 11.3.2 Unattended user equipment
- 11.3.3 Clear desk and clear screen policy

020104 Managing Network Access Controls

Purpose: To establish requirements for the access and use of the College Network.

STANDARD

Access to networks operated by College Network, shall be controlled to prevent unauthorized access and to prevent malicious attacks on the networks. Access to all college computing and information systems shall be restricted unless explicitly authorized.

1. When end users on the college networks access resources, they shall comply with all college acceptable use policies.
2. Users shall not extend or retransmit network services without appropriate management approval.

3. Users shall not install network hardware or software that provides network services, such as routers, switches, hubs and wireless access points, without appropriate management approval.
4. Non-College computer systems that require connectivity to the College Network shall conform to college information security standards.
5. Users shall not download, install or run security programs or utilities, such as password-cracking programs, packet sniffers, network-mapping tools or port scanners, that:
 - a) Reveal weaknesses in the College Network without prior written approval from the College CIO; or
 - b) Reveal weaknesses of the college network without appropriate management approval.
6. Users shall not be permitted to alter network hardware in any way.

ISO 27002 REFERENCES

11.4 Network access control

020105 Controlling Access to Operating System Software

Purpose: To limit access to operating system administrative software to those individuals authorized to perform system administration/management functions.

STANDARD

Only those individuals designated as system administrators shall have access to operating system administrative commands and programs.

1. Internal network configuration and other system design information shall be limited to only those individuals who require access in the performance of tasks or services essential to the fulfillment of a work assignment, contract or program.
2. College staff shall maintain a list of administrative contacts for their systems.
3. All authorized users of administrative-access accounts shall receive appropriate training on the use of those accounts.
4. Each individual who uses an administrative-access account shall use the account only for administrative duties. For other work being performed, the individual shall use a regular user account.
5. When special-access accounts are needed for internal or external audit, software development, software installation, or other defined need, they shall be:
 - a) Authorized in advance by college management;
 - b) Have a specific expiration date; and
 - c) Be removed when the work is completed.
6. Administrative-access accounts must connect in a secure manner at all times, and their activity must be logged.

ISO 27002 REFERENCES

11.5 Operating System Access Control

020106 Managing Passwords

Purpose: To prevent unauthorized access and to establish user accountability when using IDs and passwords to access College information systems.

STANDARD

The combination of a unique user credential and a valid password shall be the minimum requirement for granting access to an information system when IDs and passwords are used as the method of performing identification and authentication. If passwords are used, colleges shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access a College resource.

Password Management Standards

1. Where technically feasible, passwords shall be at least eight (8) characters long for access to all systems and applications.
2. Passwords shall be composed of a variety of letters, numbers and symbols² with no spaces in between.
3. Passwords shall be random characters from the required categories of letters, numbers and symbols.
4. Passwords shall not contain dictionary words or abbreviations.
5. Passwords shall not contain number or character substitutes to create dictionary words (e.g., *d33psl33p* for *deep sleep*³).
6. Passwords for internal College resources shall be different from passwords for external, non-College resources.
7. College approved password generators that create random passwords shall be allowed.
8. Application or system features that allow users to maintain password lists and/or automate password inputs shall be prohibited, except for simplified/single sign-on systems approved by the College CIO.
9. Passwords shall not be revealed to anyone, including supervisors, help desk personnel, security administrators, family members or co-workers.
10. Users shall enter passwords manually for each application or system, except for simplified/single sign-on systems that have been approved by the College CIO.
11. Passwords shall not be stored in clear text on hard drives, diskettes, or other electronic media. If stored, passwords shall be stored in encrypted format.
12. Passwords shall not be displayed in clear text during the logon process or other processes.
13. All typical user passwords (e.g., UNIX, Windows, personal computing, RACF, applications, etc.) shall be changed at least every ninety (90) days. This includes Government employee and contractor passwords (e.g., email, Web and calendar) used to access systems and applications. Passwords shall not be reused until six additional passwords have been created.
14. Passwords for citizens and business users do not need to be changed; use of strong passwords and periodic password changes, however, are recommended.
15. Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption. Attempts to gain access to a user's password through these social engineering means must be reported to the college security administrator.

² For Resource Access Control Facility (RACF), valid symbols are @, \$, #, and _, and the first character of a password must be a letter and the password must contain a number.

³ Other examples of numbers/symbols for letters are 0 for o, \$ for S, 1 for i, and l for l, as in *capta1n k1rk* or *mr5pock*.

16. Where technically possible, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less, or as required by law, regulation, or industry standard.
17. Passwords shall be changed whenever there is a chance the password or system is compromised.
18. There shall be a college approved process for validating the identity of an end user who requests a password reset. Initial passwords and subsequent password resets shall utilize a unique password for each user account.

Password Management Standards—System Administration

1. Passwords for administrative accounts, including any user accounts with more privileges than those of a typical user, shall be changed at least every thirty (30) days whenever possible but must not exceed every sixty (60) days.
2. Credentials with administrative privileges, more privileges than a typical user account, or programs with elevated access shall have a different password from all other accounts held by that user.
3. Password files shall be retrievable only by the system administrator or other designated personnel.
4. The password for a shared administrative-access account shall change when any individual who knows the password leaves the college that owns the account or when job responsibilities change.
5. All systems should have more than one administrator. In situations where a system has only one administrator, colleges shall establish a password escrow procedure so that, in the absence of the administrator, someone can gain access to the administrator account.

Password Management Standards—Service Accounts

1. As used in this standard, a service account is an account created by system administrators for automated use by an application, operating system or network device for their business purpose.
2. Service accounts must be dedicated solely to their business purpose.
3. Service accounts shall be separate from any other accounts.
4. College approved controls must be in place to prevent misuse of a service account.
5. All service accounts must have appropriate logging as specified by the college of account activity. The application/device owner must audit the service account usage at least every 30 days.
6. All service account passwords must meet system administrator password complexity standards.
7. Whenever possible, service account passwords must have change intervals appropriate to the level of risk posed by a potential compromise of the system. At a minimum, change intervals shall not exceed 180 days (6 months).
8. In the special case where an application or other control software is specifically designed for service accounts to use 'non-expiring' passwords to complete their business purpose, these accounts must be preapproved by college management and the college's security liaison. College approved controls, policies, and procedures must be in place to closely

monitor and mitigate the risk of non-expiring passwords.

9. A service account password must be changed immediately after any potential compromise or any individual who knows the password leaves the college or changes roles within the college.

ISO 27002 REFERENCES

- 11.2.3 User password management
- 11.3.1 Password use
- 11.5.1 Secure log-on procedures
- 11.5.2 User identification and authentication
- 11.5.3 Password management system

020107 Monitoring System Access and Use

Purpose: To establish requirements and guidelines for monitoring user activity.

STANDARD

Colleges shall have the right and ability to monitor use of information systems by employee and third-party contractor users. Colleges that monitor the use of their systems shall do the following:

1. Examine the relevant information technology processes and determine all instances in which individually identifiable information is collected when an employee or third-party contractor uses college information resources.
2. Establish policies that provide adequate notice to all system users of the scope and manner of monitoring for any information system and never exceed the scope of any written monitoring statement in the absence of any clearly stated exception. The policies shall also state that users shall have no expectation of privacy unless expressly granted by a college.
3. Obtain a written receipt from College employees and third-party contractors acknowledging that they have received, read and understood the college's monitoring policies. End users on the College network should have no expectation of privacy.
4. Inform College employees and third-party contractors of any activities that are prohibited when using the college's information systems.

ISO 27002 REFERENCES

10.10.2 Monitoring system use

020108 Controlling Remote User Access

Purpose: To require users of College information technology systems who access college information technology systems remotely to do so in a secure manner.

STANDARD

Where there is a business need and prior college management approval, authorized users of college computer systems, the College Network and data repositories shall be permitted to remotely connect to those systems, networks and data repositories to conduct College-related business through secure, authenticated and carefully managed college approved access methods.

1. Access to the College network via external connections from local or remote locations including homes, hotel rooms, wireless devices and off-site offices shall not be automatically granted with network or system access. Systems shall be available for on- or off-site remote access only after an explicit request is made by the user and approved by the manager for the system in question.
2. Access shall be permitted through a college-managed secure tunnel such as a Virtual Private Network (VPN) or Internet Protocol Security (IPSec) that provides encryption and secure authentication. Virtual private networks (VPNs) shall require user authentication and encryption strength compliant with the College-wide encryption standard, 030501 – Using Encryption Techniques.

Authentication

1. Access shall require authentication and authorization to access needed resources, and access rights shall be regularly reviewed. The authentication and authorization system for remote access shall be managed by the college. Colleges that need centralized network - infrastructure services shall use the College-wide authentication and authorization service

known as NCID.

2. Each user who remotely accesses an internal network or system shall be uniquely identifiable. Account passwords shall not traverse the network in clear text and must meet minimum requirements of the College-wide password management standards.
3. All users wishing to establish a remote connection via the Internet to the college's internal network must first authenticate themselves at a firewall or security device.

Users

1. **User Credentials:** All users who require remote access privileges shall be responsible for the activity performed with their user credentials. User credentials shall never be shared with those not authorized to use the credential. User credentials shall not be utilized by anyone but the individuals to whom they have been issued. Similarly, users shall be forbidden to perform any activity with user credentials belonging to others.
2. **Revocation/Modification:** Remote access shall be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections. Remote access privileges shall be terminated upon an employee's or contractor's termination from service. Remote access privileges shall be reviewed upon an employee's or contractor's change of assignments and in conjunction with other regularly scheduled user account reviews.
3. **Anonymous Interaction:** With the exception of Web servers or other systems where regular users are anonymous, users are prohibited from remotely logging into any College computer system or network anonymously (for example, using "guest" accounts). If users employ system facilities that allow them to change the active user ID to gain certain privileges, such as the switch user (su) command in Unix/Linux, they must have initially logged in with a user ID that clearly indicates their identity.

Configuration

1. **Default to Denial:** If a college computer or network access control system is not functioning properly, it shall default to denial of access privileges to users. If access control systems are malfunctioning, the systems they support must remain unavailable until such time as the problem has been rectified.
2. **Privilege Access Controls:** All computers permanently or intermittently connected to external networks must operate with privilege access controls approved by the college. Multi-user systems must employ user credentials unique to each user, as well as user privilege restriction mechanisms, including directory and file access permissions.
3. **Antivirus and Firewall Protection:** External computers or networks making remote connection to internal computers or networks shall utilize a college-approved active virus scanning and repair program and an agency-approved personal firewall system (hardware or software). The college shall ensure that updates to virus scanning software and firewall systems are available to users. External computers or networks making a remote connection to a public Web server are exempted.
4. **Time-out:** Network-connected single-user systems, such as laptops and PCs, shall employ college-approved hardware or software mechanisms that control system booting and that include a time-out after-no-activity (for example, a screen saver).
 - To the extent possible, all systems accepting remote connections from public-network-connected users, such as users connected through dial-up phone modems, dial-up Internet service providers, DSL or cable modems, shall include a time-out system.
 - This time-out system must terminate all sessions that have had no activity for a period of thirty (30) minutes or less. For some higher risk information systems, the requirement for a session idle timeout may be more stringent as determined by college policy, industry standard (e.g., PCI DSS) or other regulations.

- An absolute time-out shall occur after twenty-four (24) hours of continuous connection and shall require reconnection and authentication to re-enter the College Network. In addition, all user credentials registered to networks or computers with external access facilities shall be automatically suspended after a period of ninety (90) days of inactivity.
 - Colleges shall conduct a risk assessment and determine the appropriate system time-out period for hand-held devices, (e.g., smart phones, tablets, etc.), that connect to the College Network. The risk assessment shall balance the business needs for immediate access to the hand held device against the security risks associated with the loss of the device. Colleges shall also comply with any legal and regulatory requirements associated with the information that may be contained on the device, such as requirements for confidentiality, security and record retention.
5. Failure to authenticate: To the extent possible, all systems accepting remote connections from public-network-connected users shall temporarily terminate the connection or time out the user credential following three (3) unsuccessful attempts to log in. For example, if an incorrect password is provided three (3) consecutive times, remote access systems shall drop the connection.
 6. Modems: Dial-up modems shall be disabled by removing the modem device or uninstalling the modem device driver and disabling the modem within the operating system, unless College management has approved their use and the communications software used with them. If used, dial-up modems shall not be left in auto-answer mode.
 7. For client-to-server/gateway VPN solutions with split tunneling options, the college must evaluate the associated risks and implement mitigating controls before enabling the split tunneling option to permit network bridging. Colleges that decide to use split tunneling must take responsibility for the security of their endpoints, implementing appropriate mechanisms (such as access controls, firewalls, antivirus, etc.) to enforce standards that will reduce risk such as data loss and malware due to bridging the networks to which they are connected when the VPN is active.

Access to Single-Host Systems

1. Remote access to single-equipment hosts (e.g., college servers, Web-hosting equipment) shall be permitted provided the equipment requires authenticated access, is appropriately protected by a VPN, and prevents onward connection to the College network.
2. Management consoles and other special needs: Users requiring telecommunications access, such as dial-up modem access, for “out of band” management or special needs must obtain college management approval as set forth in college policy and procedures. Any dial-up server that grants network access must authenticate each user, minimally, by a unique identification with password and shall encrypt the data stream. All calls must be logged, and logs of access shall be retained for ninety (90) days. At the completion of each dial-up session to a server, the accessing workstation shall be secured via password.

Miscellaneous

1. Administrators shall take all precautions necessary to ensure that administrative activities performed remotely cannot be intercepted or spoofed by others, such as configuring timestamps, using encryption, and/or dial-back mechanisms.
2. Disclosure of systems information: The internal addresses, configurations, dial-up modem numbers, and related system design information for college computers and networks shall be kept confidential and shall not be disclosed to the public. Likewise, the security measures employed to protect college computers and networks shall be kept confidential and shall be similarly protected.
3. Systems shall log all remote access occurrences, including both policy user and administrator activity (user credential, date/time, and duration of connection at a minimum).

4. Access to diagnostic and configuration ports (especially dial-up diagnostic ports) shall be securely controlled and enabled only when needed for authorized diagnostic access.

ISO 27002 REFERENCES

11.4.2 User authentication for external connections

020109 Contracting with External Suppliers/Other Service Providers

Purpose: To address information security issues involving third parties who provide services to the College.

STANDARD

Each college shall ensure that third parties who provide information technology services agree to follow the college's information technology security policies when providing services to the college.

1. Third parties are non-College employees, such as vendors, suppliers, individuals, interns, contractors and consultants, responsible for providing goods or services to the College. In order to perform the requested services, a third party might need to use college information technology assets and access college information determined to be valuable to operations and/or classified as non-public or restricted by law.
2. Access must be granted to third-party users only when required for performing work and with the full knowledge and prior approval of the information asset owner.
3. Third parties shall be fully accountable to the College for any actions taken while completing their college assignments.
4. College staff overseeing the work of third parties shall be responsible for communicating and enforcing applicable laws, as well as College security policies, and procedures.
5. College operational and/or restricted information must not be released to third parties without properly executed contracts and confidentiality agreements. These contracts must specify conditions of use and security requirements and the access, roles and responsibilities of the third party before access is granted.

ISO 27002 REFERENCES

6.1.3 Allocation of Information Security responsibilities
6.1.5 Confidentiality agreements

Section 02 Personnel Information Security Responsibilities

020201 Accessing College Resources in an Acceptable Way

Purpose: To establish a standard pertaining to the acceptable use of the College Network and the global Internet by College employees and other College Network users.

STANDARD

1. Colleges shall develop Acceptable Use Policies (AUPs) for staff, customers and third parties to follow.
2. AUPs shall define the proper use of information assets and shall include critical technologies such as remote access technologies, removable electronic media, laptops, tablets, smartphones, email usage and Internet usage.
3. While performing work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, College employees and other College Network users shall be expected to use the College Network and the Internet responsibly and

professionally and shall make no intentional use of these services in an illegal, malicious or obscene manner.

4. Colleges shall determine the extent of personal use its employees and other College Network users, under its control, may make of the College Network and the Internet.
5. Colleges shall prohibit users from the download and installation of unapproved software as defined by each college's IT policies.
6. It shall be the responsibility of public employees and College Network users to help prevent the introduction or propagation of computer viruses.
 - o All files downloaded from a source external to the College Network, including all data received on a diskette, compact disc (CD), USB flash drive, or any other electronic medium, shall be scanned for malicious software such as viruses, Trojan horses, worms or other destructive code. This includes files obtained as email attachments and through any other file transfer mechanism.
 - o All files downloaded from a source external to the College Network shall come from a known, trusted source.
7. All colleges shall ensure that they have currently supported and patched software on their networks in order to mitigate vulnerabilities and reduce the risk of malicious activity.
8. College employees and other College Network users shall not access or attempt to gain access to any computer account which they are not authorized to access. They shall not access or attempt to access any portions of the College Network to which they are not authorized to have access.
9. Public employees and other College Network users shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to access.
10. College employees and other College Network users shall not use College computers and networks for the circumvention of copyright protections or the illegal sharing of copyrighted material. Users who receive email that they consider to be unacceptable according to this standard can forward the original email message (including all headers) to the appropriate email *abuse@<host domain name>* account.

GUIDELINES

1. Colleges may want to address other acceptable use issues in their own internal policies on subjects such as use of instant messaging, social networking, and personal use of College computers, servers, and Local Area Network (LAN).
2. Additionally, colleges should develop internal policies concerning the storage of personal files such as music, images and other files unrelated to the employees' assigned duties.

ISO 27002 REFERENCES

- 7.1.3 Acceptable use of assets
- 8.2.3 Disciplinary process
- 10.4.1 Controls against malicious code
- 15.1.5 Prevention of misuse of information processing facilities

Section 03 Training and Awareness

020301 Delivering Awareness Programs to Staff

Purpose: To provide awareness programs that ensure employees are familiar with information technology security policies, standards and procedures.

STANDARD

The senior management of each college shall lead by example by ensuring that information security is given a high priority. College senior management shall ensure that information security communications are given priority by staff and shall support information security awareness programs. All colleges shall provide new employees and contractors with mandatory information security training as part of job orientation. The college shall provide regular and relevant information security awareness communications to all staff by various means, which may include:

- Electronic updates, briefings, pamphlets and newsletters.
- Self-based information security awareness training to enhance awareness and educate staff on information technology security threats and the appropriate safeguards.
- An employee handbook or summary of information security policies, which shall be formally delivered to and acknowledged by employees before they access college resources.

Colleges shall provide information relevant to effective information security practices to staff members in a timely manner. On a periodic basis, college management shall receive input from information security staff on the effectiveness of information security measures and recommended improvements.

All levels of management must ensure employees, contractors, and vendors adhere to approved information security procedures by ensuring staff are informed about their security responsibilities and attain continued education relevant to information security and their position in the organization.

ISO 27002 REFERENCES

- 5.1.2 Review of the information security policy
- 8.2.1 Management duties
- 8.2.2 Information security awareness, education and training

020302 Third Party Contractor: Awareness Programs

Purpose: To ensure contractors are familiar with information security policies, standards and procedures.

STANDARD

All contractors shall have provisions in their contracts with the College that set forth the requirement that they must comply with all college information security policies. The college shall provide contractors with regular and relevant information security policies. The college shall provide regular and relevant information security awareness communications to contractors by various means, which include the following:

- A handbook or summary of information security policies, which shall be formally delivered to and signed by contractors before beginning work.
- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on a regular basis and whenever their work responsibilities change.
- Training in information security threats and safeguards, with the extent of technical details to reflect the contractor's individual responsibility for configuring and maintaining information security.

ISO 27002 REFERENCES

- 6.2.3 Addressing security in third party agreements
- 8.2.2 Information security awareness, education and training

020303 User: Information Security Training

Purpose: To ensure that all users receive adequate training.

STANDARD

All colleges shall provide training to users on relevant information security threats and safeguards. The extent of technical training shall reflect the person's individual responsibility for configuration and/or maintaining information security systems. When staff members change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority. College training shall include the following:

- Mandatory information security awareness training to new staff as part of job orientation.
- Formal information security training appropriate for work responsibilities, on an annual basis.
- Training in information security threats and safeguards, with the technical details to reflect the staff's individual responsibility for configuring and maintaining information security.

Colleges shall provide training to technical staff in critical areas of information security, including vendor-specific recommended safeguards to improve the following:

- Server and PC security management.
- Packet-filtering techniques implemented on routers, firewalls, etc.
- Intrusion detection and prevention.
- Software configuration, change and patch management.
- Virus prevention/protection procedures.
- Business continuity practices and procedures.

All users of new systems shall receive training to ensure that their use of the systems is effective and does not compromise information security. Colleges shall train users on how new systems will integrate into their current responsibilities. Colleges shall notify staff of all existing and any new policies that apply to new systems.

When staff members who are responsible for information technology systems change jobs, their information security needs must be reassessed, and any new training on procedures or proper use of information-processing facilities shall be provided as a priority.

ISO 27002 REFERENCES

8.2.2 Information security awareness, education and training

Chapter 3 – Securing the Network

Section 01 Networks

030101 Configuring Networks and Configuring Domain Name Servers (DNS)

Purpose: To establish a framework for the configuration of networks and domain name servers.

STANDARD

College network infrastructures shall be designed and configured using controls to safeguard the College's information systems. Failure to protect network infrastructures against threats can result in the loss of data integrity, data unavailability and/or unauthorized data use. Secure configuration of the network infrastructure shall include the following:

1. All hardware connected to the College's network shall be configured to support College/agency management and monitoring standards.
2. The cabled network infrastructure must comply with industry standards and be installed by a licensed bonded contractor or employee of the College.
3. Perimeter defense systems, including routers and firewalls, and network-connected equipment, including switches, wireless access points, personal computers and servers, shall be configured to secure specifications.
4. Critical hardware and systems, including the network infrastructure, shall be connected to an uninterruptible power supply (UPS) that is regularly tested and maintained.
5. Network devices shall be configured to support authentication, authorization and accountability mechanisms when being administered.
6. Configuration management, patch management and change management standards and procedures shall be applied to all network attached systems.
7. Extending, modifying or retransmitting network services, such as through the installation of new switches or wireless access points, in any way is prohibited, unless prior approval is granted by College's IT controlling authority or supervisors thereof or a designee of one of these authoritative positions..
8. Publicly and/or anonymously available network servers/services such as email, Web, and FTP shall be segregated from a college's file and print services and end user machines.
9. A controlled pathway shall be used in college networks to assist in secure communications and prevent unmanaged network connections. Controlled paths shall be specified for remote users and local users when accessing College resources.
10. To maintain the correct time and accuracy of data and audit logs on information systems residing within the College's Network, system clocks must be synchronized regularly. System time clocks must be updated on a daily basis from an accepted time source that agrees with the Coordinated Universal Time, and the synchronized correct time must then be disseminated to all systems on the College's network. Time synchronization data and configurations shall be protected from unauthorized modification.
11. DNS servers shall not be configured to allow zone transfers to unknown secondary servers.
 - a) If a college maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers.
 - b) If a college maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.

- c) When a domain has a US extension (*i.e.*, state.nc.us), the US Domain Registry requires the domain allow copies to be transferred to the US Domain Registry's Master Server. Therefore, all domains registered with US Domain Registry will allow transfers of copies of their zones to the Master Server for the US Domain Registry. When OITS maintains the DNS, colleges may request OITS to allow additional IP addresses to receive zone transfers. Colleges must work with OITS to define acceptable IP addresses and/or IP address ranges.

ISO 27002 REFERENCES

- 10.6 Network security management
- 10.10.6 Clock synchronization
- 11.4 Network access control
- 11.4.2 User authentication for external connections

030102 Managing the Networks

Purpose: To establish a framework for the management and protection of the College's network resources.

