Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

NORTH CAROLINA
IIPS
COMMUNITY COLLEGES

# Information Security Manual

## Prepared by the IIPS Security Standards Committee

**Approval Date:**
**7/23/14**

**(Approved as written by Office of North Carolina State CIO)**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

## 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 Information and Data

## *Section 01 Setting Classification Standards*

### 010101 Defining Information

**Purpose:** To protect 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 College or State government.

The College’s information shall be handled in a manner that protects the information from unauthorized or accidental disclosure, modification or loss. All Colleges shall maintain a comprehensive and up-to-date database of their information assets and periodically review the database to ensure that it is complete and accurate.

Each College, through its management, is required to protect and secure the information assets under its control. The basic information requirements include, but are not limited to:

- Identifying information assets and maintaining a current inventory of information assets.
- Complying with applicable federal and state laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all applicable industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS)..
- Assessing the vulnerability and risk associated with information assets.
- Determining the value of information assets to the organization and the business processes they support.
- Providing the level of information protection for information assets that is appropriate to their vulnerability, risk level, and organizational value.
- Maintaining a business and disaster recovery plan with respect to information technology and process.

**ISO 27002 REFERENCE**
7.2.1 Classification guidelines

## 010102 Labeling Classified Information

**Purpose:** To protect the College's information through proper classification.

**STANDARD**

All data shall be labeled to reflect their classification, including their confidentiality, criticality and value to the College and the public. All data must be clearly labeled so that all users are aware of the custodian, classification and value of the data.

**ISO 27002 REFERENCE**
7.2.2 Information labeling and handling

## 010103 Storing and Handling Classified Information

**Purpose:** To protect the College's Information, including information security records, 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, if applicable, confidentiality.

The type and 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.

A College that uses confidential information from another College shall observe and maintain the confidentiality conditions imposed by the providing College if legally possible.

Colleges shall ensure that confidential information in electronic form is properly protected in transport or transmission.

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 individual census data.

The College shall manage and protect confidential information if provided to any external entity. The records disclosed that are confidential because the records disclose information technology security features shall be designated by affixing the following statement, “Confidential per G.S. §132-6.1(c)”, on each page.

The College shall be committed to the concern for and the protection of students’ rights and privacy of information The College will comply with the provisions of the Federal Family Rights and Privacy Act (FERPA), which is a federal law that governs the maintenance of students’ records. Under law, students have the right to inspect their educational records, correct inaccuracies in the records, if warranted, and the records are protected from release of information without written consent. The parent(s) of a dependent student as defined in Title 26 U.S. C.s152 of the Internal Revenue Code also has this right to inspect records that are maintained by the College on behalf of the student.

Confidential information technology security records shall be provided only to agencies and their designated representatives when necessary to perform their job functions. College shall ensure that confidential information is properly protected in transport or transmission. College shall ensure that all confidential information and related files under the college’s control in electronic format are handled properly and secured accordingly. Use of such information shall be in compliance with all applicable laws and regulations and limitations imposed by contract(s).

Confidential information technology security records shall not be transmitted electronically over public networks unless encrypted while in transit. See standard 030203 – Controlling Data Distribution and Transmission for the minimum requirement for encrypting data in transit.

Employees who are provided access to information technology security records shall sign a non-disclosure agreement that includes restrictions on the use and dissemination of the records. Colleges shall ensure that legal and business risks associated with contractors' access are determined, assessed and appropriate measures are taken. Such measures may include, but are not limited to, non-disclosure agreements, contracts, and indemnities.

**GUIDELINES**

- An appropriate set of 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

- Colleges should consider implementing practices and procedures that will ensure that electronic documents are properly managed throughout their life cycles.  A combination of manual and technical processes may be used to implement document management
- Output from systems containing information that is classified as confidential or critical should carry an appropriate classification label. The labeling should reflect the classification according to the rules established by Standard 010102, Setting Classification Standards—Labeling Information. Items for consideration include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, cassettes, USB flash memory drives), electronic messages and file transfers.
- Where appropriate, physical assets should be labeled. Physical labels are generally the most appropriate forms of labeling. However, 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.
- Documents that contain confidential information should be restricted to authorized personnel. 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.
- The originator of a telephone call, a telex/cable, a facsimile transmission, an email, a computer transaction, or any other telecommunications transmission should be aware of the possibility of compromise of confidentiality or integrity of the information transmitted and determine whether the information requires additional special protection and handling.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 7.2.2 | Information labeling and handling |
| 10.7.3 | Information handling procedures |
| 10.8.3 | Physical media in transit |

## 010104 Isolating Top Secret Information

**Standard Deleted/ does not apply to Community Colleges**

Standard deemed not applicable to the NC Community Colleges

## 010105 Classifying Information

**Purpose:** To protect the College’s information.

### STANDARD

All College information and data shall be classified as to its confidentiality, its value and its criticality. Colleges shall establish procedures for evaluating information and data to ensure that they are classified appropriately.

College shall designate and document data owners. Data owners shall designate and document data custodians based on the business needs of the College. Owners of data and their designees are responsible for College data and shall establish procedures for appropriate data handling.

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 marked with a designator that identifies the process by which such information is to be made available or accessible.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 7.2 | Information classification |
| 7.1.1 | Inventory of assets |
| 7.1.2 | Ownership of assets |

## **010106** Accepting Ownership for Classified Information

**Standard merged into Standard 010105**

## **010107** Managing Network Security

**Standard merged into 010102**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 2 – Controlling Access to Information and Systems

## *Section 01 Controlling Access to Information and Systems*

### 020101 Managing Access Control Standards

**Purpose:** To establish requirements for controlling access to the College's information assets.

**STANDARD**

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

All computers that are permanently or intermittently connected to college information systems networks shall have an approved password-based access control system. Regardless of the network connections, all computers handling confidential information shall employ approved password-based access control systems. Only authorized users shall be granted access to the College's information systems, and the principle of least privilege shall be used and enforced. Assignment of privileges shall be based on an individual's job classification, job function, and the person's authority to access information. Default access for systems containing confidential information shall be deny-all. Job duties shall be separated as appropriate to prevent any single person or user from having any access not required by their job function.

Access shall be controlled by the following:

- User profiles that define roles and access.
- Documented semi-annual review of users' rights.
- Documented review of privileged accounts every quarter.
- Restriction of connection time.
- Immediate termination of access upon severance or leaving employment.

College shall modify an individual's access to a College information technology asset upon any change of employment or change in authorization, such as a leave of absence or temporary reassignment.

To ensure that all data processed are the actual data required by the data custodian, predetermined times for processing those data must be set by the interested parties to protect the integrity of the data (e.g., preset batch file transmission times).

**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

Colleges shall be responsible for establishing policies and procedures for managing access rights for users of their networks throughout the life cycle of the user's credentials, such as user IDs, ID cards, tokens, and biometrics. There shall be a documented approval process whereby authorized parties specify required privileges for user access. Colleges shall communicate user account policies and procedures including authentication procedures and requirements to all users of an information system. Colleges shall identify a backup system administrator to assist with user account management when the primary system administrator is unavailable. Policies shall ensure that only authorized devices/persons have access as is appropriate for a College in accordance with the College's business needs.

Only authorized users shall be granted access to College information systems. Users shall be responsible for maintaining the security of their user credentials and passwords. User credentials shall be individually assigned and unique in order to maintain accountability. User credentials shall not be shared but only used by the individual assigned to the account. Each user credential shall be used by only a single individual, who is responsible for every action initiated by the account linked to that credential. 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. Default/generic user accounts and passwords shall be disabled or changed prior to a system being deployed in production.

User credentials shall be disabled promptly upon a user's termination from work for the College or upon cessation of a user's need to access a system or application. User credentials that are inactive for a maximum of 90 days must be disabled, except as specifically exempted by the security administrator. All accounts that have been disabled for greater than 365 days shall be deleted.

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.

#### Logging of Administrator Activity

All user credential creation, deletion and change activity performed by system administrators and others with privileged user credentials shall be securely logged and reviewed on a regular basis.

**Concurrent Connections**

For those systems that enforce a maximum number of concurrent connections for an individual user ID, the number of concurrent connections must be set to two (2).

**Non-Employee/Contractor Credentials**

User credentials established for a non-employee/contractor must have a specified expiration date unless the provision of a user credential without a specified expiration date is approved in writing by the agency security liaison. If an expiration date is not provided, a default of thirty (30) days must be used.

Access control may need to be modified in response to the confidentiality of information contained on the system, if existing access controls pose a risk that confidentiality may be breached.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 11.2 | User access management |
| 11.11.1 | Access control policy |

## 020103 Securing Unattended Work Stations

**Purpose:** To prevent unauthorized system access.

### STANDARD

Workstations shall be safeguarded from unauthorized access—especially when left unattended. 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. Users shall not disable the password-protected configuration specifications established by their College. Users should lock their workstations when leaving them unattended.

When not in use for an extended period of time, as defined by the agency, each desktop/laptop shall be logged off.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 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 State Network and College networks.

**STANDARD**

Access to networks operated by State Colleges, including the State 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.

- All remote access (dial-in services) to the networks shall be either through an approved modem pool or via an Internet service provider (ISP).
- Remote users shall connect to the State Network only using protocols approved by the College's CIO. Remote users with direct connections to College networks shall follow College protocols.
- When users on the College networks connect to external systems, including the State Network, they shall comply with the College's Acceptable Use Guidelines.
- Users on the State Network shall not be connected to the State Network at the same time as they are connected to an external network via a separate telecommunication device.
- Users shall not extend or retransmit network services in any way without appropriate management approval.
- 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.
- Non–State of North Carolina computer systems that require connectivity to the State Network shall conform to state wide security standards.
- Non–State of North Carolina computer systems that require connectivity to College networks shall conform to College security standards.
- Users shall not download, install or run security programs or utilities that reveal weaknesses in the State Network without prior written approval from the College CIO. Users shall not download, install or run security programs or utilities that reveal weaknesses of College networks without appropriate College management or security liaison approval. For example, State users must not run password-cracking programs, packet sniffers, network-mapping tools or port scanners while connected in any manner to the State Network infrastructure. Users shall not be permitted to alter network hardware in any way.

**ISO 27002 REFERENCE**

11.4 Network access control

## 020105 Controlling Access to Operating System Software

**Purpose:** To limit access to operating system 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. System administrators shall ensure that all current maintenance and security vulnerability patches are applied and that only essential application ports are opened in the system's firewall.

- Configuration and system design information of a sensitive nature 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.
- State Colleges shall maintain a list of administrative contacts for their systems.
- All authorized users of administrative-access accounts shall have management instructions, documentation and training.
- 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.
- Each account used for administrative access shall comply with Standard 020106, Managing Passwords.
- When special-access accounts are needed for internal or external audit, software development, software installation, or other defined need, they shall be authorized in advance by management and shall be:
  - Created with a specific expiration date.
  - Removed when the work is completed.
- Administrative-access accounts must connect in a secure manner at all times.

**ISO 27002 REFERENCE**
11.5 Operating System Access Control

## 020106 Managing Passwords

**Purpose:** To prevent unauthorized access and to establish user accountability when using credentials and passwords to access State information systems.

### STANDARD

Colleges shall manage passwords to ensure that all users are properly identified and authenticated before being allowed to access State information systems. 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 selected as the method of performing identification and authentication. A unique user credential shall be assigned to each user so that individual accountability can be established for all system activities. Management approval shall be required for each user credential created. A process shall be in place to remove, suspend or reassign user IDs that become inactive as a result of employee or contractor movements.

The information system's authentication system shall limit unsuccessful logon attempts. Where possible, unsuccessful logon attempts shall be limited to three before the user logon process is disabled. In order to facilitate intrusion detection, information shall be retained on all logon attempts in accordance with the College records retention policy. The locked out duration shall be at least 30 minutes or until an administrator re-enables the user's account.

Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members or coworkers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.

Under no circumstances shall a user respond to e-mails or other queries with their password or other account information. Attempts to gain access to a user's password through these social engineering means (i.e. phishing) must be reported to the College security administrator.

Password management capabilities and procedures shall be established to ensure secrecy of passwords and prevent exploitation of easily guessed passwords or weaknesses arising from long-life passwords. Each College shall evaluate its business needs and the associated risks for its information systems in conjunction with identification and authentication requirements. When IDs and passwords are selected as the method of performing identification and authentication, Colleges are required to select and use the appropriate standards and best practices. Depending on the operating environment and associated exposures, additional or more stringent security practices may be required.

- Where technically feasible, passwords shall be at least eight (8) characters long for access to all systems and applications
- To the extent possible, passwords shall be composed of a variety of letters, numbers and symbols[1].
- To the extent possible, passwords shall be random characters from the required categories of letters, numbers and symbols.
- Passwords shall not contain dictionary words or abbreviations.
- Passwords shall not contain number or character substitutes to create dictionary words (e.g., *d33psl33p* for *deep sleep*[2]).
- Passwords for State and College resources shall be different from passwords for external, non-State resources (i.e. website not affiliated with the State or College).
- Password generators that create random passwords shall be allowed.
- Password management application features that allow users to maintain

[1] 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.

[2] Other examples of numbers/symbols for letters are *0* for *o*, *$* or *5* for *S*, *1* for *i*, and *1* for *l*, as in *capta1n k1rk* or *mr5pock*.

password lists and/or automate password inputs shall be prohibited, except for systems approved by the College Chief Information Officer.

**Password Management Standards**

- Except as specifically allowed by the security liaison, passwords shall not be revealed to anyone, including supervisors, family members or co-workers. In special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.
- Users shall enter passwords manually, except for simplified/single sign-on systems that have been approved by the College CIO.
- No automated password input shall be allowed, except for simplified/single sign-on systems that have been approved by the College CIO.
- 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.
- Password Changes:
    - College employees and contractor passwords (e.g., email, Web and calendar) used to access systems and applications shall be changed at least every ninety (90) days. Passwords shall not be reused until six additional passwords have been created..

- Passwords shall not be inserted into email messages or other forms of electronic communication without proper encryption. Conveying a password in a telephone call is allowed when a positive identification has been established.
- Where possible and practicable, access to password-protected systems shall be timed out after an inactivity period of thirty (30) minutes or less or as required by law, if the inactivity period is shorter than thirty (30) minutes.
- Passwords shall not be displayed in clear text during the logon process or other processes. Where possible, applications that require clear-text authentication shall be converted to equivalents that can use encryption.[3]
- Passwords shall be changed whenever there is a chance that the password or the system could be compromised.
- There shall be a 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**

- All typical user passwords (e.g., UNIX, Windows, personal computing, RACF, applications, etc.) shall be changed at least every ninety (90) days. 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.
- A user account that has system-level privileges, more privileges than a typical user account, or programs such as root access shall have a different password from all other accounts held by that user.

[3] Encryption is defined in the Security Architecture Chapter, Standard 3, Use Cryptography Based on Open Standards.

- Password files shall be retrievable only by the security liaison or a designated backup security liaison.
- Vendor-supplied default and/or blank passwords shall be immediately identified and reset as soon as an information system is installed.
- The password for a shared administrative-access account shall change when any individual who knows the password leaves the College that established the account or when job responsibilities change.
- 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**

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.

- Service accounts must be dedicated solely to their business purpose.
- Service accounts shall be separate from any other accounts.
- Controls must be in place to prevent misuse of a service account.
- All service accounts must have appropriate logging of account activity. The application/device owner must audit the service account usage at least every 30 days.
- All service account passwords must meet system administrator password complexity standards.
- 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).
- 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/officer. Internal controls, policies, and procedures must be put in place to closely monitor and mitigate risk caused by non-expiring passwords.
- A service account password must be changed immediately after any potential compromise or any individual who knows the password leaves the College that established the account.

**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
8.2.3 Disciplinary process
15.1.5 Prevention of misuse of information processing facilities

## 020107 Securing Against Unauthorized Physical Access

**Standard merged into standard 090104**

## 020108 Restricting Access

**Purpose:** To ensure that information system access is granted only to authorized users.

### STANDARD

Colleges shall establish appropriate controls on access to information systems to allow only those authorized to access the data residing on those systems to do so. ~~Third party access to College resources shall be controlled using physical and logical safeguards. Third party access to College resources shall be granted on a need to have basis.~~

Users of College information systems shall be provided access to information and system functions in accordance with Standard 020101, Managing Access Control Standards.

Access to confidential information shall be restricted to authorized individuals who require access to the information as part of their job responsibilities

A College may change, restrict or eliminate user access privileges at any time.

**ISO 27002 REFERENCE**
11.6.1 Information access restriction

## 020109 Monitoring System Access and Use

**Purpose:** To establish requirements and guidelines for policies that disclose to employees and third-party contractors using State information systems the situations in which and the purposes for which filtering and monitoring may occur.

### STANDARD

Colleges shall have the right and ability to monitor and filter use of information systems by employee and third-party contractor users.

Colleges using monitoring and filtering technologies must establish policies to provide adequate notice to State employees and third-party contractors of what the College will be filtering and/or monitoring. The policies shall include the circumstances under which filtering and monitoring will take place. The policies shall also state that users shall have no expectation of privacy unless expressly granted by a College.

Colleges using filtering and monitoring must:

- 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.
- Specify in their written policies 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.
- Obtain a written receipt from College employees and third-party contractors acknowledging that they have received, read and understood the College's filtering and monitoring policies.
- Inform College employees and third-party contractors of any activities that are prohibited when using the College's information systems.

**ISO 27002 REFERENCE**
10.10.2 Monitoring system use

## 020110 Giving Access to Files and Documents

**Purpose:** To prevent the unauthorized or accidental copying, moving, editing or deleting of data and to protect the confidentiality, integrity and availability of the information assets of North Carolina.

### STANDARD

Custodians of data shall assign staff the responsibility for administering and maintaining the rights and permissions for accessing the data and information.

- Users shall be provided with access to information and systems in accordance with a defined standard of access control such as:
  - Discretionary access control.
  - Mandatory access control.
  - Lattice-based access control.
  - Rule-based access control.
  - Role-based access control.
  - Access control lists.
- The default for access is role-based access control for files and documents.
- 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.
- User rights shall be reviewed at six (6)-month intervals.

**ISO 27002 REFERENCE**
11.2.4 Review of user access rights

## 020111 Managing Higher Risk System Access

**Purpose:** To protect the confidentiality, integrity and availability of data on high-risk information technology systems in State government.

### STANDARD

Certain systems and applications, because of the nature of the data contained in them, require special management oversight and shall be classified as high-risk. Many times these high-risk systems contain confidential data. At a minimum, these systems shall require access control equal to that specified in Standard 020101, Managing Access Control Standards.

All systems and applications shall be classified through a risk assessment to determine, in part, whether they are high-risk systems.

### GUIDANCE

At a minimum, the following should be considered when implementing controls for high-risk systems:

- Whether access to the system is allowed from an external site.
- Hardening of the operating system.
- Criminal Background checks of personnel, vendors and contractors in contact with the system and applications.
- Disaster recovery planning.
- The consequences of loss of data security.

**ISO 27002 REFERENCE**

11.6.2 Sensitive system isolation

## 020112 Controlling Remote User Access

**Purpose:** To control both physical and logical access to diagnostic and configuration ports. To require users of State information technology systems who access College information technology systems remotely to do so in a secure manner.

### STANDARD

Authorized users of College computer systems, the State Network and data repositories shall be permitted to remotely connect to those systems, networks and data repositories for the conduct of College business only through secure, authenticated and carefully managed access methods.

Access to the State Network and College internal networks 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 and the approval of the College CIO.

Additionally, remote accessing of networks and systems shall include but not be limited to the following:

- Administrators shall take all precautions necessary to ensure that administrative activities performed remotely cannot be intercepted or spoofed by others. Guidance: configure timestamps, encryption, and/or dial-back mechanisms.

- Enhanced authentication and encryption mechanisms shall be used to protect data used for remote management of network devices or servers.
- Systems connecting remotely to Colleges connected to the State Network must have antivirus software installed compliant with the statewide antivirus standard.
- Systems connecting remotely to Colleges connected to the State Network must have the latest campus approved operating system and application patches installed.
- Access to diagnostic ports (especially dial-up diagnostic ports) shall be securely controlled and enabled only when needed for authorized diagnostic access.
- 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.
    - Inbound and outbound network traffic shall be controlled and limited to only that necessary to accomplish the College's mission, using a perimeter firewall and host-based firewall compliant with the statewide firewall standards.
    - Virtual private networks (VPNs) shall require user authentication and encryption strength compliant with the statewide encryption standard.
    - Internal addresses, configurations, dial-up modem numbers, and related system design information for the College's networking systems shall be kept secret and not made public knowledge.
    - Administrators must gain College management approval for any modem installed at a workstation and must not leave modems connected to computers that have auto-answer mode enabled.[4]
    - All dial-up connections with the College's systems and networks must be routed through a modem pool that includes an approved user authentication system.

Opening uncontrolled or unsecured paths into any element of the State Network that requires security or to College internal computer systems presents unacceptable risk to the entire College and State infrastructure. Diagnostic and

[4] Unless the modem is needed for business purposes, it is recommended that, in systems with built-in modems that cannot be removed from the machine, the modem driver be uninstalled and the modem device be disabled within the operating system to disable the modem functionality.

configuration ports shall be restricted to authorized individuals.

- Services that aren’t required for business use should be disabled.
- Ports that aren’t required for business use should be closed.

**Standard for Remote Access**

Access shall be permitted through a College-managed secure tunnel such as a Virtual Private Network (VPN) or other open standard protocol such as Secure Shell (SSH) or Internet Protocol Security (IPSec) that provides encryption and secure authentication.

**Authentication**

- The authentication and authorization system for remote access shall be managed by the College. Colleges that need centralized network infrastructure services, such as Public Key Infrastructure (PKI), shall use the state-wide authentication and authorization service known as NCID.
- Authentication for remote access shall be strong. Passwords shall not traverse the network in clear text and must meet minimum requirements as documented in approved security policies and standards. Each user who remotely accesses an internal network or system shall be uniquely identifiable.

**Users**

- 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 credentials. 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.
- 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 regularly scheduled security assessments.
- Anonymous interaction: With the exception of Web servers or other systems where all regular users are anonymous, users are prohibited from remotely logging into any College system or network anonymously (for example, by using “guest” user 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 employing a user ID that clearly indicates their identity.

