Information Security and Technology (ISaT) Policy Handbook

IS&T Policy Overview & Key Takeaways

The following policies have been developed to ensure the highest level of security, privacy, and compliance regarding all items within the scope of CNI College's Information (IT) Department.

Implementing campus-wide ISaT policies helps prevent redundancy and provides a benchmark for information security and technology compliance efforts against any law or regulatory requirements.

The policies and requirements are essential in ensuring that CNI College's compliance efforts are moving in the right direction in compliance with current data privacy and information security regulations. The ability to meet information security and compliance requirements is an ongoing activity. Continual refinement, updating, and monitoring will occur as regulations change and update.

Policy & Compliance Layout

Each policy will have a statement, scope, and policy attached to it to provide clarity, information, and requirements for the policy.

Update Frequency

Polices will be updated annually or as needed to ensure that all compliance measures are taken and to stay updated with security changes, laws, and regulations. CNI College reserves the right to modify and revise these policies to ensure all compliance needs are met and exceeded.

Laws & Regulations

Below are the current laws and regulations used to develop CNI College's policy framework.

- Accrediting Bureau of Health Education Schools **(ABHES)**
- California **(CA)** State Law
- Commission on Collegiate Nursing Education **(CCNE)**
- Federal Trade Commission **(FTC)**
- Family Educational Rights and Privacy Act **(FERPA)**
- Gramm-Leach-Bliley Act **(GLBA)**
- Health Insurance Portability and Accountability Act **(HIPAA)**
- National Institute of Standards and Technology **(NIST)**
- Payment Card Industry Data Security Standard **(PCI DSS)**
- United States Department of Education **(USDE)**
- Western Association of Schools and Colleges **(WASC)**

Table of Contents

Information Security and Technology (ISaT) Policies

Information & Data Security Policy

Statement & Purpose

CNI College develops and maintains its information and data security policy, which establishes the College's commitment to information security and sets its approach to managing it throughout the college.

CNI College is committed to safeguarding critical information under all state and national laws and regulations. It is important to be aware that individuals' roles and responsibilities are crucial in securing the confidentiality, integrity, and availability of information assets, both analog and digital.

Scope

This policy applies to all CNI College employees and is used to review third-party vendors' information and data security policies. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of CNI College's information assets and protects the interests of CNI College, its students, faculty, and staff.

Policy

CNI College's Information and Data Security Policy defines the role of information security throughout the college while fostering an environment to protect the college

community from all internal, external, deliberate, or accidental information security threats that may impact the confidentiality, availability, privacy, and integrity of all information assets.

The Information Security Policy is as follows:

- Establishment of acceptable uses of computing resources at CNI College – see *Acceptable Use Policy*.
- For the protection of information against unauthorized access, see the *Access Control Policy*.
- Managing risks from user authentication and access to CNI College's information assets – see *Identification and Authentication Policy*.
- Availability of information for business processes are maintained & contingency plans in place – see *Business Continuity Policy*.
- Implementation of a secure use of electronic messaging – see *Email Policy*.
- Protection of internal and external exchange of information – see *Network Security Policy*.
- Legislative and regulatory requirements are met – see *Compliance Management Policy*.
- Appropriate training and controls for individuals accessing CNI College's information – see *Personnel Security Policy*.
- Appropriate procedures for acquiring, registering, and installing Applications/Software within CNI College's systems – see *Application Security Policy*.
- Protection of CNI College's information assets during remote working/access (if applicable) arrangements with employees and/or third-party vendors—see *Remote Access Policy*.

