Neosho County Community College
Written Information Security Program

August, 2023

Dean for Operations/CIO, Phil Chaney

Revision History

- **July 2017 – Initial Revision**
- **February 2018 – Substantial revisions to sections 1, 3, 5, & 10. Grammatical corrections throughout.**
- **April 2018 – Revision 2 published.**
- **August 2023 – Minor updates to contact information in section 8. Link updates in section 10.**

Table of Contents

Contents

1. Management Directive

The Chief Information Office (CIO) is responsible for establishing, issuing, and monitoring the compliance of data security policies.

This Written Information Security Program (WISP) contains operational policies and standards intended to safeguard the security, integrity/trust, and compliance of Neosho County Community College (NCCC) data and information systems. It establishes the minimum requirements for the secure delivery of organization services through:

- Management and business processes that include and enable data security processes.
- Governance processes for data security.
- Reporting of data security incidents.
- Including data security in business continuity planning.
- Monitoring for compliance.

The CIO recognizes that data security is a process. To be effective, it requires management commitment and continuing security awareness efforts. Other principles that guide NCCC's directions are:

- Data security requires a multi-layered defense strategy.
- Data security is everyone's responsibility.

1.1 Purpose

In accordance with federal and state laws and regulations, NCCC is required to take measures to safeguard personally identifiable information, including financial information, and to provide notice about security breaches of protected information at the college to affected individuals and appropriate state agencies.

The WISP is intended to help safeguard the security, integrity/trust, and compliance of the NCCC's data assets and to comply with our obligations under the financial customer information security provisions of the federal Gramm-Leach-Bliley Act (GLBA) [15 USC 6801(b) and 6805(b)(2)] and the General Data Protection Regulation (GDPR).

It forms part of NCCC's Data Security Program whose objectives are to:

- Establish a coordinated, enterprise approach to data security.
- Establish employee responsibilities in safeguarding data according to its classification level.
- Establish administrative, technical, and physical safeguard data to ensure the security of sensitive data.
- Implement modern, fit-for-use security and data protection technologies.
- Implement effective systems for handling security breaches and data loss.
- Ensure that data under the care of organization is safeguarded appropriately.
- Reduce NCCC's risk profile.

1.2 Review

The WISP must be reviewed at least once per year and updated when required.

The CIO must, at least annually, review the information security policies, standards, and guidelines in an effort to ensure their continuing adequacy and effectiveness. Reviews must consider:

- Feedback from stakeholders.
- Legislative, regulatory, or policy changes that impact data security and/or data management.
- The planning and implementation of new or significantly changed technology.
- Major initiatives (e.g. new information systems or contracting arrangements).
- Audit reports or reviews of security controls that identify high risk vulnerabilities.
- Threat or vulnerability trends produced from automated monitoring processes that indicate an increased risk to information assets.
- Reports from security incident investigations.
- The introduction or revision of national, international, or industry standards for data security that address emerging technology issues.
- Reports from associated external agencies (e.g. SANS, CIS, etc..) that identify emerging trends related to data security.

2. Scope

This policy applies to all NCCC employees, whether full or part time, paid or unpaid, temporary or permanent. This policy applies to all data collected, stored, or used by, or on behalf of, any operational unit or department. In the event that any particular information at NCCC is governed by more specific requirements under other policies or procedures, the more specific requirements shall take precedence over this policy to the extent there is any conflict.

3. Definitions

3.1 People

1. **Clients.** All people receiving services from NCCC.
2. **External Parties.** Any respective NCCC business partner entity or other non-organizational entity.
3. **User.** Any staff or individual who has been authorized for access to and use of a system.
4. **External User.** A user of a system who is not NCCC Staff.
5. **Data Owners.** A user who is responsible for a data selection, typically a manager and/or administrator.

3.2 Systems

1. **System.** Any of NCCC’s respective information systems, including shared electronic information system.
2. **Firewall.** A system that controls network access between two or more networks or networked devices.
3. **Vulnerability.** Weakness of any system that can be exploited by one or more threats.
4. **Remote access.** Accessing a system from outside NCCC’s main facility or remote sites.
5. **Media.** Any device, including network infrastructure, information resources, and systems that store the organization’s personal and confidential data.
6. **Malicious code.** Software used to exploit, infiltrate, or damage a system without informed consent. Also known as malware, and includes viruses, worms, spyware, Trojan horses, and other unwanted software.