**Configuration**

- 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.
- 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.
- Antivirus and firewall protection: External computers or networks making remote connection to internal College computers or networks shall utilize a College-approved active virus scanning and repair program and a College-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.
- 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 (users connected through dial-up phone modems, dial-up Internet service providers, or broadband, i.e., 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 agency policy, industry standard (i.e. 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 State Network. In addition, all user IDs 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 time-out period, if any, for hand held devices, (e.g. smart phones, personal data assistants, and Blackberry-like devices), 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 credentials following a sequence of several unsuccessful attempts to log in. For example, if an incorrect dynamic password is provided three consecutive times, dial-up systems shall drop the connection. Repeated unsuccessful attempts to remotely establish a connection using a privileged user credential shall not result in the revocation (suspension as opposed to time-out) of the user credential because this could interfere with the ability of authorized parties to respond to security incidents.
- Modems on desktop/laptop systems: College management shall set policies and procedures for approved modem usage. Management must approve the use of modems and the communications software used with modems. Existing modems connected to a LAN that are used for remote control and file transfer from a remote location to LAN desktops must be replaced as soon as possible with a secure TCP/IP or VPN connection. Unless a dynamic password system is installed, workers with home-based, mobile or telecommuting PCs shall not leave modems in auto-answer mode, with communications software enabled, such that incoming dial-up calls could be received.
- VPN and/or other secure communication protocols shall be used to communicate with College business systems.
- 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 rules 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**

- Remote access to single-equipment hosts (i.e., College servers, Web-hosting equipment) shall be permitted provided that these requirements are met:
  - Dial-up modem service: A College shall provide dial-up modem service *only if* that service is limited exclusively to College employees and contractors.
  - Web-hosting servers can provide anonymous or authenticated access to pages *only if* the service host prevents onward connection to the State Network.
- Management consoles and other special needs: Users requiring modem

[5] *See,* **120201** Managing Media Storage and Record Retention

access for “out of band” management or special needs must obtain College security administrator approval for the modem and its use as set forth in College procedures. Each College shall establish procedures to approve modems on an individual basis. Any dialup 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**

- Disclosure of systems information: The internal addresses, configurations and related system design information for College computers and networks shall be kept confidential and shall not be released to third parties who do not have a demonstrable need to know such information. Likewise, the security measures employed to protect College computers and networks shall be kept confidential and shall be similarly protected.
- Systems shall support the capability for all remote access occurrences to be logged (user credential, date/time, and duration of connection at a minimum).
- There may be certain remote-access users who warrant use of file/disk encryption technology. This is based on whether confidential records are included in the information that they are able to store on their local systems. File/disk encryption shall be employed as needed and shall follow the requirements of the encryption standard 030801 – Using Encryption Techniques**.**
- Systems connecting remotely to agencies connected to the State Network must have the latest operating system and application patches installed.
- Access to diagnostic and configuration ports (especially dial-up diagnostic ports) shall be securely controlled and enabled only when needed for authorized diagnostic access.
- Audit: Audit logs of remote-access activities shall be maintained for at least ninety (90) days.

**ISO 27002 REFERENCE**
11.4.2 User authentication for external connections
11.4.4 Remote diagnostic and configuration port protection

## 020113 Types of Access Granted to Third Parties

**Standard merged into standard 020108**

## 020114 Why Access is Granted to Third Parties

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

**Standard merged into standard 020108**

## 020115 Access Control Framework for Network Security

**Purpose:** To establish standards for Colleges accessing the State network.

### STANDARD

Colleges shall follow the attached matrix, Access Control Framework (ACF), to prevent unauthorized access to information systems through appropriate placement and configuration that provides protective measures that are commensurate with the security level required to protect the data contained in those systems.

Colleges shall assess the risk associated with each business system to determine what security rules apply to the system and/or application. 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. The assessment assigns correlative security requirements. As the critical nature of the data and applications increases, the security measures required to protect the data and applications also increase.

**Security Requirements**

Security for the network infrastructure and for distributed systems operated by state Colleges shall comply with the security requirements of the template, which is attached and 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.

The Access Control Framework for Network Security Template 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. For the Application and Database secure zones, a College approved firewall or other network segmentation mechanism, such as ACLs, is required to segregate application servers and database servers. . Where end user access is allowed to a resource, it is designated with "Opt." for optional. Client-server applications that operate on a college local area network (LAN) and are not public facing (i.e. Internet accessible) may fall under the College Internal LAN column of the matrix below. For the purpose of the framework, software components installed on end points (i.e. thick clients) do not constitute a valid network zone.

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 NC Community College standards included in this manual.

**Special Assembly Security Requirements**

Colleges not able to adhere to the DMZ and/or other security requirements in the ACF shall develop a Special Assembly zone and document the rationale for developing the Special Assembly zone. This should be done under the supervision and approval of the local College CIO. CIO will be responsible for audit, documentation, and maintenance of 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. 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**

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. 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). Where feasible, colleges should consider separating high risk virtual machine farms from low risk machine farms on to separate physical servers. 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. The approach to virtual machine security control and segregation shall balance the business needs, practical approach, industry standard practices and the associated risk.

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 Information Security standards when the College utilizes such services through SLAs and contracts.

## *Access Control Framework for Network Security Template*

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

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

## *Access Control Framework for Network Security Template*

| | DMZ | | | Secure Zone | | | | Special Assemblies | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Web / User Facing | | | Application Services | | DB Services | | Mgmt. Domain | Application Unique Domain***** | College Internal LAN | | |
| | **Public** | **State** | **Vendor** | **Std.** | **High** | **Std.** | **High** | | | | | |
| **User Access** | 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 | | |
| | | | | | | | | | | | | |
| **Operational Controls** | | | | | | | | | | | | |
| **Firewall/Access Control**** ** | Req. | Req. | Req. | Req. | Req. | Req. | Req. | Req. | Req. | Req. | | |
| **IDS/IPS - Network******** | Req. | Req. | Req. | Req. | Req. | Req. | Req. | Opt. | TBD | Opt. | | |
| **IDS/IPS - Host** | Opt. | Opt. | Opt. | Opt. | Opt. | Opt. | Opt. | Opt. | TBD | 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 NC Community College Vulnerability Management Standard**

****** Must follow NC Community College Firewall Standard**

******* Application Unique Domain To Be Determined (TBD) 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. Each College shall determine if this meets their specific requirements.**

**ISO 27002 REFERENCE**
11.11.1 Access control policy

## 020116 Access Standard

**Standard merged into standard 20102**

## 020117 Controlled Pathway

**Purpose:** To establish a standard to limit access to business resources.

### STANDARD

A controlled pathway shall be used in College networks to assist in secure communications. Controlled paths shall be specified for remote users and local users when accessing College resources.

### GUIDELINES

Special considerations should be given to limit roaming on wireless networks and restricting access to business applications through the use of zones listed in the Table set forth in Standard 020115.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 11.4.2 | User authentication for external connections |

## 020118 Node Authentication

**Purpose:** To verify authentication processes are operating properly.

### STANDARD

Procedures that verify node authentication measures shall be developed and tested on a semi-annual basis.

### GUIDELINES

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 REFERENCE**

| | |
|---|---|
| 11.4.2 | User authentication for external connections |

## 020119 Diagnostic and Configuration Port Controls

**Stardard merged into standard 020112**

## 020120 Granting Access to Non-College Individuals

**Purpose:** To ensure security arrangements are in place prior to granting customer or third party system access.

### STANDARD

Students and third parties must agree to adhere to all applicable College security policies and standards prior to receiving access to building facilities or information systems.

### GUIDELINES

Safeguards to ensure customers agree to policies and standards should include:

- A written justification or purpose for access.
- Guest badges or alternate identification so staff may recognize the identity of the visiting person.
- Informational material to inform the accessing person(s) of responsibilities.
- A discrete notification of services authorized to access.
- A discrete disclaimer that system access may be monitored.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 6.2.2 | Addressing security when dealing with customers |

## 020121 Acceptable Usage of Information Assets

**Purpose:** To ensure information assets are used in an acceptable fashion by customer or third parties.

### STANDARD

Colleges shall develop Acceptable Use Policies (AUP's) or standards for staff, customers and third parties to follow. 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, e-mail usage and Internet usage.

### GUIDELINES

AUP's and/or standards should focus at a minimum on the use of E-mail, Internet, and computing devices.

**ISO 27002 REFERENCE**
7.1.3 Acceptable use of assets

## **020122** Management Duties

**Purpose:** To use ensure management duties include compliance to information security policies and procedures.

### STANDARD

All levels of management must ensure that employees, contractors, and third parties adhere to approved information security procedures.

Management duties shall include, but not be limited to ensuring staff:

- Become informed about security responsibilities.
- Attain continued education relevant to information security and their position in the organization.
- Are held contractually accountable for the proper use of those procedures, if applicable.
- Possess the necessary skills and qualifications to carry out their task(s) appropriately.
- Work to keep skills current within the technology

**ISO 27002 REFERENCE**
8.2.1 Management duties

## **020123** Third Party Service Management

**Purpose:** To use ensure management of contracts with third parties. To monitor third party contracts and invoke penalty clauses as appropriate.

### STANDARD

Colleges shall manage third parties to meet or exceed mutually agreed upon signed contracts. Colleges shall also ensure that third parties meet or exceed all State policies, standards and procedures.

Services, outputs and products provided by third parties shall be reviewed and checked regularly.

To monitor third party deliverables, Colleges shall:

- Monitor service performance of third party vendor to ensure service levels are up to contract requirements.
- Review reports provided by third parties and arrange regular meetings as required by contract(s).
- Local College CIO will provide information concerning security incidents to the Enterprise Security and Risk Management Office (ESRMO) as deemed necessary based on CIO's assessment of the incident.
- Review third party reports including the following, but not limited to, audit logs, operational problems, failures, fault analysis, as they relate to services being delivered, including security events.
- Resolve and manage any identified problem areas.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 10.2.1 | Service delivery |
| 10.2.2 | Monitoring and review of third party services |

## **020124** Monitoring Third Party Services

This standard is addressed in 020123 – Third Party Service Management.

## **020125** Third Party Service Changes

**Purpose:** To ensure changes to services by third parties are agreed upon prior to the changes taking place.

### STANDARD

Any changes to services being provided by a third party must be approved by the College administration or responsible designee prior to implementation. Contracts need to be updated to reflect the changes that occur.

Examples to changes in contracts 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 REFERENCE**

| | |
|---|---|
| 10.2.3 | Managing changes to third party services |

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 3 – Processing Information and Documents

## *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 but not be limited to the following:

- The cabled network infrastructure must comply with industry standards and be installed by a licensed, bonded contractor or employee.
- 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 approved by security institutes such as the SANS Institute or the National Security Agency (NSA).
- Primary network address space (Internet Protocol [IP]/Internet Packet Exchange [IPX]) shall be distributed, registered and managed by NCREN.
- Critical hardware and systems, including the network infrastructure, shall be connected to an uninterruptible power supply (UPS).
- Network devices shall be configured to support authentication, authorization and accountability mechanisms when being administered.
- Configuration management, patch management and change management standards and procedures shall be applied to all applicable systems.
- 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.
- Configuration shall include elimination of the possibility of bridging

networks via secondary Internet connections.

- Publicly and/or anonymously available network servers/services such as email, Web, and ftp shall be segregated from a College's internal user LAN.
- Configuration shall include accommodations for flexibility, scalability and reliability to meet growing user demands and conserve IT funds of the future.

DNS servers shall not be configured to allow zone transfers to unknown secondary servers.

- If a College maintains a primary DNS server, zone transfers will be allowed only to trusted (known) servers.
- If a College maintains a secondary DNS server, zone transfers will be allowed to the primary DNS server only.
- When a domain has a US extension (*i.e.,* state.nc.us), the US Domain Registry requires that 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 ITS maintains the DNS, Colleges may request ITS to allow additional IP addresses to receive zone transfers. Colleges must work with ITS to define acceptable IP addresses and/or IP address ranges.

**ISO 27002 References**

| | |
|---|---|
| 10.6 | Network security management |
| 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

Network security shall be managed by each College based on business needs and the associated risks.

Access to information available through the State and College network shall be strictly controlled in accordance with approved access control procedures. Users shall have direct access only to those services that they have been authorized to use.

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.

Secure management of the network infrastructure shall include but not be limited to the following:

- Use of secure protocols such as Secure Shell (SSH), Secure Sockets Layer (SSL), and Internet Protocol Security (IPSec).  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.
- Use of authentication, authorization and accountability mechanisms when administering network devices.
- Monitoring for attempts to deny service or degrade the performance of n**e**twork systems (including computers, microcomputers, networks, telephone systems and video systems).
- Where performance and quality of service are at risk, restrict the transfer of large amounts of data[6] between computing systems during business hours, unless required or authorized by senior management.
- 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 |

## **030103** Accessing Your Network Remotely

**Standard merged into standard 020112**

[6] Because each service and network is different and because bandwidth capabilities differ, "large amounts of data" must be a subjective term.

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

## **030104** Defending Network Information from Malicious Attack

**Purpose:** To protect information residing on State and College networks.

### STANDARD

Colleges shall implement layers of information security (defense in depth) to defend against attacks on the College’s information resources. System usage shall be monitored and reviewed for activities that may lead to business risks.

System usage shall be monitored and reviewed 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.

### GUIDELINES

●

All safeguards and network security plans shall incorporate the following controls:

- Configuration of system hardware, operating systems and applications software and network and communication systems to information security 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 industry guidelines and security standards from institutes such as the SANS Institute or the National Institute of Standards and Technology (NIST).
- Implementation of preventive measures to limit internal and external parties’ abilities to inflict harm on the College’s information technology resources.
- Implementation of measures to prevent snooping, sniffing, network reconnaissance and other means of gathering information about the network infrastructure.
- Implementation of measures to filter unwanted traffic (spam, bots, etc.) attempting to enter the internal network.
- Installation of antivirus software that protects the College’s infrastructure from downloads, media transfers, electronic-mail attachments of malicious software, or other malware.
- Continuous monitoring for attempts to deny service or degrade the

performance of information systems (including computers, microcomputers, networks, telephone systems and video systems).

- Periodic review of system logs for signs of misuse, abuse or attack.
- Items to monitor may include, but not 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. Examples of such technologies are server clustering, redundant links, link load balancing and redundant array of independent disks (RAID) backups.

**ISO 27002 References**

| | |
|---|---|
| 10.4.1 | Controls against malicious code |
| 10.10.2 | Monitoring system use |

## **030105** Network Segregation

**Purpose:** To help protect internal networks through network segregation.

### STANDARD

Colleges' internal network infrastructures (i.e., College local area networks [LANs]) shall be segregated into internal network zones to protect servers from the user LAN and to segregate test and production environments.

Wireless networks shall be physically or logically segregated from internal networks such that an unknown external user cannot access a College's internal network unless it was designed for that specific use.

### GUIDELINES

Colleges should consider segregating network management protocols onto a separate internal network zone from the production zone. For example, network monitoring traffic and network administration traffic should be logically segregated from end users and from the production network.

Segregation may be achieved by one or both of the following common methods or through similar methods of achieving logical segregation:

- Implementing virtual LANs (VLANs) with access control lists in a switched network environment.
- Using routers or internal firewalls with access control lists.

**RELATED INFORMATION**

Standard 020115 – Access Control Framework
Standard 090301 – Electronic Eavesdropping

**ISO 27002 References**
11.4.5 Segregation in networks

## 030106 Controlling Shared Networks

This standard is addressed in 030102 – Managing the Networks.

## 030107 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:

- Positive source and destination address checking to restrict rogue networks from manipulating the College's routing tables.
- Authentication to ensure that routing tables do not become corrupted with false entries.
- Network address translation (NAT) or PAT (Port Address Translation) to screen internal network addresses from external view.
- 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. Default: The default firewall policy is for all ports to be closed. Only those ports for which College has written, documented business reasons for opening shall be open. 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 achieve best practice compliance. Each college shall manage its own risk through this process in accordance with the Information Technology Risk Management Policy with Guidelines. 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[7]. 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. 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. Identity: 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.

2. Physical Security Firewalls shall be installed in locations that are physically secure from tampering. The College security information technology liaison shall approve the physical location of the firewalls. Firewalls shall not be relocated without the prior approval of the IT security liaison or IT department manager.

3. Firewall Rule sets Firewall rule sets shall always block the following types of network traffic[8]:

   - 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 State 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

[7] A security specialist for firewall configuration is an individual who understands firewall technology and security requirements. If ITS manages the firewall, ITS will provide the security specialist.

[8] Exceptions to the blanket rules are included in the applicable bullets.

inbound to the State 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.

5. 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 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.

6. Monitoring and Filtering
   - Logging features on state 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 ITS, 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 |

## **030108** Network Security

**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**

ITS is responsible for the security of the infrastructure of the state's network.

Organizations with connections to the state network are responsible for managing risk and providing appropriate security for their networks. Security measures must conform to applicable enterprise network security standards, architecture, and policies. College internal security measures shall be deployed only on College internal networks and must not adversely affect the state network.

Any and all actions that jeopardize the integrity and stability of the state network will be addressed commensurate to the level of risk. ITS is authorized to immediately suspend network service to any organization when the level of risk warrants immediate action. When network service is suspended, ITS will provide immediate notice to the organization. When possible, ITS will notify any organization of any such action in advance of such an action. ITS will work with the organization to rectify the problem that caused the suspension. Any violations of this network security standard are subject to review by the College Chief Information Officer (CIO) and College management and are subject to action that conforms to state disciplinary policies and any and all relevant law. These actions may include termination of service. Termination requires appropriate notification by ITS, including notification to its upstream providers, and the termination should be at the lowest level necessary to safeguard network security and minimize disruption of business activities.

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.

### RELATED INFORMATION

070104 Using External Service Providers for E-Commerce

**ISO 27002 References**

| | |
|---|---|
| 10.6.2 | Security of network services |

## **030109** Time-out Facility

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

### STANDARD

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. 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.

All terminals, workstations, and laptops connected to the College network shall enable a terminal time-out mechanism to prevent unauthorized viewing or use when the terminal, workstation, or laptop is unattended.

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. 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 industry standards or other regulations.

### GUIDELINES

Terminal time-outs may be achieved through the use of College approved, password protected screen savers (sometimes called "screen locks").

**ISO 27002 References**
11.5.5 Session time-out

## **030110** Exploitation of Covert Channels

**Purpose:** To limit the risk of information leakage through the use and exploitation of covert channels.

### STANDARD

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.

See the Related Information section, below, for references to the policies that address specific protection mechanisms.

### RELATED INFORMATION

030301 Downloading Files and Information from the Internet
030304 Receiving Electronic Mail
030314 “Out of the Box” Web Browser Issues
030318 Certainty of File Origin
030505 Receiving Information on Disks
030902 Loading Personal Screen Savers
060107 Defending Against Hackers, Stealth- and Techno-Vandalism
060109 Defending Against Virus Attacks
060111 Installing Virus Scanning Software
080201 Software Development
080206 Separating Systems Development and Operations

**ISO 27002 References**

| | |
|---|---|
| 12.5.4 | Information leakage |

## **030111** Authentication of Network Connecting Equipment

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

### STANDARD

To protect the College and State 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.

### GUIDELINES

Equipment identification 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.

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”).

**ISO 27002 References**

| | |
|---|---|
| 11.4.3 | Equipment identification in networks |

## *Section 02 System Operation and Administration*

## 030202 Administering Systems

**Purpose:** To establish security roles and duties for system administrators.

### STANDARD

Colleges must clearly define security responsibilities for system administrators, who shall protect their assigned information technology resources and the information contained on those resources. Colleges must also provide appropriate training for their system administrators.

System administrators shall:

- 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 Reference**

6.1.3 Allocation of Information Security responsibilities

## 030203 Controlling Data Distribution and Transmission

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

### STANDARD

Technical access controls or procedures shall be implemented to ensure that data and information are distributed only as authorized and as appropriate. Access controls and/or procedures shall, in part, be based on college business requirements. Once a business justification is provided, personnel shall adhere to the following standards:

- Confidential information should not be stored on personally owned devices.
- If information includes both confidential data and data available for public inspection, the classification level shall default to confidential.
- Electronic media entering or leaving offices, processing areas or storage facilities shall be appropriately controlled.
- Storage areas and facilities for media containing

confidential data shall be secured and all filing cabinets provided with locking devices.

- Confidential information shall not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements and return dates.
- When confidential information is shipped, the delivery shall be verified.
- All confidential information shall be encrypted when transmitted across wireless or public networks[9], including transmissions such as FTP and electronic mail.
- Confidential data shall be encrypted when stored on non-State owned devices and only by authorized users. Federally protected confidential data shall not be stored on non-State owned/managed devices.
- Encryption algorithms for the transmission of confidential data include, at a minimum, Secure Socket Layer (SSL) RC4 128 bit algorithms, SSL Server-Gated Cryptography (SGC) 128 bit algorithms, TLS 1.11 128 bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST)[10].

**ISO 27002 Reference**
9.1 Secure Areas

## **030204** Permitting Third-Party Access

**Purpose:** To secure third-party access and prevent unauthorized access to information systems and data.

### STANDARD

Colleges shall implement security controls in accordance with Standard 020104, Managing Network Access Controls, and Standard 090104, Physical Access Control to Secure Areas, when granting third-party access to College information systems. Third-party contracts shall specify the access, roles and responsibilities of the third party before access is granted.

**ISO 27002 Reference**

[9] 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.

[10] NIST http://csrc.nist.gov/groups/STM/cavp/index.html

6.2.1 Identification of risks from third party access

## **030205** 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 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 that:

- Separation of duties or dual control procedures is enforced.
- Any theft or loss of electronic keys results in the notification of management.
- All keys are protected against modification and destruction, and secret/private keys are protected against unauthorized disclosure.
- 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.
- Physical protection is employed to protect equipment used to synchronize, store and archive keys.
- 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.
- Custodians of cryptographic keys formally acknowledge they understand and accept their key-custodian responsibilities.
- Encrypted data are recoverable, at any point in time, even when the person(s) who encrypted the data is no longer available.

Agencies 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 |

## 030206 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

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. Any decision to upgrade should take into account the security of the release (i.e., the introduction of new security functionality).