- Security controls for mobile devices used within and throughout CNI College – see *Mobile Device Policy*.
- Establish a set of rules to enhance security best practices for passwords – see *Password Policy*.
- Confidentiality of information is assured, and integrity of information is maintained – see *Cryptography Policy*.
- A formal change control process – see *Change Management Policy*.
- Mitigating and managing risks associated with Third Party vendors – see *Third Party Services Policy*.
- Implementation of physical and environmental security controls to secure CNI College's sensitive information – see *Physical and Environmental Security Policy*.
- Risk assessment and management to identify threats and vulnerabilities and mitigate the impact – see *IT Risk Assessment and Management Policy*.
- All actual and suspected information security breaches are reported and properly investigated – see *Information and Cyber-Security Incident Response Policy*.
- Protection of all CNI College assets according to their value and sensitivity – see *Asset Management Policy*.
- Information security training, awareness, and education are available to all employees – see *Security Awareness & Training Policy*.
- Identify sensitive information and monitor and place security measures for CNI College's assets – see *Information Classification Policy*.
- Establishment of mandatory requirements for the installation, configuration, and implementation of information technology systems throughout CNI College – see *Configuration Management Policy*.

- Monitoring and logging of all system events to protect information assets from suspicious incidents – see *Audit Logging & Reporting Policy*.
- Retention and disposal plan of CNI College's information assets – see *Record Retention and Data Disposal Policy*.
- End-user computing protection – see *End User Computing Policy*.
- Rules for network protection and maintenance of CNI College's IT infrastructure – see *Network Security Policy*.
- Safeguarding CNI College's vulnerabilities with monthly vulnerability scans, biannual penetration tests, continuous patches and system updates – see *Vulnerability and Patch Management Policy*.

Roles & Responsibilities

The Roles and Responsibilities are as follows:

- The college community, including employees, contractors, vendors, and guests, is expected to comply with all federal, state, and local laws pertaining to the protection of confidential information and college policies meant to protect the security of information systems.
- All college employees who work with sensitive students' personal and financial information cannot have their non-work mobile devices at their desks.
- The responsibility of every user includes being aware of and practicing safe computing habits.
- Information resources for authorized purposes are being used under the *Acceptable Use Policy*.
- Situations that could cause a potential security incident are reported to the IT Department.

- Pay attention to unexplained system behavior and unsolicited requests for information.
- Watch for inappropriate conduct from all employees and visitors.
- All 3rd party vendors and contractors are subject to review per this policy.
- The CNI College community is expected to comply with the specified information security procedures.

Information Classification Policy

Statement & Purpose

CNI College provides with this policy a classification system for all data, assets, and documentation within the college. This is done to ensure proper assignment for each security class. CNI College houses various information assets (both analog and digital) that must be protected against unauthorized access, disclosure, modification, and any other use deemed inappropriate. The management of these assets is necessary to maintain compliance with any legal obligations, such as those established by the United States Department of Education (USDE), Gramm-Leach-Bliley (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), and the Federal Trade Commission (FTC).

Appropriate classification is essential for adequate data security and management for all types of information assets, as they require different measures of security. The security classes are listed below and have defined data management controls that assist in determining how information assets should be processed throughout their lifecycle; the controls apply to all information assets within CNI College.

Scope

This policy applies to all information assets (analog and digital) produced and maintained by CNI College, its employees, and 3rd party vendors that also host any of the college's sensitive information. This includes but is not limited to, data and documents related to students, staff, faculty, teaching, research, and administration.

Adherence to this policy helps safeguard the confidentiality, integrity, and availability of CNI College's information assets and protects the interests of the college, its students, faculty, and staff. The policy covers all storage, access, sharing, and resilience of information assets, both analog and digital.

Policy

Data classification establishes a well-managed and maintained risk tolerance through data categorization. This highlights the required safeguards for information confidentiality, integrity, and availability. The measures to ensure protection are based on qualified information value and risk acceptance.

The following classification of data considers the reputational, financial, operational, strategic, and compliance impact on CNI College and is based on the level of sensitivity, value, and impact incurred when the data is altered, disclosed, and/or destroyed.

CNI College data is classified into the following three categories:

- **Category I**: Restricted Protected Data
- **Category II**: Private Protected Data
- **Category III**: Non-Public and Public Data

Category I - Restricted Protected Data

Risk = **High**

Description:

Personally identifiable data is any information whose unauthorized access or loss could seriously or adversely impact CNI College, contracted vendors,

any specified personnel, or the public to any extent. Any breach of this information may be subject to notification laws as required.