STANDARD

Colleges shall manage the security of their respective networks based on business needs and the associated risks. Colleges' network infrastructure shall be managed using controls to safeguard the College's information systems. Failure to protect against threats can result in loss of data integrity, data unavailability and/or unauthorized use of data. Access to information available through the College network shall be strictly controlled in accordance with approved access control policies and procedures. Secure management of the network infrastructure shall include but not be limited to the following:

1. Users shall have direct access only to those services that they have been authorized to use.
2. Use of secure protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), and Internet Protocol Security (IPSec).
3. For public networks, management software tools that communicate with devices shall use Simple Network Management Protocol (SNMP) version 3 for network management. For private networks, management software tools that communicate with devices may use SNMP version 2 or version 3 for network management.
4. Use of authentication, authorization and accounting mechanisms when administering network devices.
5. Monitoring for attempts to deny service or degrade the performance of information systems (including computers, microcomputers, networks, telephone systems and video systems).
6. Definition of tasks/roles/responsibilities involved in management and security of college IT resources in job descriptions.

ISO 27002 REFERENCES

- 8.1 Prior to employment
- 10.6.1 Network controls
- 11.4.1 Policy on use of network services
- 11.4.2 User authentication for external connections
- 11.4.6 Network connection control

030103 Defending Network Information from Malicious Attack

Purpose: To protect information residing on College networks.

STANDARD

Colleges shall implement layers of information security (defense in depth) to defend against attacks on the College's information resources. All safeguards and network security plans shall incorporate the following:

1. Configuration of system hardware, operating systems and applications software and network and communication systems to standards and secure specifications required by the North Carolina Community College Information Security standards. When such standards do not exist, colleges are expected to conform to security standards from institutes such as the SANS Institute or the National Institute of Standards and Technology (NIST).
2. Implementation of measures to prevent snooping, sniffing, network reconnaissance and other means of gathering information about the network infrastructure.
3. Implementation of measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network.
4. Installation of antivirus software that protects the College's infrastructure from downloads, media transfers, electronic-mail attachments of malicious software, or other malware.
5. Monitoring and reviewing system usage for activities that may lead to business risks by personnel who are able to quantify and qualify potential threats and business risks. Appropriate controls and separation of duties shall be employed to provide review and monitoring of system usage of personnel normally assigned to this task. Some events that should be monitored include over utilization of bandwidth, unauthorized login attempts, and unauthorized attempts to make changes to system settings.
6. Periodic review of system logs for signs of misuse, abuse or attack. Items to monitor may include but not necessarily be limited to the following:
 - Over utilization of bandwidth
 - Un-authorized login attempts
 - Un-authorized attempts to make changes to system settings
 - Trending activity, such as to monitor for repeated information security attacks.

GUIDELINES

Colleges should consider technologies that eliminate single points of failure on critical systems, such as server clustering, redundant links, load balancing and redundant array of independent disks (RAID).

ISO 27002 REFERENCES

- 10.4.1.1 Controls against malicious code
- 10.10.2 Monitoring system use

030104 Network Segregation

Purpose: To help protect internal networks through network segregation.

STANDARD

1. Colleges' internal network infrastructures (*i.e.*, College local area networks [LANs]) shall be segregated into network zones to protect application servers from the user LAN. In addition, production and non- production environments (*e.g.*, test, development, QC, etc.) shall be segregated from one another.
2. Wireless networks shall be physically or logically segregated from internal networks such that an unknown external user cannot access an college's internal network.
3. Colleges shall follow the matrix below, the Access Control Framework for Network Security Matrix, to prevent unauthorized access to information systems through appropriate placement and configuration of state resources that provide protective measures commensurate with the security level required to protect the data contained in those systems.
4. Colleges shall assess the risk associated with each business system to determine what security requirements apply to it. The security assessment determines the appropriate placement of each system and application within the security framework and evaluates the network resources, systems, data and applications based upon their criticality. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase.

Security Requirements

1. Security for the network infrastructure and for distributed systems operated by Colleges shall comply with the security requirements of the matrix below, which is expressly made part of this policy. All Colleges capable of meeting the security requirements for the Demilitarized Zone (DMZ) and/or Secure Zone as listed in the template shall do so.
2. The Access Control Framework for Network Security Matrix below describes the network security requirements for devices attached to the College's network. The columns represent network zones that are segregated by college approved firewalls or other network segmentation mechanism.
3. For the Application and Database secure zones, a college approved firewall or other network segmentation mechanism, such as VLANs, is required to segregate application servers and database servers.
4. Where end user access is allowed to a resource at the college's discretion, it is designated with "Opt." for optional. Client-server applications that operate on a college LAN and are not public facing (*i.e.*, Internet accessible) may fall under the college Internal LAN column of the matrix below.
5. For the purpose of the framework, software components installed on end points (*i.e.*, thick clients) do not constitute a valid network zone.
6. Facility management systems, such as heating, ventilation or air conditioning (HVAC), badge access, electrical generators, power distribution, water, and closed-circuit television (CCTV) may be excluded from the Access Control Framework network zoning requirements, provided those systems are not publicly accessible, are logically isolated (*i.e.*, VLANs) from other networked systems and cannot access other shared systems/services, and have appropriate access control mechanisms in place, such as Access Control Lists (ACLs), authentication mechanisms, or a VPN. These systems shall comply with other statewide information security standards mentioned in this manual.

Special Assembly Security Requirements

1. Colleges not able to adhere to the DMZ and/or other security requirements in the Access Control Framework shall develop a Special Assembly zone and document the rationale for developing the Special Assembly zone. Security controls in the Special Assembly area are not as structured as controls in the DMZ/Secure zones. Colleges acknowledge that additional security risks are associated with the Special Assembly zone.
2. College CIOs shall develop a process for creating Application Unique Domain (AUD) special assembly zones and maintain a list of their AUDs.

Virtual Environment Requirements

1. Virtual machines are hosted on physical machines. Virtual machines (guests) shall use equivalent security controls as is required in a physical computing environment to assure data availability, integrity and confidentiality. The approach to virtual machine security control and segregation shall balance the business needs, practical approach, and the associated risk.
2. Virtual computing environments shall use secure communication between the virtual machines and shall use equivalent network zoning as the physical environment does (See the Access Control Framework for Network Security Matrix below).
3. Colleges should consider separating high risk virtual machine farms from lower risk virtual machine farms on to separate physical servers.
4. Whereas a virtual machine may store or process confidential data, the virtual machine image file shall use appropriate controls to protect the data at rest.
5. The virtual environment requirements apply to cloud computing in which dynamically scalable and often virtualized resources are provided as a service to customers over the Internet. Vendors of cloud computing services or other types of hosted solutions shall agree to comply with all statewide information security standards through SLAs and contracts when the College utilizes such services.

Access Control Framework for Network Security Matrix

	DMZ			Secure Zone				Special Assemblies			
Destination ->	Web / User Facing			Application Services		DB Services		Mgmt. Domain	Application Unique Domain*****	Agency Internal LAN	Infrastructure College WAN
	Public	College	Vendor	Std.	High	Std.	High				
Operational Controls											
User/Device											
Access	Yes	Yes	Yes	Opt.	No	No	No	No	Yes	Yes	Yes
Authentication*	Opt.	Opt.	Opt.	Req.	N/A	N/A	N/A	N/A	TBD	Opt.	Req.
Authorization	Opt.	Opt.	Opt.	Req.	N/A	N/A	N/A	N/A	TBD	Opt.	Req.
Encryption**	Opt.	Opt.	Opt.	Opt.	N/A	N/A	N/A	N/A	TBD	Opt.	Opt.
Administrator											
Access	Yes	Yes	Opt.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication*	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Req.	Req.
Authorization	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Req.	Req.
Encryption**	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	TBD	Opt.	Req.

Access Control Framework for Network Security Matrix

	DMZ			Secure Zone				Special Assemblies			
Destination ->	Web / User Facing			Application Services		DB Services		Mgmt. Domain	Application Unique Domain****	Agency Internal LAN	Infrastructure College WAN
Application to Application/Server to Server	Public	College	Vendor	Std.	High	Std.	High				
Access	Opt.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentication*	Opt.	Req.	Req.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.
Authorization	Opt.	Req.	Req.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.
Management Controls											
Asset Management	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Ad-Hoc	Req.
Configuration Management***	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
Physical Access Controls	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
Documented User Access / Certificate Policy & Process	Opt.	Opt.	Opt.	Opt.	Req.	Opt.	Req.	Opt.	TBD	Opt.	Opt.
Audit Controls											
Configuration Audit & Integrity Check	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Physical Access Audit	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc

Access Control Framework for Network Security Matrix

	DMZ			Secure Zone				Special Assemblies			
	Web / User Facing			Application Services		DB Services		Mgmt. Domain	Application Unique Domain*****	Agency Internal LAN	Infrastructure College WAN
	Public	College	Vendor	Std.	High	Std.	High				
User Access	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
Vulnerability Assessment	Ad-Hoc	Ad-Hoc	Ad-Hoc	Annual	Semi-Annually	Annual	Semi-Annually	Ad-Hoc	Ad-Hoc	Ad-Hoc	Ad-Hoc
Operational Controls											
Firewall/Access Control****	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Req.
IDS/IPS – Network*****	Req.	Req.	Req.	Req.	Req.	Req.	Req.	Opt.	TBD	Opt.	Req.
IDS/IPS - Host	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.	Opt.	TBD	Opt.	Opt.

* Authentication shall be performed via an encrypted channel when used for system administration or confidential data access.

** Encryption applies to data in transit.

*** Must follow Collegewide Vulnerability Management Policy.

**** Refer to 030105 – Routing Controls and Firewall Configuration Policy.

***** Application Unique Domain provides the ability for non-conforming applications to have a custom designed network security architecture that provides additional security measures as needed to mitigate identified risks.

***** Enterprise IDS/IPS deployment may already provide an appropriate IDS/IPS solution. The Enterprise IDS/IPS is the minimum to meet the requirements of the IDS/IPS in the Access Control Framework. Minimum security level for IDS/IPS deployment in the enterprise infrastructure is determined by the SCIO.

ISO 27002 REFERENCES

11.4.5 Segregation in networks

11.11.1 Access control policy

030105 Routing Controls and Firewall Configuration

Purpose: To protect access to the College's routed networks.

STANDARD

Colleges shall deploy mechanisms to control access to the College's network backbone and/or routed infrastructure. Protective controls shall at a minimum include the following:

1. Positive source and destination address checking to restrict rogue networks from manipulating the College's routing tables.
2. Authentication to ensure that routing tables do not become corrupted with false entries.
3. Network address translation (NAT) to screen internal network addresses from external view.
4. Firewalls shall control inbound and outbound network traffic by limiting that traffic to only that which is necessary to accomplish the mission of the colleges.

Firewall Configuration and Installation

1. The default firewall policy is for all ports to be closed. Only those ports for which a College has written, documented business reasons for opening shall be open.
2. Each College shall establish a process for evaluating policy changes that, at a minimum, incorporates requirements for compliance to the security matrix for communications across trust levels and emphasizes alternative methodologies to comply with industry best practices.
3. All Colleges shall designate a minimum of two (2) authorized firewall administrators. At least one of the designated firewall administrators will be a security specialist who is consulted before firewall policy changes are approved and implemented.⁴
4. The process methodology shall incorporate an approach to block all ports then permit specific ports which have a business requirement access while incorporating additional hardening as necessary to have a comprehensive security policy.
5. For temporary or emergency port openings, the College process shall establish a maximum time for the port to be open, which shall not exceed 15 days. The College authorized firewall policy administrators, or the entity managing the firewall, shall subsequently close the port or develop additional hardening.
6. System administrators shall configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.
7. Firewalls shall be installed in locations that are physically secure from tampering. The college security liaison shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the college security liaison.
8. Firewall rules sets shall always block the following types of network traffic:
 - Inbound network traffic from a non-authenticated source system with a destination address of the firewall system itself.
 - Inbound network traffic with a source address indicating that the packet originated on a network behind the firewall.
 - Traffic inbound to the College Network containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter with the following exceptions: To allow testing initiated from internal IT support groups, ICMP echo replies and ICMP TTL expired will be permitted inbound to the College

⁴ A security specialist for firewall configuration is an individual who understands firewall technology and security requirements. If OITS manages the firewall, OITS will provide the security specialist.

Network but will be limited to specific IP addresses or small subnets representing the internal support group. A ping point can be established at the perimeter, for troubleshooting purposes, with the sole purpose and sole capability of responding to a ping.

- Inbound network traffic containing IP Source Routing information.
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0
- Inbound or outbound network traffic containing directed broadcast addresses.

9. Minimum Firewall Requirements:

- Local user accounts shall be configured on network firewalls, for the sole purpose of eliminating possible extended outages.
- Local accounts shall be configured to only become active when the device cannot make contact with the central authentication and/or control unit. During normal operation, the local account exists but is unusable.
- Firewalls must use an authentication mechanism that provides accountability for the individual.
- Passwords on firewalls shall be kept in a secure encrypted form.

10. Monitoring and Filtering

- Logging features on College network firewalls shall capture all packets dropped or denied by the firewall, and college staff or the entity managing the firewall shall review those logs at least monthly.
- Each College's firewall policy shall be reviewed and verified by College staff at least quarterly. If an outside entity, such as OITS, manages the firewall, then that entity shall be responsible for reviewing and verifying the college's firewall policy at least quarterly.

ISO 27002 REFERENCES

11.4.7 Network routing control

030106 Responsibilities and Agreements

Purpose: To protect the integrity and ensure the stability of the statewide network from fraudulent use and/or abuse resulting from access and use of the network and to define the security attributes delivered with network services.

STANDARD

1. OITS is responsible for the security of the infrastructure of the state's network.
2. Any and all actions that jeopardize the integrity and stability of the state network will be addressed commensurate to the level of risk.
3. OITS is authorized to immediately suspend network service to any organization when the level of risk warrants immediate action. When network service is suspended, OITS will provide immediate notice to the organization. When possible, OITS will notify any organization of any such action in advance of such an action. OITS will work with the organization to rectify the problem that caused the suspension.
4. Organizations with connections to the state network are responsible for managing risk and providing appropriate security for their networks. Security measures must conform to statewide information security standards and statewide architecture.
5. Agency internal security measures shall be deployed only on college internal networks and must not adversely affect the state network.
6. Any violations of this network security standard are subject to review by the College Chief Information Officer (College CIO) and organization management and are subject to action that conforms to state disciplinary policies and all relevant laws. These actions may include termination of service. Termination requires appropriate notification by OITS, including notification to its upstream providers, and the termination shall be at the lowest level necessary to safeguard network

security and minimize disruption of business activities.

7. Network service agreements shall specify detailed information and requirements regarding the security features, service levels, and management requirements for all network services provided. When network services are outsourced, the agreement shall include provisions for the college to monitor and audit the outsourced provider's adherence to the agreement.

ISO 27002 REFERENCES

10.6.2 Security of network services

030107 Time-Out Facility

Purpose: To prevent network misuse, and unauthorized access through the implementation of time-out mechanisms.

STANDARD

1. Colleges shall implement time-out mechanisms that terminate sessions after a specified period of inactivity, such that the user must re-authenticate his identity to resume the session. This criteria may be met via a password protected screen saver or some other mechanism that locks an account or system after a given period of inactivity.
2. If the user is connected via external networks (e.g., a telecommuter logging in from home), the time-out mechanism must also terminate the network connection.
3. The period of inactivity for session and terminal time-outs shall be established based on the College's needs, system or application criticality, the confidentiality of the information accessed through the system or application, or other risk factors, but shall not exceed 30 minutes.
4. For some higher risk information systems, such as systems that process health care data, tax data, or credit card information, the requirement for a session idle timeout shall be 15 minutes or less, as determined by law or industry standards.

ISO 27002 REFERENCES

11.5.5 Session time-out

030108 Authentication of Network Connecting Equipment

Purpose: To control and/or detect the installation of unknown equipment on a network.

STANDARD

1. To protect the college network from vulnerabilities that can be introduced when users access the network with unmanaged devices, colleges shall require that all users accessing the college network with any devices adhere to required security configurations for those devices, including required patches and updated anti-virus signature files on those devices.
2. In the use of wireless networks, users shall be required to follow locally established methods of authentication. The use of captive portal and acknowledgment of local acceptable use policy is strongly encouraged. Using wireless networks to access the campus administrative computer system by employees without the use of a virtual private network is prohibited.
3. Procedures that verify node authentication measures shall be developed and tested on a semi-annual basis.

GUIDELINES

1. Equipment identification for physically attached devices may be achieved through various methods, including validation of the media access control (MAC) address, validation of other unique equipment identifiers, or through the use of digitally signed certificates that are associated with a specific server or device.
2. Network routing controls should be implemented to supplement equipment identification by allowing specific equipment to connect only from specified external networks or internal sub-networks (“subnets”).
3. Testing should occur on the following connections to verify proper operational behavior:
 - Remote user – VPN authentication.
 - Dial back; dial backup and dial-up authentication mechanisms.
 - Wireless authentication.
 - Server authentication (email, domain logon, secure portals, etc.)

ISO 27002 REFERENCES

11.4.2 User authentication for external connections

11.4.3 Equipment identification in networks

Section 02 System Operation and Administration

030201 Controlling Data Distribution and Transmission

Purpose: To protect the College’s data and information from unauthorized disclosure.

STANDARD

1. Colleges shall manage the electronic exchange or transfer of data to ensure that the confidentiality and integrity of the data are maintained during the transfer process.
2. Colleges shall address the risk involved in the transfer of different types of data and implement safeguards through the means of exchange used, such as through email, the Internet, or exchange of electronic media and tapes.
3. Technical access controls or procedures shall be implemented to ensure that data and information are transmitted only as authorized and as appropriate.
4. Access controls and/or procedures shall, in part, be based on college business requirements.
5. All confidential data shall be encrypted when transmitted across wireless or public networks⁵, including transmissions such as FTP and electronic mail. For the encryption requirements of secure transmission of confidential data, please see 030501 - Using Encryption Techniques.

ISO 27002 REFERENCES

9.1 Secure Areas

10.8.1 Information exchange policies and procedures

030202 Controlling On-Line Transactions

Purpose: To protect on-line transactions and the parties involved in on-line transactions.

STANDARD

When colleges accept or initiate on-line transactions, they shall implement controls or verify that controls exist to:

1. Validate the identity of the parties involved in the transaction.

⁵ For the purpose of this standard, a public network includes the College Network. It does not apply to internal college networks. Internal college networks are considered private networks.

2. Gain proper approval for the transaction, if necessary.
3. Protect the confidential data involved in the transaction.
4. Ensure the integrity of the transaction.
5. Obtain proof that the transaction is completed correctly.
6. Prevent unauthorized or accidental replay of a transaction so that it will not be duplicated.

GUIDELINES

Methods to implement the controls above are dependent on the nature of the transaction and the level of risk but could include:

1. Using electronic signatures that are validated through an approved, known certificate authority (CA).
2. Using enhanced authentication techniques, such as multi-factor authentication.
3. Implementing automated two-person controls for approving transactions.
4. Encrypting the message content when transmitted over an unsecured communications link.
5. Encrypting the communications link through secure protocols.
6. Storing transaction details in a secure location not accessible to unauthorized persons.

ISO 27002 REFERENCES

11.5.6 Limitation of connection time

Section 03 Email and Internet Communication

030301 Sending and Receiving Electronic Mail (Email)

Purpose: To establish requirements for sending electronic mail.

STANDARD

Colleges shall develop policies regarding unacceptable use of email and set forth the extent to which users may use college-provided email for personal use.

1. College personnel shall exercise due care when addressing email correspondence to ensure that the correspondence is addressed correctly and that the intended recipient is authorized to view content within emails or documents. Examples of email content that constitute unacceptable use include the following:
 - a. Private or personal for-profit activities. This includes personal use of email for marketing or business transactions, advertising of products or services or any other activity intended to foster personal gain.
 - b. Unauthorized not-for-profit business activities.
 - c. Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.
 - d. Unauthorized distribution of College data and information including the unauthorized use of email auto-forwarding.

- e. Use for, or in support of, unlawful/prohibited activities as defined by federal, State and local laws or regulations.
2. Prohibited activities relating to Internet and network access include the following:
 - a. Tampering with computer hardware or software.
 - b. Knowingly vandalizing or destroying computer files.
 - c. Transmitting threatening, obscene or harassing materials.
 - d. Attempting to penetrate a remote site/computer without proper authorization.
 - e. Using the Internet in an effort to access data that are protected and not intended for public access.
 - f. Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret.
 - g. Sending confidential information without encrypting that information, exposing the data to discovery by unintended recipients.
 - h. Intentionally seeking information about, obtaining copies of or modifying contents of files, other data belonging to other users, unless explicitly authorized to do so by those users.
 - i. Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these standards by sharing information or passwords is also unacceptable behavior.
 - j. Deliberate interference or disruption of another user's work or system. Users must not take actions that cause interference to the network or cause interference with the work of others on the network. Users are prohibited from performing any activity that will cause the loss or corruption of data, the abnormal use of computing resources (degradation of system/network performance) or the introduction of computer worms or viruses by any means.
3. Misdirected or unsolicited email shall be treated with caution. Recipients shall not open or respond to unsolicited email. Colleges shall develop policies and/or training to educate users about the potential security risks involved in responding to unsolicited commercial email (spam), including responding to an invitation contained in such email to have one's email address removed from the sender's list.
4. Colleges shall develop policies to encourage due care by users when forwarding messages so that users do not do the following:
 - a. Auto-forward email without first obtaining college approval.
 - b. Knowingly send out an email message that contains viruses, Trojan horses or other malware.
 - c. Use the electronic-mail system or network resources to propagate chain letters, misinformation or hoax information.
 - d. Forward any confidential information to any unauthorized party without the prior approval of a local department manager.
 - e. Forward any confidential information without appropriate protections such as encryption.
 - f. Forward the wrong attachment.
 - g. Send information or files that can cause damage to the College, its students or employees or the State of North Carolina or its citizens.
 - h. Send unsolicited messages to large groups of people except as required to conduct college business.
5. Colleges shall provide training on the security issues involved in receiving email to ensure that employees are aware of potential problems that can be introduced into the network and how to avoid them.
6. Colleges shall protect College and State resources by not taking action on unsolicited commercial electronic mail. Colleges shall also establish procedures that address the following issues:

- a. Attacks on electronic mail (e.g., viruses, interception, user identification, defensive systems).
 - b. Activating or clicking on hyperlinks in documents or email messages that are from unknown sources or part of unsolicited messages (spam).
 - c. Responding to or following hyperlinks asking for user names and passwords when asked to do so by unsolicited phishing emails.
 - d. Protection of electronic mail attachments using such techniques as filtering, stripping and store and forward.
 - e. Use of cryptography to protect the confidentiality and integrity of electronic messages.
7. Communications sent or received by college email systems and/or email communications on State business in personal email accounts may be public records as defined by the North Carolina Public Records Law, N.C.G.S. §132.1, *et seq.*, and shall be managed according to the requirements of a college's record retention policy or as set forth in the General Schedule for Electronic Records published by the Department of Cultural Resources.

GUIDELINES

Colleges not using the State's email system should encourage the attachment of a statement to email(s) that the message and any response to the message received by the college are being sent on a State email system and may be subject to monitoring and disclosure to third parties, including law enforcement personnel.

An example is as follows:

Email correspondence to and from this sender may be subject to the North Carolina Public Records Law and may be disclosed to third parties, including law enforcement personnel.

Instructions and disclaimers should be reviewed and approved by the college or State legal staff prior to use.

ISO 27002 REFERENCES

- 10.4.1 Controls against malicious code
- 10.8.2 Exchange agreements
- 10.8.4 Electronic messaging
- 10.8.5 Business information systems
- 12.2.3 Message integrity

030302 Using the Internet for Work Purposes

Purpose: To provide standards for the College's infrastructure and Internet use.

STANDARD

Persons responsible for setting up Internet access for a college shall ensure that the college's network is safeguarded from malicious external intrusion by deploying, at a minimum, a configured and managed firewall. The configuration shall ensure that only the minimum services are installed to allow the business functions. All unnecessary ports and services shall be uninstalled or denied.

While performing work-related functions or while using publicly owned/publicly provided information-processing resources, College employees and authorized users shall use network resources and the Internet responsibly. Users accessing the College Network shall do the following:

1. Ensure that there is no intentional use of such services in an illegal, malicious or obscene manner.
2. Ensure compliance with College acceptable use policies.
3. Ensure that all applicable software copyright and licensing laws are followed.
4. Guard against wasting College Network resources, such as excessive personal use.