### GUIDELINES

- Whenever possible, critical applications should be separated from databases.
- An audit log should be maintained to reflect all updates to operational program libraries.

**ISO 27002 References**

| | |
|---|---|
| 10.10.4 | Administrator and operator logs |
| 12.4.1 | Control of operational software |

## **030207** Managing System Documentation

**Purpose:** To ensure that the system documentation for all the organization's information systems is accurate and available.

### STANDARD

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.

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.

**ISO 27002 References**

| | |
|---|---|
| 10.7.4 | Security of system documentation |
| 12.5.1 | Change control procedures |

## **030208** Monitoring Error Logs

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

### STANDARD

Error logs generated by those information technology systems designated as mission critical, data sensitive or network security related shall be regularly monitored and reviewed for abnormalities and shall be:

- Cross-checked for known security events based on network, size, system type and logical and physical location.
- 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. Logs may be maintained by a centralized logging server or individual devices.
- Monitored on a weekly basis at a minimum.

- Routinely checked for time and date accuracy. See Standard 030212, Synchronizing System Clocks, for more on clock synchronization.
- Retained as required under the College records retention policy or other external policy adhered to by the College to meet needed requirements. (ex. PCI compliance standard).

Error logs shall be 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 |

## **030209** Scheduling System Operations

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

### STANDARD

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:

- 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.

**ISO 27002 Reference**

10.1.1 Documented operating procedures

## 030210 Scheduling Changes to Routine System Operations

**Purpose:** To ensure that the College's information system operations change control procedures are adequate and properly implemented and documented.

### STANDARD

Colleges shall develop change control procedures to accommodate resources or events that require changes to system operations. 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.

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.

All documentation shall be approved by management and reviewed on an annual basis for accuracy and relevancy.

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 Branch of the Department of Cultural Resources.

**ISO 27002 References**

10.1.2 Change management

## 030211 Monitoring Operational Audit Logs

**Purpose:** To protect the integrity and availability of information systems by monitoring operational audit logs.

## STANDARD

Colleges shall implement a program for continuous monitoring and auditing of system use to detect unauthorized activity. 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.

Audit logs, whether on-line or stored on backup media, shall be protected so that no users, including system administrators, can alter them.

Colleges should ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations. Colleges should 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.

Colleges shall designate trained staff to regularly review operational audit logs, including system, application and user event logs, for abnormalities. Audit logs of high risk information systems, such as those that process credit card data, shall be reviewed on a daily basis. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to management. Appropriate personnel shall be designated by College to review logs. Log review and retention shall be documented and adhered to by the College. 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. Audit files shall be written to a log server on the internal network and subsequently backed up to a secure location. To the extent possible, audit logs shall include at least the following information when recording system 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.
- Attempt to initialize, remove, enable, and disable accounts or service
- Changes to the auditing function, including enabling or disabling auditing and changing events to be audited.

- User ID creation, deletion, and privilege change activity.
- All uses of special system privileges.
- User ID responsible for system restart or shutdown and date and time of restart or shutdown.
- User ID responsible for application start up, restart and/or shutdown and date and time of start-up or shutdown.
- User credential creation and deletion.
- Attempts to create, remove or set passwords or change system privileges.
- Successful and failed login attempts.
- Unauthorized attempts to access network and system files.
- Attempts to initialize, remove, enable or disable accounts or services.
- System errors and corrective action(s) taken.
- Failed read-and-write operations on the system directory.
- All actions taken with administrative privileges.
  Agencies should ensure that processing and storage capacity requirements are sufficient to capture and store the events cited above without adversely impacting operations. Agencies should 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.

Personnel responsible for audit logs must ensure:

- 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 Agency Records, Information Technology Records as established by the Government Records Branch of the Department of Cultural Resources.

**ISO 27002 References**

| | |
|---|---|
| 10.10.4 | Administrator and operator logs |
| 15.3.1 | Information systems audit controls |
| 10.10.2 | Monitoring system use |

## **030212** Synchronizing System Clocks

**Purpose:** To prevent operations failure, data loss or security holes resulting from the inaccuracy of system clocks.

### STANDARD

To maintain the correct time and accuracy of audit logs on information systems residing within the State Network, system clocks must be synchronized regularly across various College platforms.

System time clocks must be updated on a daily basis from a time source that agrees with the Coordinated Universal Time, and the synchronized correct time must then be disseminated to all systems on a College's network. Additionally, change control procedures, log monitoring, and root login restrictions shall be utilized to protect from unauthorized modification of systems. Time synchronization data and configurations shall be protected from unauthorized modifications.

### GUIDELINES

When evaluating the accuracy of a time source, Colleges should consider the following:

- The location of the time source itself.
- The availability of the time source.
- The reliability of the time server to maintain accurate time received from the time source.
- The latency between the time source and College systems.
- The reputation of the company hosting the time source.
- Configuring authentication mechanisms for clock synchronization with hosts.
- Industry accepted

**ISO 27002 Reference**

| | |
|---|---|
| 10.10.6 | Clock synchronization |

## **030213** Responding to System Faults

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

### STANDARD

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).

Authorized staff members shall be defined by local Information Technology Governance hierarchy. Authorized staff shall describe the fault as clearly and completely as they can, and if a reason is known for the fault, the reason shall be provided as well.

Data Owners or Data Custodians shall request that the 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 Reference**

| | |
|---|---|
| 10.10.5 | Fault logging |

## **030214** Managing or Using Transaction/Processing Reports

**Purpose:** To ensure that validation checks are incorporated to detect possible corruption or loss of system and data integrity.

### STANDARD

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.

**ISO 27002 Reference**

| | |
|---|---|
| 12.2.2 | Control of internal processing |

## **030215** Commissioning Facilities Management for Information Technology

**Purpose:** To ensure that information technology facilities are managed with regulatory security frameworks and provide effective planning and operation.

### STANDARD

The College’s facilities management personnel shall work with appropriate departments (IT, Security, etc.) while fulfilling their duties to ensure that proper precautions are taken in regard to physical security, including:

- Limiting ingress and egress route vulnerabilities.
- Restricting available entrances, while emphasizing the availability of emergency exits.
- Assigning individuals to survey each area to ensure that all individuals have left the building.
- Building perimeter security considerations.

If the College determines to outsource its facilities management, the outsource vendor must comply with Standard 100103, Contracting with External Suppliers/Other Service Providers.

### GUIDELINES

Colleges should establish the security of construction, modification, maintenance and related facility management concerns for facilities and premises within the care and custody of the College.

**ISO 27002 Reference**

| | |
|---|---|
| 6.2.1 | Identification of risks related to external parties |

## 030216 Third Party Service Delivery

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

### STANDARD

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.

College shall maintain a list of all service providers who store or access student data. SLA shall clearly state the importance of data integrity. A clear, concise statement shall be included in SLA placing responsibility on service provider for any student data shared with the provider.

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.

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.

Changes to the SLA and services provided shall be controlled through a formal change management process.

Colleges shall develop a process of reengaging service providers and maintain a list of all services providers who store or share confidential data. The SLA shall also state how the service provider is responsible for data stored or shared with the provider

**ISO 27002 References**
10.2Third party service delivery management

## **030217** Log-on Procedures

**Purpose:** To reduce the risk of unauthorized system access.

### STANDARD

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.

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.

Colleges shall configure systems to limit the number of consecutive unsuccessful log-on attempts. If the number of consecutive unsuccessful log-on attempts exceeds three (3) attempts, 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.

### GUIDELINES

When developing the secure log-on procedures, Colleges should include the following considerations.

- Do not display information about the system or services until the log-on process has successfully completed.
- Log on windows should display a minimal amount of information.
- Do not validate the log-on process 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.
- Display only generic “log-on failed” messages if the user does not complete the log-on process successfully. Do not identify in the message the precise piece of log-on information that is preventing successful log-on.

Also see Standard 020106, Managing Passwords, for instructions that complement this standard.

**ISO 27002 Reference**
11.5.1 Secure log-on procedures

## 030218 System Utilities

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

### STANDARD

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.

These system utilities shall be segregated from other applications and software such that they can only be accessed by authorized users.

### GUIDELINES

Colleges should develop procedures for granting and documenting authorization for specific individuals to use powerful system utilities, whether or not such use is temporary.

Use of system utilities should be audited or logged.

Colleges should remove or disable system utilities that are not needed.

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 Reference**
11.5.4 Use of system utilities

## 030219 System Use Procedures

**Standard merged into standard 030211**

## **030220** Internal Processing Controls

**Standard merged into standard 030221**

## **030221** Corruption of Data

**Purpose:** To minimize, detect, or prevent corruption or loss of information in applications.

### STANDARD

Colleges shall develop clear policies, standards, and/or procedures to detect, correct, and manage corrupted data files. 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.

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

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

- Add, modify, and delete functions should be carefully controlled.
- 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.
- 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.
- 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.

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

**RELATED INFORMATION**
030214 Managing or Using Transaction/Processing Reports
030220 Internal Processing Controls
030222 Corrupt Data Controls

**ISO 27002 Reference**
12.2.2 Control of internal processing

## 030222 Corrupt Data Controls

**Standard merged into standard 010221**

\

## 030223 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:

- Validate the identity of the parties involved in the transaction.
- Gain proper approval for the transaction, if necessary.
- Protect the confidential data involved in the transaction.
- Ensure the integrity of the transaction.
- Obtain proof that the transaction is completed correctly.
- 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:

- Using electronic signatures that are validated through an approved, known certificate authority (CA).
- Using enhanced authentication techniques, such as multi-factor authentication.
- Implementing automated two-person controls for approving

transactions.

- Encrypting the message content when transmitted over an unsecured communications link.
- Encrypting the communications link through secure protocols.
- Storing transaction details in a secure location not accessible to unauthorized persons.

**ISO 27002 Reference**
10.9.2 On-Line Transactions

---

## *Section 03 E-mail and the Worldwide Web*

### **030301** 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 standards that address desktop and laptop security, including those listed below.

Safeguards that shall be in place to limit the risk of downloading files that may contain malware include, but are not limited to:

- Use of antivirus software that scans files before they are downloaded
- Validating before installation the source of software and the reputation of the site from which it is downloaded
- Not opening files from people not known to the user or files that are spammed via email
- Software that is in violation of copy-right laws.
- Not downloading or using software or any other materials that may constitute a copyright or licensing violation or implicate the College for licensing agreements
- Not running P2P applications to facilitate the downloading and sharing of copyrighted material
- Not utilizing the internet to download applications designed to remove copyright protections from protected content such as DVD media

**RELATED INFORMATION**
020103 – Securing Unattended Work Stations
020106 – Managing Passwords

030902 – Loading Personal Screensavers
050402 – Issuing Laptop/Portable Computers to Personnel
050403 – Using Laptop/Portable Computers
050408 – Day to Day Use of Laptop/Portable Computers
050705 – Clear Screen
050706 – Logon and Logoff from your Computer

**ISO 27002 References**

| | |
|---|---|
| 10.4.1 | Controls against malicious code |
| 11.1.1 | Access control policy |

## **030302** Using and Receiving Digital Signatures

**Purpose:** To protect the integrity of College and State data through the use of digital signatures.

### STANDARD

A public key infrastructure (PKI) for issuing and managing digital certificates and digital signatures to College employees is an enterprise-wide infrastructure. It must be implemented and centrally maintained as a statewide initiative.

Digital certificates are a core technology for securing the College’s infrastructure. Digital certificates provide strong and flexible authentication services for individuals and applications and must be consistent with the architecture and standards in the Statewide Technical Architecture.

The enterprise PKI must meet the following requirements:

- Security — an enterprise PKI provides a secure environment for generation, distribution, and management of encryption keys and digital certificates. It supports strong authentication, minimizes application-based passwords and integrates into the College’s security infrastructure.
- Management — a certificate authority[11] (CA) provides secure storage of master keys used to sign digital certificates for college employees. Registration authority[12] for issuing and revoking certificates is delegated to Colleges.
- Consistency — an enterprise PKI ensures that digital certificates will be issued and managed to minimize interoperability and acceptance problems. A lack of consistency will increase infrastructure management costs for

[11] A CA maintains a highly secure environment to ensure that master keys and certificate generation cannot be compromised.

[12] A registration authority authorizes requests for digital certificates, verifies the identity of requestors and authorizes revocation of digital certificates.

security.

- Scalability — an enterprise PKI is required to support long-term needs for college-wide security of networks, systems, and data. There shall be no technical limitation that precludes servicing any audience permitted by general statute.

**ISO 27002 Reference**
10.9.1 Electronic commerce

## **030303** Sending Electronic Mail

**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. Colleges that connect to the State Network are subject to the statewide acceptable use policies.

Examples of email content that constitute unacceptable use are:

- 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.
- Unauthorized not-for-profit business activities.
- Seeking/exchanging information, software, etc., that is not related to one's job duties and responsibilities.
- Unauthorized distribution of College data and information including the unauthorized use of email auto-forwarding.
- Use for, or in support of, unlawful/prohibited activities as defined by federal, State and local laws or regulations. Illegal activities relating to Internet and network access include, but are not limited to:
- Tampering with computer hardware or software.
- Knowingly vandalizing or destroying computer files.
- Transmitting threatening, obscene or harassing materials.
- Attempting to penetrate a remote site/computer without proper authorization.
- Using the Internet in an effort to access data that are protected and not intended for public access.
- Violating federal and State laws dealing with copyrighted materials or materials protected by a trade secret.
- Sending confidential information without encrypting that information, exposing the data to discovery by unintended recipients.
- Intentionally seeking information about, obtaining copies of or modifying contents of files, other data or passwords belonging to other users, unless explicitly authorized to do so by those

users.

- Attempts to subvert network security, to impair functionality of the network, or to bypass restrictions set by network administrators. Assisting others in violating these rules by sharing information or passwords is also unacceptable behavior.
- 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.

**ISO 27002 References**

| | |
|---|---|
| 10.8.2 | Exchange agreements |
| 10.8.4 | Electronic messaging |
| 12.2.3 | Message integrity |

## **030304** Receiving Electronic Mail

**Purpose:** To provide security training for receiving electronic mail.

### STANDARD

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. . Colleges shall protect State resources by not taking action on unsolicited commercial electronic mail. Colleges shall also establish procedures that address the following issues:

- Attacks on electronic mail (e.g., viruses, interception, user identification, defensive systems).
- Activating or clicking on hyperlinks in documents or e-mail messages that are from unknown sources or part of unsolicited messages (spam)
- Responding to or following hyperlinks asking for user names and passwords when asked to do by unsolicited phishing e-mails
- Use of cryptography to protect the confidentiality and integrity of electronic messages.

**ISO 27002 References**

| | |
|---|---|
| 10.4.1 | Controls against malicious code |
| 12.2.3 | Message integrity |

## **030305** Retaining or Deleting Electronic Mail

**Purpose:** To provide guidance on retaining or deleting electronic mail (email).

**STANDARD**

As determined by the System Office Legal Affairs Office and communicated by a Memorandum from Dr. Saundra Williams on February 23, 2010, the North Carolina Community Colleges do not have a legal requirement to comply with North Carolina Executive Order 18.

www.ncdps.gov/cit/executiveorders/EO18.pdf

The System Office recommends that community colleges comply to the extent possible with Executive Order 18. Community Colleges should maintain a documented policy that reflects their current process and requirements for their respective record retention and deletion of e-mail.

**ISO 27002 References**

15.1.3 Protection of organizational records

## **030306** Setting Up Intranet and Extranet Access

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

**STANDARD**

**Intranet**

Colleges that have Intranet sites shall provide the same controls on access to the Intranet site as to the files located on the network, in accordance with Standard 020101, Managing Access Control, and Standard 020108, Restricting Access to Information Systems.

Traffic to the Intranet site from an external location shall be blocked unless it is tunneled through a virtual private network (VPN).

**Extranet**

Colleges that have Extranet sites shall provide the same access controls to the Extranet site as to the files located on the internal network, in accordance with Standard 020101, Managing Access Control and Standard 020108, Restricting Access to Information Systems.

All new connections between third parties and State 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

Before placing a new Intranet or Extranet into production, Colleges should conduct a risk and/or business impact analysis.

When setting up access to the Intranet, Colleges should implement the following best practices:

- A documented approval process should be created before any information is posted to the Intranet site.
- Before posting material to the Intranet, 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.
- All legal issues such as disclosure of confidential information and copyright infringement should be resolved prior to posting.

When setting up access to the Extranet, Colleges should implement the following best practices:

- A documented approval process should be created before any information is posted to the extranet site.
- Before posting material to the Extranet, 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.
- Workers should also be required to confirm the information's accuracy, timeliness and relevance to the College’s mission before posting it.
- Likewise, all legal issues such as disclosure of confidential information and copyright infringement should be resolved prior to posting.

**ISO 27002 References**

| | |
|---|---|
| 11.1.1 | Access control policy |

## **030307** Setting Up Extranet Access

**This standard merged with standard 030306**

## **030308** Setting Up Internet Access

**Purpose:** To protect information technology resources from malicious attack and/or misuse.

### 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.

**ISO 27002 References**

| | |
|---|---|
| 11.1.1 | Access control policy |

## **030309** Developing a Web Site

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

### STANDARD

Colleges shall use only qualified personnel to develop Web sites. Web site development shall incorporate secure-development best practices. Development Web sites shall be isolated from production networks to prevent remote compromise while the server is being built and the Web application developed. Development servers/applications shall be developed and tested with input validation to protect against data validation weaknesses in the Web application's design. Web sites that accept citizen or public input through a web form shall automatically collect the submitter's known/receive IP address along with a current timestamp, for example web server logs. This information must be stored with data collected and provided in any e-mail or other generated output as a result of the web form submission. Information collected shall be kept in accordance with state and College retention policies and shall be mentioned in Colleges privacy statement.

A Web server operating system and its related applications shall have the latest patches installed to protect against known patch-related vulnerabilities. (See also Standard 040106 – Technical Vulnerability Management)

### GUIDELINES

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

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.

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 Chapter Two, Section 020106.

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.

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.

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.

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 |

## 030310 Receiving Misdirected Information by Email

**Purpose:** To establish standards for the handling of misdirected email.

### STANDARD

Misdirected or unsolicited email shall be treated with caution and not opened or responded to.

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.

### GUIDELINES

Colleges should follow best practices relating to email by:

- Installing spam-filtering software or an appliance on the network.
- Installing personal desktop firewalls on user computers to prevent the internal spreading of spam- or email-borne viruses.
- Configuring a packet-screening firewall to safeguard College networks from unsolicited activity.
- Providing informational notices requesting that users not reply to spam.

**ISO 27002 References**

10.8.4 Electronic messaging

## **030311** Forwarding Email

**Purpose:** To establish standards for properly forwarding email.

### STANDARD

Colleges shall develop policies to encourage due care by users when forwarding messages so that users do not:

- Auto-forward email without first obtaining College approval.
- Knowingly send out an email message that contains viruses, Trojan horses or other malware.
- Use the electronic-mail system or network resources to propagate chain letters, misinformation or hoax information.
- Forward any confidential information to any unauthorized party without the prior approval of a local department manager.
- Forward any confidential information without appropriate protections such as encryption.
- Forward the wrong attachment.
- Send information or files that can cause damage to College.
- Send unsolicited messages to large groups of people except as required to conduct College business.

### GUIDELINES

Colleges should consider including these items in the College’s individual acceptable use policy.

**ISO 27002 References**

10.8.4 Electronic messaging

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

## 030312 Using the Internet for Work Purposes

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

### STANDARD

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

- Ensure that there is no intentional use of such services in an illegal, malicious or obscene manner.
- Ensure compliance with State and College acceptable use policies.
- Ensure that all applicable software copyright and licensing laws are followed.
- Guard against wasting College Network resources, such as excessive personal use.
- Not use the College Network for distributing unsolicited commercial advertising or personal Web hosting.
- 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.
- 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, harassing, defamatory, obscene or pornographic in content.
- Not access or attempt to gain access to any computer account or network that they are not authorized to access.
- Not intercept, attempt to intercept, forge or attempt to forge data transmissions that they are not authorized to access or send.

#### 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:

- Develop a policy on the purpose and appropriate use of the social networking site by the College.
- Provide guidance to authorized College personnel for use and maintenance of any social networking sites used in connection with College business.
- 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.
- To help prevent fraud and unauthorized access, Colleges shall advise users:
  - To use a different user credential and password on each social networking and other non-State 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 the State government.
  - To guard against disclosing too much personally identifiable information, such as birthdates.
  - Prohibit users from 1) any action or statement that implies the user is speaking, or may speak, on behalf of the state, unless the user is specifically authorized to do so, and 2) disclosure of State information learned as a result of their employment when visiting social networking sites for their own personal use.
  - Train users on appropriate practices for use of social networking sites.
  - Institute data preservation and loss prevention measures.

**ISO 27002 References**
11.1.1 Access control policy

## **030313** 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:

- Ensure that all College credit or debit card details are kept confidential (including personal identification numbers [PINs], account numbers and details).

- Make every effort to verify that the third party is a legitimate e-business.
- Consider potential risks involved in conducting business on a Web site that has been compromised or is insecure.
- 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.
- Revert to ordering goods via telephone if any doubts or suspicions arise.
- 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 |

## **030314** Out-of-the-Box Web Browser Issues

**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’s information technology systems.

System administrators, support personnel, and system users must be aware that:

- 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.
- Confidential data may be stored on cookies on their machine automatically and that these cookies are updated automatically.
- Viruses, spyware, Trojan applications and other malicious code may be able to cause damage to the College’s infrastructure via Web browsers.
- They must use built-in security features to ensure the best security for Web browsers.
- Web browser vulnerabilities must be routinely addressed through the distribution of any 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 and scanning for spyware that may reside on Web browsers.

**ISO 27002 References**

| | |
|---|---|
| 10.9.3 | Publicly available information |

## 030315 Using Internet Search Engines

**Purpose:** To encourage users to verify information gathered from the Internet

### STANDARD

Users of Internet search engines shall take precautions to verify the integrity of the information provided by the search engine. As users collect information gathered from the Internet, they must:

- Check data for their integrity and accuracy before using them for business purposes.
- Observe all copyrights, end user licensing agreements, and other property rights.
- Use caution when downloading files from Web sites, ensuring that all downloads are scanned for viruses and other malicious code.