Regulated data is all information subject to federal, state, or business regulations such as FERPA, the USDE, GLBA, PCI DSS, or FTC, which require levels of protection to prevent any unauthorized access or use of this information and data.

Examples:

Statutory Data is information that includes but is not limited to:

- Social security numbers
- Driver's license numbers
- DMV state-issued ID numbers
- passport numbers
- bank/financial account numbers.
- credit/debit card numbers.
- Electronic health information **(HIPAA)**
- **FERPA** protected data and information.
- Electronic credentials (e.g., passwords, PINs, etc.)
- Any law enforcement active investigation information such as background checks.

Declared Data is information that includes but is not limited to:

- System administration/network ID authentication credentials
- Attorney-client privilege information

As mentioned above, this list of examples is only a portion of what is included in the policies. For further information, contact the IT Department.

Category II - Private Protected Data

Risk = **Moderate**

Description:

Data subjected to FERPA and/or other federal, state, or business regulations and laws. This includes any data and information exempt from release or disclosure to the public by regulation.

Examples:

Private Protected Data includes but is not limited to the following examples:

- Academic transcripts.
- Student disciplinary or judicial action information.
- Law enforcement investigation information.
- HR employee data.
- IT infrastructure data, intellectual property, and proprietary information belonging to CNI College.
- Non-public financial data belonging to CNI College.
- Non-public meeting minutes.
- Licensed software.
- Data is protected in non-disclosure agreements.
- Final course grades that contain exam questions with answers.

As mentioned above, this list of examples only includes a portion of the policies. For further information, contact the IT Department.

Category III - Non-Public and Public Data

Risk = **Low**

Description:

This category pertains to any data and/or information included in Categories I and II and other data whose disclosure has limited impact or risk to CNI College or personnel.

Examples:

Non-Public and **Public Data** includes but is not limited to the following examples:

- course catalogs
- CNI College's website
- faculty and student handbooks
- any FERPA information that is not blocked via privacy regulations.

As mentioned above, this list of examples is only a portion of what is included in the policies. For further information, contact the IT Department.

Acceptable Use Policy

Statement & Purpose

This policy covers the acceptable use of all computational equipment and devices at CNI College. Any use deemed inappropriate and/or wrongful exposes the college to various risks, such as viruses and ransomware attacks, which may compromise network systems and services, causing financial loss and legal issues.

Scope

This policy applies to all CNI College employees. Adherence to it helps safeguard the confidentiality, integrity, and availability of CNI College's information assets and protects the interests of CNI College, its students, faculty, and staff.

Policy

Technological resources are available for CNI College's faculty, administrators, staff, students, and others authorized. Access to and use of these resources and services are privileges and are to be used in compliance with all applicable laws and regulations. The highest standards of ethical behavior are to be always maintained when accessing and using the computing resources provided by CNI College.

Any use deemed inappropriate and/or wrongful exposes the college to various levels of risks, such as viruses, ransomware attacks, compromised network systems and services, financial loss, and legal issues.

The terms and conditions below are established for using all technological and computational resources within CNI College. The list of acceptable and unacceptable uses is not exhaustive. CNI College is the sole and conclusive authority on questions relating to the acceptable use of its resources.

If a question or concern about use arises, the use should be considered "prohibited" until the IT Department and Executive Administration deem it otherwise.

Policy Acknowledgments and Information Regarding Acceptable/Unacceptable Use

- All information stored on electronic and computing devices remains the sole property of CNI College. This includes but is not limited to work developed on the college computers or any new documents brought in by an employee. All proprietary information is protected through legal and/or technical means, following all policies related to information security.
- Theft, loss, or unauthorized disclosure of CNI College's proprietary information must be promptly reported to the IT Department and Executive Administration.
- All employees are expected to exercise sound judgment and rationality when using computing resources at CNI College. If they are uncertain, they should contact the IT Department.
- All employees must protect any classified materials being sent, received, stored, or processed according to the classification level assigned to them per the Information Classification Policy. This includes analog and digital information and materials.