3.3 Controls

1. **Administrative Controls** - Administrative controls include, but are not limited to institutional policies, classification of confidential information, security awareness training and communications, internal and external audit, and processes and procedures for granting and revoking access to physical and electronic forms of information. Access to institutional information is based on the least privilege concept, where access to information is granted to persons at the minimum level necessary to complete their job duties and scope of employment. Security practices are reviewed, modified and/or added based on academic, research, business needs, regulation, and evaluation of the threat landscape conducted by the Technology Services Department in conjunction with other business units within the college.
2. **Technical Controls** - Technical controls include but are not limited to perimeter firewalls, intrusion prevention systems, interior firewalls, encryption, authentication and authorization systems, system logging, file backup, virtual private network connectivity, and network monitoring solutions.
3. **Physical Controls** - Physical controls include but are not limited to electronic and physical card/key access control systems, locking mechanisms for areas and devices containing sensitive information and information-processing assets, creation of backup media, offsite storage of media, intrusion detection systems with central monitoring, closed circuit television monitoring and recording systems, fire detection, reporting and suppression systems, and water leak detection systems.

3.4 Other Definitions

1. **Information Security Event.** An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
2. **Information Security Incident.** A single or a series of unwanted or unexpected Information Security Events that have a significant probability of compromising business operations and threatening information security.

4. Data Classification

Objective: To ensure that organization data receives an appropriate level of protection in accordance with it sensitivity and value.

4.1 Inventory of Data Source Locations

Objective: To identify organization information assets and define appropriate protection responsibilities.

An inventory of all important assets associated with information systems must be documented and maintained.

Data Owners must identify and document assets under their control including:

- Software (e.g. applications, system software, development tools and utilities).
- Hardware (e.g. computer and communications equipment, removable media, etc..).
- Services (e.g. computer and communications services, general utilities).
- Information assets and their security classification.

- Data assets include databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails and archived information.

The inventory must not duplicate other inventories unnecessarily but reference them where appropriate.

The following information must be recorded to facilitate system planning and asset recovery in the case of interruption, corruption, loss, or destruction:

- Type of asset
- Ownership
- Format
- Location
- Assigned user (where applicable)
- Backup information
- License information
- Security requirements (confidentiality, integrity, and availability)
- Consequence of loss

The loss, theft, or misappropriation of assets must be reported immediately to the CIO. When information is lost, stolen, or misappropriated the procedures outlined in Section 8, "Data Security Incident Management," must be followed.

4.2 Data Classification

Information must be classified in accordance with its value, sensitivity, and intended use.

The Chief Information Officer is responsible for developing an information classification system. The system must take into account the confidentiality, integrity, and availability requirements and the financial value of information assets.

NCCC's data classification levels are:

1. **Public/Unclassified Data.** Information that is generally available to anyone within or outside of the institution. Access to this data is unrestricted, may already be available, and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, financial statements [and other data as applicable].

2. **Confidential Data.** Personal or institutional information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc..]. Confidential data includes, but is not limited to, social security numbers, credit card numbers, passwords, tax forms, accounting data, security procedures [and other data as applicable]. NCCC considers it a top priority to protect the privacy of our clients and employees.

3. **Sensitive/Restricted Data.** Sensitive data which, if leaked, would be harmful to NCCC, its employees, contractors, customers, [and other parties as applicable]. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes, but is not limited to personnel issues/disciplinary actions, audit reports, legal documentation, business strategy details, identification

numbers [and other data as applicable].

5. Data Security Policy Statements

5.1 Compliance with Security Policies and Standards

The CIO must ensure security procedures are followed in each area and facilitate regular reviews to ensure compliance with security policies and standards.

Data Owners must ensure security policies and processes are implemented and adhered to by:

- Conducting periodic self-assessments.
- Initiating independent assessments, reviews or audits.
- Ensuring personnel receive regular data security awareness updates.