5. Not use the College Network for distributing unsolicited commercial advertising or personal Web hosting.
6. Avoid using Internet streaming sites except as consistent with the mission of the college and for the minimum amount of time necessary to obtain the desired amount of information.
7. Not take actions that would constitute a criminal offense or make the College liable to civil suits, such as stalking, or actions that are abusive, fraudulent, hateful, defamatory, obscene or pornographic in content.
8. Not access or attempt to gain access to any computer account or network that they are not authorized to access.
9. Not intercept, attempt to intercept, forge or attempt to forge data transmissions that they are not authorized to access or send.
10. Users of Internet search engines shall take precautions when using Internet search engines to verify the integrity of the information provided by the search engine. As users collect information gathered from the Internet, they must do the following:
 - a. Check data for their integrity and accuracy before using them for business purposes.
 - b. Observe all copyrights, end user licensing agreements, and other property rights.
 - c. Use caution when downloading files from websites, ensuring that all downloads are scanned for viruses and other malicious code.

Using Social Media and Networking Sites

Each college must assess risk and determine under what circumstances if any, social media and networking sites are appropriate for use in connection with performing its College business activities. Social networking tools use customized, web based environments for collaborative communication and dissemination of relevant information. Social media sites such as Facebook, Twitter, MySpace and LinkedIn, etc., enable users to post and exchange information, in order to develop and maintain online connections and relationships. These sites allow a community of users, usually with common interests, to communicate information and feedback about those interests. When a particular social networking site is approved for use by a college, then the college shall do the following:

1. Develop a policy on the purpose and appropriate use of the social networking site by the college.
2. Provide guidance to authorized college personnel for use and maintenance of any social networking sites used in connection with college business.
3. Provide guidance to college personnel for appropriate use or disclosure of employment or other College-related information in connection with personal use of social networking sites.
4. To help prevent fraud and unauthorized access, colleges shall advise users:
 - a. To use a different user credential and password for each social networking and other non-College owned/hosted site. Accounts and passwords used to access social networking sites used by colleges shall never be the same as accounts and passwords used for other personal or professional business. In particular, an employee's NCID username or password must never be used for access to any other site or account outside of the College network.
 - b. To guard against disclosing too much personally identifiable information, such as birthdates.
5. Prohibit users from:
 - a) Any action or statement that implies the user is speaking, or may speak, on behalf of the college, unless the user is specifically authorized to do so; and
 - b) Disclosure of College information learned as a result of their employment when visiting social networking sites for their own personal use.
6. Train users on appropriate practices for use of social networking sites.
7. Monitor user access and use of all social networking sites.

8. Institute data preservation and loss prevention measures.

ISO 27002 REFERENCES

11.1.1 Access control policy

030303 Downloading Files and Information from the Internet

Purpose: To establish restrictions pertaining to downloading files and use of the Internet.

STANDARD

Personnel shall only download files that aid in the performance of work-related functions. While downloading files or information from the Internet, College employees and College network users shall comply with the college's acceptable use policy and the statewide information security standards that address the security of all devices connecting to the network, including those listed below. Safeguards that shall be in place to limit the risk of downloading files that may contain malware include the following:

1. Use of antivirus software that scans files before they are downloaded.
2. Having only approved software installed to a system.
3. Validating before installation the source of software and the reputation of the site from which it is downloaded.
4. Not opening files from people not known to the user or files that are spammed via email.
5. Not downloading or using software or any other materials that may constitute a copyright or licensing violation or implicate the College for licensing agreements.
6. Not running unauthorized P2P applications to facilitate the downloading and sharing of copyrighted material.
7. Not utilizing the Worldwide Web to download applications designed to remove copyright protections from protected content such as DVD media.

ISO 27002 REFERENCES

10.4.1 Controls against malicious code

11.1.1 Access control policy

030304 Setting Up Intranet / Extranet Access

Purpose: To implement and manage a college Intranet in a secure manner.

STANDARD

1. Colleges that have Intranet / Extranet sites shall provide the same controls on access to the site as to the files located on the network, in accordance with other statewide access control standards.
2. Traffic to the Intranet site from an external location shall be blocked unless it is tunneled through a virtual private network (VPN).
3. All new connections between third parties and College colleges shall be documented in an agreement that includes information technology security requirements for the connections. The agreement shall be signed by a college employee who is legally authorized to sign on behalf of the college and by a representative from the third party who is legally authorized to sign on behalf of the third party. The signed document must be kept on file with the relevant extranet/network group.

GUIDELINES

When setting up access to the Intranet / Extranet site, colleges should implement the following best practices:

1. A documented approval process should be created before any information is posted to the site.
2. Before posting material to the site, workers should be required to thoroughly check all information and programs to make sure they do not include viruses, Trojan horses, or other malicious code.
3. All legal issues such as disclosure of confidential information and copyright infringement should be resolved prior to posting.
4. Workers should also be required to confirm the information's accuracy, timeliness and relevance to the college's mission before posting it.

ISO 27002 REFERENCES

11.1.1 Access control policy

030305 Giving Information When Ordering Goods on the Internet

Purpose: To provide awareness that there are potential security risks in revealing confidential information when ordering items via the Internet.

STANDARD

College employees who are responsible for ordering goods and services via the Internet must be cognizant that they are responsible for protecting College information. When making payments via the Internet, personnel must do the following:

1. Ensure that all College credit or debit card details are kept confidential (including personal identification numbers [PINs], account numbers and details).
2. Make every effort to verify that the third party is a legitimate e-business.
3. Consider potential risks involved in conducting business on a Web site that has been compromised or is insecure.
4. Verify that the third party is using the desired secure Web site by checking that the site address starts with https, not http, and that the Web uniform resource locator (URL) is accurate and has been typed in directly.
5. Revert to ordering goods via telephone if any doubts or suspicions arise.
6. Reconcile any credit card(s) used against credit card statements and scan statements for fraudulent or bogus charges.

ISO 27002 REFERENCES

10.9.1 Electronic commerce

10.9.3 Publicly available information

030306 Web Browser Security

Purpose: To ensure the proper settings of Web browsers and other Internet software.

STANDARD

Colleges shall ensure that Web browser software is properly configured to protect the College and State's information technology systems. System administrators, support personnel, and system users must be aware of the following:

1. Most Web servers automatically collect information about any user visiting the site, including the user's Internet Protocol (IP) address, browser type and referrer, by reading this information (which every browser provides) from the user's browser.
2. Confidential data may be stored on cookies on their machine automatically and that these cookies are updated automatically.
3. Viruses, spyware, Trojan applications and other malicious code may be able to cause damage to the State's infrastructure via Web browsers and therefore shall be continuously scanned.
4. Built-in security features must be used to ensure the best security for Web browsers.
5. Web browser vulnerabilities must be addressed through the installation of software patches needed to mitigate the vulnerabilities.

GUIDELINES

Users should exercise caution when prompted to download or run programs from a web site. Also, support personnel should consider removing cookies from machines on a regular basis.

ISO 27002 REFERENCES

10.9.3 Publicly available information

030307 Filtering Inappropriate Material from the Internet

Purpose: To protect the College from the accessing of inappropriate Internet sites and material.

STANDARD

If a college determines that it should filter access to Internet sites and materials, it shall develop a policy that sets forth the criteria by which it will determine when filtering will be performed and shall notify users of the policy. The implementation of access controls or other techniques to filter out inappropriate Internet sites and materials may be necessary to protect network resources and ensure the following:

1. Employees do not accidentally or deliberately view, access or download inappropriate materials from the Internet that may cause concern or distress to themselves or other employees.
2. Employees are restricted from inappropriate use that may result in criminal or civil penalties to the College.
3. Corrective actions can be taken for repeated instances of inappropriate use.

GUIDELINES

Colleges should consider the installation of a proxy server or content filtering appliance.

ISO 27002 REFERENCES

11.1.1 Access control policy

030308 Mobile Device Applications

Purpose: To protect the College Network from mobile code that performs unauthorized and malicious actions.

STANDARD

Colleges shall develop a policy to protect their network from mobile code that may perform unauthorized and harmful actions. Mobile code is software that is transferred between systems and executed on a local system without explicit installation or execution by the recipient. Active X and Java are examples of mobile code that can inadvertently breach college network defenses.

GUIDELINES

Colleges should implement measures based on the level of access and the level of risk the college is willing to accept. Listed below are sample access and security settings that a college may use to refine their policy.

- **Internet Server Usage.** These policies would cover the usage of mobile code served via the Internet by the organization's servers. A typical security setting should be high.
- **Internet Client Usage.** These policies would cover which categories of mobile code a client or user could access via the Internet. A typical security setting should be medium.
- **Intranet Usage.** These policies would cover the usage of mobile code only on the organization's intranet. A typical security setting might be medium or medium low.
- **Mobile Device Usage.** Similar to an Internet client, these policies are for mobile devices accessing various mobile code resources. A typical security setting might be medium.

Security Settings

HIGH

- a. The safest way to browse but also the least functional
- b. Few secure features are disabled
- c. Appropriate setting for avoiding sites that may have harmful content

MEDIUM

- a. Safe browsing and still functional
- b. Prompts before downloading potentially unsafe content
- c. Unsigned ActiveX controls are not downloaded
- d. Appropriate setting for most Internet sites

MEDIUM-LOW

- a. Same as Medium without prompts
- b. Most content will be run without prompts
- c. Unsigned ActiveX controls will not be downloaded
- d. Appropriate for sites on your local network (Intranet)

LOW

- a. Minimal safeguards and warning prompts are provided
- b. Most content is downloadable and run without prompts
- c. All active content can run
- d. Appropriate for sites that you absolutely trust

ISO 27002 REFERENCES

10.4.2 Controls against mobile code

Section 04 Telephones and Faxes

030401 Making Conference Calls

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

Confidential information shall not be discussed on speakerphones or other electronic media, including Voice over IP systems, during conference calls unless:

1. All authorized parties participating in the call have been authenticated.
2. All authorized participating parties have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation.
3. The conference call is made in an area of the building that is secure (*i.e.*, offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls).
4. All parties involved in the conference call are openly identified.

GUIDELINES

1. Use of publicly available Voice over IP systems should be avoided when a college or state operated Voice over IP system is available.
2. When use of a publicly available Voice over IP provider is necessary, due diligence should be taken to ensure the call is conducted in accordance with this standard.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

030402 Using Videoconferencing Facilities

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

Confidential information shall not be discussed on videoconferences or other electronic media, including Voice over IP, unless:

1. All authorized participants have been authenticated.
2. All authorized participants have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation.
3. The videoconference call is being made in an area of the building that is secured (*i.e.*, offices or conference rooms where the door can be closed and conversations cannot be overheard through thin walls).
4. All parties involved in the conference call are openly identified.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

030403 Recording of Telephone Conversations

Purpose: To establish requirements for policies that disclose to employees and third-party contractors using College telephone systems that their use of such systems may be monitored.

STANDARD

Colleges using monitoring technologies shall establish policies to provide appropriate notice to College employees and third-party contractors of what the college will be monitoring. The policies shall include the circumstances under which the monitoring will take place.

GUIDELINES

1. Specify the scope and manner of monitoring for telephones and never exceed the scope of any written monitoring statement in the absence of any clearly stated exception.
2. When appropriate, obtain a written receipt from College employees and third-party contractors acknowledging that they have received, read and understood the college's monitoring policy.
3. Inform College employees and third-party contractors of any activities that are prohibited when using college telephones.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

030404 Receiving Misdirected Information by Facsimile

Purpose: To ensure that confidential information is provided only to authorized individuals.

STANDARD

1. Colleges shall develop guidelines for handling the receipt of unsolicited facsimiles, including advertising material, as well as misdirected facsimiles.
2. When a college receives a facsimile in error (wrong number, person, office, location or department), it shall notify the sender, if appropriate.
3. Misdirected facsimiles shall be treated as confidential documents.
4. Facsimiles that carry advertisements may be discarded.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

030405 Providing Confidential Information over the Telephone

Purpose: To provide awareness that giving information over the telephone presents security risks.

STANDARD

1. To reduce the possibility that confidential information will be provided to unauthorized individuals, colleges shall establish procedures for employees and contractors to follow when conveying confidential information over the telephone.
2. When confidential information (e.g., credit card number, social security number) is required or requested while conducting business (i.e., ordering goods) using the telephone, employees must ensure that they know exactly to whom they are speaking and whether that person is authorized to receive such information.
3. Confidential information must not be left on answering machines or other recording devices.

4. Care must be taken to ensure that confidential information cannot be overheard when it is disclosed over the telephone.
5. Colleges shall provide employees and contractors with awareness training on social engineering and the requirements for protecting confidential data.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

Section 05 Securing Data

030501 Using Encryption Techniques

Purpose: To protect the College’s confidential information using encryption techniques.

STANDARD

1. Each college shall document and retain on file a case-by-case risk management determination for each type of confidential information as to the appropriateness of its unencrypted transmission to a party not served by the college’s internal network.
2. All laptops that are used to conduct the public’s business shall use encryption to protect all information from unauthorized disclosure, including confidential information, such as personal information.
3. All other mobile computing devices and portable computing devices such as personal digital assistants (PDAs), smart phones, tablets and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players) and flash drives that are used to conduct the public’s business, shall use encryption to protect all Personally Identifiable Information (PII) and confidential information from unauthorized disclosure.

Device	Encryption Requirements
Laptops, Notebooks, and Netbooks	All devices shall use Full Disk Encryption (sector-level) using a FIPS 140-2 Level 1 certified AES-256 encryption algorithm. ⁶
Mobile and portable computing devices, such as tablets, smart phones and personal digital assistants. Removable Media such as CDs, DVDs, memory sticks (flash drives), tape media, or any other portable device that stores data.	All Personally Identifiable Information (PII) and other confidential information shall be encrypted using a FIPS 140-2 Level 1 certified algorithm of at least a 128-bit strength. Whenever possible, College data should be stored on College issued and owned removable media.

4. Colleges using key-based encryption systems must provide for an encryption key escrow to ensure present and future college access to encrypted data.
5. Colleges must ensure that only authorized personnel have access to keys used to access confidential information.
6. Proper management control of encryption keys and processes must be ensured when archiving confidential electronic files or documents.

⁶ For a list of validated cryptographic modules and products, refer to the following NIST publication: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm>.

7. Colleges shall develop and enforce policies concerning the storage of the College's confidential data on all portable and removable media devices.
8. Confidential data shall be encrypted only by authorized users when stored on non-College owned devices.
9. Federally protected confidential data shall not be stored on non-College owned/managed devices.
10. All confidential data shall be encrypted when transmitted across wireless or public networks, including transmissions such as FTP and electronic mail. Secure transmission of confidential data shall include the following:
 - Protocol version: Secure Socket Layer (SSL) v3, Transport Layer Security (TLS) v1.1, or Datagram Transport Layer Security (DTLS) v1.0.
 - Key algorithms: 2048 bit RSA or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST).
 - Key hashing: SHA-1 (Note: Industry standard is moving to SHA-2, (e.g., SHA-256), minimum on or around January 2016). MD5, equivalent, or less hashing algorithms shall not be used.
 - Cipher algorithms: 128 bit GCM, SGC, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST). 256 bit is recommended for high confidential data. The RC4 algorithm is not recommended, due to a low vulnerability, until it is fixed but may be used if no other cipher algorithm is supported and a risk assessment has been done. NULL, Anonymous, and Export ciphers shall not be used for confidential data.

GUIDELINES

1. Colleges should consider encrypting all confidential information or data, regardless of the data's storage location, where a compromise of such information would have an adverse impact on the college's services or functions.
2. Due to the greater likelihood for theft or loss, users should be instructed to avoid storing confidential information on portable media and devices whenever possible. If possible, colleges should consider encrypting all mobile communication devices regardless of the confidentiality of the information stored.
3. For satellite locations, or for locations where weaker physical access controls are present, colleges should strongly consider deploying full-disk encryption on desktops that store confidential information.
4. Since a virtual machine image file contains the entire virtual machine (server and all data), colleges should consider securing virtual machine image files using encryption technologies, particularly where the image file is backed up to another storage media outside of the college's control.

ISO 27002 REFERENCES

10.9.1 Electronic commerce

030502 Managing Electronic Keys

Purpose: To ensure that electronic key systems are managed under proper controls.

STANDARD

Colleges using key-based data encryption systems must implement a key escrow system to guarantee college access to encrypted data when needed. Key escrow data shall be routinely backed up. Recovery procedures must be tested at least annually to ensure college access and availability to encrypted data.

When a college implements an electronic key system, it must establish proper controls to protect the key and the data encrypted. The system must be designed so that no single person has full knowledge of any single key. The system design must also ensure the following:

1. Separation of duties or dual control procedures are enforced.
2. Any theft or loss of electronic keys results in the notification of management.
3. All keys are protected against modification, substitution, and destruction, and secret/private keys are protected against unauthorized disclosure.
4. Cryptographic keys are replaced or retired when keys have reached the end of their life or the integrity of the key has been weakened or compromised.
5. Physical protection is employed to protect equipment used to synchronize, store and archive keys.
6. An electronic key management and recovery system, including all relevant key escrow procedures, is documented and in place. This shall be handled through key escrow procedures.
7. Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities.
8. Encrypted data are recoverable, at any point in time, even when the person(s) who encrypted the data is no longer available.

Colleges shall use strong cryptographic keys when protecting confidential data. Colleges also must comply with the applicable regulations established by the North Carolina Secretary of State.

ISO 27002 REFERENCES

- 12.3.1 Policy on the use of cryptographic controls
 - 12.3.5 Key management
-

Section 06 E-Commerce Issues

030601 Configuring E-Commerce Systems

Purpose: To protect College e-commerce sites by minimizing risks.

STANDARD

A college's e-commerce website(s) must be configured with technical controls that minimize the risk of misuse of the site and its supporting technology. The configuration shall ensure that if any confidential data are captured on the site, it is further secured against unauthorized access and/or disclosure.

The configuration of e-commerce Web sites shall include the following:

1. Removal of all sample files included with the default installation.
2. Disabling of unnecessary services and applications.
3. Application of current application and operating system patches, within business constraints.
4. Establishment of user accounts that are set to the least level of privilege that job duties require.
5. Maintenance of operating systems in accordance with approved college information technology security requirements.
6. Restriction of the use of root/administrator privilege to only when required to perform duties.
7. Establishment of normal change controls and maintenance cycles for resources.
8. Logging of systems and protecting applications through access control methods.
9. Use of secure channels, such as VPN, for administrative purposes.
10. A secure physical environment for e-commerce servers.

GUIDELINES

When implementing e-commerce applications, colleges should consider using the following:

1. End-to-end encryption while data are in transit, if applicable.
2. Encryption while data are at rest.
3. Limited trust relationships between systems.

ISO 27002 REFERENCES

10.9.1 Electronic commerce

030602 Using External Service Providers for E-Commerce

Purpose: To protect the College's data when using external service providers for e-commerce solutions.

STANDARD

1. When colleges contract with external service providers for e-commerce services, the services shall be governed by a formal agreement.
2. In order to support service delivery, the agreements shall contain, or incorporate by reference, all of the relevant security requirements necessary to ensure compliance with the statewide information security standards, the college's record retention schedules, its security policies, and its business continuity requirements.

ISO 27002 REFERENCES

6.2.1 Identification of risks related to external parties

6.2.3 Addressing security in third party agreements

10.9.1 Electronic commerce

12.5.5 Outsourced software development

Section 07 Wireless Networks

030701 Wireless Networks

Purpose: To prevent unauthorized access to information and to College information technology systems through eavesdropping on electronic signals, specifically IEEE 802.11 wireless communications with the North Carolina Community College Network or its components.

STANDARD

All Institutes for Electrical and Electronics Engineers (IEEE) 802.11 wireless network access points on the College Network shall have the following security measures implemented to prevent electronic eavesdropping by unauthorized personnel:

- **Physical access**
 - All network access points (APs) and related equipment such as base stations and cabling supporting wireless networks shall be secured with locking mechanisms or kept in an area where access is restricted to authorized personnel.
 - The reset function on APs shall be used only by and accessible only to authorized personnel.
- **Network access**

- APs shall be segmented from a college's internal wired local area network (LAN).
 - The Service Set Identifier (SSID) shall be changed from the default value.
 - The SSID may indicate the name of the college. The SSID name should be communicated to college employees utilizing the wireless network to ensure they are connecting to the college network and not a rogue access point attempting to impersonate the official college wireless network.
 - A device must be prevented from connecting to a wireless network unless it can provide the correct SSID.
- **System access**
 - Every device used to access the College Network over an IEEE 802.11 wireless connection shall have a personal firewall (software or hardware) and up-to-date antivirus software. Devices incapable of running antivirus or personal firewall software, such as personal digital assistants (PDAs) and radio frequency identification (RFID) tags, shall be exempt from this requirement.
 - All access points shall require a password to access its administrative features. This password shall be stored and transmitted in an encrypted format.
 - The ad hoc mode for IEEE 802.11, also referred to as peer-to-peer mode or Independent Basic Service Set (IBSS), shall be disabled. The ad hoc mode shall be allowed in the narrow situation in which an emergency temporary network is required.
 - Every device used to access the College Network over an 802.11 wireless connection shall, when not in use for short periods of time, be locked (via operating system safeguard features) and shall be turned off when not in use for extended periods of time, unless the device is designed to provide or utilize continuous network connectivity. Such items might include wireless cameras, RFID tag readers and other portable wireless devices.
 - If supported, auditing features on wireless devices shall be enabled and the audits reviewed periodically by designated staff.
 - **Authentication**
 - Except for college approved guest access, all wireless access to the College Network via an 802.11 wireless network shall be authenticated by requiring the user to supply the appropriate credentials as supported by the Wi-Fi directly or via the Extensible Authentication Protocol (EAP) extensions.
 - Where a documented business case exists, user devices may authenticate using compliant service accounts but must require a user to re-authenticate to the Wi-Fi once the user has authenticated to the device.
 - Additional authentication shall also be performed through such technologies as Secure Sockets Layer (SSL), Secure Shell (SSH), or Virtual Private Network (VPN) when a LAN is extended or a wide area network (WAN) is created using 802.11 wireless technology.
 - 802.1x credentials for individual users shall be deactivated in accordance with a college's user management policy or within twenty-four (24) hours of notification of a status change (for example, employee termination or change in job function).
 - College approved guest access shall give users access to only the Internet and shall use a captive portal that at least requires the guest users to agree to terms of service and states user activity on the wireless network is monitored.
 - **Encryption**
 - Depending on the type of information traversing a wireless LAN, encryption is required at varying levels as noted in the section below on wireless LAN defense-in-depth architecture. At a minimum, public information requires Wi-Fi Protected Access (WPA) encryption and confidential data require

802.11i (WPA2)-compliant Advanced Encryption Standard (AES) encryption. End-to-end encryption is highly recommended for the confidential data classification.

- Wired Equivalent Privacy (WEP) shall not be used for wireless security. If WPA is used, the highest level of encryption supported on the device shall be enabled.
- If the Temporal Key Integrity Protocol (TKIP) is the highest level of encryption available for WPA, then WPA2 shall be used.
- When WPA2 is used, AES encryption shall be enabled and shall be no less than 128 bits.
- WPA2 (802.11i) encryption must use TKIP, Counter Mode CBC-MAC Protocol (CCMP), or other IEEE- or NIST-approved key exchange mechanism.
- When end-to-end encryption is required across both an 802.11 wireless and a wired network, then in addition to WPA2 (802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include SSL, SSH, IP Security (IPSec) and VPN tunnels.
- Pre-shared keys shall be strong in nature, randomly generated and redistributed to users at least quarterly to protect against unauthorized shared-key distribution or other possible key exposure situations. Pre-shared keys sent by email shall be encrypted.
- **Wireless system management**
 - Simple Network Management Protocol (SNMP) shall be disabled if not required for network management purposes.
 - If required for network management purposes, SNMP shall be read-only, with appropriate access controls that prohibit wireless devices from requesting and retrieving information.
 - If SNMP is required for dynamic reconfiguration of access points to address AP failures and rogue AP's, the SNMP protocol used shall adhere to SNMP version 3 standards and take place only on the wired side of the network.
 - Predefined community strings such as *public* and *private* shall be removed.
 - The latest version of SNMP supported by both device and management software tools shall be implemented and support for earlier versions of SNMP disabled. Devices capable of using SNMP version 3 shall do so, SNMP version 2 may be used until devices are capable of running version 3.
- **WAN connections**
 - Authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.
- **Audit**
 - Colleges using 802.11 wireless LANs must enable rogue access point detection in the management software of the WLAN, if available. If automatic rogue access point detection is not available, the organization must search their sites using wireless sniffers or vulnerability assessment scans and operating system detection at least quarterly to ensure that only authorized wireless access points are in place.
 - The management system shall monitor the airspace in and around college facilities for unauthorized access points and ad hoc networks that are attached to the college's network. If unauthorized devices are found, the management system shall allow personnel to take appropriate steps toward containment.