- All employees must not transmit unprotected personal account numbers and sensitive information through messaging platforms such as non-encrypted emails, instant messengers, chat, etc.
- All employees must enter and verify the correct recipient for email addresses and other communication platforms so that classified information is not compromised.
- All employees must not record any credit/debit card data on personal devices at any time.
- All technological resources and technology may be subject to monitoring and/or recording for lawful purposes.
- All employees accept responsibility for using and protecting user credentials that they are provided with (e.g., user accounts, passwords, etc.).
- All employees and vendors acknowledge that they are not to use another user's account and password to access systems or attempt to access any unauthorized computer system or accounts.
- All employees will ensure that they are not being overlooked "shoulder surfing" by unauthorized personnel when working and take proper care when printing classified information.
- Classified printed materials are to be securely stored and correctly destroyed when no longer needed or in use.
- All employees are not to leave their computers unattended so that unauthorized access is gained while away from their desks or workstations.
- If a breach is detected or suspicion is raised, it must be reported to a direct supervisor and the IT Department.
- All employees are not to attempt to bypass or subvert system security controls or use them for any purpose other than their intended use.

- CNI College equipment/devices and information are not to be removed from the college without appropriate approval.
- If approved to use equipment/devices or information outside CNI College, the employee is responsible for protecting and ensuring precautions are taken. This includes leaving a device unattended or elsewhere that would encourage theft.
- All employees are prohibited from introducing viruses, malware, or other software or hardware into the college's systems or network.
- All employees are not to disable virus protection on their devices.
- All employees must comply with any legal, statutory, or contractual obligations relevant to their role.
- All employees must inform supervisors of any information held within their accounts before departure.
- All employees must not use the college's computing resources to send chain letters, junk mail, profane, obscene, threatening, libelous, or harassing messages.
- All employees are not to use the college's computing resources in any manner that will interfere with using shared resources. This includes large bandwidth, disk space, etc., that can impact the college and its users.
- All employees are not to use any of the college's computing resources for commercial and/or personal profit-making purposes, soliciting, and/or any activities that may violate local, state, and/or federal law.

As mentioned above, this list of examples only includes a portion of the policies. For further information, contact the IT Department.

If a question or concern about use arises, it should be considered "prohibited" until the IT Department and Executive Administration deems it otherwise.

Mobile Device Policy

Statement & Purpose

CNI College's Mobile Device Policy outlines our guidelines for using mobile devices, both personal and those provided by the college. This policy mitigates the following risks: loss or theft of mobile devices (including the data on them), compromise of classified information, introduction of viruses and malware to the network, and damage to reputation.

It is understandable that mobile devices, especially smartphones, are integral to everyday life. When properly used, they are an asset in day-to-day life but may become problematic when used inappropriately.

The guidelines in this policy must be always observed.

Scope

This policy applies to **ALL** CNI College employees.

Those working with sensitive student information such as social security numbers and financial information are required to comply with the "No Personal Mobile Devices at Desk" section.

Adherence to this policy helps safeguard the confidentiality, integrity, and availability of CNI College's information assets and protects the interest of the college, its students, faculty, and staff.

Policy

Mobile devices include but are not limited to, such items as:

- Laptops
- Notebooks
- External storage devices **(not allowed)**
- Tablets
- Smartphones
- Smart watches (e.g., Apple watches, Fitbits, etc.)

Unless authorized, only devices provided by CNI College may be used to hold and process classified information.

If an employee is required to use any mobile equipment, they will be provided with the appropriate device(s) configured to comply with CNI College's policies.

The following list applies to all employees using CNI College approved and provided devices:

- Mobile devices provided through CNI College will be accessible and require access from the IT Department for problem resolution and maintenance.
- Each mobile device provided through CNI College has proper security measures implemented to protect all information and data during device usage.
- All CNI College employees are to ensure the device is protected in a case when possible and not exposed in a manner that may cause damage.
- Identifying markings such as asset tags or serial numbers are not to be removed.
- All CNI College employees must ensure the devices are stored in a secure location that is not easily accessible.