**ISO 27002 References**

| | |
|---|---|
| 10.9.1 | Electronic commerce |

## 030316 Maintaining A Web Site

**Purpose:** To protect and maintain the College's Web sites

### STANDARD

Colleges shall designate qualified individuals to administer and maintain their Web sites.

College management and College system administrators shall ensure that:

- College Web sites are kept up to date and secure and the information they present is accurate.
- Public Web sites are hardened and standard security configurations, based on industry guidelines and State standards, are adhered to.
- Secure authentication is used to protect the security of Web servers that have access to confidential information or that perform critical functions.

- Web sites have the latest operating system and application patches.
- Web site logs are periodically reviewed.
- The number of personnel with administrative access is limited to only qualified individuals.
- The sites are available to the appropriate users (public and private).
- Unauthorized modification of the Web site information is quickly discovered and resolved.
- All sites that a College is responsible for are periodically tested for vulnerabilities.
- All sites comply with all applicable laws and regulations.

**ISO 27002 References**
10.9.1 Electronic commerce

## 030317 Filtering Inappropriate Material from the Internet

**Purpose:** To protect the State 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 that:

- 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.
- Employees are restricted from inappropriate use that may result in criminal or civil penalties to the College or State.
- Corrective actions can be taken for repeated instances of inappropriate use.

### GUIDELINES

Colleges should consider the installation of a proxy server, content filtering appliance or intrusion detection or prevention devices.

**ISO 27002 References**
11.1.1 Access control policy

## **030318** Certainty of File Origin

**Purpose:** To protect the College from incorrect, malicious or inappropriate data.

### STANDARD

When possible, information or computer file originality and authenticity should be verified to ensure that:

- No malicious or unauthorized software is downloaded.
- Decisions that depend upon the information or computer file are made using data that are as accurate as possible.

**ISO 27002 References**
10.4.1 Controls against malicious code

## **030319** Instant Messaging Communications

**Purpose:** To identify the risks of using instant messaging and establish standards for mitigation of those risks.

### STANDARD

If College determines that the use of instant messaging (IM)[13] is critical to its mission, the College CIO must document, in a risk assessment, the reasons for using the software and its compliance features including:

- A detailed business case.
- The circumstances under which IM can be used.
- The access controls that will ensure that the College has taken sufficient steps to mitigate or isolate the associated threats.
- Any legal and regulatory requirements associated with information that may be used in electronic communications, such as requirements for confidentiality, security and record retention.[14]
- Architectural details.
- The capturing and logging the use of IM.

The risk assessment results shall be used to identify the policies and controls

[13] Instant Messaging (IM) covers a broad range of technologies that allow individuals to digitally_communicate in real time over a LAN or the Internet. These technologies can require the installation of client software or they can be web based. IM is similar to a telephone conversation but uses text-based, not voice, communication. IM conversations can occur PC-to-PC, phone-to-phone, PC-to-phone and phone-to-PC. Personal computing (PC) devices include, but are not limited to, desktops, PDAs, laptops, tablets, and smart phones.

[14] *See,* **120201** Managing Media Storage and Record Retention

that are required to appropriately protect these communications.

Colleges must not use IM unless the risks have been identified and appropriate risk mitigation measures have been implemented. Designated users must install IM software as directed by their security or IT department. College users must not use, download, or install any nonstandard software without obtaining permission as defined by College policy. Records and supporting documentation must be maintained by the College so that compliance with this standard can be verified.

College's use of IM may be periodically assessed by the College CIO for compliance with this standard.

## GUIDELINES

The risk assessment for IM should include the following considerations:

- Communications sensitivity
- What are the consequences of unauthorized or accidental access, modification, or loss of the communications?
- Is there a consequence for misdirected or incorrectly addressed messages?
- Denial of service and impact on business practices
- Are communications time sensitive?
- Is reliability and availability of the communications service a factor?
- Legal considerations
- Are there requirements for proof of origin, delivery, and/or acceptance?
- Is non-repudiation a factor such that the sender cannot claim that they did not send or receive a message?
- Remote user access
- Are controls needed to allow secure remote access to e-mail accounts?
- File Transfers / File Attachments
- Will the College forbid or restrict the transfer of files between users to prevent the possible dissemination of malware?[15]

In addition,

- Colleges should deploy an IM service that will allow College to enforce policies of data retention, confidentiality, acceptable use, etc. When choosing a product, college should give consideration to those products

[15] *See,* Statewide Information Security Standards **030501** - Transferring and Exchanging Data and, **100301** – Using the Internet in and Acceptable Way.

that interoperate with public services. This is especially important if the College regularly deals with the public over IM.

- Colleges interacting with the public over IM should consider taking steps to protect confidential information. Installation of pattern matching filters or key word filters should be considered in order to flag (and possibly drop) patterns that represent potential policy violations such as driver's license numbers, social security numbers, credit card numbers, passwords etc. Alerts can be sent to the user (pop up policy reminders), system administrators, security officers, privacy officers etc.

- AntiVirus / Malware products should be used to protect IM users and the network from this attack vector. Policies should also be updated to handle the practice of sending file attachments or URLs over the IM system, and restrict its use as much as possible.
- Colleges should consider installing URL filtering or a web proxy in order to reduce threat of Spam over IM (SPIM) or phishing attacks via IM.
- Colleges should update their Acceptable Use Policies to incorporate the acceptable use of IM.[16]
- Colleges should provide end users with annual security awareness training that advises them of new or changed IM policies as well as educates them on current IM threats. This should include the following:
  - o Instructions on setting the IM client to only accept connections from persons in the user's contact list.
  - o Utilizing profile settings to only allow persons in the user's contact list to view their on-line status.

**ISO 27002: 2007 References**
10.8.4 Electronic messaging

## 030320 Standard on Electronic Business Communications

**Purpose:** To prevent corruption or loss of information in applications.

### STANDARD

Colleges shall develop clear policies, standards, and/or procedures to detect,

[16] *See,* The State Chief Information Officer's policies found at https://www.scio.nc.gov/mission/itPoliciesStandards.aspx as well as Security Information Technology Standard **100301 –** Using the Internet in an Acceptable Way.

correct, and manage corrupted data files.

**ISO 27002 References**
10.8.4 Electronic messaging

## **030321** Data Validation Controls[17]

**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:

- Carefully controlled add, modify, and delete functions.
- Implementation of automatic reconciling of balances from run-to-run or system-to-system in systems to compare opening balances against previous closing balances.
- 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.
- 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

## **030322** Data Recovery Controls[18]

[17] Original section title was “Cryptographic Keys”

[18] Original section title was “Key Management Procedures”

**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

## 030323

### Controlling Mobile Code

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

### STANDARD

Colleges shall develop a policy to protect the State Network and local networks 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**

College 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**

1. 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

2. 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

3. 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)

4. 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 Fax*

## **030401** Making Video/Conference Calls

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

### STANDARD

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

- All parties participating in the call have been authorized or authenticated to receive the confidential information.
- All authorized participating parties have previously verified that no unauthorized persons are in such proximity that they might overhear the conversation.
- 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).
- All parties involved in the conference call are openly identified.

### GUIDELINES

- Use of publicly available Voice over IP systems should be avoided when a College or state operated Voice over IP system is available.
- When use of 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

**Standard merged into standard 030401**

## **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 shall have the right and ability to monitor the use of government telephones by employees and third-party contractors, including the recording of telephone conversations conducted on government telephone equipment.

Colleges using monitoring technologies shall establish policies to provide appropriate notice to State 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

- 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.
- 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.
- 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

Colleges shall develop guidelines for handling the receipt of unsolicited facsimiles, including advertising material, as well as misdirected facsimiles.

When a College receives a facsimile in error (wrong number, person, office, location or department), it shall notify the sender, if appropriate.

Misdirected facsimiles shall be treated as confidential documents and shall be shredded.

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**

When confidential information (e.g., credit card number, social security number) is required 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:

- Confidential information must not be left on answering machines or other recording devices.
- Care must be taken to ensure that confidential information cannot be overheard when it is disclosed over the telephone.

**ISO 27002 References**

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

## 030406 Persons Giving Instructions over the Telephone

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

**STANDARD**

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, including verifying that the recipients of the information are who they say they are. Colleges shall also provide employees and contractors with awareness training on social engineering and the legal requirements for protecting confidential data.

**ISO 27002 References**

| | |
|---|---|
| 10.8.1 | Information exchange policies and procedures |

## 030407 Persons Requesting Information over the Telephone

**Purpose:** To require that the identity of persons requesting confidential information over the phone is verified.

**STANDARD**

If confidential instructions or information are requested over the telephone, the identity of the caller shall be verified as a caller authorized to receive such information before the instructions or information is disclosed.

**ISO 27002 References**

| | |
|---|---|
| 10.8.1 | Information exchange policies and procedures |

| | |
|---|---|
| 10.8.5 | Business information systems |

## 030408 Receiving Unsolicited Facsimiles

**Standard merged into standard 030404**

## *Section 05 Data Management*

## 030501 Transferring and Exchanging Data

**Purpose:** To protect the College's confidential information during the electronic exchange or transfer of data.

### STANDARD

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. 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.

**ISO 27002 References**

| | |
|---|---|
| 10.8.1 | Information exchange policies and procedures |

## 030502 Managing Data Storage

**Purpose:** To protect the College's information resident on electronic data storage.

### STANDARD

Colleges shall ensure the proper storage of data and information files for which they are responsible. Stored data shall be protected and backed up so that a restoration can occur in the event of accidental or unauthorized deletion or misuse. Colleges shall also meet all applicable statutory and regulatory requirements for data retention, destruction, and protection.

The primary security control available to the College to protect confidential data in storage is using a data encryption method approved by the College CIO. Colleges shall exercise due diligence to ensure encryption keys are properly stored (separate from data) and available, if needed, for later decryption. When using encryption to protect data, College shall follow the security standard 030801 – Using Encryption Techniques.

Colleges shall protect the State's information and comply with agency records retention policy and the General Schedule for State Agency Records, Information Technology Records.

The standard recommended by ISO 27002 for this category is also covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

**GUIDELINES**

Colleges should keep stored public data to a minimum of what is necessary to adequately perform their business functions. Confidential data that is not needed for normal business functions should not be stored. Additionally, designated data owners should develop process for auditing stored confidential data and determine if it is still relevant and required.

Colleges should keep stored public data to a minimum of what is necessary to adequately perform their business functions. Sensitive of 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, as least quarterly, stored confidential data, like cardholder data, that exceeds the requirements defined in the college's data retention policy.

**RELATED INFORMATION**
Standard 030801 – Using Encryption Techniques
Chapter 9 - Dealing with Premises Related Considerations

**ISO 27002 References**

| | |
|---|---|
| 10.7.3 | Information handling procedures |
| 15.1.3 | Protection of organizational records |

## **030503** Managing Databases

**Purpose:** To protect the College's information databases.

### STANDARD

Colleges shall properly safeguard the confidentiality (where applicable), integrity and availability of their databases. Data from these databases shall be protected from unauthorized deletion, modification or misuse and shall meet all applicable statutory and regulatory requirements.

Critical data files shall be backed up, and if confidential data is backed up, the backup media shall receive appropriate security controls.

### GUIDELINES

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.

Databases that store critical, confidential information such as client records, accounting data, medical history data and data on sales and purchases should require more stringent mean time between failures (MTBF) and mean time to repair (MTTR) configurations.

**ISO 27002 References**

12.2Correct processing in applications
15.1.3 Protection of organizational records

## 030504 Permitting Emergency Data Amendment

**Purpose:** To protect the College's information

### STANDARD

Colleges shall establish change management procedures for the emergency amendment of data that occurs outside normal software functions and procedures.

All emergency amendments or changes shall be properly documented and approved and shall meet all applicable statutory and regulatory requirements.

**ISO 27002 References**

12.5.1 Change control procedures

## 030505 Receiving Information on Disks

**Purpose:** To protect the College's information systems.

### STANDARD

All data or files received by a College on a diskette, compact disc (CD) or any other electronic medium from an external source shall be downloaded to a College system only if:

- The data or files come from a known, trusted source.
- The data or files first pass virus scan using College CIO approved and current antivirus software.

This standard applies as well to files obtained as e-mail attachments and through any other file transfer mechanism.

**ISO 27002 References**

10.4.1 Controls against malicious code

## **030506** Setting Up a New Folder/Directory

**Purpose:** To provide directory-level protection for the College’s information resources.

### STANDARD

Colleges shall establish policies and procedures for creating, amending, and managing access to directory structures based on the most restrictive set of privileges needed for the performance of authorized tasks. New directory/folder structures shall be designed with the appropriate access controls to restrict access to authorized personnel only.

Colleges shall establish and manage access controls governing the modification or amendment of the directory structures on network or shared drives

New folders/directories shall prohibit the modification or deletion of files and folders from personnel other than the data creator/owner or system administrators. New folders/directories designed for holding confidential information shall be password protected.

### GUIDELINES

Colleges should consider limiting the ability of users to create new folders/directories on network or shared drives, which could cause security vulnerabilities or cause data to be difficult (or impossible) to locate.

Modification of directory structures by anyone other than the creator/owner or system administrators should be prohibited.

Colleges should consider password-protecting directories.

**ISO 27002 References**

| | |
|---|---|
| 11.11.1 | Access control policy |

## **030507** Amending Directory Structures

**Standard merged into standard 030506**

## **030508** Archiving Documents

**Standard merged into standard 030506**

## 030509 Information Retention Standard

**Standard merged into standard 030502**

## 030510 Creating New Spreadsheets

**Purpose:** To protect the College's confidential information on spreadsheets.

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate

### GUIDELINES

To mitigate security issues with spread sheets, Colleges should consider:

- Validating the formulas in the spread sheet.
- Implement read, write and deletion controls on access to control the spreadsheet's distribution.
- Maintaining retention and version control.
- Saving the spreadsheet in a directory that is backed up regularly.

**ISO 27002 References**

| | |
|---|---|
| 10.1.2 | Change management |
| 10.3.2 | System acceptance |

## 030511 Creating New Databases

**Purpose:** To protect the College's confidential information on databases.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate.

### GUIDELINES

To mitigate security issues with databases, Colleges should:

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

**ISO 27002 References**

| | |
|---|---|
| 10.1.2 | Change management |
| 10.3.2 | System acceptance |

## **030512** Linking Information between Documents and Files

**Purpose:** To protect the College’s confidential and critical information.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate.

### GUIDELINES

If a College employee creates a link between documents or files containing confidential information, the confidential data affected by the link should be properly labeled and appropriately controlled.

To mitigate security issues with linkages, Colleges should:

- Consider that:
  - They may not have control of source document and information.
  - It may be possible for documents to be changed without College knowledge.
  - Validation of completeness of linked information may be required. Retention and version control may be difficult to maintain.
  - Integrity of linked files can be compromised.
- Check links on at least a semiannual basis for validity.

**ISO 27002 Reference**
10.7.4 Handling information procedures

## **030513** Updating Draft Reports

**Standard removed**

## **030514** Deleting Draft Reports

**Standard removed**

## **030515** Using Version Control Systems

**Standard removed**

## **030516** Sharing Data on Software and Information Systems

**Purpose:** To protect the College’s confidential information while utilizing software or information systems.

### STANDARD

Software or information systems that allow 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 such as when a file is modified. Audit logs shall be retained in accordance with College records retention policy or the General Schedule for State for State Agency Records, Information Technology Records

Appropriate security controls shall include:

- 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 project 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.

These controls may be supplemented by operating-system-level controls (e.g., file and directory access control lists and system audit logs) only if the project management software does not bypass these controls.

**ISO 27002 References**

11.1.1 Access control policy

## 030517 Updating Citizen and Business Information

**Purpose:** To protect the confidentiality and integrity of the College's electronic information on citizens and businesses.

### STANDARD

Only authorized individuals shall perform updates to College databases. When changing information, College employees must be diligent in protecting confidential information and shall adhere to all applicable laws and regulations. Access to citizen and business or agency confidential data shall be controlled through various appropriate access control mechanisms. Colleges may include NDAs in their format agreements with custodians.

### 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**

15.1.4 Data protection and privacy of personal information

## 030520 Using and Deleting "Temp" Files

**Purpose:** To protect the College's confidential information residual on systems.

### STANDARD

College employees must remove old or unnecessary "temp" files from their desktop and laptop to prevent unauthorized access of confidential information.

### GUIDELINES

Some of the "temp" files that should be examined and removed are:

- Clipboard files.
- Printer files.
- Automatic saves.
- Temporary backups of "deleted files."
- Cached Web pages/uniform resource locators (URLs).
- Trash Can or Recycle Bin (should be emptied periodically).

**ISO 27002 References**

10.5.1 Information back-up

## 030521 Using Customer and Other Third-Party Data Files

**Standard merged into standard 010103**

## 030522 Saving Data/Information by Individual Users

**Standard merged into standard 030602**

## *Section 06 Backup, Recovery and Archiving*

## 030601 Restarting or Recovering of Systems

**Purpose:** To ensure that College information technology systems restart successfully after a voluntary or forced shutdown.

### STANDARD

Colleges shall establish procedures for the adequate backup and the restarting or recovery of their information technology systems.

Procedures for the restarting of information technology systems shall be properly tested and documented.

These procedures shall:

- Document backup frequencies and schedules.
- Document where the correct system information backup medium is stored.
- Specify the approved processes for restoring the system.
- Be in compliance with College change management procedures.
- Be tested on a regular basis, as established by College management.
- Provide guidance for restart documentation.

**ISO 27002 References**
10.5.1 Information back-up

## **030602** Backing Up Data on Portable Computers

**Purpose:** To protect the College's information stored on mobile/portable computers via regular backup plans.

### STANDARD

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. Colleges shall ensure that all appropriate data stored on mobile/portable computing devices is regularly and properly backed up. Data stored on any mobile/portable computing device shall be backed up according to the schedule specified in the Colleges' business continuity plans.

When a mobile/portable computer is outside 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.

When using encryption to protect data, Colleges shall follow the statewide information security standard 030801 – Using Encryption Techniques.

College employees shall periodically save data files from their desktop and laptop computers to an appropriate backup drive or disk.

**ISO 27002 References**
11.7.1 Mobile computing and communications

## **030603** Managing Backup and Recovery Procedures

**Purpose:** To ensure recoverability and availability of the College's information technology resources.

### STANDARD

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.

### GUIDELINES

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.
- Validate the integrity of the backup or image file through file hashes for backups, restores, and virtual machine migrations.
- Classify back up media so the sensitivity of the data can be determined.
- Store media back-ups in a secure location, preferably an off-site facility.
- Physically secure all back up media from theft and destruction.
- Send media by secured courier or other delivery method that can be accurately tracked.
- Ensure management approval for any media moved from a secure area.
- Properly maintain inventory logs of all media and conduct media inventories at least annually.

**ISO 27002 Reference**
10.5.1 Information back-up

## 030604 Archiving Information

### Standard removed

## 030605 Archiving Electronic Files

**Purpose:** To protect the College's information through the archiving of relevant data.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate. The Department of Cultural Resources, Government Records Branch, has established requirements for archiving records.

### GUIDELINES

Colleges should consult with the North Carolina Department of Cultural Resources, Government Records Branch, to select archival media that will protect the integrity of the data stored on those media for as long as the data are archived.

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 |

## **030606** Recovery and Restoring of Data Files

**Purpose:** To ensure the integrity of the College's information during recovery and restoration.

### STANDARD

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.

Data recovery must be conducted by authorized parties and recovered data must be tested for potential corruption.

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.

**ISO 27002 References**

| | |
|---|---|
| 10.5.1 | Information back-up |
| 10.7.3 | Information handling procedures |

## *Section 07 Document Handling*

**030701** Managing Hard-Copy Printouts
**030702** Photocopying Confidential Information

The standards above are addressed in 010103 – Storing and Handling Classified Information.

**030703** Filing of Documents and Information
**030704** Countersigning of Documents
**030705** Checking Document Correctness
**030706** Approving Documents
**030707** Verifying Signatures
**030708** Receiving Unsolicited Mail
**030709** Style and Presentation of Reports

The standards above are appropriate for individual college to address at local level.

**030710** Transporting Confidential Documents

**Standard merged into standard 010103**

**030711** Shredding of Unwanted Hard Copy

**Standard removed**

**030712** Using Good Document Management Practices

**Standard merged into standard 010103**

### *Section 08 Securing Data*

## 030801 – Using Encryption Techniques

**Standard:**

**030801** Using Encryption Techniques

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

**STANDARD**

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. Encryption techniques shall be employed when encryption is appropriate.

All laptops that are used to conduct College business shall use encryption to protect all information from unauthorized disclosure, including confidential information, such as personal information.

All other 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) 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, such as personal information, from unauthorized disclosure.

Colleges using key-based encryption systems must provide for an encryption key escrow to ensure present and future College access to encrypted data. Colleges must ensure that only authorized personnel have access to keys used to access confidential information.

Proper management control of encryption keys and processes must be ensured when archiving confidential electronic files or documents.

| **Device** | **Encryption Requirements** |
|---|---|
| Laptops, Notebooks, and Netbooks | All devices shall use the most current US Government cryptography standard available for systems.[19] |
| Removable Media such as CDs, DVDs, memory sticks (flash drives), tape media, or any other portable device that stores data, including mobile and portable computing devices, such as tablets, smart phones and personal digital assistants | All Personally Identifiable Information (PII) and confidential information shall be encrypted using a FIPS 140-2 Level 1 certified algorithm of at least a 128-bit strength.<br>Whenever possible, state data should be stored on state issued and owned removable media. |

Colleges shall develop and enforce policies concerning the storage of the College's confidential data on all portable and removable media devices. Confidential data should not be on non-College owned devices. Confidential data shall be encrypted when stored on non-State owned devices and only by authorized users. Federally protected confidential data shall not be stored on non-State owned/managed devices.

[19] 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.

### GUIDELINES

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.

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 agencies should consider encrypting all mobile communication devices regardless of the confidentiality of the information stored.

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.

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**

| | |
|---|---|
| 12.3.2 | Key management |
| 15.1.6 | Regulation of cryptographic controls |

## **030802** Sharing Information

**Purpose:** To protect confidential data belonging to North Carolina Colleges.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate.