○ **Wireless LAN defense-in-depth architecture**

Access	Isolated WLAN	Credential Management	Rotating SSID/PSK	MAC ACL	WPA w/ Strong PSK	802.11i w/ Strong PSK	802.11i w/ 802.1x*	Encryption	VPN	Personal Firewall + AV **
Public Citizens										
Open WLAN for On-Site Citizen Use	Firewall***	SSID	Required	—	—	—	—	—	—	—

Public Information	WLAN Gateway	PSK	Required	Optional	Minimum	Recommended	—	Required	—	Required
Confidential Information	WLAN Gateway	802.1x	—	Optional	—	—	Minimum	Required	Recommended	Required
Remote Access										
Access into Agency Network from Wi-Fi Hot Spot by College Employees/Contractors	—	VPN	—	—	—	—	—	—	Required	Required

* Third-party or vendor-specific WLAN security solutions that provide equivalent levels of authentication and encryption are acceptable.

** PDAs and other devices incapable of running personal firewall and antivirus software are exempt from this requirement.

*** Limit traffic from public WLAN to college application needed by citizens, if Internet access is allowed—limit usage with proxy authentication (activity logging is required).

ISO 27002 REFERENCES

13.1.2 Reporting security weaknesses

Chapter 4 – Securing Systems

Section 01 *Purchasing and Installing Software*

040101 Selecting and Purchasing Software

Purpose: To help minimize security risks when purchasing and installing software.

STANDARD

1. Colleges shall ensure that a formal selection process is used to purchase business-critical software necessary to deliver college services. The selection process shall include a review of security measures needed to protect the confidentiality, availability and integrity of the data.
2. Colleges shall ensure that software packages installed on college computers comply with the college's security requirements and meet business needs.
3. Colleges shall ensure that management-approved criteria for the selection of software packages are defined and documented.
4. Colleges shall avoid purchasing software for which minimum support for security patches and updates is not readily available.
5. Colleges shall ensure that all software is licensed and that users adhere to the terms of the end user license agreement. Such adherence is necessary to comply with legislation and to ensure continued vendor support, including vendor provision of patches and updates that address security flaws.
6. Colleges shall comply with State purchasing and contracting laws, standards and policies when negotiating software development contracts with third-party developers. All contracts with vendors for software development must meet the college's functional requirements specification and offer appropriate product support.
7. Colleges shall initiate formal contracts defining third-party access to the organization's information-processing facilities. Such contracts shall include or refer to all security requirements and expected performance and support levels to ensure there is no misunderstanding between parties.
8. Colleges shall ensure that a business justification accompanies all requests for new application systems or software enhancements. The justification shall include the following:
 - a) Documented business needs and expectations of the new system or enhancement.
 - b) Preliminary risk assessment and cost analysis identifying the business value of the assets involved, the security requirements for the system and the compatibility with other system parts.
 - c) Statement of College management approval, prior to procurement.

GUIDELINES

When selecting software, Colleges should consider the following:

1. Colleges should ensure that software under consideration for acquisition works with the majority of peripherals and systems currently in use.
2. Software that has been highly customized introduces higher risks.
3. Old or outdated software typically poses a higher security risk than updated software.

4. The standard office software package is more effective when universally used across State colleges to ensure compatibility among divisions and Colleges.

ISO 27002 REFERENCES

- 6.1.4 Authorization process for information processing facilities
- 6.2.3 Addressing security in third party agreements
- 12.1.1 Security requirements analysis and specification
- 15.1.2 Intellectual property rights (IPR)

040102 Implementing New / Upgraded Software

Purpose: To control security risks involved when implementing new or upgraded software.

STANDARD

1. Colleges shall design security into systems used for data processing so that the systems have the proper technical and procedural security controls.
2. Only standard approved software shall be installed on college owned assets with any deviations being pre-approved by college management and review by an college security administrator assigned to perform the review.
3. Colleges shall mitigate risks of exploitation of covert channels by obtaining third-party applications from reputable sources and by protecting the source code in custom developed applications.
4. Default settings for applications such as email, calendar, and Internet access tools must be set to support a secure environment.
5. Vendor-supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed.
6. Configuration management regarding the installation of software/systems shall include the following:
 - o Maintenance of reliable backups of critical data and programs.
 - o Periodic review of overall controls to determine weaknesses.
 - o Limiting use of software to that which can be verified to be free of harmful code or other destructive aspects.
 - o Retention of complete information about the software, such as the vendor address and telephone number, the license number and version, and update information.
 - o Retention of configuration reports of all installed software, including the operating system. This information will be necessary if the software must be reinstalled later.
 - o Reinstalling software programs only from validated media.
 - o Storing software in a secure, tamper-proof location.

GUIDELINES

New or upgraded software should not be made available to users until the risks are understood. Colleges should develop the following:

1. A step-by-step implementation plan.
2. A software implementation plan that follows change control procedures.
3. Management and user acceptance criteria, including the following:
 - o Desired acceptance tests and their desired results.
 - o Demonstration that computer capacity and performance requirements are not

- adversely affected.
 - Assurance that system security controls will remain effective.
 - Amendments to system documentation and business continuity plans to reflect the software implemented.
 - A rollback plan for use in the event the implementation has unacceptable ramifications.
4. Colleges should also consider the potential impact software upgrades may have on the following:
- Interdependent systems that rely on some functionality of the upgraded system.
 - Overall information security throughout the college's environment.
 - Training needs for business and technical users covering new features and security controls introduced by the upgrade.

ISO 27002 REFERENCES

12.5.1 Change control procedures

040103 Interfacing Applications Software / Systems

Purpose: To mitigate risks associated with linking various software programs or systems together.

STANDARD

Colleges that develop interfacing systems shall ensure that the interfacing systems integrate appropriate security to ensure the confidentiality, as applicable, and the integrity and availability of data. When implementing interfacing applications software/systems, due-diligence measures shall include the following:

1. Utilizing risk management practices to align the business value of the information assets (e.g., database programs to Web applications) being integrated and the potential loss or damage that might result from a security failure.
2. Meeting with developers to determine whether data will need to be reformatted or otherwise modified to meet the needs of the interfacing system.
3. Ensuring that software development procedures begin with planning and have adequate process and management controls.
4. Utilizing qualified software development staff experienced in interfacing systems.

GUIDELINES

Colleges should consider the following issues when analyzing or justifying interfacing system projects:

1. Developing interfacing systems is a technical task that is accompanied by high risks.
2. Application security is more efficient and more cost effective when implemented at the beginning of a project.
3. Prior permission should be secured for the reading of databases not normally under the control of the application that will read them.
4. Interfacing software/systems should be designed so that levels of authority among the software or systems are clearly defined to protect the integrity of data on the interfaced application/system.

ISO 27002 REFERENCES

- 12.1.1 Security requirements analysis and specification
 - 12.2.1 Input data validation
 - 12.5.2 Technical review of operating system changes
-

Section 02 Software Maintenance, Upgrade, and Disposal

040201 Technical Vulnerability Management

Purpose: To establish requirements for an ongoing program of vulnerability mitigation that includes information review and analysis, as well as metrics tracking and reporting.

STANDARD

System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application services and ports are enabled and opened in the system's firewall. Vulnerabilities that threaten the security of the state's network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings.

Vulnerability Risk Ratings

The risk ratings assigned to a vulnerability are as follows:

- High-level Risk: A vulnerability that could cause grave consequences if not addressed and remediated immediately. This type of vulnerability is present within the most sensitive portions of the network or IT asset, as identified by the data owner. This vulnerability could cause functionality to cease or control of the network or IT asset to be gained by an intruder.
- Medium-level Risk: A vulnerability that should be addressed within the near future. Urgency in correcting this type of vulnerability still exists; however, the vulnerability may be either a more difficult exploit to perform or of lesser concern to the data owner.
- Low-level Risk: A vulnerability that should be fixed; however, it is unlikely that this vulnerability alone would allow the network or IT asset to be exploited and/or it is of little consequence to the data owner. Vulnerabilities of this nature are common among most networks and IT assets and usually involve a simple patch to remedy the problem. These patches can also be defined as enhancements to the network or IT asset.

Vulnerability Mitigation

1. Mitigation timeframes for identified or assessed vulnerabilities shall be based on the assigned Vulnerability Risk Rating:
 - "High-level risk" vulnerabilities must be mitigated as soon as possible. It is recommended that "High-level risk" vulnerabilities be mitigated within 7 days, but must be remediated within 21 days.
 - "Medium-level risk" vulnerabilities must be mitigated within thirty (30) days.
 - "Low-level risk" vulnerabilities must be mitigated within ninety (90) days.
2. College vulnerability mitigation plans must specify, at a minimum, the proposed resolution to address identified vulnerabilities, required tasks necessary to affect

changes, and the assignment of the required tasks to appropriate personnel.

3. Vulnerability exceptions are permitted in documented cases where a vulnerability has been identified but a patch is not currently available. When a vulnerability risk is 'high-level' and no patch is available, steps must be taken to mitigate the risk through other methods (e.g., workarounds, firewalls, router access control lists). A patch needs to be applied when it becomes available. When a 'high-level' risk vulnerability cannot be totally mitigated within the requisite time frame, Colleges need to notify College management and the College Chief Information Officer of the condition.
4. Appropriate testing and assessment activities shall be performed after vulnerability mitigation plans have been executed to verify and validate that the vulnerabilities have been successfully addressed.
5. Appropriate notification shall be provided after vulnerability mitigation plans have been executed.
6. In the event of a zero-day vulnerability, a situation where an exploit is used before the developer of the software knows about the vulnerability, Colleges shall mitigate the vulnerability immediately, if possible, and apply patches as soon as possible after the vendor provides them.

Vulnerability Information Review and Analysis

1. Relevant vulnerability information from appropriate vendors, third party research, and public domain resources shall be reviewed on a regular basis, per the college's policies and procedures.
2. Relevant vulnerability information, as discovered, shall be distributed to the appropriate college employees, including Information Security.
3. Appropriate College personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

Requirements for Compliance

1. Colleges must develop procedures to ensure the timely and consistent use of security patches and use a consistent vulnerability naming scheme to mitigate the impact of vulnerabilities in systems.
2. Colleges shall have an explicit and documented patching and vulnerability policy, as well as a systematic, accountable, and documented set of processes and procedures for handling patches.
3. The patching and vulnerability policy shall specify techniques an organization will use to monitor for new patches and vulnerabilities and personnel who will be responsible for such monitoring.
4. An organization's patching process shall define a method for deciding which systems are patched and which patches are installed first, as well as the method for testing and safely installing patches.
5. A College process for handling patches shall include the following:
 - Using organizational inventories
 - Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring (See <http://cve.mitre.org>)
 - Patch prioritization techniques
 - Organizational patch databases
 - Patch testing, patch distribution, patch application verification, patch training,

automated patch deployment, and automatic updating of applications.

6. Colleges shall develop and maintain a list of sources of information about security problems and software updates for the system and application software.
7. Colleges shall establish a procedure for monitoring those information sources.
8. Colleges shall evaluate updates for applicability to the systems.
9. Colleges shall plan the installation of applicable updates.
10. Colleges shall install updates using a documented plan.
11. Colleges shall deploy new computers with up-to-date software.
12. After making any changes in a system's configuration or its information content, Colleges shall create new cryptographic checksums or other integrity-checking baseline information for the system.

ISO 27002 REFERENCES

12.6.1 Control of technical vulnerabilities

040202 Applying Patches to Software

Purpose: To protect from risks associated with software patches.

STANDARD

Colleges shall develop procedures to ensure the timely and consistent use of security patches. A consistent vulnerability-naming scheme to mitigate the impact of vulnerabilities in computer systems must be used across the college and State. Colleges shall ensure the following:

1. System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.
2. Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.
3. The patch application process follows formal change control procedures that include the following controls prior to installation:
 - Verification of the source of the patch.
 - Verification of the need for the patch.
 - Testing of the patch.
 - Documenting of the processes and procedures.

GUIDELINES

When applying software patches, Colleges should consider the following:

1. Ignored and unpatched software vulnerabilities can represent a great risk to the security of State information assets.
2. Patch application is no different than introducing a new or updated program into the system and carries the same potential for damage and system compromise.
3. Appropriate updates should be made to both system documentation and business

continuity plans.

ISO 27002 REFERENCES

12.5.1 Change control procedures

040203 Upgrading Software

Purpose: To protect against the security risks associated with software upgrades.

STANDARD

1. Colleges shall implement vendor-recommended upgrades for use in a production environment only after the following conditions are met:
 - Security is not compromised by any upgrade and security controls are in place.
 - There is a business justification that warrants software upgrades.
 - Qualified College staff members validate the technical need for a vendor-recommended upgrade.
2. Software upgrades shall not be installed in a production environment (mainframes, servers and desktop computers) until the following conditions are met:
 - Qualified personnel certify that the upgrade has passed acceptance testing.
 - System security controls remain effective.
 - Computer capacity and performance requirements are not adversely affected.
 - System documentation and business continuity plans are amended to reflect upgrade.
 - A rollback plan has been developed in the event the upgrade has unacceptable ramifications.
 - Management has agreed that the desired acceptance criteria have been met.

GUIDELINES

1. Colleges should consider the potential impact that vendor-recommended upgrades may have on the following:
 - The potential for information security vulnerabilities inherent in new or upgraded software.
 - Increased technical requirements and costs associated with a software upgrade.
 - The balance between the need to continue current operations and the understanding that certain levels of software currency must be maintained to receive continued vendor support for the software.
 - The possibility that systems that rely on functionality provided by the system that is being upgraded may prove to be incompatible with the upgrade.
 - Additional training necessary for business and technical users to cover new features and security controls introduced by the upgrade.
2. Colleges should remember that software upgrades may have impacts on other systems. The change control process should not be classified as complete until team members can verify the following:
 - There are not any additional risks imposed on information security throughout the college's environment.
 - There are not any interdependent systems that have had loss of functionality due

to the upgraded software.

ISO 27002 REFERENCES

- 10.3.2 System acceptance
- 12.5.1 Change control procedures

040204 Supporting Application Software

Purpose: To protect application software by providing adequate technical support.

STANDARD

Colleges shall provide adequate levels of technical support necessary to support business processes, which includes appropriate vendor support for purchased software. Levels of technical support shall require the following:

- Security measures are used to mitigate risks and security vulnerabilities.
- Software issues are handled efficiently.
- Software problems are resolved in a timely fashion.

GUIDELINES

If one is available, a College's primary avenue for user software support should be a help desk. The help desk should have formal software problem resolution procedures that promote the following best practices:

- Tracking problems from initial reporting through to resolution.
- Monitoring status of reported problems and confirming that satisfactory resolutions have been achieved.
- Providing reports and metrics for system development and software support management (*i.e.*, for trend analysis, lessons learned, etc.)
- Maintaining a pool of software technicians with the appropriate skill sets to assist with software problem resolution.
- Building a database of institutional knowledge that reflects trends, common problems, etc., and sharing it with other Colleges.

ISO 27002 REFERENCES

- 6.2.3 Addressing security in third party agreements
- 12.1 Security requirements of information systems
- 12.5 Security in development and support processes

040205 Operating System Software Upgrades

Purpose: To mitigate risks associated with upgrading operating systems.

STANDARD

Operating system (OS) upgrades shall be carefully planned, executed and documented as a project. Colleges involved in operating system software upgrades to systems shall perform the following steps before commencement of the upgrade project:

1. Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade.
2. Locate change control processes and procedures.

3. Document agreement of technical staff and management to acceptance criteria.
4. Document that qualified personnel have certified the upgrade and that it has passed user acceptance testing.
5. Establish a rollback plan in the event the upgrade has unacceptable ramifications.

GUIDELINES

Colleges should consider the following security issues when upgrading an OS:

1. An OS failure can have a cascading adverse effect on other systems and perhaps even the network.
2. System documentation and business continuity plans should be amended to reflect the OS upgrade.
3. Since OS upgrades typically affect many systems within a College, such upgrades should be part of the annual maintenance plan/budget. OS upgrade testing and review cycles should also be included in this budget.

ISO 27002 REFERENCES

12.5.2 Technical review of applications after operating system changes

040206 Support for Operating Systems

Purpose: To provide maximum availability, security and stability of operating systems.

STANDARD

Each College shall ensure that the operating systems used to run the production environment are regularly monitored for security risks and maintained in approved secure configurations to support business operations.

GUIDELINES

Colleges should consider the following issues when supporting operating systems:

1. New security risks and vulnerabilities are discovered from time to time that may require the operating system configuration to be updated to mitigate the identified risks and vulnerabilities.
2. Periodic maintenance improves the performance of operating systems (e.g., hard drive defragmentation).
3. The operating systems on servers, minicomputers and mainframes usually require daily maintenance tasks and routines that may be initiated manually as a result of an alert or logged event or may be scripted to run automatically when a certain threshold or limit is exceeded.
4. Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure that:
 - Maintenance tasks continue to function as expected.
 - Operating systems continue to operate within accepted thresholds.
 - System security is not being compromised by maintenance tasks.
 - Maintenance tasks do not adversely affect computer capacity or performance.

ISO 27002 REFERENCES

12.5.2 Technical review of applications after operating system changes

040207 Recording and Reporting Software Faults

Purpose: To identify and correct software faults efficiently and effectively.

STANDARD

1. Each College are strongly encouraged to designate a quality control team that consistently checks for software faults and that is responsible for reporting them software support and maintenance. The local College Core Team may be sued for this purpose.
2. Software faults that pose a security risk shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability.
3. Colleges shall include the following security issues when establishing or reviewing software support procedures:
 - Software fault-reporting procedures shall be taught and encouraged through security training and awareness programs.
 - Colleges shall designate a quality control team that consistently checks for faults and that is responsible for reporting them to software support.
 - Colleges shall use a formal recording system for the following:
 - Tracks faults from initial reporting through to resolution.
 - Monitors the status of reported faults and confirms that satisfactory resolutions have been achieved.
 - Provides reports and metrics for system development and software support management.
4. While faults are being tracked through to resolution, research shall also be conducted to ensure no IT security controls have been compromised and resolution activities have been appropriately authorized.

ISO 27002 REFERENCES

10.10.5 Fault logging

040208 Disposing of Software

Purpose: To protect information by using secure software disposal techniques.

STANDARD

Software removal and disposal may be initiated only after a formal decision to stop using the software has been made by senior management and steps have been taken to protect the information contained in the software application. Before disposal of software, Colleges shall protect information developed using the software by doing the following:

1. Following orderly termination procedures to avoid disruption of business operations.
2. Migrating data to another system or archiving data in accordance with applicable records management regulations and policies for potential future access.
3. Using a State-approved technique to ensure that no data remain on the media (e.g., by incineration, shredding, degaussing or sanitizing of data for use by another application within the organization).
4. Logging the disposal of media containing confidential information to maintain an audit trail.

GUIDELINES

Colleges should consider the following issues and controls when involved in software disposal:

1. Emphasis should be given to the proper preservation of the data processed by the system so that:
 - Sufficient vital information about the system is preserved so that some or all of the system may be reactivated in the future.
 - The backup strategy that is utilized is able to recover the actual program and program files to enable retrieval or access of data stored in the application.
2. Software media storage and disposal should follow industry best practices and vendor and manufacturer specifications.

ISO 27002 REFERENCES

10.7.2 Disposal of media

Section 03 *Controlling Software Code*

040301 Managing Operational Program Libraries

Purpose: To protect college software by restricting access to operational program libraries.

STANDARD

Managing the directories or locations used to store production (live) software and configuration files is an integral part of risk management. To prevent the corruption of information systems or the disruption of business operations, Colleges shall ensure that their program libraries are adequately protected. Colleges shall restrict access to operating system and operational or production application software/program libraries to designated staff only.

GUIDELINES

Appropriate technical controls and procedures for protecting program libraries should be designed to prevent unauthorized use (intentional and unintentional). Colleges should consider processes, controls or best practices. Refer to the guidelines in 040405 - Managing Change Control Procedures.

ISO 27002 REFERENCES

12.4.1 Control of operational software

12.5.1 Change control procedures

040302 Managing Program Source Libraries

Purpose: To protect the integrity of business operations software by managing source code libraries.

STANDARD

Colleges shall exercise strict control over program source libraries by implementing the following:

1. A combination of technical access controls and robust procedures to restrict access to source program libraries to authorized personnel only.

2. A system to keep production source code and development source code libraries separate and backed up.
3. Formal change control procedures
4. Comprehensive audit trails

GUIDELINES

Formal change control procedures can aid in the investigation of changes made to college program source libraries. Colleges should establish a regular review of audit reports and event logs to ensure that incidents that have potentially compromised program source libraries are detected.

ISO 27002 REFERENCES

- 12.4.3 Access control to program source code
- 12.5.1 Change control procedures

040303 Controlling Software Code during Software Development

Purpose: To protect information systems from corruption by controlling software change.

STANDARD

When developing or modifying software, Colleges shall establish a change control management process that implements the following rules:

1. Authorization is required to initiate or make changes to software.
2. Change control procedures that govern changes to system software are defined and utilized.
3. All changes must be tested in a test environment and must pass acceptance testing prior to moving into a live or production environment.
4. Senior management may only authorize emergency exceptions to this policy to avoid imminent failure of business operations.
5. Colleges shall maintain and control current electronic and hard copy listings of application/program source code that runs on college systems.
 - Program listings are the primary tool for identifying system problems. Loss or unavailability of a listing could delay problem identification and resolution, the consequence of which could put college services at risk.
 - Unauthorized access to program listings compromises system security by making exact logic and system routines available for exploitation.

GUIDELINES

1. Many System Development Lifecycle (SDLC) models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle.
2. A general SDLC should include the following phases:
 - Initiation
 - Acquisition / Development

- Implementation / Assessment
- Operations / Maintenance
- Sunset (disposition)

Each of these five phases should include a minimum set of tasks to incorporate security in the system development process. Including security early in the SDLC will usually result in less expensive and more effective security than retrofitting security into an operational system. (More information regarding the Software Development Life Cycle (SDLC) may be found in the NIST publication “Information Security in the SDLC Brochure.”)

The following questions should be addressed in determining the security controls that will be required for a system:

- How critical is the system in meeting the organization’s mission?
- What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?
- What regulations, statutes, and policies are applicable in determining what is to be protected?
- What are the threats that are applicable in the environment where the system will be operational?

ISO 27002 REFERENCES

- 10.7.4 Security of system documentation
- 12.4.3 Access control of program source code
- 12.5.1 Change control procedures
- 12.5.3 Restrictions on changes to software packages

040304 Controlling Old Versions of Programs

Purpose: To protect system integrity with software version control.

STANDARD

Colleges shall control old versions of programs by establishing the following:

1. Comprehensive procedures for auditing removals or updates to program libraries.
2. Formal change control procedures to process the application code used to write programs within college systems when that code has been superseded or discontinued.

GUIDELINES

The following information security issues should be considered when implementing a College policy in regards to old versions of programs:

1. When application code within College systems has been superseded or discontinued, Colleges should be prepared to roll back or access the superseded or discontinued code if required, because decommissioned code must often be resurrected if major bugs are found in the newer version.
2. Version control is essential because there is a real danger of losing the latest program enhancements or of causing the failure of other systems that depend on recently added features if an older version of a program is confused with a newer version.

ISO 27002 REFERENCES

- 12.4.1 Control of operational software
- 12.5.1 Change control procedures

Section 04 Software and System Development

040401 Software Development

Purpose: To protect production/operational software during all phases of the development process.