- All CNI College employees must not hold classified information on devices that are not approved and that lack proper security measures (encryption).
- Peripherals should only be added with the consent of the IT Department.
- If the device(s) are to be taken out of the state or country, the IT Department must be notified to ensure that it will work and that proper measures, such as insurance, have been taken.
- Passwords must not be stored on the device in a manner that is easily accessible.
- Devices provided by CNI College are for business use only and must not be shared with friends or family for any reason.
- All CNI College employees may be asked to return the device to the IT Department for inspection or audit.
- CNI College employees are not to install software not authorized by the IT Department or modify configurations without consulting the IT Department.
- Classified information is not to be stored or backed up on any personal devices such as flash drives.
- When in public, ensure that the device is locked and stored away from possible unauthorized use and in a manner that unauthorized personnel cannot view, record, or photograph the screen.

If the CNI College provided device is lost or stolen, the employee must inform the IT Department as soon as possible, giving details of the circumstances of the loss and the sensitivity of the information stored on the device. CNI College reserves the right to remotely wipe the device as a security precaution.

Upon leaving the organization, the device owner must allow the device to be audited and remove all business-related data and applications.

No Personal Mobile Devices at Desk

Security issues can arise from inappropriate use of a personal mobile device while working with sensitive student information, such as social security numbers and financial information. To maintain compliance with the Gramm-Leach-Bliley Act (GLBA), CNI College employees are responsible for safeguarding sensitive personal and financial student information.

The following issues and security challenges can arise from personal devices:

- Shared device with family and others not authorized by CNI College.
- Increased exposure to potential loss.
- Connection to insecure networks.
- Lack of anti-virus protection and how often the device is updated/patched.
- Install potentially malicious applications onto the device.

Personal mobile devices may be kept in a container such as a bag, backpack, purse, etc., and may be allowed in a pocket, but they cannot be left on a desk or in desk drawers. Personal calls may be taken outside in the lobby area and in areas not surrounded by sensitive and/or classified information. In emergencies, please have relatives or friends contact CNI College's front desk.

Password Policy

Statement & Purpose

The Password Policy establishes a set of rules and guidelines to enhance the security best practices provided by the Federal Trade Commission (FTC), the USA National Institute of Standards and Technology (NIST), and the Payment Card Industry Data Security Standard (PCI DSS).

Scope

This policy applies to all employees. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of CNI College's information and data assets and protects the interests of CNI College, its students, faculty, and staff.

Policy

All CNI College employees must take appropriate measures to protect their passwords and ensure that they are secured and not available to unauthorized users. Multifactor authentication will be always enforced to maintain classification and integrity, and authentication will be kept in place at all times.

It is vital that policies and guidelines are in place to ensure that passwords and classified information remain secure to protect CNI College's systems and data.

General Password Guidelines should be as follows:

- A minimum length of at least eight characters.

- Passwords will not expire as there is no judgment for increased security.
- Single Sign-On (SSO – where a user is authenticated once and has access to many systems) will be used where available and appropriate.
- Throttling techniques (where an increasing delay is introduced between login attempts) will be used where available.
- After five unsuccessful login attempts, the user account will be locked out and need to be re-enabled by the IT Department.
- A password blacklist will be utilized to prevent the use of common, easily guessed passwords.
- The user must re-authenticate if a session has been idle for 30 minutes.
- Newly issued passwords will be subject to change immediately after first use.
- System default accounts/passwords will be disabled/changed immediately as part of the initial setup and configuration.
- Multi-factor authentication (MFA) must be used to enhance security authentication via a secondary device or alternative method, such as biometrics.