Any NCCC employees, contractors, volunteers, or authorized user discovered to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Unauthorized disclosure of regulated data, such as personally identifiable information, may lead to legal repercussions.

5.2 Data Asset Management

5.2.1 Return of Assets

Personnel must return all organizational assets upon termination or change of employment as defined in the NCCC Employee Non-Disclosure Agreement. Managers must ensure the recovery of:

- Documents, files, data, books, and manuals in electronic and hard copy formats.
- Information assets developed or prepared by an employee or contractor in the course of his/her duties.
- Computer hardware, software, and related equipment.
- Mobile devices and portable media.
- Access cards, keys, key fobs, ID cards, and other organization-issued devices.

The user must copy all **personal** electronic files to removable media and delete the originals from organization systems.

Unreturned access devices must be documented and steps taken to ensure they cannot be used for unauthorized access to organization building, information systems, and/or data.

5.2.2 Regulation of cryptographic controls (Encryption)

Cryptographic controls must be used in conjunction with relevant agreements, laws, and regulations.

Data Owners must:

- Ensure the use of cryptographic controls when transmitting or storing any confidential data as defined in section 4.2.
- Consult with Technology Services regarding records management, electronic commerce, information access, privacy, and security issues prior to acquiring cryptographic controls.
- Ensure encrypted organization data assets do not become unavailable due to unavailability or loss of cryptographic keys by implementing a process to manage cryptographic keys as defined by CIO.
- If acquiring cryptographic controls from outside the United States the procurement must be from a reputable vendor who can provide reasonable assurance on the legality of import into the United

States.

5.2.3 Disclosure of Personal Information

NCCC will supply personal information to:

- Those who are entitled to the information.
- Any authority we are required to do so by law.
- Anyone to whom we are required to disclose it.

5.3 Data Asset Handling

Data must be appropriately handled in accordance with its assigned level of sensitivity.

Data Owners must develop and implement procedures for handling, processing, storing and communicating information. Those procedures must consider:

- The level of sensitivity of the information.
    - **Public/Unclassified Data –** Data does not require any special procedures.
    - **Confidential Data –** Data is required to be securely transmitted, handled, communicated, and stored. Data Owners must consult the Technology Services Department any time there is a need to transmit or store Confidential Data to determine the best method of securing and transmission.
    - **Sensitive/Restricted Data –** Data access should be limited to only those that require access and should not be widely shared but does not have to be securely transmitted, handled, communicated, or stored.
- Access restrictions supporting the safeguards for each level of sensitivity.
- Maintenance of a formal record of the authorized recipients of assets.
- Safeguarding temporary or permanent copies to a level consistent with the original.
- Storage of information technology assets in accordance with the manufacturers' specifications.
- Clear marking of all copies of media for the attention of the authorized recipient.

5.3.1 Disposal of Data

Media must be disposed of securely using formal procedures that consider the sensitivity of the data stored.

Data Owners must ensure that media that is no longer required operationally is disposed of securely.

5.3.2 Physical Transfer of Data

When transporting physical media with sensitive information between sites:

- Use a trusted courier.
- Inspect the identification of couriers at pickup and delivery.
- Obtain and retain receipts.
- Pack the media in a manner that will prevent loss or damage.
- Pack the media in a manner that does not disclose the level of sensitivity.

- Pack it in a manner to make evident any attempted tampering.

When supported by a Threat and Risk Assessment or if enhanced security is required for other reasons:

- Use a courier service that has a tracking number.
- Hand deliver the media where necessary.
- Use a double envelope (or double package) where the inner layer is marked with the level of sensitivity and instructions and it is packaged in another envelope.
- Use a lockable container.
- Encrypt the information stored on the media.

5.3.3 Management of Removable Media

All removable computer media must be managed and appropriate controls applied considering the sensitivity of the data they store.

Data Owners must:

- Ensure that confidential data on removable media is encrypted with approved methods.
- Authorize the use of removable media during travel.
- Ensure users are familiar with the operation of removable media.
- Ensure users are familiar with the policies on security incident reporting as described in Section 8.2.
- Ensure all users who are authorized to use removable media are aware of the need to safeguard organization information in accordance with this policy.