### GUIDELINES

Colleges should consider training personnel on their duty to protect confidential information from unauthorized disclosure or modification, including training on applicable policies, statutes and records that apply when such information is released to a third party or shared with other Colleges.

**ISO 27002 References**

| | |
|---|---|
| 7.2.1 | Classification guidelines |
| 15.1.4 | Data protection and privacy or personal information |

## **030803** Sending Information to Third Parties

**Purpose:** To protect the College's confidential information in dealings with third parties.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate

### GUIDELINES

Colleges should consider protecting confidential information sent to third parties by developing processes, procedures and business agreements that set forth the allowable use and distribution of confidential information. Agreements for the exchange of information with third parties should clearly document the third party's commitment to ensuring the privacy of the College's information and the third party's obligations in regard to handling, storage and further dissemination, as well as the consequences of failing to fulfill these obligations

**ISO 27002 References**

| | |
|---|---|
| 10.8.3 | Exchange agreements |

## **030804** Maintaining Customer Information Confidentiality

**Purpose:** To protect the confidential information of individuals.

### STANDARD

Colleges shall manage and protect electronic information received from customers, constituents and third parties in accordance with all applicable federal and State statutes and regulations.

Appropriate security controls shall be put in place to ensure the confidentiality, integrity, and availability of confidential customer, constituent, third-party or State information.

**ISO 27002 References**

| | |
|---|---|
| 15.1.4 | Data protection and privacy of personal information |

## **030805** Handling of Customer Credit Card Details

The standard recommended by ISO 27002 in this category is governed by policies and standards established by the Office of the State Controller concerning PCI Compliance. (if applicable). Colleges NOT utilizing E-Commerce are not subject to this standard.

## **030806** Fire Risks to the College's Information

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

### STANDARD

Colleges shall take proper care to manage the risks of fire to the State's data and information technology resources.

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

- Colleges should consider storing duplicate copies of information at alternate locations.
- The use of file cabinets that are  fire-, smoke- and/or water-safe is encouraged depending on the College's risk assessment..
- 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 |

## 030807 Sending Out Reports

**Purpose:** To ensure that data or software is appropriately secured when sent to third parties.

### STANDARD

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate

### GUIDELINES

When exchanging electronic data or software with third parties, Colleges should ensure that the data are correct, that the exchange is properly approved, and that the third party has in place adequate security to protect the confidentiality (if applicable), integrity and availability of the data/software exchanged.

**ISO 27002 References**

| | |
|---|---|
| 10.8.2 | Exchange agreements |

## 030808 Dealing with Sensitive Financial Information

**Purpose:** To ensure strong control of financial information.

### STANDARD

Colleges that have confidential financial information in electronic format shall deploy, test, assess and maintain adequate technical and administrative security controls to ensure the confidentiality, integrity and availability of the financial information.

### GUIDELINES

Colleges should consider using separation-of-duties techniques for input and control of financial data.

To help ensure the confidentiality and (where applicable) the integrity of data at rest, it is recommended that Colleges apply cryptographic algorithms that meet the most current US Government cryptography standard available for systems.

**ISO 27002 References**

| | |
|---|---|
| 7.2.1 | Classification guidelines |

## **030809** Deleting Data Created/Owned by Others

**Purpose:** To protect the integrity and availability of College data.

### STANDARD

The standard recommended by ISO 27002 for this category is covered by N.C.G.S. §§121-5 and 132-1, *et seq*. and rules adopted by the Department of Cultural Resources.

### GUIDELINES

Colleges should consider document handling procedures to properly manage the data for which they are responsible and guard against misuse or unauthorized deletions.

Colleges should consider employing mitigation techniques such as, but not limited to, the following:

- Password-protecting files and folders so that personnel other than the data custodian may not delete data that they are not responsible for.
- Version control methods for tracking of changes, so users will know if data have been altered and by whom.
- Daily, weekly and monthly backups for immediate recovery of deleted or changed data.

**ISO 27002 References**

| | |
|---|---|
| 11.1.1 | Access control policy |

## **030810** Protecting Documents with Passwords

The standard recommended by ISO 27002 for this category raises an issue for individual Colleges to address, if appropriate.

### GUIDELINES

Colleges should consider protecting confidential files with unique passwords to augment their current technical and administrative security access controls.

If Colleges require passwords for confidential files, Colleges should provide for a password escrow to facilitate future access to password-protected documents. File passwords should be used to augment access control mechanisms. They are not meant to replace strong access controls.

**ISO 27002 References**

11.1.1 Access control policy

## 030811 Printing Confidential Documents

**Purpose:** To protect printed confidential documents.

**STANDARD**

Where possible, Colleges shall develop and employ a process to properly clear the memory from a printer (or copier) that has been used to print confidential information. Authorized personnel must be present to safeguard the confidentiality of the material both during and after printing.

**ISO 27002 References**

11.3.3 Clear desk and clear screen policy

# *Section 09 Other Information Handling and Processing*

## 030901 Using Dual-Input Controls

**Purpose:** To protect information using dual-input comparisons.

**STANDARD**

Dual-input controls shall be used when data entry is critical to the business process. Colleges shall manage the input of financial information with the use of dual controls whenever possible.

**ISO 27002 References**

10.1.3 Segregation of duties

## 030902 Loading Personal Screen Savers

**Purpose:** To protect the College's assets by eliminating non-approved screen savers.

**STANDARD**

Personnel shall load only those screen savers that have been approved by their Colleges.

Colleges shall train their employees on the risks of acquiring malware such as viruses, spyware and Trojan horses by downloading and installing unauthorized screen savers.

**ISO 27002 References**

| | |
|---|---|
| 10.4.1 | Controls against malicious code |

## 030903 Using External Disposal Firms

**Purpose:** To protect the College's assets during third-party disposal.

### STANDARD

Colleges must ensure that all 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.

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. Service level agreements with external firms/third parties shall include, but not necessarily be limited to, the following:

- Stipulations to ensure compliance with the College's security policies and standards, enforceable by suit for breach of contract.
- 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 |
| 10.7.2 | Disposal of media |

## 030908 Using Clear Desk Standard

**Purpose:** To reduce the risk of confidential information being viewed by unauthorized persons.

### STANDARD

Colleges shall inform personnel of the risks involved in leaving confidential work on their computer screens while away from their desks.

Personnel shall be given training on this standard on an annual basis. The training shall include information on any civil or criminal penalties that may apply to individuals who breach confidentiality statutes.

### GUIDELINES

Security measures that should be implemented include, but are not limited to:

- Shutdown/powering off of computers.
- Logging off or locking computers while away from the desk.
- Clearing all printers and fax machines of confidential printouts.

**ISO 27002 References**

| | |
|---|---|
| 11.3.3 | Clear desk and clear screen policy |

## **030909** Misaddressing Communications to Third Parties

**Purpose:** To reduce the risk of communicating misinformation or confidential information to unauthorized persons.

### STANDARD

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.

### GUIDELINES

Colleges 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:

> 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 shall be reviewed and approved by the College or State legal staff prior to use.

**ISO 27002 References**

| | |
|---|---|
| 10.8.5 | Business information systems |

## **030910** Verifying Correctness of Information

**Purpose:** To reduce the risk of propagating incorrect information.

### STANDARD

Colleges shall validate data output from application systems to ensure that the data-processing function correctly stores the data.

**ISO 27002 References**

| | |
|---|---|
| 12.2.4 | Output data validation |

## 030911 Traveling on Business

**Purpose:** To reduce the risk of losing College assets.

### STANDARD

Colleges shall address employee responsibilities for safeguarding information technology assets and information when traveling on College/State business. Colleges shall train their employees in regard to their responsibilities and provide guidance on how they can reduce the risks of disclosing confidential information and avoid having College property stolen.

**ISO 27002 References**

| | |
|---|---|
| 11.7.1 | Mobile computing and communications |

## 030912 Checking Customer Credit Limits

**Standard removed**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 4 – Purchasing and Maintaining Commercial Software

## *Section 01 Purchasing and Installing Software*

### **040101** Specifying User Requirements for Software

**Purpose:** To require business justifications for applications software purchases/enhancements.

**STANDARD**

Colleges shall ensure that a business justification accompanies all requests for new application systems or software enhancements. The justification shall include the following:

- Documented business needs and expectations of the new system or enhancement.
- 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.
- Statement of senior management approval, prior to procurement.

**GUIDELINES**

Each College should have a formal business justification procedure to identify business, security and technical requirements that new systems and software enhancements should meet. Using a well-defined process explores technical, security and business issues and helps the College avoid:

- Security risks arising from inadequate security controls.
- Failing to meet business needs and expectations by choosing less than the best solution.
- Unexpected cost and wasted time retrofitting an inadequate solution.

**ISO 27002 REFERENCE**
6.1.4 Authorization process for information processing facilities

### **040102** Selecting Business Software Packages

**Purpose:** To protect College resources during the software selection process.

**STANDARD**

Colleges shall ensure that a formal selection process is used to purchase business-critical software necessary to deliver public services such as accounting, general ledger, and inventory control. The selection process shall include a review of security measures needed to protect the confidentiality, availability and integrity of the data. Colleges shall not use software for which support is not readily available.

### GUIDELINES

Colleges should minimize the likelihood of selecting poorly designed or inadequate software by taking the following steps:

- Avoiding software that fails to meet business needs.
- Reviewing proprietary software used in a production environment annually to assess the exposure from using old or outdated programming languages, databases and protocols.
- Ensuring that software under consideration for purchase works with the majority of peripherals and systems currently in use.
- Avoiding software packages that have been highly customized.

**ISO 27002 REFERENCE**

6.1.4 Authorization process for information processing facilities

## **040103** Selecting Office Software Packages

**Purpose:** To increase interoperability by standardizing software packages.

### STANDARD

Colleges shall ensure the following:

- That office software packages installed on College computers comply with the College’s security requirements.
- That management-approved criteria for the selection of software packages are defined and documented.
- That software under consideration for acquisition works with the majority of peripherals and systems currently in use.

### GUIDELINES

When selecting office software packages, Colleges should consider that:

- Old or outdated software typically poses a higher security risk than updated office software.
- The standard office software package is more effective when universally used across State Colleges to ensure compatibility among divisions and Colleges.
- Upgrading office automation software may necessitate the purchase of

new hardware.

**ISO 27002 REFERENCE**

12.1.1 Security requirements analysis and specification

## 040104 Using Licensed Software

**Purpose:** To require compliance with software licensing agreements.

### STANDARD

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.

**ISO 27002 REFERENCE**

15.1.2 Intellectual property rights (IPR)

## 040105 Implementing New / Upgraded Software

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

### STANDARD

Colleges shall design security into systems used for data processing so that the systems have the proper technical and procedural security controls.

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 liaison assigned to perform the review.

Default settings for applications such as e-mail calendar, and Internet access tools must be set to support a secure environment.

System configuration management regarding the installation of software shall include the following:

- Maintenance of good backups of critical data and programs.
- Periodic review of overall controls to determine weaknesses.
- Limiting use of software to that which can be verified to be free of harmful code or other destructive aspects.
- Complete information about the software shall be maintained, such as the vendor address and telephone number, the license number and version, and update information. This information will be necessary if the software must be reinstalled later.
- Software programs shall be reinstalled only from validated media.
- Software shall be stored in a secure, tamper-proof location.

**GUIDELINES**

New or upgraded software should not be made available to users until a risk analysis (RA) and/or business impact analysis (BIA) is performed and the risks are understood.

In conjunction with the RA and/or BIA, Colleges should develop the following:

- A step-by-step implementation plan.
- A software implementation plan that follows change control procedures.
- Management and user acceptance criteria, including:
    - Desired acceptance tests and their desired results.
    - 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.

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 REFERENCE**
12.5.1 Change control procedures

## **040106** 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**

Vulnerabilities that threaten the security of the College’s network or IT assets shall be addressed through updates and patches based upon assigned vulnerability ratings.

**2.1 Vulnerability Risk Ratings**

The risk ratings assigned to a vulnerability are:

- *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 asset 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, and they 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 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, and router access control lists). The 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 have procedures in place to notify College management and the College CIO of the existing 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. Zero-day vulnerabilities, where an exploit is used before a software vendor knows about it, Colleges should mitigate these immediately 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 should 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 but not limited to Information Security, Information Technology, and Internal Audit.

3. Appropriate College personnel shall be alerted or notified in near real-time about warnings or announcements involving "High-risk" vulnerabilities.

**Vulnerability Metrics Tracking and Reporting**

1. The following vulnerability task assignment metrics must be routinely tracked for specific administrators and vendor technologies:
   - Number of new vulnerability task assignments
   - Number of closed vulnerability task assignments
   - Number of overdue vulnerability task assignments
2. College managers, including but not limited to Information Security, Information Technology, and Internal Audit, shall be provided with a quarterly report on the following vulnerability metrics:

   - Number of total vulnerabilities for the current quarter including those open at the beginning of the quarter
   - Number of vulnerabilities closed for the current quarter
   - Number of vulnerabilities open for the current quarter
   - Number of vulnerability exceptions for the current quarter

- Severity level of vulnerabilities
- Previous quarter vulnerability metrics

3. Vulnerability metrics and mitigation plans shall be retained for a minimum of two (2) years or as prescribed by legal or regulatory requirements.

**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 computer systems. 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. The patching and vulnerability policy shall specify what techniques an organization will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring. An organization's patching process shall define a method for deciding which systems get patched and which patches get installed first. It shall also include a methodology for testing and safely installing patches.

2. A College process for handling patches shall include:
   - Using organizational inventories
   - Using the Common Vulnerabilities and Exposures vulnerability naming scheme for vulnerability and patch monitoring[20]
   - Patch prioritization techniques
   - Organizational patch databases
   - Patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications.

3. Develop and maintain a list of sources of information about security problems and software updates for the system and application software.

4. Establish a procedure for monitoring those information sources.

5. Evaluate updates for applicability to the systems.

6. Plan the installation of applicable updates.

7. Install updates using a documented plan.

[20] *See,* http://cve.mitre.org

8. Deploy new computers with up-to-date software.

9. After making any changes in a computer's configuration or its information content, create new cryptographic checksums or other integrity-checking baseline information for that computer.

**ISO 27002 REFERENCE**
12.6.1 Control of technical vulnerabilities

## *Section 02 Software Maintenance and Upgrade*

## **040201** 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 that:

- System and application bug fixes or patches shall only be accepted from highly reliable sources, such as the software vendor.
- Software patches addressing significant security vulnerabilities are prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.
- 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.
    - Management approval.

### GUIDELINES

When applying software patches, Colleges should consider that:

- Ignored and unpatched software vulnerabilities can represent a great risk to the security of College information assets.
- They should have and implement a procedure for identifying and applying

patches that address security vulnerabilities.

- 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.
- Applying a patch or upgrade requires the same strict control as any other system change.
- Whenever a patch is implemented, the application systems it affects should be tested to ensure that business operations and security controls perform as expected.
- Appropriate updates should be made to both system documentation and business continuity plans.

**ISO 27002 REFERENCE**

| | |
|---|---|
| 12.5.1 | Change control procedures |

## **040202** Upgrading Software

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

### STANDARD

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 and demonstrate the following:

- 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 shall be developed in the event the upgrade has unacceptable ramifications. Management will agree that the desired acceptance criteria have been met.

### GUIDELINES

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 |

## 040203 Responding to Vendor Recommended Upgrades to Software

**Purpose:** To mitigate the risks associated with applying vendor-recommended software upgrades

### STANDARD

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.

### GUIDELINES

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.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 10.3.2 | System acceptance |
| 12.5.1 | Change control procedures |

## 040204 Interfacing Applications Software / Systems

**Purpose:** To mitigate risks associated with linking various application 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, but shall not be limited to, the following:

- Implementing recommended security controls.
- 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.
- Meeting with developers to determine whether data will need to be reformatted or otherwise modified to meet the needs of the interfacing system.
- Ensuring that software development procedures begin with planning and have adequate process and management controls.
- Utilizing qualified software development staff experienced in interfacing systems.

### GUIDELINES

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

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

## **040205** 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. Levels of technical support shall require that:

- 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 |

## 040206 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:

- Document that system security controls will remain effective or will be modified to appropriately respond to the OS upgrade.
- Locate change control processes and procedures.
- Document agreement of technical staff and management to acceptance criteria.
- Document that qualified personnel have certified the upgrade and that it has passed user acceptance testing.
- Establish a rollback plan in the event the upgrade has unacceptable ramifications.

### GUIDELINES

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

- An OS failure can have a cascading adverse effect on other systems and perhaps even the network.
- System documentation and business continuity plans should be amended to

reflect the OS upgrade.
- 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 REFERENCE**
12.5.2 Technical review of applications after operating system changes

## 040207 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:

- 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.
- Operating systems performance is benefited by periodic maintenance (e.g., hard drive defragmentation).
- 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.
- May be scripted to run automatically when a certain threshold or limit is exceeded.
- Logs of operating system maintenance should be regularly reviewed and compared to other system logs to ensure that:
  - Maintenance tasks continue to perform 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

## 040208 Recording and Reporting Software Faults

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

**STANDARD**

Each College shall ensure that software faults or bugs are formally recorded and reported to those responsible for software support and maintenance.

Software faults that pose a security risk shall be prioritized and addressed promptly to minimize the exposure resulting from the security vulnerability.

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 that:
  - 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.

While faults are being tracked through to resolution, research shall also be conducted to ensure that:

- No IT security controls have been compromised.
- Resolution activities have been appropriately authorized.

**ISO 27002 REFERENCES**
10.10.5 Fault logging

---

## *Section 3 Other Software Issues*

### **040301** 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:

- Following orderly termination procedures to avoid disruption of business operations.

- Migrating data to another system or archiving data in accordance with applicable records management regulations and policies for potential future access.
- 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).
- Logging the disposal of media containing confidential information to maintain an audit trail.

## GUIDELINES

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

- 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.
- Software media storage and disposal should follow industry best practices and vendor and manufacturer specifications.

**ISO 27002 REFERENCES**

10.7.2 Disposal of media

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 5 – Securing Hardware, Software, Peripherals and Other Equipment

## *Section 01 Purchasing and Installing Hardware*

### 050101 Specifying Information Security Requirements for New Hardware

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

**STANDARD**

Colleges shall ensure that new hardware purchases are supported by documented operational, technical and security requirements.

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.

**ISO 27002 References**
12.1.1 Security requirements analysis and specification

### 050102 Specifying Detailed Functional Needs for New Hardware

**Purpose:** To ensure that functional requirements are part of the acquisition process.

**STANDARD**

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.

## GUIDELINES

Colleges should develop a process to define hardware functionality prior to purchasing.

Other requirements to consider and include in RFPs are the following:

- If hardware will support a critical function: replacement availability and times.
- 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.)
- 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

## **050103** Installing New Hardware

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

## STANDARD

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 the operational and security requirements.

The review process shall include, but not be limited to, the following:

- Notification of all impacted parties prior to the installation of new hardware.
- Circulation to appropriate individuals of planned changes or disruptions to operational status or information security for the new installation.
- Installation of equipment in an appropriately secured and environmentally controlled environment.
- 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.
- Performing a risk analysis on the hardware installation process, including possible worst-case scenarios.

Security reviews shall be performed internally on a regular basis to ensure compliance with the standard requirements.

**ISO 27002 References**
12.1.1 Security requirements analysis and specification

## **050104** Testing Systems and Equipment

**Purpose:** To require that new systems and equipment undergo user acceptance testing before being placed into a production environment.

### STANDARD

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:

- 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.
- Assessment of compatibility with other system components.
- Determination that technical and functional specifications are met.
- 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 02 Cabling, UPS, Printers and Modems*

## **050201** 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

The three primary methods for providing continuous power are:

- Multiple electric feeds to avoid a single point of failure in the power supply.
- Backup generator(s).

- Uninterruptible power supply (UPS).

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 the techniques.

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.
- Using 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.
  - 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.

Other practices that help mitigate the risk of power outages include:

- 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
  - Geothermal electricity

**ISO 27002 References**
9.2.2 Supporting utilities

## 050202 Supplying Continuous Power to Critical Equipment

**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:

- Regularly inspect the generator to ensure that it:
    - Remains compliant with both safety and manufacturer maintenance requirements.
    - Has an adequate supply of fuel.
- Ensure that the generator:
    - Has the capacity to sustain the power load required by supported equipment for a prolonged period of time.
- Is tested regularly according to the manufacturer's specifications but no less than quarterly.

**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

## 050203 Using Fax Machines/Fax Modems

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

**STANDARD**

Colleges may transmit confidential information using facsimile machines or facsimile modems only when security is in place to protect the information being sent.

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**

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.

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

## 050204 Using Modems and Broadband Connections[21]

**Purpose:** To protect confidential information being transmitted over public networks.[22]

### STANDARD

College management shall set policies and procedures for approved modem and broadband connection usage.

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:

- 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.
- 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

## 050205 Using Centralized, Networked or Stand-Alone Printers

**Purpose:** To prevent the release of confidential information to unauthorized persons via printers.

### STANDARD

Personnel shall transmit confidential information to printers residing in common areas only when there is a person authorized to receive the information present to

[21] Original section title was “Using Modems and ISDN/DSL Connections”

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

protect the confidentiality of the material coming off the printer.

**ISO 27002 References**
10.7 Media handling
11.3.3 Clear desk and clear screen policy

## 050206 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[23], 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.

### GUIDELINES

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

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

**ISO 27002 References**
9.2.3 Cabling security

---

## *Section 03 Consumables*

## 050302 Using Removable Storage Media, Including Diskettes and CDs

**Purpose:** To protect the College’s data contained on removable storage

[23] Chapter 8, Article 830 of the code addresses “Network Powered Broadband Systems”. Other provisions apply as well.

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 the following:

- Damage to data stored on the removable storage media.
- Theft.
- Unauthorized access of data stored on the media.
- Software licensing violations.

### GUIDELINES

Authorized data users may use removable media to transfer information to another authorized data user in compliance with all applicable policies, regulations and laws.