STANDARD

Each College shall follow and manage a formal development process when it develops software. Safeguards shall include the following:

1. A Standard Software Development Life Cycle (SDLC) that is managed by a project office/team.
2. A combination of appropriate:
 - Technical access controls.
 - Restricted privilege allocations.
 - Robust procedures which include security checkpoints in each cycle.

GUIDELINES

Colleges should address the following issues when updating or formalizing development processes:

1. Potential compromise to production systems.
2. The threat of insertion of malicious code within software.
3. Disruption of live operations.
4. Confidentiality, criticality and value of the systems and data to the college and public.

ISO 27002 REFERENCES

- 10.1.4 Separation of development, test, and operational facilities
- 12.1.1 Security requirements analysis and specifications
- 12.5.1 Change control procedures

040402 Making Emergency Amendments to Software

Purpose: To protect production software during emergency modifications.

STANDARD

1. College personnel must fully justify their requests for emergency modifications to software and must obtain senior management authorization.
2. College personnel making emergency modifications must not deviate from the college's change control procedures.

GUIDELINES

1. Each College should establish an emergency procedure that personnel agree to follow if it becomes necessary to amend the live software environment quickly. The procedure should include management approval.
2. When developing emergency change control procedures, Colleges should consider

how these procedures will deviate from normal everyday change control procedures and best practices. Refer to the guidelines in 040405 - Managing Change Control Procedures.

ISO 27002 REFERENCES

12.5.1 Change control procedures

040403 Establishing Ownership for System Enhancements

Purpose: To protect systems by defining responsibilities and authority levels required for system change.

STANDARD

1. Colleges shall establish custodians for each system who will have responsibility for all system enhancements.
2. All proposed system enhancements must be driven by the business needs of the College and supported by a business case that has both user and management acceptance.
3. Ownership for any such system enhancements ultimately lies with the system custodian and requires his/her commitment and personal involvement.

GUIDELINES

Allocation of information security responsibilities should be an integral part of each College's information security program. Information security policy and job descriptions should provide general guidance on the various security roles and responsibilities within the college. However, in the case of individual systems, the system custodian and a designated alternate manager should have more detailed guidelines governing enhancements to the system(s) for which they are ultimately responsible.

Colleges should consider the following areas when they are defining security job responsibilities for system custodians and other managers with focused security positions (e.g., security analysts and business continuity planners):

1. Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible.
2. Clearly defining and documenting the agreed-upon authorization levels that the position holder will have to make enhancements, modify source code, promote updated code, etc.
3. Documenting the following for each asset:
 - Management's assignment of system responsibility to a specific manager/custodian.
 - Manager/custodian acceptance of responsibility for the system.
4. Detailed description of manager/custodian responsibilities.

ISO 27002 REFERENCES

6.1.3 Allocation of Information Security responsibilities

040404 Justifying New System Development

Purpose: To require business case justification of custom system development projects.

STANDARD

When proposing the development of custom software, Colleges shall make a strong business case that:

1. Supports the rationale for not enhancing current systems;
2. Demonstrates the inadequacies of packaged solutions; and
3. Justifies the creation of custom software.

Colleges shall consider custom software development only when the following conditions are met:

1. A strong business case demonstrates that business requirements can be met only with the proposed software.
2. Existing software cannot be economically updated to fulfill these business requirements.
3. No suitable packaged solution can be found.
4. The development is supported by College management.
5. The College has adequate resources to support the estimated project timeline.
6. The College can support and maintain the product during its required lifetime.

GUIDELINES

Developing a system to meet a business need is a major decision that frequently carries significant risk. Colleges should consider the following issues when weighing the decision to outsource a major system development effort:

1. High risk of failure - Signing a contract with a vendor for outsourced development can be high risk and may pose a substantial risk to the college.
2. Senior management support and financial backing - When projects last more than 12 months, there is an increased potential for a reduction in both commitment and financial support that could have an impact not only on the project but on business operations as well.

ISO 27002 REFERENCES

12.1.1 Security requirements analysis and specifications

040405 Managing Change Control Procedures

Purpose: To safeguard production systems during modification.

STANDARD

Each College shall manage changes to its systems and application programs to protect the systems and programs from failure as well as security breaches. Adequate management of system change control processes shall require the following:

1. Enforcement of formal change control procedures.

2. Proper authorization and approvals at all levels.
3. Successful testing of updates and new programs prior to their being moved into a live environment.
4. Updates addressing significant security vulnerabilities shall be prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.
5. Whenever an update is implemented, the application system the update affects shall be tested to ensure that business operations and security controls perform as expected.

GUIDELINES

Managing change control procedures is an integral part of risk management.

Each College should enforce strict change control procedures because application software fundamentally affects the college's ability to do its work and deliver services. Inadequate or poorly managed change control procedures can result in compromises and failures not only in the operational system being modified, but also in other systems that are dependent on the new functionality provided by the updated system.

When possible, Colleges should integrate application change control and operational change control procedures. This effort should include the following processes, controls, and best practices:

1. Controls and approval levels for updating libraries.
2. Requiring formal agreement and approval for any changes.
3. Restricting library content.
4. Restricting programmers' access to only those parts of the system necessary for their work.
5. Version control for each application.
6. Tying program documentation updates to source code updates.
7. Audit logs that track all:
 - Accesses to libraries.
 - Change requests.
 - Copying and use of source code.
 - Updates posted to libraries.
 - Defining job responsibilities/restrictions and establishing authority levels for the following:
 - Program librarian(s).
 - Developers (*i.e.*, should neither test their own code nor promote it into production).
 - Other IT staff.
8. Personnel authorized to make or submit changes to the source library (*i.e.*, a program librarian should be appointed for each major application to control check-in/check-out).
9. Rollback procedures designed to recover to old, stable version of programs.

ISO 27002 REFERENCES

040406 Separating System Development and Operations

Purpose: To reduce the risk of college system misuse and fraud by segregation of duties

STANDARD

Separation of duties is an integral part of a successful information security program that reduces the risk of accidental or deliberate system misuse. Separation of duties reduces opportunities for unauthorized modification or misuse of information by segregating the management and execution of certain duties or areas of responsibility. Although smaller Colleges without the manpower to staff separate sections or groups will find this method of control more challenging to implement, the principle should be applied to the extent possible. College management must ensure that there is proper segregation of duties to reduce the risk of college system misuse and fraud.

1. System administration and system auditing shall be performed by different personnel.
2. System development and system change management shall be performed by different personnel.
3. System operations and system security administration shall be performed by different personnel.
4. Insofar as is possible, security administration and security audit shall be performed by different personnel.
5. Administrators of multi-user systems must have at least two user credentials. One of these user credentials must provide privileged access, with all activities logged; the other must be a normal user credential for performing the day-to-day work of an ordinary user.

GUIDELINES

Colleges should consider taking the following actions in regard to information security issues when implementing a separation-of-duties policy:

1. When separation of duties is difficult, consider other controls such as:
 - a. Monitoring of activities
 - b. Audit trails
 - c. Management supervision
2. Keep the responsibility for security audit separate from other audit powers.
3. Identify and segregate activities that require collusion to defraud (e.g., exercising a purchase order and verifying receipt of goods).
4. Consider dual control in instances in which collusion might allow the college to be defrauded.
5. Prohibit development staffs (who have powerful privileges in the development environment) from extending their administrative privileges to the operational environment.

ISO 27002 REFERENCES

- 10.1.3 Segregation of duties
- 10.1.4 Separation of development, test, and operational facilities

040407 Systems Documentation

Purpose: To protect information technology assets by maintaining comprehensive system documentation.

STANDARD

1. Whether the system is developed or updated by in-house staff or by a third-party vendor, Colleges shall ensure that each new or updated system includes adequate system documentation.
2. Colleges shall create, manage and secure system documentation libraries or data stores that are available at all times but shall restrict access to authorized personnel only.
3. Colleges shall ensure that system documentation is readily available to support the staff responsible for operating, securing and maintaining new and updated systems.
4. Colleges shall control system documentation to ensure that it is current and available for purposes such as auditing, troubleshooting and staff turnover. Examples of system documentation include descriptions of applications processes, procedures, data structures and authorization processes.
5. The following controls must be considered to protect and maintain system documentation:
 - Internal system documentation must be stored securely and in an area known by management.
 - Access to internal system documentation must be limited and be authorized by management.
 - Documentation and user procedures shall be updated to reflect changes based on the modification of applications, data structures and/or authorization processes.

GUIDELINES

Colleges should consider the following information security issues as they define their system documentation management strategies:

1. A lack of adequate documentation, whether because the documentation is missing, out of date, or simply unavailable, can:
 - Greatly increase the risk of a serious incident.
 - Compromise performance of routine maintenance, especially as the complexity of the system increases.
 - Increase the likelihood that errors and omissions will slip through peer reviews of source code into system testing and perhaps beyond into user acceptance testing.
2. System documentation should be a required component of the system's inventory of assets (along with the physical and software assets that constitute the system).
3. System documentation should be protected from unauthorized access by keeping it stored securely and by utilizing an access list limited to a small number of staff, all of whom have been authorized by the system custodian.
4. A copy of system documentation should be maintained for disaster recovery and business continuity and stored off site.

ISO 27002 REFERENCES

7.1.1 Inventory of assets

- 10.7.4 Security of system documentation
- 12.5.1 Change control procedures

Section 05 Software and Systems Operations

040501 Managing System Operations and System Administration

Purpose: To ensure that College systems are operated and administered using documented procedures that are efficient and effective in protecting the college's data.

STANDARD

1. For IT transaction records, which include access and audit logs related to the activities of IT systems, Colleges must establish and maintain an adequate system of controls. For financial transactions and accounting records the standard is addressed by the North Carolina Office of the State Controller.
2. Colleges shall employ and document controls to provide for the management of system operations and system administration. To minimize the risk of corruption to operating systems or integrated applications, the controls shall include, but not necessarily be limited to, the following:
 - Develop and document daily operational security procedures.
 - Assigned staff shall perform the updating of the operating systems and program/application backups.
 - Operating system software patches shall be applied only after reasonable testing verifies full functionality.
 - Physical or logical access shall be given to suppliers for support purposes only when necessary and with documented management approval. The suppliers' activities shall be continuously monitored.
 - Vendor-supplied software used in operating systems shall be maintained at a level supported by the vendor.
3. Colleges must clearly define security responsibilities for system administrators, who shall protect their assigned information technology resources and the information contained on those resources.
4. Colleges must also provide appropriate training for their system administrators.
5. System administrators shall do the following:
 - Ensure that user access rights and privileges are clearly defined, documented and reviewed for appropriateness.
 - Consider the risk of exposure when administering system resources.
 - Take reasonable actions to ensure the authorized and acceptable use of data, networks and communications transiting the system or network.

ISO 27002 REFERENCES

- 6.1.3 Allocation of Information Security responsibilities
- 10.10.4 Administrator and operator logs
- 12.2.2 Control of internal processing
- 12.4.1 Control of operational software

040503 Log-on Procedures

Purpose: To reduce the risk of unauthorized system access.

STANDARD

1. Colleges shall develop secure log-on procedures to be applied to all network components, operating systems, applications, and databases that implement a user identification and authentication mechanism. These procedures shall be designed to minimize the risk of unauthorized access.
2. Colleges shall follow the security policies for Managing User Access (020102) and Managing Passwords (020106).
3. Colleges shall display a message to users before or while they are prompted for their user identification and authentication credentials that warns against unauthorized or unlawful use.
4. Colleges shall configure systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds the established limit, the configuration shall either force a time delay before further log-on attempts are allowed or shall disable the user account such that it can only be reactivated by a system or security administrator or an authorized service desk staff member.
5. Information about the system or services shall not be displayed until the log-on process has successfully completed.
6. Log on windows should display a minimal amount of information.
7. The log-on process should not be validated until all log-on data is input. Failing the process as each input field is completed will provide an attacker with information to further the attack.
8. Only generic "log-on failed" messages should be displayed if the user does not complete the log-on process successfully. Do not identify in the message whether the user identification, password, or other information is incorrect.

ISO 27002 REFERENCES

11.5.1 Secure log-on procedures

040504 System Utilities

Purpose: To control the use of system utilities that can bypass or override security controls.

STANDARD

1. Access to system utilities that are run with elevated privileges capable of bypassing or overriding system or application controls shall be strictly limited to users and administrators with a recurring need to run or use those utilities. Other uses of and access to those utilities shall only be granted on a temporary basis.
2. These system utilities shall be segregated from other applications and software such that they can only be accessed by authorized users.

GUIDELINES

1. Colleges should develop procedures for granting and documenting authorization for

specific individuals to use powerful system utilities, whether or not such use is temporary.

2. Use of system utilities should be audited or logged.
3. Colleges should remove or disable system utilities that are not needed.
4. Colleges should consider whether granting authorization for an individual to use a system utility may violate segregation of duties if the utility allows bypassing or overriding of segregation controls. If granting authorization to use a system utility could potentially violate segregation controls, the college shall enact precautions to ensure that this violation does not occur. Detailed auditing or two-person control could provide assurance that segregation of duties is maintained.

ISO 27002 REFERENCES

11.5.4 Use of system utilities

040505 Data Validation Controls

Purpose: To minimize and detect corruption or loss of information in applications.

STANDARD

The design of applications shall ensure that data validation controls are implemented to minimize the risk of processing failures leading to a loss of integrity and to detect any corruption of information through processing errors or deliberate acts.

GUIDELINES

Examples of controls that could be used to ensure data validation are:

1. Carefully controlled add, modify, and delete functions.
2. Implementation of automatic reconciling of balances from run-to-run or system-to-system in systems to compare opening balances against previous closing balances.
3. Requiring that processes fail securely such that no further processing will occur. For example, internal controls in processes should be designed to detect if a process is running out of order or without the proper input and fail without further processing.
4. The maintenance of running hash totals of records or files and the comparison of those records and files to hash totals of backups or recovered records or files. They could also be compared run-to-run or system-to-system to ensure that the end of one transaction period is the same as the beginning of the next.

ISO 27002 REFERENCES

12.3.2 Key management

040506 Data Recovery Controls

Purpose: To correct corrupted data and prevent corruption or loss of data in applications when recovering from system or processing failure.

STANDARD

The design of applications shall ensure that data validation controls are implemented such that Colleges can correct corrupted data. These controls shall also ensure the correct processing of data in the event of recovery from system or processing failure.

GUIDELINES

An example of a method to rebuild corrupted records or files from a last known good state is a transaction log or log of activities. Colleges should take precautions to ensure that the transaction or activity log does not contain the action that corrupted the data in the first place.

ISO 27002 REFERENCES

12.3.2 Key management

040507 Corruption of Data

Purpose: To minimize and detect corruption or loss of information in applications.

STANDARD

The design of applications shall ensure that data validation controls are implemented to minimize the risk of processing failures leading to a loss of integrity and to detect and correct any corruption of information through processing errors or deliberate acts. Colleges shall develop clear policies, standards, and/or procedures to detect, correct, and manage corrupted data files.

GUIDELINES

Examples of controls that could be used to ensure data validation are:

1. Add, modify, and delete functions should be carefully controlled.
2. Automatic reconciling of balances from run-to-run or system-to-system can be implemented in systems to compare opening balances against previous closing balances.
3. Processes should fail securely such that no further processing will occur. For example, internal controls in processes should be designed to detect if a process is running out of order or without the proper input and fail without further processing.
4. Running hash totals of records or files can be maintained and compared to hash totals of backups or recovered records or files. They could also be compared run-to-run or system-to-system to ensure that the end of one transaction period is the same as the beginning of the next.
5. An example of a method to rebuild corrupted records or files from a last known good state is a transaction log or log of activities. Colleges should take precautions to ensure that the transaction or activity log does not contain the action that corrupted the data in the first place.

ISO 27002 REFERENCES

12.2.2 Control of internal processing

040508 Monitoring Error Logs

Purpose: To protect college information technology assets from unintentional and malicious attacks.

STANDARD

Error logs generated by information technology systems shall be regularly monitored and reviewed for abnormalities and shall be:

1. Cross-checked for known security events based on network, size, system type and logical and physical location.
2. Enabled on each device or system on the network, such as servers, firewalls, routers, switches, cache engines, intrusion detection systems (IDSs) and applications, as long as performance requirements are not affected.
3. Monitored on a weekly basis at a minimum.
4. Routinely checked for time and date accuracy. See Standard 030101, Configuring Networks and Configuring Domain Name Servers (DNS), for more on clock synchronization.
5. Retained as required under the College records retention policy or the General Schedule for State College Records, Information Technology Records.
6. Checked against baselines to effectively verify variations from normal work-related activities.

ISO 27002 REFERENCES

- 10.10.1 Audit logging
- 10.10.2 Monitoring system use
- 10.10.3 Protection of log information

040509 Scheduling System Operations

Purpose: To ensure that modifications to information system operations are implemented and maintained properly.

STANDARD

1. To maintain the highest level of system availability and protect the college's infrastructure, maintenance operations must be performed at predetermined, authorized times or on an approved, as-needed basis. Documented operational procedures must be created, implemented and maintained during system operations and take into consideration the following:
 - Computer start up, shutdown, and recovery procedures.
 - Scheduling requirements (length, time frame, etc.).
 - Processes for handling errors and unforeseen issues that may arise during job execution.
 - Contact lists.
 - System restrictions.
 - Instructions for handling output, including failed jobs.
 - Proper media handling and storage.
 - Incident handling and escalation procedures.
 - Configuration management.
 - Patch management.
 - General system hardware and software maintenance.
 - All documentation of operational procedures must be approved by management and reviewed at least annually for accuracy and relevancy.
 - When special or emergency situations make it necessary to perform maintenance operations outside of the normal system operations schedule, these situations must be documented, management must be notified, and the operation processes used must be recorded.

2. Colleges shall develop change control procedures to accommodate resources or events that require changes to system operations.
3. Changes to system baselines require effective communication to ensure that information systems maintain secure operations and avoid lag due to processing consumption and to minimize downtime due to unforeseen problems during such changes.
4. Change control procedures must be documented and followed during the scheduled maintenance windows and take into consideration:
 - Periods of maximum and minimum workflow.
 - The approval and notification process.
 - Interfaces with other applications, systems or processes.
 - External college and departmental interdependencies.
 - Change categories, risk and type.
 - The change request process.
 - Rollback plans and the point of no return.
 - Modifications to change control procedures for special or emergency circumstances.
5. All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy.
6. Upon the completion of a baseline change, the audit change logs must be retained in accordance with the General Schedule for State College Records, Information Technology Records as established by the Government Records Section of the Department of Cultural Resources.

ISO 27002 REFERENCES

- 10.1.1 Documented operating procedures
- 10.1.2 Change management

040510 Monitoring Operational Audit Logs

Purpose: To detect unauthorized activity and to protect the integrity and availability of information systems by monitoring operational audit logs.

STANDARD

1. Colleges shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity.
2. All network components and computer systems used for college operations must have the audit mechanism enabled and shall include logs to record specified audit events.
3. Colleges shall designate staff to regularly review operational audit logs, including system, application and user event logs, for abnormalities.
4. Audit logs of high risk information systems, such as those that process credit card data, shall be reviewed on a daily basis.
5. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to college management.
6. Access to audit logs shall be restricted to only those authorized to view them and the logs shall be protected from unauthorized modifications, and if possible, through the use of file-integrity monitoring or change-detection software.

7. Audit files shall be written to a log server on the internal network and subsequently backed up to a secure location.
8. To the extent possible, audit logs shall include at least the following information when recording system events:
 - User identification
 - Type of event
 - Date and time
 - Success or failure indication
 - Origination of event
 - Identity or name of affected data, system component, or resource
9. Personnel responsible for audit logs must ensure the following:
 - That the college has established a current, reliable baseline that can be compared to audit logs to determine whether any abnormalities are present.
 - That all operational audit logs are retained in accordance with the General Schedule for State College Records, Information Technology Records as established by the Government Records Section of the Department of Cultural Resources.
10. For audit logs on internal college systems and network components, Colleges shall record, at a minimum, the following types of security-related events:
 - User login activity, both failed and successful, including user IDs, log-in date/time, log-out date/time.
 - Unauthorized access attempts to network or system resources, including audit files.
 - Changes to critical application system files.
 - Changes to system security parameters.
 - System start-ups and shut-downs.
 - Application start up, restart and/or shutdown.
 - Attempts to initialize, remove, enable or disable accounts or services.
 - Changes to the auditing function, including enabling or disabling auditing and changing events to be audited.
 - User credential creation and deletion.
 - Attempts to create, remove or set passwords or change system privileges.
 - All uses of special system privileges.
 - System errors and corrective action(s) taken.
 - Failed read-and-write operations on the system directory.
 - All actions taken with administrative privileges.
11. Colleges shall ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations.
12. Colleges shall also ensure that on-line audit logs are backed-up to protected media well before the on-line logs are filled to capacity so that no audit information is lost or overwritten.

ISO 27002 REFERENCES

- 10.10.2 Monitoring system use
- 10.10.4 Administrator and operator logs

040511 Responding to System Faults

Purpose: To properly respond to faults and take corrective action.

STANDARD

1. All users and system administrators shall be responsible for reporting system faults (*i.e.*, problems, errors and incidents) that affect routine operations to the appropriate authorized staff or third-party technician(s).
2. Staff shall describe the fault as clearly and completely as possible, and provide a reason for the fault, if known.
3. College staff shall request that authorized staff or third-party technician(s) log the fault, provide College staff with a tracking or ticket number and implement clear procedures for handling the reported fault(s).

ISO 27002 REFERENCES

10.10.5 Fault logging

Section 06 Testing & Training

040601 Using Live Data for Testing

Purpose: To protect the integrity and confidentiality of data during system development and testing.

STANDARD

1. Colleges shall permit the use of production data during the testing of new systems or systems changes only when no other alternative allows for the validation of the functions and when permitted by other regulations and policies.
2. Confidential data shall not be used for testing purposes.

If production data is used for testing, the same level of security controls required for a production system shall be used.

ISO 27002 REFERENCES

12.4.2 Protection of system test data

040602 Testing Software before Transferring to a Live Environment

Purpose: To protect College systems by testing software prior to transferring it to the production environment.

STANDARD

1. To maintain the integrity of college information technology systems, software shall be evaluated and certified for functionality in a test environment before it is used in an operational/production environment.
2. Test data and accounts shall be removed from an application or system prior to being deployed into a production environment if the application or system does not have a dedicated testing environment.

ISO 27002 REFERENCES

- 10.3.2 System acceptance
- 12.5.1 Change control procedures

040603 Capacity Planning and Testing of New Systems

Purpose: To safeguard new system investments by projecting capacity demands and conducting load acceptance testing.

STANDARD

1. New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the college.
2. To understand current specifications, Colleges shall establish a baseline of current operational systems, including peak loads and stress levels and power, bandwidth and storage requirements.
3. Colleges must also test to demonstrate that the new system's performance meets or exceeds the college's documented technical requirements and business needs.

GUIDELINES

College capacity plans should consider new business, security and system requirements and any trends in the college's information processing. The college's system-testing process should verify that new or amended systems have:

1. Sufficient capabilities to process the expected transaction volumes (actual and peak).
2. Acceptable performance and resilience.
3. Reasonable scalability for growth of system.

ISO 27002 REFERENCES

- 10.3.1 Capacity management
- 10.3.2 System acceptance

040604 Parallel Running

Purpose: To safely demonstrate the reliability and capability of new or updated systems.

STANDARD

If Colleges test new or updated applications by running parallel tests, the Colleges shall incorporate a period of parallel processing into system-testing procedures that demonstrates that the new or updated system performs as expected and does not adversely affect existing systems, particularly those systems that depend on the new or updated system's functionality.

GUIDELINES

Colleges should use parallel processing as the final stage of acceptance testing and should consider the following issues and controls when developing acceptance criteria and acceptance test plans for the parallel testing of new or updated systems:

1. Capacity requirements - both for performance and for the computer hardware needed.
2. Error response - recovery and restart procedures and contingency plans.
3. Routine operating procedures - prepared and tested according to defined college

policies.

4. Security controls - agreed to and put in place.
5. Manual procedures - effective and available where feasible and appropriate.
6. Business continuity - meets the requirements defined in the college's business continuity plan.
7. Impact on production environment - able to demonstrate that installation of new system will not adversely affect college's current production systems (particularly at peak processing times).
8. Training - of operators, administrators and users of the new or updated system.
9. Logs - logs of results should be kept for a period of time once testing is completed.