Additional Password Guidelines to follow:

- Passwords should not be revealed to anyone at any time on any medium (phone, email, messengers, etc.).
- Passwords should not be written down (e.g., post-it notes, under the keyboard).
- Dictionary words, names of family members, or information about oneself that could be easily found should not be used when creating passwords.
- If a password has been compromised, notify the IT Department immediately.
- If users are offered 'password hints' when creating a password, they should not make the hint easy enough for anyone to guess the password (e.g., password hint = my surname).

- Where possible, use passphrases instead of passwords. A passphrase is a longer version of a password and is, therefore, more secure. It is typically composed of multiple words, reducing the risk of dictionary attacks.
- When entering a password, be mindful of your surroundings to ensure that unauthorized users are not watching, recording, or taking photographs.

Password Protection Guidelines

- Passwords must not be transmitted over the network in clear/plain text or in any reversible form.
- Applications must not transmit passwords in clear/plain text over the network.
- All passwords stored must be encrypted using the appropriate cryptography technologies. See *Cryptography Policy*.
- All systems make use of role-based access to data in storage.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA), often referred to as two-factor authentication, is required for the following areas:

- Accessing IT systems where sensitive data is available to view or modify (e.g., cardholder data).
- When working remotely.
- When vendors or third-party suppliers require access to the organization's IT Systems.

MFA requires the user to have at least two of the following three authentication methods to gain access to the appropriate IT System:

- Something you know, such as a password or passphrase.

- Something you have, such as a token device/app or smart card.
- Something you are such as biometric (e.g., fingerprint readers).

Where smart card or token device/app methods are used as part of MFA, additional considerations are required and are as follows:

- These methods must be assigned to individual accounts – not shared with multiple accounts.
- Physical and/or logical controls must be in place to ensure only intended users access the appropriate system.

The IT Department will verify compliance with this policy through methods that include, but are not limited to:

- Periodical walks through campus offices.
- Technology monitoring.
- Business tool reports.
- Internal and external audits.

Any exceptions to this policy must be approved in advance by the Information Security Officer (ISO) and Executive Administration.

It is the responsibility of all CNI College employees and vendors to comply with all policies. Failure to do so will result in disciplinary action.

Security Awareness and Training Policy

Statement & Purpose

The Security Awareness and Training Policy will ensure that the CNI College community achieves and maintains a foundational level of understanding of information and data security through training provided by a qualified cybersecurity professional. Best practices will follow general obligations under various policies, standards, laws, regulations, contractual terms, and generally held standards of ethics and acceptable use of information and data resources.

Security awareness and training will be conducted bi-annually and when needed for all new and current college employees. Training and awareness activities will be conducted through qualified individuals to maintain a reasonable, consistent level of technology training and security awareness.

Scope

This policy applies to all CNI College employees. Adherence to it helps safeguard the confidentiality, integrity, and availability of CNI's information assets and protects the interests of CNI College, its students, faculty, and staff.

Policy

All CNI College employees will receive sufficient training to protect data and resources belonging to the college. Additional training will be required for personnel with

responsibilities that have greater needs. Awareness and training will be conducted following compliance laws and regulations such as those by the FTC, NIST, GLBA, etc. If access is granted to CNI College's computing resources, assets, and information, appropriate training will be conducted before it is granted.

CNI College's IT Department is responsible for developing and maintaining training and awareness to provide the following:

- Initial and ongoing security awareness training on acceptable use of IT resources.
- Proper information security training as related to functional responsibilities.
- Educational opportunities to ensure information security personnel are equipped with the necessary security skills, knowledge, and competencies.
- Awareness of cardholder data security.
- Information security training that is incorporated into the new hire orientation processes. Access to systems may not be provided until training is completed and a signed acknowledgment of security training has been received by the IT Department.
- Annual information security awareness refresher training that must be completed by all CNI College employees.
- Cybersecurity training on best practices related to password management, sensitive information that is passed through every department, phishing, etc.

Access Control Policy

Statement & Purpose

The Access Control Policy ensures that access control mechanisms provide for the control, administration, and tracking of access to CNI College's information assets, and protect information assets from unauthorized access, tampering, and destruction.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College ensures that its systems and processes strictly prohibit unauthorized access to its critical data. Access to CNI College's critical information is based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

Several general principles are used when designing access controls for CNI College's systems and services.