Users of removable media must:

- Have authorization to use removable media and store confidential information on it.
- Ensure that removable media in his or her care is only accessed by those authorized to do so.
- Ensure that, where applicable, the media is password-protected and the password applied.
- Ensure that removable media is transported securely and not left unattended.
- Ensure that confidential information stored on removable media is encrypted by approved methods.
- Ensure that data on removable media are not the only copies that exist, i.e. originals are on network shares.
- Ensure that any removable media received from an external party is scanned for malware prior to use.
- Ensure that removable media is not used for the storage of confidential information when encryption is not available, e.g. storage card on a digital camera.
- Ensure that confidential information is not accessed while in a public place (e.g. coffee shop, airport, park, etc..).
- Immediately report the loss or theft removable media to the user’s supervisor and/or the data owner.

5.3.4 Data Backup

Objective: To protect against loss of data.

Backup copies of information, software, and system images must be made, secured, and be available for recovery.

Technology Services must work with Data Owners to define and document backup and recovery processes that consider the confidentiality, integrity, and availability requirements of data and data systems.

Backup and recovery processes must comply with:

- Business continuity plans (if applicable).
- Policy, legislative, regulatory, and other obligations.

The documentation for backup and recovery must include:

- Types of information to be backed up.
- Schedules for the backup of information and information systems.
- Backup media management.
- Methods for performing, validating, and labeling backups.
- Methods for validating the recovery of data and data systems.

5.3.5 Remote working

Appropriate security controls must be implemented to mitigate risks associated with working remotely.

Before granting permission to enter into a telework arrangement, the following must be considered:

- The sensitivity of information accessed or stored at the location.
- The physical security at the remote location.
- Likelihood of unauthorized access at the remote location.
- The security of home wired and wireless networks.
- Remote access threats.
- Remote (VPN) access must be requested/approved by the user’s immediate supervisor before access will be granted.
- Technology Services may disable VPN access at any time.

Mandatory controls are:

- Confidential organization data in electronic format cannot be stored at a remote site unless it is encrypted with approved methods.
- Confidential organization data in hard copy format cannot be stored at a remote site unless it is in a locked cabinet.
- Only organization-issued computers can be used for the processing of organization data.
- Only approved remote access methods can be used to access NCCC network.
- Remote access to NCCC’s networks and systems should be through a secure medium such as a VPN. The operating system(s) for all remote systems must be kept up to date to ensure the latest security patches have been applied.

5.3.5.1 Vendor/Consultant Remote working

Vendors/consultants that require NCCC systems on a temporary basis will have their accounts enabled upon request. Once work is complete their accounts should be immediately disabled.

Vendors/consultants that are contracted with NCCC to provide services/etc. on an ongoing basis will be allowed to have their account(s) enabled until they are no longer contracted with NCCC or their services are no longer needed.

Active vendor accounts will be reviewed at least annually by the CIO to determine if access is still required.

5.3.6 Computer Security Requirements

Appropriate security controls must be implemented to ensure the safety and integrity of NCCC data. Any user of NCCC systems must take the following steps to ensure that all data is properly secured:

- Password protect your NCCC devices
- Keep your password secret
- Lock your computer when you leave your desk
- Do not access confidential NCCC information from personal devices unless approved in writing by the CIO.
- When Encrypting files with Microsoft Office they should be saved as Office 2007 or later versions (I.E. .XLSX, .DOCX, etc...)

5.3.7 Physical Data Security Requirements

In addition to digital security controls, physical security controls must be followed as well to mitigate the risk of unauthorized access.

- Do not allow someone into an unauthorized area unless you have been authorized to do so
- If you have lost a key or key card report it to Vice President for Operations or his designee immediately as referenced in section 8.2.
- If a person in uniform such as a delivery man or electrician asks you to let them in, contact maintenance or housekeeping so they can confirm validity and let them in.
- If you see a suspicious person or activity in the workplace, report it immediately as reference in section 8.2.

5.3.8 Password Requirements

Passwords are an essential aspect of computer security, providing important front-line protection for electronic resources by preventing unauthorized access. Passwords help the College limit unauthorized or inappropriate access to various network resources including user-level accounts, web accounts, email accounts, screen saver protection, and local network hardware.