**ISO 27002 References**
10.7 Media handling

## *Section 04 Working Off Premises or Using Outsourced Processing*

### 050401 Contracting or Using Outsourced Processing

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

### STANDARD

Colleges that outsource their information processing must ensure that the service provider demonstrates compliance with industry quality standards.

Outsourcing agreements shall include a contract that, at a minimum, meets State information technology security requirements.

Outsourcing agreements shall include:

- 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

## 050402 Issuing Laptop/Portable Computers to Personnel

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

### STANDARD

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. Portable devices covered by this standard are those that connect to College and State networks and/or store College data and include:

- 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.

When using encryption to protect data, Colleges shall follow the IIPS security standard 030801 – Using Encryption Techniques.

### GUIDELINES

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

- Check-in procedures for portable devices that verify that the device is free of unauthorized software, viruses, or any other malicious code prior to reissue or reconnection to the network.
- Training to raise user awareness of the additional risks that accompany mobile computing and the controls with which users must comply.

**ISO 27002 References**
11.7.1 Mobile computing and communications

## 050403 Using Laptop/Portable Computers

**Purpose:** To promote the secure use of laptops and other portable devices.

### STANDARD

Colleges shall implement appropriate safeguards to ensure the security of laptops and other portable computing devices. Specifically, portable computing devices shall:

- Adhere to the mobile data encryption standard.
- 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.
  - 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.)

### GUIDELINES

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, but are not limited to, 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

## 050404 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

Personnel shall not work from home or off site using College-issued or personally owned computers or devices (commonly known as teleworking or telecommuting) unless authorized by College management. Colleges that authorize teleworking for their personnel shall ensure the following:

- Colleges shall define standards for authorized personnel to securely access systems from off site. Standards shall include:
    - Use of College-approved virus prevention and detection software.

  - Use of personal firewalls.
  - Securing home wireless networks, and properly using other non-State WIFI 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. The college shall follow proper procedures to address this requirement to maintain Payment Card Industry Compliance (PCI).
- Use of encryption products to protect data stored on off-site systems, if applicable. Colleges shall follow the NC Community College security standard 030801 – Using Encryption Techniques when using encryption mechanisms to protect data.
- 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.
- 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.
- Colleges shall document and retain evidence of training provided to a user during the time that the individual is authorized to access systems remotely.

College employees who are authorized to work from home shall ensure that the College-defined standards 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, sometimes called Hotspots, users should consider the following:

- When possible, use more secure access points that require a key and which encrypt the wireless communication.
- Ensure your device's firewall is enabled and is configured to block unauthorized incoming connections.
- Configure your wireless LAN settings to not allow automatic joining of any wireless network. Make sure your 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 |

## **050405** 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.

### GUIDELINES

Colleges should consider the following information security issues when moving hardware:

- The confidentiality and integrity of data can be compromised if unauthorized persons gain possession of the hardware.
- Equipment can be damaged if handled improperly.

**ISO 27002 References**

| | |
|---|---|
| 9.2 | Equipment security |

## **050406** Using Mobile Communication Devices

**Purpose:** To protect College resources and confidential information during mobile communication device use.

### STANDARD

The amount of personal conversations and/or personal business on College-provided mobile communication devices shall be controlled in accordance to the College's acceptable use policy. Confidential college information transmitted, accessed, and/or stored on mobile communication devices shall be appropriately secured.

For purposes of this standard, 'mobile communication devices' includes mobile phones, IP phones, pagers, BlackBerry devices, iPhones, iPads, tablets, smart phones 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.

Colleges that allow mobile communication devices (personal or business owned) to connect to college systems, such as e-Mail, 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 College's service desk or to College management within 24 hours of confirmation.

Personnel using College-provided mobile communication devices shall do the following:

- Adhere to state and college acceptable use standards and policies.
- Adhere to the NC Community College encryption standard (030801 – Using Encryption Techniques), if applicable.
- Adhere to NC Community College standards for removing all data before disposing of the device (030903 - Using External Disposal Firms and 040301 - Disposing of Software).
- Change the default password for connecting to a wireless enabled device (i.e. WIFI or Bluetooth) on applicable mobile communication devices.
- Disable wireless functionality (i.e. WIFI or Bluetooth) on appropriate devices with wireless functionality (i.e. WIFI 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 college business should make them aware of the following information security issues:

- The risk of others eavesdropping physically and electronically in both private and public areas.
- The risks involved in storing and/or transmitting confidential information on calendars, address books, etc.
- 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.

- Do not open attachments from untrusted sources.

- Do not follow links from untrusted sources, especially from unsolicited email or text messages.
- Report lost devices immediately to your carrier and/or organization. Use the remote erase function if enabled.
- Review the mobile device security settings to ensure appropriate protection.
- For Bluetooth enabled devices, consider the following[24]:
  - Choose PIN codes that are sufficiently random and long.
  - Disable the ability for the Bluetooth device to be discovered, except when needed for pairing.
  - Pair devices only in a secure area.
  - When possible, enable encryption to secure data transmissions.
  - When possible, enable device mutual authentication.
  - Set the Bluetooth device to the lowest necessary and sufficient power level
  - Do not accept transmissions from unknown or suspicious devices.
  - In the event a Bluetooth enabled device is lost or stolen, immediately unpair the device.

**ISO 27002 References**

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

## **050407** Using Business Center Facilities

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

### STANDARD

College employees using external business centers to conduct business shall not process confidential information, including not transmitting confidential information via email(s) or fax(es).

When College employees use business center facilities for processing other government information (i.e., information that is not confidential), they shall:

- 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.

[24] 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.

- 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

## 050408 Day-to-Day Use of Laptop/Portable Computers

**Purpose:** To promote the secure day-to-day use of laptop/portable computers.

### STANDARD

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.

Colleges shall require that laptops and other College-issued mobile electronic devices have:

- Comply with the mobile data encryption standard.
- Be physically secured when left unattended or when taken out of a secure area.
- Regular backups.
- Current antivirus software.
- Firewalls configured to comply with State and College policies.

Where technically possible, Colleges shall require that other mobile electronic devices used for conducting the College's business comply with the same standards as laptops. Where full disk encryption is not technically possible, mobile electronic devices shall have other protection mechanisms such as BIOS password or PIN access.[25]

Colleges shall periodically audit these devices to ensure compliance with these requirements.

**ISO 27002 References**
11.7.1 Mobile computing and communications

## *Section 05 Using Secure Storage*

[25] For hand held devices (e.g. smart phones, personal data assistants, and BlackBerry or BlackBerry-like devices) that connect to the State Network, see 020112 Controlling Remote Access.

## 050502 Using Lockable Filing Cabinets

**Purpose:** To secure paper-based files and computer media in locked filing cabinets.

### STANDARD

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 classification status of the information.

**ISO 27002 References**

| | |
|---|---|
| 9.1.3 | Securing offices, rooms and facilities |

## 050503 Using Fire-Protected Storage Cabinets

**Purpose:** To decrease the risk of critical information being destroyed by fire.

### STANDARD

Where appropriate, Colleges shall provide fire-protected storage for documents and media containing information critical to their business function:

### GUIDELINES

Colleges should consider the following physical security issues:

- Securing critical information in a fire-resistant safe or cabinet should be part of a College’s clear desk policy.
- 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, rooms and facilities |
| 11.3.3 | Clear desk and clear screen policy |

## 050504 Using a Safe

**Purpose:** To protect critical information from theft, destruction and misuse

### STANDARD

Where appropriate, Colleges shall store information that is confidential or critical to their business functions in a safe.

When a safe is used:

- The location of the safe shall be inconspicuous, so as not to draw additional attention to the physical security of the safe.
- The location of the safe must have a load-bearing capacity sufficient to support the weight of the safe.
- The location of the safe must be in an area that is subject to regular surveillance.
- Access to the safe shall be limited to those who College management has determined require access to perform their job duties.

**GUIDELINES**

Whenever the value of confidential or critical paper-based files or computer media warrants the use of a safe, Colleges should consider the following:

- Critical information is compromised if the whole safe is stolen.
- Events surrounding a fire (heat, smoke, water, chemicals) may render the material stored in the safe unusable; therefore, off-site backups of critical information remain essential.

.

**ISO 27002 References**
9.1.3 Securing offices, rooms and facilities
11.3.3 Clear desk and clear screen policy

## *Section 06 Documenting Hardware*

### **050601** Managing Software and Hardware Documentation

**Purpose:** To effectively manage hardware assets and their documentation.

**STANDARD**

Colleges shall retain user documentation and technical specifications of information technology hardware and software. Documentation shall be secured from unauthorized use and made readily available to support system maintenance and system support staff.

**GUIDELINES**

Colleges should develop and maintain additional documentation that details hardware and software placement and configuration, provide flowcharts, etc.

Documentation should include:

- Vendor name, address, and contact information

- License number and version
- Update information
- Configuration reports  and listing for operating system and server software.
- Bios rev information
- Port listing

**ISO 27002 References**

7.1.1 Inventory of assets
10.7.4 Security of system documentation

## 050602 Maintaining a Hardware Inventory or Register

**Purpose:** To maintain accountability for hardware assets and protect them from misappropriation.

### STANDARD

Colleges shall identify and record its information technology (IT) hardware assets in a formal hardware inventory/register. 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

The formal hardware inventory/register should include only information that is available for public inspection.

**ISO 27002 References**

7.1.1 Inventory of assets

## *Section 07 Other Hardware Issues*

## 050701 Disposing of Obsolete Equipment

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

### STANDARD

Colleges shall establish a procedure for certifying that data have been properly removed from information technology equipment before it is transferred, surplused or donated.

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.[26]

**ISO 27002 References**

| | |
|---|---|
| 9.2.6 | Secure disposal or re-use of equipment |

## 050702 Recording and Reporting Hardware Faults

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

### STANDARD

Users who identify a hardware fault or information-system-processing problem shall promptly report the problem and the details to the appropriate support staff.

Each College shall establish procedures to record and track equipment faults.

**ISO 27002 References**

| | |
|---|---|
| 9.2.4 | Equipment maintenance |
| 10.10.5 | Fault logging |

## 050703 Insuring Hardware

**Standard removed**

## 050704 Insuring Laptops/Portables for Use Domestically or Abroad

**Standard removed**

## 050705 Clear Screen

**Standard removed (Addressed in Standard 020103)**

[26] Additional information regarding the secure disposal of obsolete equipment may be found in the NIST publication 800-88 titled “Guidelines for Media Sanitization.”

## 050706 Logon and Logoff from your Computer

Standard removed (Locking Work Station Addressed in Standard 020103 and rest of Standard in 020102 and 020106.)

## 050707 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

Users shall not record or leave messages containing confidential information on answering machines or voice mail systems.

### GUIDELINES

Colleges should 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 |

## 050708 Taking Equipment off the Premises

**Purpose:** To safeguard and maintain accountability for equipment.

### STANDARD

College personnel must have approval from an authorized College employee before they remove State information technology equipment from College facilities. Personnel removing equipment shall be responsible for the security of the equipment at all times.

Colleges shall establish procedures for the removal and return of College equipment. 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 |

## 050709 Maintaining Hardware (On-Site or Off-Site Support)

**Purpose:** To maintain hardware availability and integrity

### STANDARD

Each College shall provide or arrange maintenance support for all equipment that is owned, leased or licensed by the College. The College must arrange support services through appropriate maintenance agreements or with qualified technical support staff. 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. Records of all maintenance activities shall be maintained.

**ISO 27002 References**
9.2.4 Equipment maintenance

## 050710 Using Speed-Dialing Telephone Options

**Purpose:** To protect information stored in telephone system equipment.

### STANDARD

Colleges shall incorporate security measures to protect confidential information stored in speed-dialing systems, such as unlisted telephone numbers that are classified as confidential.

### GUIDELINES

Colleges should consider the information security issues and the accompanying risks involved if unlisted phone numbers are acquired by unauthorized users.

**ISO 27002 References**
10.8.1 Information exchange policies and procedures

## 050712 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 information exposed. Colleges should refer to their business impact analyses and/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 |

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 6 – Combating Cyber Crime

## *Section 01 Combating Cyber-Crime*

### 060101 Defending Against Premeditated Cyber-Crime Attacks

**Purpose:** To protect College networks from a premeditated cyber-attack.

**STANDARD**

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, but are not limited to: wireless access points, network ingress and egress points, and network-attached devices.

Colleges shall deploy controls to ensure that the College's resources do not contribute to outside-party attacks. These controls include but are not limited to:

- Securing interfaces between College-controlled and non-College-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 and/or intrusion prevention systems.
- Signatures for Intrusion Detection Systems/Intrusion Prevention Systems shall be kept up to date to ensure systems are operating at most optimum level.

**ISO 27002 REFERENCE**
11.4 Network access control

### 060102 Minimizing the Impact of Cyber-Attacks

**Purpose:** To minimize the impact of a cyber-attack on College networks.

**STANDARD**

Colleges shall have security incident management and response plans that address steps to be taken during and after cyber-attacks. Colleges shall also develop contingency plans for the continuation of business processes while under a cyber-attack and/or the recovery of data damaged during such an attack. The security incident management and response plans shall be integrated with the business continuity and disaster recovery plans. 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. These plans shall be developed in accordance with Standard 140102, Assessing the Business Continuity Plan Security Risk, and tested under Standard 140104, Testing the Business Continuity Plan.

Incident response plans shall incorporate information from intrusion detection/prevention systems (IDS/IPS), and other monitoring systems. Plans shall be tested at least annually. Colleges should also develop a process to modify plans according to lessons learned and industry developments.

**ISO 27002 REFERENCE**
14.1.2 Business continuity and risk assessment

## 060103 Collecting Evidence for Cyber-Crime Prosecution

**Purpose:** To ensure that evidence gathered as a result of cyber-crime is admissible as evidence in the prosecution of cyber-crime.

### STANDARD

In the event of a suspected cyber-crime, evidence shall be collected and preserved in a manner that is in accordance with State and federal requirements. 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.

When dealing with a suspected cyber-crime, Colleges shall:

- 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.
- Report the incident to the College CIO within twenty-four (24) hours of occurrence. College CIO will contact other off-campus support as deemed necessary by law.

**ISO 27002 REFERENCE**
13.2.3 Collection of evidence

## 060104 Defending Against Premeditated Internal Attacks

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

### STANDARD

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

- Access to files shall be granted only on as required for the performance of job duties.
- Networks that serve different College user groups (Faculty/staff and students) shall be segregated, and access to those segmented networks shall be established as appropriate through the use of VLANs, routers, firewalls, etc.
- Access badges shall be programmed to allow entry only into assigned places of duty, if possible.
- Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.
- 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.

**ISO 27002 REFERENCES**

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

## 060105 Defending Against Opportunistic Cyber-Crime Attacks

**Purpose:** To reduce the threat of cyber-crime attacks

### STANDARD

To protect against opportunistic cyber-crime attacks, authentication mechanisms shall be required before access is granted to any College network resource. Authorization levels shall be reviewed regularly to prevent disclosure of information through unauthorized access.

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 follow local procedures to request assessments as needed and/or required to maintain Payment Card Industry Compliance (PCI).

**ISO 27002 REFERENCE**

| | |
|---|---|
| 11.4 | Network access control |

## 060106 Safeguarding Against Malicious Denial of Service Attacks

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

### STANDARD

Each College shall have the following responsibilities:

- 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 Colleges ability to accept the risk for a possible disruption in service from a successful attack.

- To deny all inbound traffic by default, thus limiting the channels of network attacks.
- To periodically scan for bots (software robots) and Trojan horse programs.
- To deploy authentication mechanisms wherever possible.
- To design and implement networks for maximum availability.
- To develop specific plans for responding to DoS and DDoS attacks in the College incident management plan and the business continuity plan.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 9.4 | Network access control |
| 13.2.1 | Responsibilities and procedures |

## 060107 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 the amount of potential exploits within the network infrastructure.

The following duties shall be performed by system administrators or security personnel:

- 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.
- Denial of all inbound traffic by default through the perimeter defense. Exceptions for traffic essential for daily business must be requested through network security.
- Configuration of public facing systems in accordance with Standard 070103, Configuring E-Commerce Web Sites.
- Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate College 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 College and employee.
- 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 |

## 060108 Handling Hoax Virus Warnings

**Purpose:** To minimize the threat of hoax virus warnings.

### STANDARD

To minimize the threat of hoax virus warnings, incident management procedures shall contain a provision that virus threats are verified before warnings about them are distributed. Appropriately verified warnings shall be distributed by management, College security administrators, or the Enterprise Security and Risk Management Office (ESRMO) through recognized government or verified vendor source, according to State and College standards, policies and procedures. Colleges shall direct their staffs to follow established standards, policies and procedures and not to forward un-verified virus warnings to others.

**ISO 27002 REFERENCES**

6.1.3 Allocation of information security responsibilities
10.4.1 Controls against malicious code

## 060109 Defending Against Virus Attacks

**Purpose:** To minimize virus attacks.

### STANDARD

Colleges shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the College network. In addition, system antivirus software, including virus signature files, shall be promptly updated as updates are released by the software vendor.

All files downloaded to the College network might potentially harbor computer viruses, Trojan horses, worms or other destructive programs (collectively, “virus” or “viruses”); therefore, all downloaded files must be scanned for such viruses. Virus 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. All Colleges shall be responsible for ensuring that they have current software on their network to prevent the introduction or propagation of computer viruses.

Additionally, All virus scanning software shall be current, actively running on deployed workstations and servers, and capable of generating audit logs of virus events.

Colleges shall select and use virus prevention and mitigation standards and best practices as appropriate.

Virus controls, procedures, education and training shall include the following:

- Use of antivirus software.
- Performing frequent backups on data files.
- Use of write-protected program media, such as diskettes or CD-ROMs.
- Validating the source of software before installing it.

- Scanning for viruses on files that are downloaded from the Internet or any other outside source.
- Scanning for viruses on all external media, such as flash drives, CDs, etc., brought from home or any other outside source.
- 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.
- Prohibition of network connection to outside organizations without a mutual review of security practices
- System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.

**ISO 27002 REFERENCE**

10.4.1 Controls against malicious code

## 060110 Responding to Virus Incidents

**Purpose:** To establish an effective response to virus incidents.

### STANDARD

To mitigate the propagation of viruses and to protect College networks, each College shall develop a cyber-security incident management plan for controlling the potential negative consequences of an incident.

College plans shall include:

- Incident response team members and contact information.
- Procedures for detecting, responding to and recovering from virus incidents.
- Procedures for notifying the College CIO.
- Staff training.
- Testing of the plan.

Each College shall collect and preserve evidence of information technology security incidents in accordance with Standard 060103, Collecting Evidence for Cyber Crime Prosecution. Documentation of any incident shall be thoroughly performed for later review.

A College’s incident management plan shall include the following elements:

- Verification of a virus threat, to rule out possibility of hoax, before notification of the threat is broadcast.
- The identity of personnel responsible for mitigation of virus threats.
- Internal escalation procedures and severity levels.
- Processes to identify, contain, eradicate, and recover from virus events.
- A contact list of antivirus software vendors.
- Reporting to the College CIO.
- Review by staff, after each information technology security incident, of the lessons learned from the incident, with any necessary changes subsequently made to the College incident management plan.

**ISO 27002 REFERENCES**

10.4.1 Controls against malicious code

| | |
|---|---|
| 13.1.1 | Reporting information security events |
| 13.2.1 | Responsibilities and procedures |

## 060111 Installing Virus Scanning Software

**Standard merged into standard 060109 and 040105**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 7 – Controlling E-Commerce Information Security

## *Section 01 E-Commerce Issues*

### 070101 Structuring E-Commerce Systems including Web Sites

**Purpose:** To protect the College's information resources when conducting business or providing services via e-commerce.

**STANDARD**

Colleges that conduct business via e-commerce shall ensure that information transmitted and/or stored and the supporting information technology applications used are protected by appropriate policies, procedures and security measures. In addition, Colleges must comply with relevant portions of the State technical architecture, the requirements of the Office of the State Controller, and applicable legal requirements. Colleges must also maintain PCI Compliance standards as outlined by the PCI Security Standards Council. (https://www.pcisecuritystandards.org/)

**GUIDELINES**

Considerations for electronic-commerce security include but are not limited to:

- End-to-end encryption while data are in transit.
- Encryption while data are at rest.
- A consistent approach to securing servers in use. Measures taken would include, but are not limited to:
  - Removing sample files.
  - Disabling unnecessary services.
  - Keeping resources, both application programs and operating systems, up to date with patches.
  - Enforced paths restricting user access to authorized programs and data.
  - Appropriate agreements with information service providers and value-added network providers.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 10.9.1 | Electronic commerce |
| 11.4 | Network access control |
| 12.1.1 | Security requirements analysis and specification |

## 070102 Securing E-Commerce Networks

**Purpose:** To protect the College's e-commerce systems by securing the networks that support the operation of those systems.

**STANDARD**

The College's e-commerce systems and supporting networks shall be secured to prevent and detect intrusion and misuse. The level of monitoring and logging required for systems and networks shall be determined by a risk assessment. Because e-commerce system risks are increased when system users are connecting to the Internet, it is important to monitor and log these systems.

Both e-commerce Web sites and College networks need appropriate security controls, including:

- Authentication of users.
- Access control rules and rights for users.
  - Authority levels and permissions.
  - Proper authorization of content providers.
- Measures to safeguard the confidentiality, integrity and availability of data, such as encryption in transit and/or in storage and monitoring of user IDs.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 10.9.1 | Electronic commerce |
| 10.10.2 | Monitoring system use |
| 11.1.1 | Access control policy |
| 11.4 | Network access control |

## 070103 Configuring E-Commerce Web Sites

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

**STANDARD**

A College's e-commerce Web site(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:

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

### GUIDELINES

When implementing e-commerce applications, Colleges should consider using:

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

**ISO 27002 REFERENCE**
10.9.1 Electronic commerce

## 070104 Using External Service Providers for E-Commerce

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

### STANDARD

When Colleges contract with external service providers for e-commerce services, the services shall be governed by a formal agreement. 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 College's record retention schedules, its security policies, its security standards, 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

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 8 – Developing and Maintaining In-House Software

## *Section 01 Controlling Software Code*

### 080101 Managing Operational Program Libraries

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

**STANDARD**

Colleges shall restrict access to operating system and operational or production application software/program libraries to designated staff only.