These principles are:

- **Defense in Depth** – security should not depend upon any single control but be the sum of several complementary controls.
- **Least Privilege** – the default approach taken should be to assume that access is not required, rather than to assume that it is
- **Need to Know** – access is only granted to the information required to perform a role, and no more.
- **Need to Use** – Users are only able to access physical and logical facilities required for their role.

Adherence to these basic principles helps to keep systems secure by reducing vulnerabilities—and, therefore, the number and severity of security incidents that occur. CNI College implements a mechanism to restrict access based on user's Need to Know principle to ensure that data, including cardholder data, is only accessible to those that require such information. Additionally, a default "denial-all" setting will be set to ensure that no accidental grant is provided to users. On a regular basis (at least annually), asset and system owners are required to review who has access within their areas of responsibility and the level of access in place.

This will be to identify the following:

- People who should not have access (e.g. employees who have been dismissed)
- User accounts with more access than required by the role.
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification (e.g. generic or shared accounts)
- Any other issues that do not comply with this policy.

CNI College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. Instances of non-compliance must be presented to, reviewed, and approved by the Chief Operating Officer (COO) and the Director of Information Technology and Security. All information security breaches, actual or suspected, must be reported to and investigated by the COO and the Director of Information Technology and Security. Those who violate security policies, standards, or security procedures are subject to disciplinary action, up to and including loss of computer access and appropriate disciplinary actions as defined by CNI College's Human Resource Department.

Identification & Authentication Policy

Statement & Purpose

The purpose of the Identification and Authentication policy is to manage risks from user authentication and access to CNI College's information assets by establishing an effective identification and authentication program. The program helps CNI College implement identification and authentication security best practices.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College implements and maintains proper controls on IT systems to confirm user identity before access. CNI College's access protection measures assure individual accountability through identifying and authenticating each IT system user.

CNI College's policy is to protect the confidentiality, integrity, and availability of information systems.

CNI College's IT Department:

- Ensures all CNI College information systems can enforce user accountability for system activity (both authorized and unauthorized) to be traced to a specific user or to an approved user group.
- Ensures all information systems have a method of user and device identification and authentication. Systems that do not meet this requirement must explicitly request in writing a policy deviation.
- Manages identifiers and authenticators for users and devices to ensure appropriate authorization, assignment, and termination.
- Ensures CNI College's systems use standard approved cryptographic authentication.
- Ensures all authenticator feedback is encrypted.
- Ensures all users are identified and authenticated under the same requirements.
- Ensures that individual authentication information is not shared among users or system personnel.

Business Continuity & Recovery Policy

Statement & Purpose

The Business Continuity and Recovery policy defines CNI College's overall contingency goals and establishes the agenda and responsibilities for the institution's Business Continuity. The risk of network vulnerabilities and natural disasters impacting critical hosts is a constantly evolving concern.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College implements formal contingency plans to counteract interruptions to business activities and protect critical business processes from major failures, disasters, or security breaches. Contingency plans are developed, implemented, and tested to ensure that essential business processes can be restored promptly while always maintaining an appropriate level of security control.

CNI College's IT Department focuses on:

- Business Impact Assessment planning focuses on and identifies the criticality and continuity of the business processes, information, and information resources to ensure controls are applied commensurate with those levels of availability requirements, sensitivity, and criticality.
- Disaster recovery plans are developed and tested for CNI College systems to ensure that the IT systems security controls continue essential functions if IT support is interrupted. CNI College's Recovery Plan (DRP) and IT contingency plans follow established standards. At a minimum, disaster recovery plans are updated annually.
- All staff involved in disaster recovery efforts are trained in specific procedures and the logistics of their respective plans. Training takes place annually or as significant changes to the plan are made.
- Business Impact Assessments are reviewed annually with business stakeholders. Disaster recovery plans are tested and exercised at least annually, with the results documented and used to update the plans. IT Disaster recovery plan test results may be included as an Appendix in the IT disaster recovery plan.