A poorly chosen password may result in the compromise of College systems, data, or the network. All NCCC students, faculty, and staff are responsible for taking the appropriate steps, as outlined below, to select appropriate passwords and protect them. Contractors and vendors with access to College systems also are expected to observe these requirements.

A department and/or system administrator may implement a more restrictive policy on local systems where deemed appropriate or necessary for the security of electronic information resources. The CIO can require a more restrictive policy in protection of confidential information or data.

Creation of Passwords

Passwords created by users of College systems, and on systems where technology makes it possible, should conform to the following guidelines:

- Should be different from the user’s login name or the reverse of the name and must avoid use of identifiable personal information (names of family, etc.).
- Must be at least eight characters.
- Must include digits (0-9), and both upper and lower case characters (a-z, A-Z).
- Should use a special character (Examples: *, &, %, or $).

These provisions will be enforced electronically whenever possible.

Protecting a Password

- Passwords should be treated as confidential College information.
- Passwords should never be written down or posted for reference.
- Passwords should not be included in email messages or other forms of unsecured electronic communication.

Sharing a Password

- Sharing or allowing another person to use an individual account password is a violation of this policy unless the person is an information technology professional assisting you with a technical problem.
- Departmental account passwords should be shared only with appropriately designated departmental personnel.
- Passwords may be shared via phone when necessary. However, users need to beware of “phishing” or other social engineering scams where a user may have his or her password requested over the phone. Technology Services personnel, as a best practice, do not normally request a user’s password over the phone. Password phone communications may be necessary with external information technology vendors.
- Approval by the College's CIO is required prior to sharing a password with a vendor (approval may be granted on a one-time or continuing basis), and this vendor access may require implementing the appropriate technology infrastructure to accommodate the access (depending on the circumstance, and as determined by CIO).
- It is recommended that passwords be changed after allowing use as permitted in this section.

Reporting a Password Compromise

- Suspected compromises of passwords must be reported immediately to the NCCC help desk.
- The password in question should be changed immediately.

Responsibilities of the Chief Information Officer

- The CIO may require a more restrictive policy, such as stronger passwords, in some circumstances.
- The CIO or its delegates may perform password assessments on a periodic or random basis. If a password is guessed or cracked during one of these assessments, the CIO will promptly notify the listed contact and require the password be changed.

6. Audit Considerations

Objective: To minimize the impact of audit activities on operational systems.

Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.

Prior to commencing compliance checking activities such as audits or security reviews of operational systems the CIO must document and approve the activities. Among the items upon which they must agree are:

- The audit requirements and scope of the checks.
- Audit personnel must be independent of the activities being audited.
- The checks must be limited to read-only access to software and data, except for isolated copies of system files, which must be erased or given appropriate protection if required when the audit is complete.
- The resources performing the checks must be explicitly identified.
- Existing security metrics will be used where possible.
- All access must be monitored and logged and all procedures, requirements and responsibilities must be documented.
- Audit tests that could affect system availability must be run outside business hours.
- Appropriate personnel must be notified in advance in order to be able to respond to any incidents resulting from the audit.

7. Training and Awareness

Objective: To properly train and give awareness to end users of potential dangers and mitigate end user risk.

All college employees will be required to go through Data Security Training as directed by the CIO, at least annually. Employees who have not successfully completed the training program may have their access from NCCC systems removed at the discretion of the CIO. Supervisor(s) of the user will be notified if this occurs.

Additional compliance and/or departmental specific training may be required at the discretion of the CIO. Additional departmental specific training is also available upon request to the CIO.

8. Data Security Incident Management

8.1 Responsibilities and procedures

Objective:

To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

Incident management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents.

The CIO is responsible for the following procedures:

- Incident response planning and preparation.
- Monitoring, detecting, analyzing, and reporting of information security events and incidents.

- Logging incident management activities.
- Handling of forensic evidence.
- Assessment of and decision on information security events and assessment of information security weaknesses.
- Response and recovery from an incident.

8.2 Reporting information security events

Information security events must be reported through appropriate management channels immediately.