ISO 27002 REFERENCES

- 10.3.2 System acceptance
- 12.5.1 Change control procedures

040605 Training in New Systems

Purpose: To ensure that personnel are adequately trained on new and updated systems.

STANDARD

Colleges shall provide training to users and technical staff in the operation and security of all new and updated systems.

GUIDELINES

Colleges should consider the following issues and training requirements when developing plans for training on new and updated systems:

1. When administrative training is inadequate, small problems can unnecessarily escalate as a result of lack of knowledge of new functions or security controls.
2. When user training is inadequate, work production often drops because of frustration or because of adjustments that must be made as users learn how to use the new system.
3. Changes in information security processes, features and controls are inherent in new systems.

ISO 27002 REFERENCES

- 8.2.2 Information security awareness, education, and training

Section 07 Web Site Development and Maintenance

040701 Developing a Web Site

Purpose: To provide protection of information technology resources when developing Web sites.

STANDARD

1. Colleges shall use only qualified personnel to develop Web sites.
2. Web site development shall incorporate secure-development best practices.

3. Development Web sites shall be isolated from production networks to prevent remote compromise while the server is being built and the Web application developed.
4. Development servers/applications shall be developed and tested with input validation to protect against data validation weaknesses in the Web application's design.
5. Web sites that accept citizen or public input through a web form shall automatically collect the submitter's known/received IP address along with a current timestamp, for example web server logs.
6. Information collected must be stored with data collected and provided in any email or other generated output as a result of the web form submission.
7. Information collected shall be kept in accordance with state and college retention policies and shall be mentioned in college privacy statements.
8. Colleges shall follow 040201, the Technical Vulnerability Management policy, for web server operating systems and its related applications in order to reduce the risk of known patch-related vulnerabilities.
9. Any accounts used by a server, Web server, Web application, or any other related applications (considered service accounts) need to meet appropriate password management standards as established in 020106 - Managing Passwords.

GUIDELINES

Industry standards for securing operating systems and Web server software, such as National Institute for Technology and Standards (NIST), the Open Web Application Security Project (OWASP), and SANS Institute guidelines, should be used for guidance in securely configuring and hardening Web sites. Colleges should consider the following:

1. Network and application (Web/database) vulnerability scans should be run against development servers during and after the development process to ensure that a server/Web application is built securely.
2. Completed Web sites should be periodically searched with a Web search engine by development staff to ensure that there is no access to Web information beyond what is intended.
3. Because of the public nature of Web servers, the use of file-integrity-checking software to detect the modification of static or critical files on the server is strongly recommended.
4. Web applications should be developed to use a minimum number of ports to allow for easy integration in traditional demilitarized zone (DMZ—filtered subnet) environments.
5. It is strongly recommended that network access web servers, both development and test; require a VPN connection to prevent exploitation of potential vulnerabilities that may exist in these environments.

ISO 27002 REFERENCES

10.9.1 Electronic commerce

040702 Maintaining a Web Site

Purpose: To protect and maintain the State's Web sites.

STANDARD

Colleges shall designate qualified individuals to administer and maintain their Web sites. College management and college system administrators shall ensure the following:

1. College Web sites are kept up to date and secure and the information they present is accurate.
2. Public Web sites are hardened and standard security configurations, based on industry guidelines and State policies, are followed.
3. Secure authentication is used to protect the security of Web servers that have access to confidential information or that perform critical functions.
4. Web sites have the latest operating system and application patches.
5. Web site logs are periodically reviewed.
6. The number of personnel with administrative access is limited to only qualified individuals.
7. The sites are available to the appropriate users (public and private).
8. Unauthorized modification of the Web site information is quickly discovered and resolved.
9. All sites that an college is responsible for are periodically tested for vulnerabilities.
10. All sites comply with all applicable laws and regulations.

ISO 27002 REFERENCES

10.9.1 Electronic commerce

Section 08 Purchasing and Installing Hardware

040801 Specifying Requirements for New Hardware

Purpose: To ensure that security requirements are a part of the hardware acquisition process.

STANDARD

1. Colleges shall ensure that new hardware purchases are supported by documented operational, technical and security requirements.
2. Colleges shall follow State procurement policies when acquiring hardware to ensure that the purchase meets specified functional needs. Colleges shall include specific requirements for performance, reliability, cost, capacity, security, support and compatibility in Requests for Proposals (RFPs) to properly evaluate quotes.
3. Prior to hardware purchase, the college shall formally document, at a minimum, how the new hardware acquisition meets the following evaluation criterion:
 - Proposed vendor hardware design complies with information security and other State policies and standard security and technical specifications, such as the following:
 - The vendor has configured the system with adequate capacity to fulfill the functional requirements stated in the college’s design document.
 - The vendor has configured hardware security controls to adequately protect data. (Optionally, the vendor may assist the college with the configuration of software security controls to provide adequate data protection on the vendor’s hardware.)
 - The vendor shall provide system availability data to demonstrate that the proposed hardware meets minimum downtime requirements.

GUIDELINES

Colleges should develop a process to define hardware functionality prior to purchasing. Other requirements to consider and include in RFPs are the following:

1. If hardware will support a critical function: replacement availability and times.
2. If hardware will be used outside of a permanent facility (such as mobile equipment): requirements for survivability (*i.e.*, extreme conditions such as temperature, dust, humidity, etc.)
3. If data confidentiality, criticality and integrity needs dictate: hardware-based encryption or other applicable security requirements.

ISO 27002 REFERENCES

12.1.1 Security requirements analysis and specification

040802 Installing New Hardware

Purpose: To ensure new hardware is subjected to operational and security review prior to installation.

STANDARD

1. Colleges involved with the installation of new hardware shall establish a formal review process that allows entities affected by the new hardware to review and comment on the implementation plans and operational and security requirements.
2. The review process shall include the following:
 - o Notification of all impacted parties prior to the installation of new hardware.
 - o Circulation to appropriate individuals of planned changes or disruptions to operational status or information security for the new installation.
 - o Installation of equipment in an appropriately secured and environmentally controlled environment.
 - o Restricting access to the proposed changes (*i.e.*, network diagrams, security features, locations, configurations, etc.) to those who require the information to perform their job duties.
3. Security reviews shall be performed internally on a regular basis to ensure compliance with the standard requirements.
4. Colleges shall develop a process to ensure that new systems and equipment are fully tested against operational and security requirements and formally accepted by users before management accepts the systems and places equipment into the operational environment.

GUIDELINES

Full and comprehensive testing of systems and equipment should entail following a written test plan that includes, but is not limited to, the following:

1. Approval from the manager responsible for the correct functioning of the information system to ensure that all relevant security policies and requirements are met and the system provides an acceptable level of risk.
2. Assessment of compatibility with other system components.

3. Determination that technical and functional specifications are met.
4. Beta testing from cross-sections of users in different departments of the college.

ISO 27002 REFERENCES

12.1.1 Security requirements analysis and specification

Section 09 Cabling, UPS, Printers and Modems

040901 Supplying Continuous Power to Critical Equipment

Purpose: To minimize the risks of critical equipment downtime and data loss caused by power outages or electrical anomalies.

STANDARD

Colleges shall protect critical information technology systems from damage and data loss by installing and routinely testing a source of continuous power that ensures that the systems continue to perform during power outages and electrical anomalies (e.g., brownouts and power spikes).

GUIDELINES

1. The three primary methods for providing continuous power are as follows:
 - Multiple electric feeds to avoid a single point of failure in the power supply.
 - Backup generator(s).
 - Uninterruptible power supply (UPS).
2. Each College should examine the availability requirements for critical equipment and determine which combination of these three methods best meets the needs of the college. Most scenarios will require at least two of these methods.
3. When analyzing the power requirements of critical systems, Colleges should consider the following best practices:
 - Both power and communication lines should be protected.
 - Multiple power feeds should not enter a building in proximity to each other.
 - Use of a UPS is usually required to avoid abnormal shutdowns or to provide a clean power source during brownouts or surges. Because most UPS batteries do not last for more than four (4) hours without a continuous supply of power, the following actions should be taken:
 - Development of contingency plans that include procedures to follow if the UPS fails.
 - Inspections of UPS equipment to ensure that the equipment has the ability to sustain, for a predefined period, the power load of the systems and equipment it supports, and is serviced according to the manufacturer's specifications.
 - A backup generator should be used when requirements demand continuous processing in the event of a prolonged power failure. Colleges that require a backup generator should ensure that:
 - The generator is serviced regularly in accordance with the manufacturer's specifications.
 - An adequate supply of fuel is available to ensure that the generator can perform for a prolonged period.
4. Other practices that help mitigate the risk of power outages include the following:
 - Locating emergency power switches near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency.

- Providing emergency lighting in case of a main power failure.
- Installing lightning protection in all buildings.
- Fitting all external communications lines with lightning protection filters.
- Utilizing alternate fuel sources such as solar energy, fuel cell electricity, biogas, or geothermal electricity.

ISO 27002 REFERENCES

9.2.2 Supporting utilities

040902 Managing and Maintaining Backup Power Generators

Purpose: To ensure continuity of backup power during power outages.

STANDARD

Colleges with business requirements that demand uninterrupted information processing during power outages shall deploy backup power generators. When a backup generator is employed, Colleges shall do the following:

1. Regularly inspect the generator to ensure it remains compliant with both safety and manufacturer maintenance requirements and has an adequate supply of fuel.
2. Ensure the generator has the capacity to sustain the power load required by supported equipment for a prolonged period of time.
3. Ensure the generator is tested at least quarterly according to the manufacturer's specifications.

GUIDELINES

- Backup generators are usually combined with an uninterruptible power supply to protect critical information technology systems that demand high availability. Such a combination both supports an orderly shutdown if the generator fails, minimizing potential for equipment damage or data loss, and can also provide continuous business operations if the cutover to the generator is too slow to provide power immediately with no interruption.
- Contingency plans should include procedures to be followed in the event the backup generator fails.

ISO 27002 REFERENCES

9.2.2 Supporting utilities

040903 Using Fax Machines/Fax Modems

Purpose: To protect confidential information transmitted via facsimile machines or facsimile modems.

STANDARD

1. Colleges may transmit confidential information using facsimile machines or facsimile modems only when security is in place to protect the information being sent.
2. Where receiving facsimile machines are in open areas, personnel using facsimiles to transmit confidential information shall notify the intended recipient when the information is being sent and the number of pages to expect, so that facsimiles

containing confidential information are not left unattended on a facsimile machine.

GUIDELINES

1. Colleges should implement formal procedures that require both the sender of the information and the intended recipient to authorize the facsimile transmission and recipient facsimile phone number before the transmission occurs and to verify successful transmission upon receipt.
2. Colleges should incorporate reminders and education about the security issues that surround the use of facsimile machines and facsimile modems into their ongoing information security training and awareness programs.

ISO 27002 REFERENCES

10.8.5 Business information systems

040904 Using Modems and Broadband Connections

Purpose: To protect confidential information being transmitted over public networks*.

*For the purpose of this standard, a public network includes the State Network. It does not apply to internal college networks. Internal college networks are considered private networks

STANDARD

1. College management shall set policies and procedures for approved modem and broadband connection usage.
2. Colleges using modem (cable or telephone)/broadband (*i.e.* ISDN, DSL, etc.) connections to transmit confidential information over public networks shall implement the following security measures to prevent disclosure of the confidential information:
 - o The college shall require personnel to encrypt or transmit through a secure connection such as VPN or SSL all confidential information, including user passwords and Social Security numbers, to protect the confidentiality and integrity of the information.
 - o The college shall require those who transmit information via these types of connections to notify the intended recipient that the information is being sent.

ISO 27002 REFERENCES

10.8.5 Business information systems

040905 Installing and Maintaining Network Cabling

Purpose: To ensure the availability and integrity of data by protecting network cabling.

STANDARD

In addition to complying with the NC Electrical Code*, Colleges that install and/or maintain network cabling shall use only qualified personnel to perform tasks involving this cabling. Colleges shall implement safeguards to protect network cabling from being damaged and to reduce the possibility of unauthorized interception of data transmissions that take place across such cabling.

*Chapter 8, Article 830 of the code addresses "Network Powered Broadband Systems." Other provisions apply as well.

GUIDELINES

Colleges installing or maintaining network cabling should consider the following practices to increase the security and physical protection of cabling where appropriate:

1. Using underground cabling, where possible, or providing lines with adequate alternative protection.
2. Running network cabling through overhead cable troughs, pipes or similar conduits.
3. Limiting the amount of exposed cabling within public areas.
4. Eliminating interference by segregating power cables from communications cables.
5. Installing fiber-optic cabling.

ISO 27002 REFERENCES

9.2.3 Cabling security

Section 10 Using Portable Computing and Storage Devices

041001 Using Removable Storage Media, Including Diskettes and CDs

Purpose: To protect the State's data contained on removable storage media from unauthorized disclosure and modification.

STANDARD

Security controls shall be put in place to protect the confidentiality and integrity of data contained on removable storage media throughout the life of those storage media, including disposal. Access controls shall include physical protection of and accountability for removable media to minimize the risk of damage to data stored on the removable storage media, theft, unauthorized access of data stored on the media, and software licensing violations.

ISO 27002 REFERENCES

10.7 Media handling

041002 Using Laptop/Portable Computers

Purpose: To protect data on laptop/portable computers and other handheld computing devices.

STANDARD

1. Colleges shall authorize the assignment of portable personal computers to employees and require that users comply with all information technology security policies when using the portable devices, including the college and statewide acceptable use policies, as applicable.
2. Portable devices covered by this standard are those that connect to College and State networks and/or store college data and include the following:
 - Laptop, notebook, netbook and tablet computers.
 - Mobile computing devices and portable computing devices such as personal digital assistants (PDAs), electronic organizers, smart phones, cellular phones, and pagers.
 - Portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players), flash drives, thumb drives, or other similar devices.

3. Colleges shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. Specifically, portable computing devices shall:
 - Be physically secured when the users have taken them out of a secure area.
 - Be labeled with tamper-resistant tags identifying the device as property of the State, or a permanently engraved serial number or both.
 - Comply with all applicable security requirements for desktops.
 - If not protected by encryption software, the BIOS password on such devices must be enabled if technically possible.
 - Use current antivirus software to scan for malware.
 - Have regular backups.
 - Have firewalls configured to comply with College and State policies.
4. When a laptop is outside a secure area, data on the laptop must be backed up, and the backup must be kept separate from the laptop. (The college shall define the policies and procedures for backing up mobile computing data, which shall include a classification of what data will be backed up.)
5. Personnel who use a College laptop/portable computer shall ensure that the laptop/portable computer and the information it contains are suitably protected at all times.
6. Colleges shall periodically audit these devices to ensure compliance with these requirements.

GUIDELINES

College management should consider using the following additional security controls, as appropriate:

1. Check-in procedures for portable devices that verify the device is free of unauthorized software, viruses, or any other malicious code prior to reissue or reconnection to the network.
2. Training to raise user awareness of the additional risks that accompany mobile computing and the controls with which users must comply.
3. The small size and mobility of portable computing devices are the primary causes of the attendant security risks. Information security controls that Colleges should consider include the following:
 - Procedures governing appropriate use of portable devices in unprotected areas (meeting rooms and off-site locations).
 - Restricting use of such devices via a wireless connection that originates from anywhere other than State- or college-approved networks.
 - Training on how to physically secure devices against theft when left in cars or other forms of transport, hotel rooms, conference centers and meeting places.
 - Training to raise user awareness of the additional risks that accompany mobile computing and the controls that should be implemented.

ISO 27002 REFERENCES

- 9.2.5 Security of equipment off-premises
- 11.7.1 Mobile computing and communications

041003 Working from Home or Other Off-Site Location (Teleworking)

Purpose: To secure and protect communications with college information resources while personnel are working at off-site locations.

STANDARD

1. Colleges shall define policies for authorized personnel to securely access systems from off-site. Policies shall include the following:
 - Use of college-approved virus prevention and detection software.
 - Use of personal firewalls that are configured to block unauthorized incoming connections.
 - Securing home wireless networks, and properly using other non-State Wi-Fi connections.
 - Protecting mobile computing devices and portable computing devices such as personal digital assistants (PDAs), smart phones, and portable storage devices such as compact disks (CDs), digital video disks (DVDs), media players (MP3 players), flash drives, or other similar devices that are used to conduct the public's business.
 - Use of virtual private networking (VPN) software or other technologies for protecting communications between off-site systems and college information resources.
 - Use of two-factor authentication products (such as one-time password tokens or biometric devices) to authenticate users, if applicable or if required by statute or industry standard.
 - Use of encryption products to protect data stored on off-site systems, if applicable. Colleges shall follow the statewide information security standard for encryption.
2. Colleges shall provide training to personnel for properly accessing systems from off-site and for keeping antivirus software and personal firewall software up to date with the latest signature files and patches.
3. Colleges shall also provide instructions and training for protecting confidential information transferred to, processed on or stored on non-State-issued systems, such as personal computers at home.
4. Colleges shall document and retain evidence of training provided to a user during the time that the individual is authorized to access systems remotely.
5. College employees who are authorized to work from home shall ensure that the college-defined policies for off-site work are strictly followed. Personnel shall take extra precautions to ensure that confidential information stored on personal computers or electronic devices is not divulged to unauthorized persons, including family members.

GUIDELINES

When working from public wireless networks, (*i.e.*, Hotspots), users should consider the following:

- When possible, use access points that require a key and which encrypt the wireless communication.
- Configure wireless LAN settings to not allow automatic joining of any wireless network. Make sure the mobile device allows you to choose whether to connect to a WLAN access point and which one.
- Disable file and print sharing.

- Access only web based resources that utilize secure connections, such as SSL.

ISO 27002 REFERENCES

- 9.2.5 Security of equipment off-premises
- 11.7.2 Teleworking

041004 Using Mobile Communication Devices

Purpose: To protect state resources and information during mobile communication device use.

STANDARD

For purposes of this standard “mobile communication devices” includes mobile phones, IP phones, pagers, BlackBerry devices, iPhones, smart phones, tablets, etc. Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks.

1. Confidential College information transmitted, accessed, and/or stored on mobile communication devices shall be appropriately secured.
2. The amount of personal conversations and/or personal business on College-provided mobile communication devices shall be controlled in accordance with College and State policies. Colleges that allow mobile communication devices (personal or business owned) to connect to state systems, such as email, shall require the following:
 - A minimum 4-digit numeric, user defined, personal identification number (PIN) that is changed every 90 days.
 - A time out of inactivity that is 10 minutes or less.
 - If technically possible, the ability to remotely erase the contents of the device, at the user’s request, management request via a help desk service request, or by the user’s own action. Colleges shall make end users aware that they are accepting the risk of personal data being lost.
 - Users shall report lost or stolen mobile communication devices to a College’s service desk or to college management within 24 hours of confirmation.
3. Personnel using College-provided mobile communication devices shall do the following:
 - Adhere to College acceptable use standards and policies.
 - Adhere to the statewide encryption standard, if applicable.
 - Adhere to statewide information security policies for removing all data before disposing the device. Change the default password for connecting to a wireless enabled device (*i.e.*, Wi-Fi or Bluetooth) on applicable mobile communication devices.
 - Disable wireless functionality (*i.e.*, Wi-Fi or Bluetooth) on appropriate devices with wireless functionality (*i.e.*, Wi-Fi or Bluetooth) if it is not in use.

GUIDELINES

Colleges that issue mobile communication devices to personnel and/or permit personnel to use their own mobile communication devices to conduct state business should make them aware of the following:

1. The risk of others eavesdropping physically and electronically in both private and public areas.

2. The risk of storing and/or transmitting confidential information on calendars, address books, etc.
3. Their responsibility for the safekeeping of mobile communication devices.

The following measures should be used to protect mobile communication devices used to conduct state business whenever possible.

1. If possible, Colleges should consider encrypting all mobile communication devices regardless of the confidentiality of the information stored on a device.
2. Users should not open attachments from untrusted sources.
3. Users should not follow links from untrusted sources, such as from unsolicited email or text messages.
4. Users should utilize a remote wipe feature, if available, to remotely set the device to factory defaults if it is lost or stolen.
5. Users should report lost devices immediately to the carrier and/or organization.
6. Users should review the mobile device security settings to ensure appropriate protection.
7. For Bluetooth enabled devices, consider the following:
 - o Choose PIN codes that are sufficiently random and long.
 - o Disable the ability for the Bluetooth device to be discovered, except when needed for pairing.
 - o Pair devices only in a secure area.
 - o When possible, enable encryption to secure data transmissions.
 - o When possible, enable device mutual authentication.
 - o Set the Bluetooth device to the lowest necessary and sufficient power level.
 - o Do not accept transmissions from unknown or suspicious devices.
 - o In the event a Bluetooth enabled device is lost or stolen, immediately unpair the device.

(For additional guidance on Bluetooth Security, refer to the NIST document SP 800-121 "Guide to Bluetooth Security" located on the NIST Special Publications web page.)

ISO 27002 REFERENCES

- 9.2.5 Security of equipment off-premises
- 10.8.5 Business information systems

041005 Using Business Center Facilities

Purpose: To establish appropriate use requirements when information is processed in external business centers or facilities.

STANDARD

1. College employees using external business centers to conduct business shall not process confidential information, including transmitting confidential information via email(s) or fax(es).
2. When college employees use business center facilities for processing other college information (*i.e.*, information that is not confidential), they shall do the following:
 - o Refrain from using auto-save features on the facility's equipment and delete, prior to leaving the facility, any files that were temporarily saved to the hard disk of the

equipment they were using.

- Clear history and cache memory and delete cookies prior to leaving the facility.
- Never leave the computer on which they are working unattended.
- Clear the facility's printer(s) of all documents they have printed.

ISO 27002 REFERENCES

11.7.1 Mobile computing and communications

Section 11 Other Hardware Issues

041101 Managing and Using Hardware Documentation

Purpose: To effectively manage hardware assets and their documentation.

STANDARD

1. Colleges shall retain user documentation and technical specifications of information technology hardware.
2. Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff. Each College shall identify and record its information technology (IT) hardware assets in a formal hardware inventory/register.
3. Each College shall develop a process to ensure that IT hardware is identified with College-unique physical asset tags and that the inventory/register is kept up to date.

GUIDELINES

1. Colleges should develop and maintain additional documentation that details hardware placement and configuration, provides flowcharts, etc.
2. The formal hardware inventory should include only information that is available for public inspection.

ISO 27002 REFERENCES

7.1.1 Inventory of assets
10.7.4 Security of system documentation

041102 Moving Hardware from One Location to Another

Purpose: To protect hardware during moves.

STANDARD

To protect College hardware and the data residing on the hardware, only authorized personnel shall be allowed to move hardware from one location to another. Equipment can be damaged if handled improperly and the confidentiality and integrity of data can be compromised if unauthorized persons gain possession of the hardware.

ISO 27002 REFERENCES

9.2 Equipment security

041103 Disposing of Obsolete Equipment

Purpose: To protect data confidentiality and integrity through proper disposal of obsolete equipment.

STANDARD

1. Colleges shall establish a procedure for certifying that data have been properly removed from information technology equipment before it is transferred, surplused or donated.
2. The data contained on information technology equipment must be permanently removed by destroying, purging, or clearing. The method chosen must be appropriate for the media used and approved by the National Institute of Standards and Technology (NIST) or comply with approved Department of Defense standards so that previously recorded information is not recoverable. The method of data removal shall be based on what is reasonable and practical.

(Additional information regarding the secure disposal of obsolete equipment may be found in the NIST publication 800-88 titled "Guidelines for Media Sanitization.")

3. Colleges must ensure that all State/college information is fully removed from obsolete information technology equipment and not recoverable before the equipment is released to the State Office of Surplus Property or a third-party disposal facility.
4. Colleges involved in the disposal of obsolete material shall utilize only companies that specialize in secure waste disposal and that can comply with service level agreements established by the college.
5. Service level agreements with external firms/third parties shall include the following:
 - Stipulations to ensure compliance with the college's security policies and standards, enforceable by suit for breach of contract and the right to monitor compliance.
 - Development of procedure(s) for certifying that data have been properly removed from government- controlled equipment before it is transferred, resold, donated, or disposed of.
 - Removal of data from floppy disks, CD-ROMs, magnetic tapes and all other electronic storage media or subsequent destruction (e.g., degaussing, shredding, etc.).
 - Scheduled disposal periods and/or processes involved in waste collection.