**GUIDELINES**

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 should ensure that their program libraries are adequately protected. 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 in the following areas:

- Updating of libraries.
- Restricting library content to executable code.
- Version control for each application.
- Tying system documentation updates to application software library updates.
- Rollback procedures designed to recover to old, stable versions of programs.
  Audit logs that track all:
    - Accesses to libraries.
    - Change requests.
    - Copying and use of operational information.
    - Updates posted to libraries.
    - Defining job responsibilities and establishing authority levels for:
        - Program librarian(s).
        - Personnel authorized to make or submit changes to program libraries. (Developers should not be permitted to promote their own code into libraries.)

**ISO 27002 References**

12.4.1 Control of operational software

12.5.1 Change control procedures

## 080102 Managing Program Source Libraries

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

### STANDARD

Colleges shall manage access to source code or source program libraries, limiting access to authorized individuals.

- Production source code and development source code libraries must always be kept separate.
- Colleges shall implement a combination of technical access controls and robust procedures to restrict access to source program libraries to authorized personnel only.

**RELATED INFORMATION**

| | |
|---|---|
| Standard 080104 | Controlling Program Listings |
| Standard 080105 | Controlling Program Source Libraries |
| Standard 080106 | Controlling Old Versions of Programs |

**ISO 27002 References**

12.4.3 Access control to program source code

## 080103 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:

- Authorization is required to initiate or make changes to software.
- Change control procedures that govern changes to system software are defined and utilized.
- All changes must be tested in a test environment and pass acceptance testing prior to moving changed code into a live or production environment.
- Senior management may authorize emergency exceptions to this standard only to avoid imminent failure of business operations.

### GUIDELINES

- 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.

- A general SDLC should include the following phases: initiation, acquisition/development/implementation/assessment, operations/maintenance, and 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.[27]
- 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**
12.5.1 Change control procedures
12.5.3 Restrictions on changes to software packages

## 080104 Controlling Program Listings

**Purpose:** To protect the integrity of software by controlling program listings.

### STANDARD

Colleges shall maintain and control current electronic copy listings of application/program source code that runs on College systems. This is only applies to locally developed custom program code.

### GUIDELINES

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.

**ISO 27002 References**
10.7.4 Security of system documentation
12.4.3 Access control of program source code

[27] More information regarding the Software Development Life Cycle (SDLC) may be found in the NIST publication "Information Security in the SDLC Brochure."

## 080105 Controlling Program Source Libraries

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

### STANDARD

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

- Formal change control procedures.
- Comprehensive audit trails.
- Monitoring**.**

### 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

## 080106 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:

- Comprehensive procedures for auditing removals or updates to program libraries.
- 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 College policy in regards to old versions of programs:

- When application code within college systems has been superseded or discontinued, College 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.

- 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 02 Software Development*

### **080201** 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:

- A Standard Software Development Life Cycle (SDLC) that is managed by a project team.
- 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 information security issues when updating or formalizing development processes:

- Potential compromise to production systems.
- The threat of insertion of malicious code within software.
- Disruption of live operations.
- Confidentiality, criticality and value of the systems and data to the College and public.

### **080202** Making Emergency Amendments to Software

**Purpose:** To protect production software during emergency modifications

### STANDARD

College personnel must fully justify their requests for emergency modifications to software and must obtain senior management authorization.

College personnel making emergency modifications must not deviate from the College's change control procedures.

### GUIDELINES

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.

When developing emergency change control procedures, Colleges should consider how these procedures will deviate from normal everyday change control procedures and best practices in the following areas:

- Updating of libraries.
- Restricting library content.
- Version control for each application.
- Tying program documentation updates to source code updates.
- Audit logs that track all:
    - Accesses to libraries.
    - Change requests.
    - Copying and use of source code.
    - Updates posted to libraries.

- Predefined job responsibilities/restrictions and establishment of authority levels that have been agreed to for:
    - Program librarian(s).
    - Developers.
    - Other IT staff.
- Personnel authorized to make or submit changes to the source library. (A program librarian should be appointed for each major application to control check-in/check-out.)
- Rollback procedures designed to recover to old, stable versions of programs.

**ISO 27002 References**
12.5.1 Change control procedures

## 080203 Establishing Ownership for System Enhancements

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

### STANDARD

Colleges shall establish custodians for each system who will have responsibility for all system enhancements.

- 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.
- 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):

- Identifying and clearly defining the various assets and security processes associated with each individual system for which the position holder will be held responsible.
- 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.
- 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.
    - Detailed description of manager/custodian responsibilities.

**ISO 27002 References**
6.1.3 Allocation of Information Security responsibilities

## 080204 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:

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

### 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:

- 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.
- 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

## 080205 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:

- Enforcement of formal change control procedures.
- Proper authorization and approvals at all levels.
- Successful testing of updates and new programs prior to their being moved into a live environment.
- Updates addressing significant security vulnerabilities shall be prioritized, evaluated, tested, documented, approved and applied promptly to minimize the exposure of unpatched resources.
- 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 healthy 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.

Appropriate technical controls and procedures for protecting program and source libraries should be designed to prevent unauthorized use. Loss of source code could make it difficult or impossible for a College to maintain its systems, and unauthorized modification of programs could result in system failure or malicious damage.

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

- Controls and approval levels for updating libraries.
- Requiring formal agreement and approval for any changes.
- Restricting library content.
- Restricting programmers’ access to only those parts of the system necessary for their work.
- Version control for each application.
- Tying program documentation updates to source code updates.
- 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:
    - Program librarian(s).
    - Developers (i.e., should neither test their own code nor promote it into production).
    - Other IT staff.

- 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).
- Rollback procedures designed to recover to old, stable version of programs.

**ISO 27002 Reference**
12.5.1 Change control procedures

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

## 080206 Separating System Development and Operations

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

### STANDARD

College management must ensure that there is proper segregation of duties to reduce the risk of College system misuse and fraud.

- System administration and system auditing shall be performed by different personnel.
- System development and system change management shall be performed by different personnel.
- System operations and system security administration shall be performed by different personnel.

Insofar as is possible, security administration and security audit shall be performed by different personnel.

Administrators of multi-user system must have at least two user IDs. One of these user IDs must provide privileged access, with all activities logged; the other must be a normal user ID for performing the day-to-day work of an ordinary user.

### GUIDELINES

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.

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

- When separation of duties is difficult, consider other controls such as:
  - Monitoring of activities.
  - Audit trails.
  - Management supervision.
- Keep the responsibility for security audit separate from other audit powers.
- Identify and segregate activities that require collusion to defraud (e.g., exercising a purchase order and verifying receipt of goods).

Consider dual control in instances in which collusion might result in the College's being defrauded.

- 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

## *Section 03 Testing & Training*

### **080301** Controlling Test Environments

**Standard removed: Addressed in standard 080103**

### **080302** Using Live Data for Testing

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

**STANDARD**

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 standards.

This is acceptable when permitted by other regulations and standards. Additionally, confidential live data shall not be used for testing purposes.

If production data is used for testing, the following controls must be met:

- Testing of production data shall take place only on non-live, non-production systems.
- Adequate controls for the security of the data are in place.
- The test shall observe and maintain the confidentiality conditions established by the College from which the data is obtained.

**ISO 27002 References**
12.4.2 Protection of system test data

### **080303** 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**

To maintain the integrity of College information technology systems, software shall be evaluated and certified by data owner for functionality in a test environment before it is used in an operational/production environment.

Test data and accounts shall be removed from an application or system prior to being deployed into a production environment. This does not apply to an application or system with a dedicated testing environment.

**ISO 27002 References**

| | |
|---|---|
| 10.3.2 | System acceptance |
| 12.5.1 | Change control procedures |

## 080304 Capacity Planning and Testing of New Systems

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

### STANDARD

New system purchases shall meet, at a minimum, current operational specifications and have scalability to accommodate for growth projected by the College. 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.

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:

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

**ISO 27002 References**

| | |
|---|---|
| 10.3.1 | Capacity management |
| 10.3.2 | System acceptance |

## 080305 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:

- Capacity requirements—both for performance and for the computer hardware needed.
- Error response—recovery and restart procedures and contingency plans.
- Routine operating procedures—prepared and tested according to defined College standards.
- Security controls—agreed to and put in place.
- Manual procedures—effective and available where feasible and appropriate.
- Business continuity—meets the requirements defined in the College's business continuity plan.
- 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).
- Training—of operators, administrators and users of the new or updated system.

**ISO 27002 References**

10.3.2 System acceptance
12.5.1 Change control procedures

## 080306 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:

- When administrative training is inadequate, small problems can unnecessarily escalate as a result of lack of knowledge of new functions or security controls.
- 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.

- 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 04 Documentation*

### **080401** Documenting New and Enhanced Systems

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

**STANDARD**

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.

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.

Colleges shall ensure that system documentation is readily available to support the staff responsible for operating, securing and maintaining new and updated systems.

**GUIDELINES**

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

- 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.

- 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).
- 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.
- 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 |

## *Section 05 - Other Software Development*

### **080501** Acquiring Vendor Developed Software

**Purpose:** To maximize the utility of vendor-developed software

**STANDARD**

Colleges shall comply with State purchasing and contracting laws, rules 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.

Colleges shall initiate formal contracts defining third-party access to the organization's information-processing facilities. Such contracts should include or refer to all security requirements and expected performance and support levels to ensure that there is no misunderstanding between the College and the vendor.

**ISO 27002 References**

| | |
|---|---|
| 6.2.3 | Addressing security in third party agreements |

# Chapter 9 – Dealing with Premises Related Considerations

## *Section 01 - Premises Security*

### **090101** Preparing Premises to Site Computers and Data Centers

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

**STANDARD**

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.

**GUIDELINES**

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

- 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.
- Security threats may expand from neighbouring premises or adjacent properties.
- Requirements for size and location will vary according to the amount of hardware being housed.
- Physical security measures adopted should reflect the:
    - Value of the hardware.
    - Sensitivity of the system’s data.
    - Required level of availability or fault tolerance.
- 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:
    - Explosion.
    - Fire.
    - Smoke.

- Water (or a failure to supply water).
- Chemicals.
- Wind.
- Seismic activity.
- Dust.
- Vibration.
- Electromagnetic radiation.
- Electrical supply interference.

**ISO 27002 References**

9.2.1 Equipment siting and protection

## 090102 Securing Physical Protection of Computer Premises

**Purpose:** To protect information assets via physical security.

### STANDARD

Each College shall safeguard sites, buildings and locations housing its information technology assets.

### GUIDELINES

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.

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.
- Equipping all fire doors on a security perimeter with alarms as well as devices that close and lock the doors automatically.

**ISO 27002 References**

9.1.1 Physical security perimeter

## 090103 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:

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

**ISO 27002 References**

9.1.3 Securing offices, rooms, and facilities

## 090104 Physical Access Control to Secure Areas

**Purpose:** To protect computer equipment by controlling physical access.

### STANDARD

Colleges shall ensure areas housing information technology assets have appropriate physical access controls. Authorized individuals may include College employees, contractors and vendors. Colleges shall develop access policies for authorized individuals as well as visitors to these areas. An audit trail of access for all individuals to datacenters shall be maintained.

Colleges shall also restrict access to publicly accessible network jacks in datacenters by disabling unused network jacks, unless they are explicitly authorized. 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:

- 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.
- Physical access authentication controls should include some form of visible identification such as an ID badge.
- An audit trail of physical access to the computer area should be maintained.
- 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

## **090105** Challenging Strangers on College Premises

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

### STANDARD

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. Where appropriate, employees and visitors shall be properly badged and escorted at all times. 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**
9.1.3 Securing offices, rooms, and facilities

## 090106 High Security Locations

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

### STANDARD

Locations that contain confidential information shall be designed and secured in accordance to the information being protected.

The use of cameras, video recorders and handheld devices (cell phones, PDAs, pocket PCs), shall be restricted from high security locations to protect the information being stored

Video cameras and/or access control mechanisms shall be used to monitor individual physical access to sensitive areas.

**ISO 27002 References**

9.1.5 Working in secure areas

## 090107 Delivery and Loading Areas

**Purpose:** To protect information and assets in loading areas.

### STANDARD

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 distributed for use.

**ISO 27002 References**

9.1.6 Public access, delivery, and loading areas

## 090108 Duress Alarm

**Purpose:** To protect personnel and confidential information using alarms.

### STANDARD

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.

**ISO 27002 References**

9.1.5 Working in secure areas

## *Section 02 Data Stores*

### **090201** Managing On-Site Data Stores

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

**STANDARD**

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

- The survivability of the data store in the face of man-made or natural disasters.
- The need for periodic testing of backup and restore procedures to verify strengths and identify areas for improvement.
- 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 |

### **090202** Managing Remote Data Stores

**Purpose:** To protect confidential information that is stored remotely.

**STANDARD**

Colleges shall ensure that remote data storage locations have adequate access controls to minimize the risk of data loss or damage. Colleges shall address the following security issues when choosing a location for a remote data store:

- 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 |

## *Section 03 Other Premises Issues*

### 090301 Electronic Eavesdropping

**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 State Network or its components.

**STANDARD**

All colleges 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:

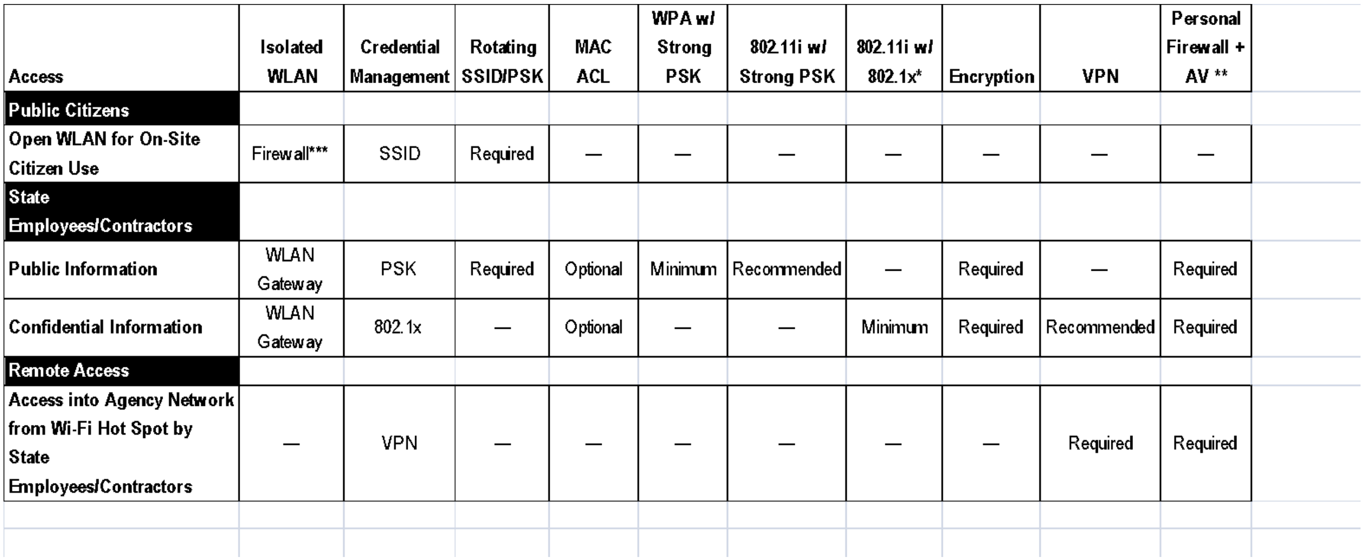
- Physical access
  - All network access points (APs) and related equipment such as base stations and cabling supporting wireless networks shall be secured with locking mechanisms or kept in an area where access is restricted to authorized personnel.
  - The reset function on APs shall be used only by and accessible only to authorized personnel.
- Network access
  - APs shall be segmented from college's internal wired local area network (LAN) using a gateway device.

  - 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 LAN WLAN.
  - 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
  - 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. 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 the 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).

- 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.
    - When WPA2 is used, AES encryption shall be enabled and shall be no less than 128 bits.
    - When WPA is used, the highest level of encryption supported on the device shall be enabled.
    - WPA encryption must use Temporal Key Integrity Protocol (TKIP) or other IEEE- or National Institute of Standards and Technology (NIST)-approved key exchange mechanism.
    - WPA2 (802.11i) encryption must use CCMP or other IEEE- or NIST-approved key exchange mechanism.
    - Wired Equivalent Privacy (WEP) shall not be relied upon for wireless security.
    - 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.
- IEEE 802.11 wireless devices shall not be used to manage other systems on the network except in temporary, ad hoc, emergency situations or by use of end-to-end encryption with authentication.

- 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, and search their sites using wireless sniffers or vulnerability assessment scans at least quarterly to ensure that only authorized wireless access points are in place. Using wireless sniffers to scan and reviewing monthly is recommended. This type of audit is also recommended for sites not using wireless technologies to detect rogue access points and end-user-installed free-agent access points.
  - The management system shall monitor the airspace in and around college facilities for unauthorized access points and ad hoc networks 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 | — | — | — | — | — | — | — |
| **State Employees/Contractors** | | | | | | | | | | |
| 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 State 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.<br>*** 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). |

- College reporting requirements.
  - Colleges shall report all 802.11 wireless LANs to the College Chief Information Officer.

**ISO 27002 References**
13.1.2 Reporting security weaknesses

## 090302 Cabling Security

**Purpose:** To provide an adequate level of confidentiality, integrity and availability for information sent via networks.

### STANDARD

Colleges shall review the security of network cabling during upgrades or changes to hardware or facilities for signs of weak or missing physical security controls.

### GUIDELINES

Colleges installing or maintaining telecommunication and/or power cabling should consider the following practices to increase the security and physical protection of the cabling:

- Underground cabling should be used, where possible, or lines with adequate alternative protection.
- Network cabling should be run through pipe or some other type of conduit and otherwise protected from possible damage.
- Power and communication cables should be segregated.
- Installers should be qualified to ensure that cabling complies with health, safety and building code requirements as appropriate.

**ISO 27002 References**
9.2.3 Cabling security

## 090303 Disaster Recovery Plan

**Standard relocated to Standard 140107**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 10 – Addressing Personnel Issues Relating to Security

## *Section 01 - Contractual Documentation*

### **100101** Preparing Terms and Conditions of Employment

The above standard recommended by ISO 27002 is addressed in Chapter 126 – State Personnel Act and in policies established by the Office of State Personnel.

### **100102** Employing/Contracting New Staff

The standard recommended by ISO 27002 for this category is addressed in Chapter 11 of this document, “Delivering Training and Staff Awareness.”

### **100103** Contracting with External Suppliers/Other Service Providers

**Purpose:** To address information security issues involving third parties who provide services to State Colleges.

**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.

Third parties are non-College employees, such as vendors, suppliers, individuals, contractors and consultants, responsible for providing goods or services to the State. 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. 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. Third parties shall be fully accountable to the College for any actions taken while completing their College assignments. College staff overseeing the work of third parties shall be responsible for communicating and enforcing applicable laws, as well as State and College security policies, and procedures.

**ISO 27002 References**
6.1.3 Allocation of Information Security responsibilities

### **100104** Using Non-Disclosure Agreements (Third Party)

**Purpose:** To protect access to and the integrity of the College's information resources.

**STANDARD**

College operational and/or restricted information must not be released to third parties without properly executed contracts and confidentiality agreements. These legal documents, which may include non-disclosure agreements, must specify conditions of use and security requirements.

**ISO 27002 References**
6.1.5 Confidentiality agreements

If appropriate, the above policies recommended by ISO 27002 should be addressed by the College personnel office or senior management.

## *Section 03 - Personnel Information Security Responsibilities*

### **100301** Using the Internet in an Acceptable Way

**Purpose:** To establish a standard pertaining to the use of the College network and the global Internet by college employees

**STANDARD**

While performing work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, College employees 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.

Each College 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.

Colleges that use the College network shall prohibit users from the download and installation of unapproved software as defined by each College's IT policies.

All files downloaded from a source external to the College network shall be scanned for viruses, Trojan horses, worms or other destructive code for such harmful contents. This includes files obtained as email attachments and through any other file transfer mechanism. It shall be the responsibility of public employees and College network users to help prevent the introduction or propagation of computer viruses. All Colleges shall ensure that they have current software on their networks to prevent the introduction or propagation of computer viruses.

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. Public employees and other college network users also shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to have access.

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.

Operators of email services must create an abuse@<*host domain name*> account and other additional internal procedures to manage their email complaints. Users who receive email that they consider to be unacceptable according to this standard can choose to forward the original email message (including all headers) to the appropriate email abuse@<*host domain name*> account.

**GUIDELINES**

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). 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.

Colleges should provide employee orientation and annual employee security awareness training providing guidance on the appropriate use of the Internet including:

- SPAM
- Phishing Attacks
- Malware Threats
- Personal use of the Internet
- Acceptable download practices
- Peer to Peer Software usage
- Copyright protections
- Unacceptable uses of the Internet

**ISO 27002 References**
8.2.3 Disciplinary process
15.1.5 Prevention of misuse of information processing facilities

## **100302** Keeping Passwords/PIN Numbers Confidential

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

Standard merged into standard 020106

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 11 – Delivering Training and Staff Awareness

## *Section 01 - Awareness*

### **110101** Delivering Awareness Programs to Permanent Staff

**Purpose:** To ensure that top management takes the lead in giving information security a high priority throughout the College.
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 in all current and future activities and initiatives. Senior management within the College shall ensure that information security communications are given priority by staff and shall support information security education programs. All colleges shall provide new employees and contractors with mandatory information security training as part of job orientation.

The College, through senior management, shall provide regular and relevant information security awareness communications to all staff by various means, which include but are not limited to the following:

- Electronic updates, briefings, pamphlets and newsletters.
- Information security awareness tools 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 signed by employees before they access College resources.