All users of NCCC information systems must report information security events immediately to the CIO or their designee. Examples of events include, but are not limited to:

- Ineffective security control.
- Breach of information confidentiality, integrity, or availability expectations.
- Human errors.
- Non-compliance with policies or guidelines.
- Breaches of physical security.
- Uncontrolled system changes.
- Malfunctions of software or hardware.
- Access violations.
- Malicious software.
- Lost or stolen information assets.

If you believe someone has accessed your NCCC account and/or device without your permission or you have been phished, immediately reset your password and contact Technology Services.

- Phone – 620.432.0498

If you believe your computer may be infected with malware/etc.:

-Shutdown your PC and contact the helpdesk at:

- Email: helpdesk@neosho.edu
- Phone: 620.432.0498

If you believe a hacker has targeted you or your organization:

- Email: helpdesk@neosho.edu
- Phone: 620.432.0498

If your device(s) and/or keys/key cards have been lost or stolen, immediately report it to the Vice President for Operations or their designee:

- During normal business hours – 620.432.0301 or 620.212.3750
- Outside normal business hours – 620.432.0498

If you see any suspicious person(s) or activity:

- Report it to Vice President for Operations (Chanute) or Dean for the Ottawa and Online Campuses (Ottawa) per the Emergency Action Plan.
- Vice President for Operations – 620.212.3750

- Dean for the Ottawa and Online Campuses – 816.810.9889

If you have any general questions:

- Email: helpdesk@neosho.edu
- Phone: 620.432.0385

8.3 Reporting information security weaknesses

Personnel using information systems must note and report any observed or suspected security weaknesses in those systems.

All users of organizational information systems must report security weaknesses to the Technology Services Helpdesk. The helpdesk may be reached during normal business hours via one of the following means:

-Email: helpdesk@neosho.edu

-Phone: 620.432.0498

No user may attempt to exploit any security weakness.

8.4 Assessment of and decision on information security events

Information security events must be assessed to determine if they are to be classified as information security incidents.

Technology Services must assess each information security event. Based on the incident classification scale it must be decided if the event must be classified as an information security incident.

Results of the assessment and decision must be recorded in detail for future reference and verification.

8.5 Response to information security incidents

Information security incidents must be responded to by the Technology Services department in accordance with documented procedures.

The response must include:

- Collecting evidence as soon as possible after the occurrence.
- Conducting information security forensics analysis, if required.
- Escalation, if required.
- Ensuring that all response activities are properly logged for later analysis;
- Communicating the existence of the incident and any relevant details to internal and external people and organizations with a “need-to-know.”
- Dealing with information security weaknesses found to have caused or contributed to the incident.
- Once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis must take place, as necessary, to identify the source of the incident.

8.6 Learning from information security incidents

Knowledge gained from analyzing and resolving information security incidents must be used to reduce the likelihood or impact of future incidents.

Technology Services is responsible for monitoring and evaluating information security incidents by:

- Using statistical analysis of incident frequency, type and location to identify trends.
- Ensuring incident reports and trends are used to promote continuous improvement of security policies and processes, security awareness and training programs, and Business Continuity and Disaster Recovery Plans.
- Advising Information owners and staff of evolving security threats and mitigation strategies.
- Evaluating the effectiveness of incident management, response and reporting.
- Evaluating the effectiveness of information security technologies.

9. Non-Compliance

When review processes indicate non-compliance with policies Data Owners must:

- Determine cause(s).
- Assess the threats and risks on non-compliant processes.
- Document the marginal risks.
- Determine and implement corrective action.

9.1 Misuse of Employee and Audit Data

Violations of this policy will be handled according to NCCC Board of Trustees policies. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable NCCC policies.
2. Termination of employment.
3. Legal action according to applicable laws and contractual agreements.

10.0 Policies Cross Referenced

The following Policies provide additional guidance as it relates to this program:

- Copyright Policy
- Email Policy
- Fair Use Policy for Electronic Information Resources
- FERPA Policy
- GLBA Policy
- HIPAA Policy
- Identity Theft Prevention Policy (Red Flag Rules)
- Higher Education Opportunity Act Compliance
- Network Policy
- Social Media Policy
- Wireless Access Policy
- Wireless Network Policy