ISO 27002 REFERENCES

- 6.2.3 Addressing Security in third party agreements
- 9.2.6 Secure disposal or re-use of equipment
- 10.7.2 Disposal of media

041104 Recording and Reporting Hardware Faults

Purpose: To maximize hardware availability and integrity through fault recording/reporting.

STANDARD

1. Users who identify a hardware fault or information-system-processing problem shall promptly report the problem and the details to the appropriate support staff.
2. Each College shall establish procedures to record and track equipment faults.

ISO 27002 REFERENCES

- 9.2.4 Equipment maintenance
- 10.10.5 Fault logging

041105 Dealing with Answering Machines/Voice Mail

Purpose: To prevent confidential information from being disclosed in messages left on telephone answering machines and voice mail.

STANDARD

1. Users shall not record or leave messages containing confidential information on answering machines or voice mail systems.
2. Colleges shall communicate in their training for personnel that confidential information is not to be left on answering machines or voice mail systems.

ISO 27002 REFERENCES

- 10.8.1 Information exchange policies and procedures
- 10.8.5 Business information systems

041106 Taking Equipment off the Premises

Purpose: To safeguard and maintain accountability for equipment.

STANDARD

1. College personnel must have approval from an authorized college employee before they remove State information technology equipment from college facilities.
2. Personnel removing equipment shall be responsible for the security of the equipment at all times.
3. Colleges shall establish procedures for the removal and return of college equipment.
4. Where appropriate, logging procedures shall be established to track the removal (sign-out) of equipment from and return (sign-in) of equipment to the college.

ISO 27002 REFERENCES

- 9.2.5 Security of equipment off-premises
- 9.2.7 Removal of property

041107 Maintaining Hardware (On-Site or Off-Site Support)

Purpose: To maintain hardware availability and integrity.

STANDARD

1. Each College shall provide or arrange maintenance support for all equipment that is owned, leased or licensed by the college.
2. The College must arrange support services through appropriate maintenance agreements or with qualified technical support staff.
3. When maintenance support is provided by a third party, nondisclosure statements shall be signed by authorized representatives of the third party before any maintenance support is performed.

4. Records of all maintenance activities shall be maintained.

ISO 27002 REFERENCES

9.2.4 Equipment maintenance

041108 Damage to Equipment

Purpose: To improve confidentiality, integrity and availability of data by requiring the reporting of property damage.

STANDARD

Each user shall report deliberate or accidental damage to college equipment or property to his or her manager as soon as it is noticed.

GUIDELINES

Damage to equipment or property that performs a security function may create a weak link in the college's security architecture and leave confidential data exposed. Colleges should refer to their business impact analyses or risk analyses to determine the level of urgency in repairing or replacing damaged equipment.

ISO 27002 REFERENCES

9.2.4 Equipment maintenance

10.10.5 Fault logging

Section 12 Data Management

041201 Managing Data Storage

Purpose: To protect the State's information resident on electronic data storage

STANDARD

1. Colleges shall ensure the proper storage of data and information files for which they are responsible.
2. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse.
3. Colleges shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.
4. Colleges shall protect the State's information and comply with the College's records retention policy or the General Schedule for State College Records, Information Technology Records.
5. Colleges shall ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, Colleges shall follow the statewide information security standard for encryption.
6. Colleges shall establish change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures.
7. All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.

GUIDELINES

Colleges should keep stored public data to a minimum of what is necessary to adequately perform their business functions. Sensitive or confidential data that is not needed for normal business functions, such as the full contents of a credit card magnetic strip or a credit card PIN, should not be stored. Colleges should consider implementing a process (automatic or manual) to remove, at least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the College's data retention STANDARD.

ISO 27002 REFERENCES

- 10.5.1 Information back-up
- 10.7.3 Information handling procedures
- 12.5.1 Change control procedures
- 15.1.3 Protection of organizational records

041202 Managing Databases

Purpose: To protect the State's information databases.

STANDARD

1. Colleges shall properly safeguard the confidentiality (where applicable), integrity and availability of their databases.
2. Data from these databases shall be protected from unauthorized deletion, modification or misuse and shall meet all applicable statutory and regulatory requirements.
3. Critical data files shall be backed up, and if confidential data is backed up, the backup media shall receive appropriate security controls.
4. To maintain the reliability of databases maintenance must be performed on the operating system of the system that hosts the databases, or there is a greater possibility that the database itself will fail.
5. Databases that store critical, confidential information such as client records, accounting data, medical history data and data on sales and purchases require more stringent mean time between failures (MTBF) and mean time to repair (MTTR) configurations.

GUIDELINES

To mitigate security issues with spreadsheets, Colleges should do the following:

1. Validate the formulas in the spreadsheet.
2. Implement read, write and deletion controls on access to the spreadsheet.
3. Control the spreadsheet's distribution.
4. Maintain retention and version control.
5. Save the spreadsheet in a directory that is backed up regularly.

To mitigate security issues with databases, Colleges should do the following:

1. Fully test any database before making it operational.
2. Control access levels (read, write, modify) to the database.
3. Validate all data before they are entered into the database.
4. Maintain retention and version control. Control database reports distribution.

ISO 27002 REFERENCES

- 10.1.2 Change management
- 10.3.2 System acceptance
- 12.2 Correct processing in applications
- 15.1.3 Protection of organizational records

041203 Managing Folders/Directories

Purpose: To provide directory-level protection for the State's information resources.

STANDARD

1. Colleges shall establish policies and procedures for creating and managing access to directory structures based on the most restrictive set of privileges needed to perform authorized tasks.
2. New directory/folder structures shall be designed with the appropriate access controls to restrict access to authorized personnel only.
3. New folders/directories shall prohibit the modification or deletion of files and folders from personnel other than the data creator/owner or system administrators.
4. New folders/directories designed for holding confidential information shall be password protected.
5. Colleges shall establish and manage access controls governing the modification or amendment of the directory structures on network or shared drives.

ISO 27002 REFERENCES

- 11.11.1 Access control policy

041204 Sharing Data on Software and Information Systems

Purpose: To protect the State's confidential information while utilizing software or information systems.

STANDARD

1. Software or information systems that allow the sharing of files and data containing confidential information shall be used to share data only if the appropriate security controls are properly configured and implemented.
2. Appropriate security controls shall include the following:
 - Authentication controls to ensure that authorized users are identified.
 - Access controls to limit an individual's access to only the confidential information necessary for that person to perform his/her role.
 - Authorization controls to enforce version control and record retention requirements such that only designated individuals are able to modify or delete sensitive or critical records.
 - Audit controls that record individual actions on files and records, such as when a file is modified. Audit logs shall be retained in accordance with the College records retention policy or the General Schedule for State College Records, Information Technology Records.
3. These controls may be supplemented by operating-system-level controls (e.g., file and directory access control lists and system audit logs).

ISO 27002 REFERENCES

041205 Updating Student and Business Information

Purpose: To protect the confidentiality and integrity of the College's electronic information on students and third parties.

STANDARD

1. Only authorized individuals shall perform updates to student and business databases.
2. When changing information, College employees must be diligent in protecting confidential information and shall adhere to all applicable laws and regulations.
3. Access to student and business or college confidential data shall be controlled through various appropriate access control mechanisms.

GUIDELINES

Colleges should provide the appropriate management structure and control to foster compliance with data protection legislation. Colleges may need to write the responsibility for data protection into one or more job descriptions to reach compliance.

ISO 27002 REFERENCES

- 8.1.1 Roles and responsibilities
- 15.1.4 Data protection and privacy of personal information

Section 13 Backup, Recovery and Archiving

041301 Backup and Recovery of Systems

Purpose: To ensure proper backup and restore procedures for college information technology systems.

STANDARD

1. Colleges shall establish procedures for the adequate backup and the restarting or recovery of their information technology systems.
2. Procedures for the restarting of information technology systems shall be properly tested and documented. These procedures shall include the following:
 - o Documented backup frequencies and schedules.
 - o Documented storage location for the correct system information backup medium.
 - o An approved process for restoring the system.
 - o Compliance with college change management procedures.
 - o Testing on a regular basis, as established by college management.
 - o Guidance for restart documentation.
3. Colleges shall manage the backup and recovery procedures of their information technology systems according to their business continuity plans. These plans must be properly documented, implemented and tested to ensure operational viability and their adherence to N.C.G.S. §147- 33.89.
4. Colleges shall ensure the proper recovery and restoration of data files from their information technology systems according to their business continuity plans. These business continuity plans, procedures and media must be properly documented,

implemented, stored and tested to ensure operational viability, reliable retrieval and adherence to N.C.G.S. §147-33.89.

5. Data recovery must be conducted by authorized parties and recovered data must be tested for potential corruption.
6. When recovering data, a test set of the data is selected as the data exist at a specific point in time. The recovered data are then compared to the test set and reviewed for their integrity.

GUIDELINES

1. In managing backup and recovery procedures, Colleges should ensure the following:
 - Backup schedules meet business system requirements.
 - Backup and restoration processes are tested on a regular basis.
 - Backup facilities are adequate for minimum levels of operation.
 - Retention periods of various data are based on operations, laws and regulations.
 - Backup and recovery procedures are periodically reviewed and updated, as necessary.
 - Validation of the integrity of the backup or image file through file hashes for backups, restores, and virtual machine migrations.
 - Classification of the backup media so the sensitivity of the data can be determined.
 - Secure storage of media back-ups in a secure location, preferably an off-site facility.
 - All backup media are physically secured from theft and destruction.
 - Media are transported by secured courier or other delivery method that can be accurately tracked.
 - Management approval for any media moved from a secure area.
 - Proper maintenance of inventory logs of all media, including media inventories at least annually.
2. Colleges should consult with the North Carolina Department of Cultural Resources, Government Records Section, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived.
3. When archiving data associated with legacy systems, Colleges should plan to provide a method of accessing those data.

ISO 27002 REFERENCES

- 10.5.1 Information back-up
- 10.7.3 Information handling procedures

041302 Backing Up Data on Portable Computers

Purpose: To protect the State's data stored on mobile/portable computers via regular backup plans.

STANDARD

1. Colleges shall define the policies and procedures for backing up mobile computing data, which shall include a classification of what data shall be backed up.
2. Colleges shall ensure that all appropriate data stored on mobile/portable computing

devices is regularly and properly backed up.

3. Data stored on any mobile/portable computing device shall be backed up according to the schedule specified in the Colleges' business continuity plans.
4. When a mobile/portable computer is outside of a secure area, the backup medium must be kept separate from the mobile/portable computer. Backup media shall be properly stored in a secure, environmentally controlled location with access control to protect data from unauthorized loss or access.

ISO 27002 REFERENCES

11.7.1 Mobile computing and communications

Section 14 Using Outsourced Processing and Third Party Services

041401 Contracting or Using Outsourced Processing

Purpose: To ensure that outsourced processing achieves acceptable service levels.

STANDARD

1. Colleges that outsource their information processing must ensure that the service provider demonstrates compliance with industry quality standards.
2. Outsourcing agreements shall include a contract that, at a minimum, meets State information technology security requirements.
3. Outsourcing agreements shall include the following:
 - The College's course of action and remedy if the vendor's security controls are inadequate such that the confidentiality, integrity or availability of the college's data cannot be assured.
 - The vendor's ability to provide an acceptable level of processing and information security during contingencies or disasters.
 - The vendor's ability to provide processing in the event of failure(s).

ISO 27002 REFERENCES

6.2.1 Identification of risks related to external parties
12.5.5 Outsourced software development

041402 Third Party Service Management

Purpose: To ensure management of contracts with third parties.

STANDARD

1. Colleges shall manage third parties to meet or exceed mutually agreed upon signed contracts.
2. Colleges shall also ensure third parties meet or exceed all College and State policies, standards and procedures.
3. Services, outputs and products provided by third parties shall be reviewed and checked regularly.
4. To monitor third party deliverables, Colleges shall do the following:
 - Monitor third party service performance to ensure service levels meet contract

- requirements.
 - Review reports provided by third parties and arrange regular meetings as required by contract(s).
 - Review third party reports including audit logs, operational problems, failures, and fault analysis (including security events) as they relate to services being delivered.
 - Resolve and manage any identified problem areas.
5. Any changes to services provided by a third party must be approved by College management prior to implementation.
 6. Contracts should be updated to reflect changes. Examples may include the following:
 - Service improvements.
 - New or updated applications.
 - New controls.
 - Changes to network design.
 - New technologies, products or tools.
 - Changes in college policies and procedures.
 - Resolve discovered exposures and changes that would improve the security posture of the college.
 - Change of vendors.
 - Services that are moved to a new or different location by the third party.

ISO 27002 REFERENCES

- 10.2.1 Service delivery
- 10.2.2 Monitoring and review of third party services
- 10.2.3 Managing changes to third party services

041403 Third Party Service Delivery

Purpose: To define, monitor, and manage service levels from third party service providers.

STANDARD

1. When Colleges contract with external service providers, service definitions, delivery levels and security requirements shall be documented in a formal service level agreement (SLA) or other documented agreement.
2. Colleges shall develop a process for engaging service providers and maintain a list of all service providers who store or share confidential data.
3. Colleges shall ensure that the SLA includes requirements for regular monitoring, review, and auditing of the service levels and security requirements as well as incident response and reporting requirements. The SLA shall state how the service provider is responsible for data stored or shared with the provider.
4. Colleges shall perform the monitoring, review, and auditing of services to monitor adherence to the SLA and identify new vulnerabilities that may present unreasonable risk. Colleges shall enforce compliance with the SLA and must be proactive with third parties to mitigate risk to a reasonable level.
5. Changes to the SLA and services provided shall be controlled through a formal change management process.

ISO 27002 REFERENCES

- 6.2.3 Addressing security in third party agreements
- 10.2 Third party service delivery management

Chapter 5 – Physical Security

Section 01 - Premises Security

050101 Securing Premises to Site Computers and Data Centers

Purpose: To protect equipment through secure site selection and preparation.

STANDARD

1. Colleges shall carefully evaluate sites and facilities that will be staffed and will house information technology equipment to identify and implement suitable controls to protect staff and college resources from environmental threats, physical intrusion and other hazards and threats.
2. Each college shall safeguard sites, buildings and locations housing its information technology assets.

GUIDELINES

When evaluating or preparing sites and locations for hardware installation, colleges should consider the following:

1. Sites and locations for installation of information technology equipment should be carefully selected because of the difficulty of relocating hardware once it is in place.
2. Security threats may expand from neighboring premises or adjacent properties.
3. Requirements for size and location will vary according to the amount of hardware being housed.
4. Physical security measures adopted should reflect the:
 - Value of the hardware.
 - Sensitivity of the system's data.
 - Required level of availability or fault tolerance.
5. Colleges should conduct a risk assessment to calculate perceived risks and the total costs involved to mitigate threats to acceptable levels. Risk assessments may reveal that security controls are needed for natural, structural and human threats such as the following:
 - Explosion.
 - Fire.
 - Smoke.
 - Water (or a failure to supply water).
 - Chemicals.
 - Wind.
 - Seismic activity.
 - Dust.
 - Vibration.
 - Electromagnetic radiation.
 - Electrical supply interference.
6. Business operations, business continuity plans and applicable contracts should ensure that natural, structural and human threats have been accurately assessed and that controls are employed to minimize unauthorized physical entry to sites, buildings and locations housing information technology assets.
7. Access to loading docks and warehouses shall be restricted to authorized personnel. Items that are received via loading areas shall be signed for and inspected for hazardous materials before being distributed for use.

8. Duress alarms shall be used in areas where the safety of personnel is a concern. Alarms shall be provisioned to alert others such as staff, the police department, the fire department, etc.
9. Security measures that Colleges should consider implementing include, but are not limited to, the following:
 - Clearly defined, layered security perimeters to establish multiple barriers:
 - Walls (of solid construction and extending from real ceiling to real floor where necessary).
 - Card-controlled gates and doors.
 - Bars, alarms, locks, etc.
 - Bollards.
 - Lighting controls.
 - Video cameras and intrusion security system.
 - Staffed reception desk.
 - Fire doors on a security perimeter shall be equipped with alarms as well as devices that close and lock the doors automatically.

ISO 27002 References

- 9.1.1 Physical security perimeter
- 9.1.4 Protecting against external and environmental threats
- 9.1.5 Working in secure areas
- 9.1.6 Public access, delivery, and loading areas
- 9.2.1 Equipment siting and protection

050102 Ensuring Suitable Environmental Conditions

Purpose: To ensure that environmental conditions are suitable for State College computing resources.

STANDARD

When locating computers and other information technology assets, Colleges shall implement appropriate controls to protect the assets from environmental threats, such as fire, flooding and extreme temperatures.

GUIDELINES

Colleges should consider the following information security issues when minimizing the risk of environmental threats:

Exposed vulnerabilities to environmental risks could hinder or make it impossible for the College to continue business operations in the event of:

1. Fire or smoke damage.
2. Flooding (pipes bursting, fire suppression system or other overhead water conduits malfunctioning, etc.)
3. Heating, ventilation or air conditioning (HVAC) failures.
4. Dust or other contaminants.
5. Relevant health and safety standards.
6. Threats that may expand from neighboring premises.

ISO 27002 References

- 9.1.3 Securing offices, rooms, and facilities

050103 Physical Access Control to Secure Areas

Purpose: To protect computer equipment by controlling physical access.

STANDARD

1. Colleges shall ensure areas housing information technology assets have appropriate physical access controls.
2. Authorized individuals may include College employees, contractors, vendors and customers.
3. Colleges shall develop access policies for authorized individuals as well as visitors to these areas.
4. An audit trail of access for all individuals to data centers shall be maintained.
5. Colleges shall also restrict access to publicly accessible network jacks in datacenters by disabling unused network jacks, unless they are explicitly authorized.
6. Physical access to wireless access points, networking equipment and cabling shall be restricted to only authorized personnel.

GUIDELINES

Colleges should control the number of people who have physical access to areas housing computer equipment to reduce the threats of theft, vandalism and unauthorized system access.

When implementing physical access controls, Colleges should consider the following measures to control and restrict access:

1. The access control system should address the following categories of personnel, each with different access needs:
 - System operators and administrators who regularly work in the computer area.
 - Technical support staff and maintenance engineers who require periodic access to the computer area.
 - Other staff that rarely need access to the area.
2. Physical access authentication controls should include some form of visible identification such as an ID badge.
3. An audit trail of physical access to the computer area should be maintained.
4. Computing facilities require additional controls for visitor access, including the following.
 - Access should be restricted to those having specific, authorized purposes for visiting the computer area.
 - Instructions should be issued to visitors explaining security requirements and emergency procedures.
 - Entry and exit dates and times should be logged.
 - Visitors should wear visible identification that clearly draws attention to their restricted status.
 - Visitors should be escorted.

ISO 27002 References

9.1.2 Physical entry controls

050104 Challenging Strangers on College Premises

Purpose: To increase the security of areas housing information technology equipment.

STANDARD

1. Each College shall educate employees to appropriately challenge strangers in areas containing information technology equipment to verify the stranger's authority to be in the controlled area.
2. Where appropriate, employees and visitors shall be properly badged and escorted at all times.

3. Where entrance to an area requires a badge or a similar controlled-access method, authorized individuals shall not allow unauthorized individuals to follow them into the controlled-access area.

ISO 27002 References

1.1.3 Securing offices, rooms, and facilities

050105 High Security Locations

Purpose: To protect information and assets in high security locations.

STANDARD

1. Locations that contain confidential information shall be designed and secured in accordance to the information being protected.
2. Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas.
3. The use of personal cameras, video recorders and handheld devices (cell phones, PDAs, pocket PCs), shall be restricted from high security locations to protect the information being stored.

ISO 27002 References

9.1.5 Working in secure areas

050106 Fire Risks to the College's Information

Purpose: To reduce the fire risks to the College's information.

STANDARD

1. Colleges shall take proper care to manage the risks of fire to the State's data and information technology resources.
2. Risk assessments shall be performed at all sites where College information is processed or stored to determine the effectiveness of current controls and the facility's risk from fire and other environmental threats.

GUIDELINES

1. Colleges should consider storing duplicate copies of information at alternate locations.
2. The use of file cabinets that are fire-, smoke- and/or water-safe is encouraged depending on the College's risk assessment.
3. Colleges should consider a dry pipe sprinkler system to protect documents from destruction in cases in which the building's sprinkler system is triggered.

ISO 27002 References

9.2.2 Supporting utilities

Section 02 Other Premises Issues

050201 Managing On-Site Data Stores

Purpose: To protect confidential information maintained in on-site data stores.

STANDARD

1. Colleges shall ensure that on-site data storage locations have adequate access controls to minimize the risk of data loss or damage.

2. Each College shall maintain duplicate copies of critical data on removable media in data stores.

GUIDELINES

Colleges should consider the following information security issues when planning or implementing on-site data stores:

1. The survivability of the data store in the face of man-made or natural disasters.
2. The need for periodic testing of backup and restore procedures to verify strengths and identify areas for improvement.
3. The importance of maintaining a low profile for the facility or its information-processing functions.

ISO 27002 References

- 9.1.2 Physical entry controls
- 9.1.3 Securing offices, rooms, and facilities

050202 Managing Remote Data Stores

Purpose: To protect confidential information that is stored remotely.

STANDARD

1. Colleges shall ensure that remote data storage locations have adequate access controls to minimize the risk of data loss or damage
2. If the College does not have direct control over the remote location, the College shall enter into a contract with the owner of the remote location that stipulates the access controls and protection the owner must implement. The remote data store contract shall also include the following:
 - The perimeter security and physical access controls to the site and to the College's individual data store.
 - Design requirements for secure data storage (i.e., fire suppression and detection equipment, heating, ventilation, and air conditioning [HVAC], measures to prevent water damage, etc.).
 - Transportation of removable media to and from the College.

GUIDELINES

Colleges may wish to consider both direction and distance when choosing a remote data store location. The distance between the main computing site and the remote site should be great enough to minimize the risk of both facilities being affected by the same disaster (e.g., fire, hurricane, explosion, etc.).

ISO 27002 References

- 9.1.1 Physical security perimeter
- 9.1.2 Physical entry controls
- 9.1.3 Securing offices, rooms, and facilities

050203 Using Lockable Storage Cupboards and Filing Cabinets

Purpose: To secure valuable material or equipment within lockable storage compartments.

STANDARD

1. Colleges shall store valuable equipment and confidential information securely, according to its classification status.

2. Where appropriate, colleges shall store resources in lockable storage cupboards where the physical security controls are sufficient to protect the equipment from theft.
3. Colleges shall use lockable file cabinets to store confidential information such as paper documents and computer media in a manner that is commensurate with the information's classification status.
4. Where appropriate, colleges shall provide fire-resistant storage for documents and media containing information critical to their business function.

GUIDELINES

Colleges should consider the following physical security issues:

1. Securing critical information in fire-resistant storage should be part of a college's clear desk policy.
2. Regardless of the rated capacity of a fire-resistant container, events surrounding a fire (heat, smoke, water, chemicals) may render any information that is stored in the container unusable; therefore, off-site backups of critical information remain essential.

ISO 27002 REFERENCES

- 9.1.3 Securing offices, room and facilities
- 11.3.3 Clear desk and clear screen policy

Chapter 6 – Cyber Security Incident Response

Section 01 Combating Cyber Crime

060101 Defending Against Cyber Attacks

Purpose: To protect college networks from a premeditated cyber attack.