**ISO 27002 REFERENCE**

5.1.2 Review of the information security policy

8.2.2 Information security awareness, education and training

### **110102** Third Party Contractor: Awareness Programs

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

**STANDARD**

All contractors shall have provisions in their contracts with Colleges that set forth the requirement that they must comply with all College information technology security policies. The College shall provide contractors with regular and relevant information technology security policies. The College shall provide regular and relevant information security awareness communications to contractors by various means, which include but are not limited to the following:

- A handbook or summary of information security policies, which shall be formally delivered to and signed by contractors before they begin 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 |

## **110103** Delivering Awareness Programs to Temporary Staff

The standard recommended for this section is covered by Standard 110101

## **110104** Drafting Top Management Security Communications to Staff

**Standard merged into standard 110101**

## **110105** Providing Regular Information Updates to Staff

**Purpose:** To ensure regular and relevant information is passed down to staff from senior management.

**STANDARD**

Colleges shall provide information relevant to effective information security practices to staff members in a timely manner.

On a periodic basis, senior management shall receive input from information security staff on the effectiveness of the organization’s information security measures and recommended improvements.

**ISO 27002 REFERENCE**
5.1.2 Review of the information security policy

## *Section 02 - Training*

### 110201 Information Security Training on New Systems

**Purpose:** To ensure that employees, contractors and temporary employees understand the security implications of new technology.

**STANDARD**

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.

**ISO 27002 REFERENCE**
8.2.2 Information security awareness, education and training

### 110202 Information Security Officer: Training

**Purpose:** To ensure that the College information security officer receives adequate training.

**STANDARD**

The information security officer of each College or his/her equivalent, at a minimum, shall receive annual formalized training on the latest threats to information technology systems and on information security protocols. Senior management shall work with the information security officer on a regular basis to provide the information security officer with knowledge of the College's operational and strategic objectives.

The training for the information security officer must include new technologies to combat threats and updates on new threats to network security and may include updated incident response protocols.

**GUIDELINES**

Training may be enhanced through:

- Membership in technical societies, clubs, boards, or focus groups.
- Subscriptions to technical documents such as newsletters, magazines and white papers.
- Self-study and certifications relevant to information security.

**ISO 27002 REFERENCE**
8.2.2 Information security awareness, education and training

## 110203 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 employee's or contractor'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 but not be limited to the following:

- Mandatory information security awareness training before beginning work.
- Formal information technology security training appropriate for work responsibilities, on an annual basis.
- Training in information security threats and safeguards, with the technical details to reflect the employee's or contractor's individual responsibility for

configuring and maintaining information security.

**ISO 27002 REFERENCE**

8.2.2 Information security awareness, education and training

## 110204 Technical Staff: Information Security Training

**Purpose:** To ensure that College technical staff receive adequate training.

**STANDARD**

Colleges shall make specialized training available for technical staff in critical areas of information technology security, including vendor specifically recommended safeguards to improve:

- 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.

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 REFERENCE**

8.2.2 Information security awareness, education and training

## 110205 Training New Recruits in Information Security

**Purpose:** To ensure that new employees are aware of good information security practices.

**STANDARD**

All Colleges shall provide new employees and contractors with mandatory information security training as part of job orientation.

**ISO 27002 REFERENCE**

8.2.2 Information security awareness, education and training

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 12 – Complying with Legal and Policy Requirements

## *Section 01 - Complying with Legal Obligations*

### 120101 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.

**STANDARD**

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.

Colleges also must ensure that each employee and other College 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.
  - 17 U.S.C.§§ 500 and 506. Copyright infringements and remedies.
- North Carolina
  - N.C.G.S. §114-15.1. Misuse of state property.
  - 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. §14-457. Extortion.

- 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.
  - N.C.G.S. §122C-52. Client rights to confidentiality.

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

## 120102 Complying with State and Federal Records Laws

**Purpose:** To ensure that Colleges comply with laws that address proper handling of data contained in information technology systems.

### STANDARD

Colleges are subject to State laws governing the use of information technology systems and the data contained in those systems. In some situations, Colleges are also subject to federal laws. Colleges shall take affirmative actions to comply with all applicable laws and take measures to protect the information technology systems and the data contained within information systems.

When penetration tests or vulnerability assessments are used, agencies must follow the requirements of G.S. §147-33.111(c).

**ISO 27002 References**
15.1.4 Data protection and privacy of personal information

## 120103 Complying with General Copyright Laws

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

**STANDARD**

Colleges shall provide employees with guidelines for obeying software licensing agreements and shall not permit the installation of unauthorized copies of commercial software on technology devices that connect to the State Network.

The guidelines shall inform employees that:

- Persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.
- Employees shall obey licensing agreements and shall not install unauthorized copies of commercial software on State College technology devices.
- College employees who make, acquire or use unauthorized copies of computer software shall be disciplined as appropriate. Such discipline may include termination.

**ISO 27002 References**
15.1.1 Identification of applicable legislation

## 120104 Complying with Database Copyright Law

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

**STANDARD**

Colleges shall inform their employees of any proprietary rights in databases or similar compilations and the appropriate use of such data. Colleges shall also inform employees of any sanctions that may arise from inappropriate use of the databases or similar compilations.

**ISO 27002 References**
15.1.2 Intellectual property rights (IPR)

## 120105 Complying with Copyright and Software Licensing Requirements

**Purpose:** To ensure that Colleges comply with copyright and licensing requirements.

**STANDARD**

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**
15.1.2 Intellectual property rights (IPR)

## 120106 Legal Safeguards against Computer Misuse

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

### STANDARD

Colleges shall provide users of information technology services with the legal policy requirements that apply to use of College information technology systems and, where practical and appropriate, Colleges shall provide notice to users of College information technology systems that they are using college computer systems.

If Colleges monitor computer users, Colleges also shall provide notice to computer users that their activities on College information technology systems may be monitored and disclosed to third parties.

### GUIDELINES

The notice required by this standard can take many forms. An Internet Web page may have a link to a privacy statement. Monitoring notices can consist of stickers pasted to a computer monitor or an electronic notice that displays when the user logs on to a computer. Where practical and appropriate, sign-on warning banners shall be posted on College computer systems to appear just before or just after login on all systems that are connected to the College Network, giving notice to users that they are accessing College resources and that their actions while they are using these resources may be subject to disclosure to third parties, including law enforcement personnel.

**Examples of warning banners**:

- WARNING: This is a College-Owned 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 College-owned 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 College-owned 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 Colleges. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection and disclosure at the discretion of the College.
- 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

## *Section 02 - Complying with Policies*

### **120201** Managing Media Storage and Record Retention

**Purpose:** To establish standard for records retention and disposition.

**STANDARD**

For the records they create or receive in the course of performing the public’s business, Colleges are required to formulate complete and accurate record retention and disposition schedules that comply with the provisions of N.C.G.S. §§121-5 and 132-1, *et seq.* Colleges must manage their records according to the schedules, as approved by the Department of Cultural Resources, State Records Branch, throughout the records’ life cycle, from creation to disposition.

**ISO 27002 References**
15.1.3 Protection of organizational records

### **120202** Complying with Information Security Standards and Policy

**Purpose:** To establish security standards and policy compliance requirements for employees.

**STANDARD**

Colleges shall establish requirements for mandatory compliance with the applicable statewide and individual College information technology security standards and policies. The requirements shall include regular policy and standard reviews for employees and contractors and periodic reviews of information technology systems to determine whether the systems are in compliance with applicable policies and standards.

**ISO 27002 References**

| | |
|---|---|
| 8.1.3 | Terms and conditions of employment |
| 15.2.1 | Compliance with security policies and standards |

## *Section 03 - Avoiding Litigation*

### **120302** Using Copyrighted Information from the Internet

**Purpose:** To comply with applicable copyright laws.

**STANDARD**

Colleges shall seek legal review before using copyrighted information.

**ISO 27002 References**

| | |
|---|---|
| 15.1.2 | Intellectual property rights (IPR) |

### **120303** Sending Copyrighted Information Electronically

**Purpose:** To comply with applicable copyright laws.

**STANDARD**

Colleges shall seek legal review before sending copyrighted information electronically.

**ISO 27002 References**

| | |
|---|---|
| 15.1.2 | Intellectual property rights (IPR) |

### **120304** Using Text directly from Reports, Books or Documents

**Purpose:** To comply with applicable copyright laws

### STANDARD

Colleges shall seek legal review before using copyrighted information contained in reports, books and documents.

**ISO 27002 References**
15.1.2 Intellectual property rights (IPR)

## 120305 Infringement of Copyright

Colleges shall define policies and procedures to comply with legal and regulatory requirements in regards to the protection of intellectual property.

### GUIDELINES

See Using the Internet for Work Purposes 030312.

**ISO 27002 REFERENCES**
15.1.2 Intellectual property rights (IPR)

## *Section 04 - Other Legal Issues*

## 120401 Recording Evidence of Information Security Incidents

**Standard merged into standard 130101 and 130102**

# Chapter 13 – Detecting and Responding to IS Incidents

## *Section01 - Reporting Information Security Incidents*

### **130101** Reporting Information Security Incidents

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

**STANDARD**

If deemed necessary by the College CIO, information technology security incidents must be reported to the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, and must include the information required on the enterprise Incident Reporting form,[28] incorporated by reference.

Colleges shall record information technology security incidents on the Incident Reporting form,[29] incorporated by reference.

Colleges shall also establish formal procedures for recording and retaining evidence relating to information security incidents to ensure that the evidence is properly preserved for any legal actions that may ensue as a result of the incidents.

The College CIO shall ensure that information technology security incidents occurring within his/her college are reported to the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of incident.

Colleges shall report incidents to the Enterprise Security and Risk Management Office by one of the following methods:

- Contacting ITS Customer Support Center 800-722-3946
- Using the incident reporting website https://incident.its.state.nc.us
- Contacting a member of the Security and Risk Management Services staff directly

**GUIDELINES**

[28] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

[29] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

Computer 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<br>GENERAL ATTACK(S)<br>**SEVERE** | ▪ Successful penetration or denial-of-service attack(s) detected with significant impact on College IT operations:<br>o Very successful, difficult to control or counteract<br>o Large number of systems compromised<br>o Significant loss of confidential data<br>o Loss of mission-critical systems or applications<br>▪ Significant risk of negative financial or public relations impact |
| 4<br>LIMITED ATTACK(S)<br>**HIGHH** | ▪ Penetration or denial-of-service attack(s) detected with limited impact on College IT operations:<br>o Minimally successful, easy to control or counteract<br>o Small number of systems compromised<br>o Little or no loss of confidential data<br>o No loss of mission-critical systems or applications<br>▪ Widespread instances of a new computer virus or worm that cannot be handled by deployed anti-virus software<br>▪ Small risk of negative financial or public relations impact |
| 3<br>SPECIFIC<br>RISK OF<br>ATTACK<br>**ELEVATED** | ▪ Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance<br>▪ Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software<br>▪ Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software |
| 2<br>INCREASED | ▪ Small numbers of system probes, scans, and similar activities detected on internal systemsExternal Penetration or denial of service attack(s) attempted with no impact to College IT operations<br>▪ |

| | |
|---|---|
| RISK OF<br>ATTACK<br>**GUARDED** | ▪ Intelligence received concerning threats to which College IT systems may be vulnerable |
| 1<br>**LOW** | ▪ Small numbers of system probes, scans, and similar activities detected on external systems<br>▪ Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software |

**ISO 27002 References**

| | |
|---|---|
| 10.10.1 | Audit logging |
| 10.10.2 | Monitoring system use |
| 13.1.1 | Reporting information security events |
| 13.2.3 | Collection of evidence |
| 15.1 | Compliance with legal requirements |

## **130102** Reporting IS Incidents to Outside Authorities

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

### STANDARD

The Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, shall determine what, if any, outside authorities need to be contacted in regard to confirmed security incidents in accordance with applicable laws and procedures, any Memorandum of Understanding between ITS, the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor as well as in accordance with federal requirements.

**ISO 27002 References**

| | |
|---|---|
| 13.1.1 | Reporting information security events |

## **130103** Reporting Information Security Breaches

**Purpose:** To ensure that all confirmed information security breaches are reported.

### STANDARD

The College's workforce has the responsibility to report security incidents to

College management in accordance with statewide information security standards and College standards, policies, and procedures. If deemed necessary, College CIO has the responsibility to report security incidents to the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, as required by N.C.G.S. §147-33.113 and in accordance with Standard 130101, Reporting Information Security Incidents, and Standard 130102, Reporting Information Security Incidents to Outside Authorities.

**ISO 27002 References**
13.1.1 Reporting information security events

## 130104 Notifying Information Security Weaknesses

**Purpose:** To reduce information technology security weaknesses.

### STANDARD

All College personnel have the responsibility to report any discovered security weaknesses to their College management in accordance with state and College standards, policies and procedures. The notification should be made as soon as possible after the weakness is discovered.

**ISO 27002 References**
13.1.2 Reporting security weaknesses

## 130105 Witnessing an Information Security Breach

**Purpose:** To protect the College's information technology assets.

### STANDARD

Upon detection, suspected fraudulent activity shall be documented and reported to College management in accordance with State and College standards, policies and procedures for appropriate action as soon as possible.

Individuals who witness a breach in a College's information technology security shall notify their management in accordance with state and College standards, policies and procedures.

**ISO 27002 References**
8.2.2 Information security awareness, education, and training
13.1.1 Reporting information security events

## 130106 Being Alert for Fraudulent Activities

**Standard merged into standard 130105**

## 130107 Software Errors and Weaknesses

**Purpose:** To ensure proper handling of software errors and weaknesses.

### STANDARD

Personnel who discover or perceive that there may be a software error or weakness must be reported immediately to College management. Management shall notify the responsible individual/organization and perform a risk analysis of the perceived threats.

Individuals who are aware of software errors or weaknesses shall not attempt proof-of-concept actions unless otherwise authorized.

**ISO 27002 References**
13.1.2 Reporting security weaknesses

## 130108 Lost or Stolen Computer Equipment

**Purpose:** To ensure proper reporting of lost or stolen state computer equipment.

### STANDARD

Recipients/end users must report loss or stolen state computer equipment (for example, workstations, laptops, mobile communication devices, etc.) immediately to their departmental management. Local college theft reporting policies shall be followed.

**ISO 27002 REFERENCES**
13.1.1 Reporting information security events

## 130109 When and How to Notify Authorities

**Purpose:** To ensure appropriate notification of authorities, regulatory and enforcement agencies about information security incidents.

### STANDARD

If deemed necessary, College CIO shall notify the Enterprise Security and Risk Management Office of information security incidents. The Enterprise Security and

Risk Management Office shall notify authorities, regulatory and law enforcement agencies about information security incidents in accordance with the State's Incident Management Plan, unless the College has already notified the authorities.

If/when college notifies authorities directly, regulatory and/or law enforcement agencies, the College shall also report the incident to the Enterprise Security and Risk Management Office.

**ISO 27002 REFERENCES**
6.1.6 Contact with authorities

## *Section 02 - Investigating Information Security Events*

### **130201** Investigating the Cause and Impact of IS Incidents

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

**STANDARD**

An investigation into an information security incident must identify its cause, if possible, and appraise its impact on systems and data. Colleges shall utilize trained personnel to perform investigations and shall restrict others from attempting to gather evidence on their own.

**ISO 27002 References**
13.2.2 Learning from information security incidents

### **130202** Collecting Evidence of an Information Security Breach

**Purpose:** To protect the College's resources through the proper collection of evidence.

**STANDARD**

Evidence of or relating to an information security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements. 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.

**ISO 27002 References**
13.2.3 Collection of evidence

### **130203** Recording Information Security Breaches

**Purpose:** To protect the College's resources through proper reporting of security breaches.

### STANDARD

If deemed necessary by College CIO, information technology security breaches must be reported to the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, and must include the information required on the enterprise Incident Reporting form,[30] incorporated by reference.

The College head shall ensure that all information technology security breaches occurring within his/her College are reported to the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of a confirmed breach, as required by N.C.G.S. §147-33.113.

**ISO 27002 References**
13.1.1 Reporting information security incidents

## 130204 Responding to Information Security Incidents

**Purpose:** To protect the College's resources through proper response to security incidents.

### STANDARD

If deemed necessary, College CIO shall notify the Enterprise Security and Risk Management Office, acting on behalf of the State Chief Information Officer, shall evaluate the proper response to all information security incidents reported to the College. The Enterprise Security and Risk Management Office shall work with Colleges to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.

**ISO 27002 References**
13.2.1 Responsibilities and procedures

## *Section 03 - Corrective Activity*

## 130301 Establishing Remedies for Information Security Breaches

**Purpose:** To help develop rapid resolutions to information security breaches.

[30] The Incident Reporting form can be found at https://incident.its.state.nc.us/ and can be filled out online.

### STANDARD

All 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.

### GUIDELINES

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

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

**ISO 27002 References**

| | |
|---|---|
| 13.2.2 | Learning from information security incidents |

## *Section 04 - Other Information Security Incident Issues*

## **130401** Ensuring the Integrity of IS Incident Investigations

**Purpose:** To ensure integrity of electronically stored records of information systems incident investigations.

### STANDARD

All Colleges shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals as determined by College management.

**ISO 27002 References**

| | |
|---|---|
| 10.10.2 | Monitoring system use |
| 15.3.1 | Information systems audit controls |
| 15.3.2 | Protection of information systems audit tools |

## **130402** Analyzing IS Incidents Resulting from System Failures

**Purpose:** To properly analyze information security system failures.

## STANDARD

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). Qualified technicians shall perform the investigations, which shall include:

- 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.

**ISO 27002 References**
13.2.1 Responsibilities and procedures

## 130403 Breaching Confidentiality

**Purpose:** To develop a method for identifying and reporting breaches of confidentiality. To monitor the release of confidential information involving information security incidents.

## STANDARD

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.

College staff shall report breaches of confidentiality to College management as soon as possible. Confirmed incidents of confidentiality breaches shall follow the reporting requirements as stated in 130203 Recording Information Security Breaches.

Breaches of confidentiality include, but are not limited to, 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

## 130404 Establishing Dual Control/Segregation of Duties

**Purpose:** To increase the integrity of data while conducting incident investigations.

**STANDARD**

Colleges shall establish controls to protect data integrity and confidentiality during investigations of information security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure that fraudulent activities requiring collusion do not occur.

If any suspicious activities are detected, responsible personnel within the affected College shall be notified to ensure that proper action is taken.

**ISO 27002 References**

| | |
|---|---|
| 10.1.3 | Segregation of duties |
| 13.2.1 | Responsibilities and procedures |

## **130405** Using Information Security Incident Reporting Form

**Standard removed: addressed in 130101**

## **130407** Monitoring Confidentiality of Information Security Incidents

**Standard merged into standard 130403**

## **130408** Risks in System Usage

**Standard merged with standard 030104**

## **130409** Reviewing System Usage

**This standard merged into standard 030104**

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 14 – Planning for Business Continuity

**Scope:** These standards apply to all Colleges, their agents or designees subject to Article 3D of Chapter 147, “State Information Technology Services.”

**Statutory Authority:** N.C.G.S. 147-33.89

## *Section 01 Business Continuity Management*

### 140101 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**

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 to the College’s citizens.

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. 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 REFERENCE**

14.1.04 Business continuity planning framework

### 140102 Assessing the BCP Risk

**Purpose:** To require that State Colleges manage information technology risks appropriately.

**STANDARD**

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.

Colleges shall conduct risk impact analysis activities that:

- 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 resulting from the inoperability of each critical function or service.
- Estimate tangible (nonfinancial) 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.
- 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.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 14.1.02 | Business continuity and risk assessment |
| 14.1.04 | Business continuity planning framework |

## **140103** 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**

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.

At a minimum, a College's business continuity plan shall:

- Help protect the health and safety of the employees of the College
- Protect the assets of the College and minimize financial, legal and/or regulatory exposure.
- Minimize the impact and reduce the likelihood of business disruptions.
    - Crisis teams and response plans for threats and incidents.
    - Communication tools and processes.
- Require that employees are aware of their roles and responsibilities in the BCP and in plan execution.
    - Training and awareness programs.
    - 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.
- Have senior management oversight and sign-off.
- 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.

**ISO 27002 REFERENCES**

| | |
|---|---|
| 14.1.03 | Developing and implementing continuity plans including information security |
| 14.1.04 | Business continuity planning framework |

## **140104** Testing the BCP

**Purpose:** To ensure that management and staff understand how the business continuity plan is executed.

**STANDARD**

The College business continuity plan shall be tested at least annually.

**GUIDANCE**

The following methods are recommended:

- Table top 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 rerunning of the test to validate any updated procedure(s) and the addition or removal of application backup procedures. The decision on what type of testing methodology to use should be defined, documented and approved by College management. The College is responsible for maintaining its ability to recover in the event of an outage.

**ISO 27002 REFERENCES**

14.1.04 Business continuity planning framework

14.1.05 Testing, maintaining and re-assessing business continuity plans

## 140105 Training and Staff Awareness on BCP

**Purpose:** To help employees understand the components of the business continuity plan and their roles in disaster planning and response.

**STANDARD**

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/adverse situation.

**ISO 27002 REFERENCES**

14.1.04 Business continuity planning framework

14.1.05 Testing, maintaining and re-assessing business continuity plans

## 140106 Maintaining and Updating the BCP

**Purpose:** To maintain an up-to-date business continuity plan that reflects actual business requirements.

**STANDARD**

The person(s) designated as the College business continuity plan (BCP) coordinator(s) has (have) the responsibility of overseeing the individual plans and files that constitute the BCP and ensuring that they are current, meet best practices and are consistent with the College's overall plan. College's BCP shall be reviewed periodically by the College CIO and recommendations shall be made for improvement, if necessary.

**ISO 27002 REFERENCE**

14.1.05 Testing, maintaining and re-assessing business continuity plans

## 140107 Disaster Recovery Plan

**Purpose:** To maintain business continuity throughout the College.

### STANDARD

College management and information custodians must ensure that business continuity and disaster recovery plans are developed, maintained, tested on a prescribed basis and subjected to a continual update and improvement process.

**ISO 27002 References**

14.1.3 Developing and implementing continuity plans including information security

Statewide Information Technology Standards

Office of the Governor
State Chief Information Officer

# Chapter 15 – Information Technology Risk Management

## *Section 01 Information Technology Risk Management Program*

### **150101** 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 the 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**

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. The risk management program must identify and classify risks and implement risk mitigation as appropriate. 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.

In general, "risk" is defined as the potential exposure of an activity to damage. 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.

**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:**  Collecting and reporting status information about risks and their mitigation plans, responding to changes in risks over time, and management ensuring corrective measures are taken in accordance with 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:

- 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 |