STANDARD

1. Colleges must identify all network access points and verify that the safeguards for the network and individual systems are adequate and operational. These systems include wireless access points, network ingress and egress points, and network-attached devices.
2. Colleges shall have security incident management and response plans that address steps to be taken during and after cyber attacks.
3. Incident response plans shall incorporate information from intrusion detection/prevention systems (IDS/IPS), and other monitoring systems.
4. Colleges shall also develop contingency plans for the continuation of business processes while under a cyber attack and/or the recovery of any data damaged or lost during such an attack.
5. The security incident management and response plans shall be integrated with the business continuity and disaster recovery plans.
6. Both plans shall be developed for use when threats result in loss, corruption, or theft of data or interruption of service due to a cyber attack.
7. These plans shall be developed and tested in accordance with the statewide information security standards for Business Continuity Planning and Testing.
8. Colleges shall develop a process to modify plans according to lessons learned and industry developments.
9. Colleges shall deploy controls to ensure that the State's resources do not contribute to outside-party attacks. These controls include the following:
 - Securing interfaces between agency-controlled and non-agency-controlled or public networks.
 - Standardizing authentication mechanisms in place for both users and equipment.
 - Controlling users' access to information resources.
 - Monitoring for anomalies or known signatures via intrusion detection systems (IDS) and/or intrusion prevention systems (IPS). IDS/IPS signatures shall be up to date.

ISO 27002 REFERENCES

- 11.4 Network access control
- 14.1.2 Business continuity and risk assessment

060102 Defending Against Cyber Attacks

Purpose: To limit the potential damage caused by internal attacks.

STANDARD

To defend against cyber attacks on agency networks and to prevent damage, access rights to files shall be controlled to maximize file integrity and to enforce separation of duties.

1. Access to files shall be granted only as required for the performance of job duties.
2. Networks that serve different agencies or departments shall be controlled through the use of VLANs, routers, firewalls, etc.
3. Access badges shall be programmed to allow entry only into assigned places of duty.
4. Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.
5. Users' activities on systems shall be monitored to ensure that users are performing only those tasks that are authorized and to provide an appropriate audit trail.
6. Authorization levels shall be reviewed regularly to prevent disclosure of information through unauthorized access.
7. Vulnerability assessments and penetration tests are tools that can minimize opportunities for cyber-crime and are part of a defense-in-depth strategy. The College shall have vulnerability assessments and penetration tests completed in accordance to the Payment Card Industry mandates.

ISO 27002 REFERENCES

- 10.10.2 Monitoring system use
- 11.1.1 Access control
- 11.4 Network access control
- 11.6.1 Information access restriction

060103 Safeguarding Against Malicious Denial of Service Attacks

Purpose: To safeguard network resources from denial of service and distributed denial of service attacks.

STANDARD

Each college shall have the following responsibilities:

1. To appropriately secure all hosts that could be a potential target for a denial of service (DoS) or distributed denial of service (DDoS) attack based on the agency's ability to accept the risk for a possible disruption in service.
2. To deny all inbound traffic by default, thus limiting the channels of network attacks.
3. To periodically scan network and devices for bots (software robots) and Trojan horse programs.
4. To deploy authentication mechanisms wherever possible.
5. To design and implement networks for maximum availability.
6. To develop specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan.

ISO 27002 REFERENCES

- 9.4 Network access control
- 13.2.1 Responsibilities and procedures

060104 Defending Against Hackers, Stealth- and Techno-Vandalism

Purpose: To defend the College from cyber-crime-related activities.

STANDARD

To defend the College's assets against hackers, stealth data-gathering software (such as spyware, adware and bots) and techno-vandalism, it is critical to limit potential exploits within the network infrastructure. The following duties shall be performed by system administrators or security personnel:

1. Periodic scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection.
2. Denial of all inbound traffic by default through the perimeter defense. Exceptions for traffic essential for daily business must be requested through network security.
3. Configuration of public facing systems in accordance with statewide information security standards.
4. Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate agency approval and outlines the process for addressing virus or other malicious threats to the network. This training shall also stress the potential exposure that email attachments present to the agency and employee.
5. Deployment of intrusion detection and/or intrusion prevention systems, as appropriate.

ISO 27002 REFERENCES

- 7.1 Responsibility for assets
- 8.1.1 Roles and responsibilities
- 8.2.2 Information security awareness, education and training
- 11.4 Network access control

060105 Defending Against Malware Attacks

Purpose: To minimize malware attacks.

STANDARD

1. Colleges shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the State network.
2. All files downloaded to the College network might potentially contain malicious software (malware), such as viruses, Trojan horses, worms or other destructive programs; therefore, all downloaded files must be scanned for such malware.
3. All malware scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events.
4. Malware detection programs and practices shall be implemented throughout colleges. Training must take place to ensure that all computer users know and understand safe computing practices.
5. Malware controls, procedures, education and training shall include information on the following:
 - o Use of up-to-date antivirus software.
 - o Performing frequent backups on data files.
 - o Use of write-protected program media, such as CD-ROMs or DVD-ROMs.
 - o Validating the source of software before installing it.
 - o Scanning for malware on files that are downloaded from the Internet or any other outside source, including all external media, such as flash drives, CDs, etc.

- Requirements that users first obtain management approval before directly adding any software to the system, whether from public software repositories, other systems or their home systems.

ISO 27002 REFERENCES

10.4.1 Controls against malicious code

Section 02 Reporting Information Security Incidents

060201 Reporting Information Security Incidents

Purpose: To increase effectiveness in assessing threat levels and detecting patterns or trends in regard to information technology security incidents through proper documentation.

STANDARD

1. The College's workforce has the responsibility to report information technology security incidents to college Chief Information Officer (CIO).
2. College CIO shall determine if incident shall be reported to the Enterprise Security and Risk Management Office (ESRMO), acting on behalf of the State Chief Information Officer. If deemed necessary, college CIO will report incident to ESRMO within twenty-four (24) hours of incident confirmation.
3. All reported information technology security incidents must include the information required on the enterprise Incident Reporting form (see below), incorporated by reference.
4. Individuals who witness a breach in a college's information technology security or suspect fraudulent activity shall document the event and notify their management in accordance with college standards, policies and procedures.
5. All college personnel have the responsibility to report any discovered security weaknesses to their college CIO in accordance with college standards, policies and procedures. The notification shall be made as soon as possible after the weakness is discovered.
6. Personnel who discover or perceive that there may be a software error or weakness must report it immediately to college CIO. College CIO shall notify the responsible individual/or organization and perform a risk analysis of the perceived threats.
7. When responding to a malware threat, perform the following tasks:
 - Verify threats to rule out the possibility of a hoax before notifying others.
 - Identify personnel responsible for mitigation of malware threats.
 - Provide internal escalation procedures and severity levels.
 - Have processes to identify, contain, eradicate, and recover from malware events.
 - Have a contact list of antivirus software vendors.
 - After an information technology security incident, review with staff the lessons learned from the incident, with any changes subsequently made to the college incident management plan.
8. Individuals who are aware of software errors or weaknesses shall not attempt proof-of-concept actions unless otherwise authorized.
9. Recipients/end users must report lost or stolen State computer equipment (for example, workstations, laptops, mobile communication devices, etc.) immediately to their management. The management shall then notify the responsible individual/organization of the security event.
10. College CIO shall report incidents to the ESRMO by one of the following methods:

- Contact OITS Customer Support Center 800-722-3946.
- Use the incident reporting website <https://incident.its.state.nc.us>.
- Contact a member of the Security and Risk Management Services staff directly.

GUIDELINES

Information technology security incidents are divided into five levels of severity based on their potential to negatively impact North Carolina agency operations, finances, and/or public image. The characteristics in the table below are intended to serve as general guidelines only, and should not be interpreted as absolutes.

Incident Severity	Incident Characteristics
5 GENERAL ATTACK(S) SEVERE	<ul style="list-style-type: none"> ▪ Successful penetration or denial-of-service attack(s) detected with significant impact on North Carolina state network operations: <ul style="list-style-type: none"> ○ Very successful, difficult to control or counteract ○ Large number of systems compromised ○ Significant loss of confidential data ○ Loss of mission-critical systems or applications ▪ Significant risk of negative financial or public relations impact
4 LIMITED ATTACK(S) HIGH	<ul style="list-style-type: none"> ▪ Penetration or denial-of-service attack(s) detected with limited impact on North Carolina state network operations: <ul style="list-style-type: none"> ○ Minimally successful, easy to control or counteract ○ Small number of systems compromised ○ Little or no loss of confidential data ○ No loss of mission-critical systems or applications ▪ Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software ▪ Small risk of negative financial or public relations impact
3 SPECIFIC RISK OF ATTACK ELEVATED	<ul style="list-style-type: none"> ▪ Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance ▪ Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software ▪ Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software
2 INCREASED RISK OF ATTACK GUARDED	<ul style="list-style-type: none"> ▪ Small numbers of system probes, scans, and similar activities detected on internal systems ▪ External penetration or denial of service attack(s) attempted with no impact to North Carolina state network operations ▪ Intelligence received concerning threats to which North Carolina ITS systems may be vulnerable
1 LOW	<ul style="list-style-type: none"> ▪ Small numbers of system probes, scans, and similar activities detected on internal and external systems ▪ Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software

ISO 27002 REFERENCES

- 8.2.2 Information security awareness, education, and training
- 13.1.1 Reporting information security events
- 13.1.2 Reporting security weaknesses

060202 Reporting Information Security Incidents to Outside Authorities

Purpose: To ensure college awareness of the State's authority to determine when confirmed security incidents shall be reported to appropriate third parties.

STANDARD

1. The Enterprise Security and Risk Management Office (ESRMO), delegates the responsibility of reporting security incidents to the college Chief Information Officer. Outside authorities should be contacted in regard to confirmed information technology security incidents in accordance with applicable laws and procedures, any Memorandum of Understanding between OITS, the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor as well as in accordance with federal requirements.
2. As deemed necessary, college CIO shall notify the ESRMO of information technology security incidents. The ESRMO shall notify authorities, regulatory and law enforcement agencies about information technology security incidents in accordance with the State's Incident Management Plan, unless the college is required to notify the authorities or has already notified the authorities.
3. If/or when the college notifies authorities directly, regulatory and/or law enforcement agencies, the agency shall also report the incident to the ESRMO.
4. If an information security incident involves the unauthorized disclosure of Social Security data, the college must then notify the Social Security Administration (SSA) Regional Office and their SSA Systems Security Contact within one (1) hour of suspecting such loss.
5. If an information security incident involves the possible breach of Federal Tax Information (FTI), the college must contact the appropriate special agent-in-charge, the Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification.

ISO 27002 REFERENCES

- 6.1.6 Contact with authorities
- 13.1.1 Reporting information security events

060203 Investigating the Cause and Impact of Information Security Incidents

Purpose: To protect the College's technology resources by conducting proper investigations.

STANDARD

1. The college CIO shall evaluate the proper response to all information technology security incidents.
2. The college CIO will work with ESRMO as needed to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.
3. An investigation into an information technology security incident must identify its cause, if possible, and appraise its impact on systems and data.
4. Colleges shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (*i.e.*, hardware or software failure).
5. Qualified technicians shall perform the investigations, which shall include the following:
 - o Checking system logs, application logs, event logs, audit trails and log files.

- Continuing to closely monitor the specified system to establish trends or patterns.
 - Researching for known failures resulting from software bugs.
 - Contacting appropriate third parties, such as vendor-specific technicians, for assistance.
6. Colleges shall utilize trained personnel to perform investigations and shall restrict others from attempting to gather evidence on their own.
 7. Evidence of or relating to an information technology security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements.
 8. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident.
 9. In the event of an active cyber crime, management has the authority to decide whether to continue collecting evidence or to lock down the system involved in the suspected crime.
 10. When dealing with a suspected cyber crime, colleges shall do the following:
 - Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.
 - Make copies of all audit trail information such as system logs, network connections (including IP addresses, TCP/UDP ports, length, and number), super user history files, etc.
 - Take steps to preserve and secure the trail of evidence.
 11. Colleges shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals as determined by agency management.
 12. Colleges shall maintain records of information security breaches and the remedies used for resolution as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned.
 13. College shall establish controls to protect data integrity and confidentiality during investigations of information technology security incidents.
 14. Controls shall either include dual-control procedures or segregation of duties to ensure that fraudulent activities requiring collusion do not occur.
 15. If any suspicious activities are detected, responsible personnel within the affected agency shall be notified to ensure that proper action is taken.

GUIDELINES

Information recorded in regard to information technology security breaches should cover the following:

1. The nature of the breach and the number of systems affected.
2. The services that were affected and the resources needed to implement a timely resolution.
3. The time at which the breach was discovered and the time at which corrective actions were implemented.
4. How the breach was detected and the immediate response after detection.
5. The escalation used to resolve the breach.

ISO 27002 REFERENCES

- 10.1.3 Segregation of duties
- 10.10.2 Monitoring system use
- 13.2.1 Responsibilities and procedures

- 13.2.2 Learning from information security incidents
- 13.2.3 Collection of evidence
- 15.3.1 Information systems audit controls
- 15.3.2 Protection of information systems audit tools

060204 Monitoring Confidentiality and Reporting Breaches

Purpose: To develop a method for identifying and reporting breaches of confidentiality.

STANDARD

1. Colleges shall monitor and control the release of confidential security information during the course of a security incident or investigation to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel or human resources.
2. College staff shall report breaches of confidentiality to college management as soon as possible. Confirmed incidents of confidentiality breaches shall follow the required reporting requirements.
3. Breaches of confidentiality include: the compromise or improper disclosure of confidential information such as Social Security numbers, medical records, credit card numbers and tax data.

ISO 27002 REFERENCES

- 6.1.5 Confidentiality agreements
- 6.2.3 Addressing security in third party agreements
- 13.2.1 Responsibilities and procedures

Chapter 7 – Business Continuity and Risk Management

Section 01 Business Continuity Management

070101 Initiating the Business Continuity Plan (BCP)

Purpose: To establish the appropriate level of business continuity management to sustain the operation of critical business services following a disaster or adverse event.

STANDARD

1. Colleges must maintain a business and disaster recovery plan with respect to information technology. Business and disaster recovery plans shall be provided to the Office of the State CIO.
2. Colleges, through their management, must implement and support an appropriate information technology business continuity program to ensure the timely delivery of critical automated business services.
3. A management team composed of representatives from all the College organizational areas has primary leadership responsibility to identify information technology risks and to determine what impact these risks have on business operations.
4. Management must also plan for business continuity, including disaster recovery, based on these risks and document continuity and recovery strategies and procedures in a defined business continuity plan that is reviewed, approved, tested and updated on an annual basis.

ISO 27002 REFERENCES

14.1.04 Business continuity planning framework

070102 Assessing the BCP Risk

Purpose: To require that Colleges manage information technology risks appropriately as required in GS 147-33.89.

STANDARD

1. Colleges shall identify the potential risks that may adversely impact their business in order to develop continuity and recovery strategies and justify the financial and human resources required to provide the appropriate level of continuity initiatives and programs.
2. Colleges shall conduct business risk impact analysis activities that include the following:
 - Define the College's critical functions and services.
 - Define the resources (technology, staff and facilities) that support each critical function or service.
 - Identify key relationships and interdependencies among the College's critical resources, functions and services.
 - Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact. (See also Statewide Glossary for Recovery Time Objective)
 - Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service. (See also Statewide Glossary for Recovery Point Objective)
 - Document any critical events or services that are time-sensitive or predictable and require a

- higher- than-normal priority (for example, tax filing dates, reporting deadlines, etc.).
- Identify any critical non-electronic media required to support the College's critical functions or services.
- Identify any interim or workaround procedures that exist for the College's critical functions or services.

GUIDELINES

The following items should be considered:

- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate financial losses over time resulting from the inoperability of each critical function or service.
- Estimate tangible (non-financial) impacts over time resulting from the inoperability of each critical function or service.
- Estimate intangible impacts over time resulting from the inoperability of each critical function or service.

ISO 27002 REFERENCES

14.1.02 Business continuity and risk assessment

14.1.04 Business continuity planning framework

070103 Developing the BCP

Purpose: To require that the appropriate level of information technology business continuity management is in place to sustain the operation of critical information technology services to support the continuity of vital business functions.

STANDARD

1. Management shall develop a business continuity plan (BCP) that covers all of the College's essential and critical business activities and that includes references to procedures to be used for the recovery of systems that perform the College's essential and critical business activities.
2. At a minimum, an College's business continuity plan must:
 - Help protect the health and safety of the employees of the State of North Carolina.
 - Protect the assets of the State and minimize financial, legal and/or regulatory exposure.
 - Minimize the impact and reduce the likelihood of business disruptions.
 - Create crisis teams and response plans for threats and incidents.
 - Include communication tools and processes.
 - Require that employees are aware of their roles and responsibilities in the BCP and in plan execution.
 - Include training and awareness programs.
 - Require simulations and tabletop exercises.
 - Have a documented policy statement outlining:
 - Framework and requirements for developing, documenting, and maintaining the plans.
 - Requirements for testing and exercising.
 - Review, sign-off and update cycles.

- Require senior management oversight and approval.
 - Assess the professional capability of third parties and ensure that they provide adequate contact with the Colleges.
 - Review dependence on third parties and take actions to mitigate risk associated with dealing with third parties.
 - Provide direction on synchronization between any manual work data and the automated systems that occur during a recovery period.
 - Set forth procedures to be followed for restoring critical systems to production.
3. Training and awareness programs shall be undertaken to ensure that the entire College is confident, competent and capable and understands the roles each individual within the College must perform in a disaster/or adverse situation.
 4. The person(s) designated as the College business continuity plan (BCP) coordinator(s) has the responsibility of overseeing the individual plans and files that constitute the BCP and ensuring that they are current, meet these standards and are consistent with the College's overall plan. At the direction of the State Chief Information Officer, a College's BCP shall be reviewed annually by the Office of Information Technology Services and recommendations shall be made for improvement, if necessary.
 5. The College business continuity plan shall be tested annually, at a minimum. All critical applications shall be tested annually.

GUIDELINES

The following methods are recommended:

- Tabletop testing (walk-through of business recovery arrangements using example interruptions).
- Simulations (especially for post-incident / post-crisis management roles).
- Technical recovery testing.
- Testing recovery at an alternate site.
- Testing of hot-site arrangements, complete rehearsal (testing organization, personnel, equipment, facilities and processes).
- Updating of plan as necessary.

Additional steps that may be taken include the repetition of the test to validate any updated procedure(s) and the addition or removal of application backup procedures. College management should define, document, and approve what type of testing methodology to use.

ISO 27002 REFERENCES

- 14.1.3 Developing and implementing continuity plans including information security
- 14.1.4 Business continuity planning framework
- 14.1.5 Testing, maintaining and re-assessing business continuity plans

070104 Disaster Recovery and/or Restoration

Purpose: To restore the operability of the systems supporting critical business processes and return to normal College operations as soon as possible.

STANDARD

The College is responsible for maintaining its ability to recover in the event of an outage. Colleges must ensure that business continuity and/or disaster recovery plans are developed, maintained, tested on a prescribed basis and subjected to a continual update and improvement process. Colleges shall conduct the following disaster recovery and/or restoration activities:

1. Define the College's critical operating facilities and mission essential service(s) or function(s).

2. Define the resources (facilities, infrastructure, and essential systems) that support each mission critical service or function.
3. Define explicit test objectives and success criteria to enable an adequate assessment of the Disaster Recovery and/or Restoration.

ISO 27002 REFERENCES

14.1.3 Developing and implementing continuity plans including information security

Section 02 Information Technology Risk Management Program

070101 Implementing a Risk Management Program

Purpose: To ensure that Colleges manage risks appropriately. Risk management includes the identification, analysis, and management of risks associated with a College's business, information technology infrastructure, the information itself, and physical security to protect the state's information technology assets and vital business functions.

STANDARD

1. The State of North Carolina recognizes that each College, through its management, must implement an appropriate Information Technology (IT) Risk Management Program to ensure the timely delivery of critical automated business services to the state's citizens.
2. The risk management program must identify and classify risks and implement risk mitigation as appropriate.
3. The program must include the identification, classification, prioritization and mitigation processes necessary to sustain the operational continuity of mission critical information technology systems and resources.
4. In general, "risk" is defined as a condition or action that may adversely affect the outcome of a planned activity. Some types of risk are as follows:
 - Business Risk – The cost and/or lost revenue associated with an interruption to normal business operations.
 - Organizational Risk – The direct or indirect loss resulting from one or more of the following:
 - Inadequate or failed internal processes
 - People
 - Systems
 - External events
 - Information Technology Risk - The loss of an automated system, network or other critical information technology resource that would adversely affect business processes.
 - Legal – Parameters established by legislative mandates, federal and state regulations, policy directives and executive orders that impact delivery of program services.
 - Reputation – General estimation, by the public, on how state services are delivered (integrity, credibility, trust, customer satisfaction, image, media relations, political involvement.)
 - Citizen Services - Program services mandated by charter, legislation, or policy that provides for the delivery of the state's business (education, human services, highways, law enforcement, health and safety, unemployment benefits, vital records, etc.)

GUIDELINES

Colleges are encouraged to select and use guidelines that support industry best practices for risk management relative to business continuity planning and security as appropriate. Some suggested guidelines are listed below.

Risk Management Program Activities:

College risk management programs at a minimum should focus on the following four types of activities:

- **Identification of Risks:** A continuous effort to identify which risks are likely to affect business continuity and security functions and documenting their characteristics.
- **Analysis of Risks:** An estimation of the probability, impact, and timeframe of the risks, classification into sets of related risks, and prioritization of risks relative to each other.
- **Mitigation Planning:** Decisions and actions that will reduce the impact of risks, limit the probability of their occurrence, or improve the response to a risk occurrence. For moderate or high rated risks, mitigation plans should be developed, documented and assigned to managers. Plans should include assigned manager's signatures.
- **Tracking and Controlling Risks:** Collection and reporting of status information about risks and their mitigation plans, response to changes in risks over time, and management oversight of corrective measures taken in accordance with the mitigation plan.

Business Continuity Risk Management Processes:

For business continuity risk management, the focus of risk management is an impact analysis for those risk outcomes that disrupt College business. Colleges should identify the potential impacts in order to develop the strategies and justify the resources required to provide the appropriate level of continuity initiatives and programs.

Colleges should conduct business risk impact analysis activities that include the following:

- Define the College's critical functions and services.
- Define the resources (technology, staff, and facilities) that support each critical function or service.
- Identify key relationships and interdependencies among the College's critical resources, functions, and services.
- Estimate the decline in effectiveness over time of each critical function or service.
- Estimate the maximum elapsed time that a critical function or service can be inoperable without a catastrophic impact.
- Estimate the maximum amount of information or data that can be lost without a catastrophic impact to a critical function or service.
- Estimate financial losses over time of each critical function or service.
- Estimate tangible (non-financial) impacts over time of each critical function or service.
- Estimate intangible impacts over time of each critical function or service.
- Document any critical events or services that are time-sensitive or predictable and require a higher- than-normal priority. (For example - tax filing dates, reporting deadlines, etc.)
- Identify any critical non-electronic media required to support the College's critical functions or services.
- Identify any interim or workaround procedures that exist for the College's critical functions or services.

Security Risk Process:

The focus of security risk management is an assessment of those security risk outcomes that may jeopardize College assets and vital business functions or services. Colleges should identify those impacts in order to develop the strategies and justify the resources required to provide the appropriate level of prevention and response. It is important to use the results of risk assessment to protect critical College functions and services in the event of a security incident. The lack of appropriate security measures would jeopardize College critical functions and services.

Security risk impact analysis activities include the following:

- Identification of the Federal, State, and Local regulatory or legal requirements that address the security, confidentiality, and privacy requirements for College functions or services.
- Identification of confidential information stored in the College's files and the potential for fraud, misuse, or other illegal activity.
- Identification of essential access control mechanisms used for requests, authorization, and access approval in support of critical College functions and services.
- Identification of the processes used to monitor and report to management on whatever applications, tools and technologies the College has implemented to adequately manage the risk as defined by the College (*i.e.*, baseline security reviews, review of logs, use of IDs, logging events for forensics, etc.).
- Identification of the College's IT Change Management and Vulnerability Assessment processes.
- Identification of what security mechanisms are in place to conceal College data (Encryption, PKI, etc.).

For more information on implementing a risk management program, including the Risk Management Guide and the Risk Assessment Questionnaire, please refer to the Risk Management Services page found on the Enterprise Security and Risk Management Office (ESRMO) web site:

<http://www.esrmo.scio.nc.gov/riskManagement/default.aspx>

ISO 27002 REFERENCES

- 4.1 Assessing security risks
- 4.2 Treating security risks