Email Policy

Statement & Purpose

The Email policy describes how to safeguard the provided CNI College's email service. It applies to all users of these services, whatever the means or location of access (e.g. via mobile devices or outside of the office). CNI College's Email service provider is Microsoft.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Email is a vital business tool for communicating internally with students, potential students, third-party vendors, suppliers, and external personnel. However, due to its flexibility and general availability, the use of electronic messaging carries with it several significant risks, and all users must remain vigilant and adopt good practices when sending and receiving messages. It is, therefore, imperative to minimize the attack surface and the opportunities for attackers to manipulate human behavior and conduct cyberattacks like social engineering to users interacting with web browsers and email systems.

CNI College's electronic messaging facilities are used when communicating with others on official business. Personal accounts must not be used for this purpose. Guidelines on the sending of classified information via electronic messaging are always observed.

Students, faculty, administrators, staff, and contractors must not send or receive information that contains Personally Identifiable Information (PII). In addition, CNI College blocks all electronic messages containing social security numbers, tax ID numbers, bank account information, or credit card information with Data Loss Prevention (DLP) in place.

Compliance Management Policy

Statement & Purpose

The Compliance Management policy provides a framework for CNI College to avoid breaches of any criminal and civil law, statutory, regulatory, or contractual obligations and of any information security policy.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Individuals authorized to access CNI College's information and Computing Resources must comply with relevant federal, state, and local legal, regulatory, and contractual requirements. Formal audits and compliance activities validate CNI College's security infrastructure, determine the level of user compliance, and assure that organizational practices align with CNI College's information security policies.

Personnel Security Policy

Statement & Purpose

CNI College recognizes that the Human Resources Department (HR) plays a significant role in the successful operations and delivery of effective IT services to ensure that appropriate guidelines for securing CNI College's information assets are in place.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College implements security measures that are defined for recruiting and retaining staff and employees' responsibilities to safeguard CNI College's informational assets.

Appropriate security measures include, but are not limited to, the following:

- Security awareness, training, and education program
- User account management (Access Request, Access Certification and Provisioning)
- Use of security mechanisms and processes during staff hiring/termination
- Employee requirements and responsibilities.

Application Development Security Policy

Statement & Purpose

CNI College uses many types of computer software to perform its institutional operations and always relies upon the correct functioning and security of the application/software. This policy sets guidance for developing and/or implementing new applications and systems at CNI College to ensure that all development work is under security controls.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College may develop its own software for purposes where a package is not available or does not fulfill the identified requirements. In such cases, a structured development method is used to ensure that software is developed to organizational standards and is tested and implemented in a managed way. Alterations to in-house developed software such as the addition of fields or screen changes are requested through the change request process. Changes to in-house developed software must not be made without following the change management process.

Application/Software developed and configured by CNI College will be used strictly for its intended purpose. Furthermore, security, specifically risk assessment and management, is considered during all phases of the development life cycle.

Complete module and design documentation is written for each new project and then modified as changes are made to existing applications/software.

Test plans for all units and modules are developed and fully documented. Software testing should be conducted according to the design requirements.

Remote Access Policy

Statement & Purpose

The Remote Access policy sets out the key information security-related elements that must be considered in agreeing to a remote working arrangement. It ensures that all the necessary issues are addressed and CNI College's information assets are protected.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

With the increased availability of broadband access and Virtual Private Networks (VPN), remote working/telecommuting has become more viable for many organizations. While remote working/telecommuting can be an advantage for users and the organization, it presents new confidentiality and data security risks. Workers linked to CNI College's network become an extension of the wide area network and require additional protection against the danger of potential security breaches, malicious code, etc.

CNI College implements the following principles to safeguard the confidentiality, integrity, and availability of its information assets within the remote working environment:

- **Need to Know**: Remote access users have access based on the same "need to know" they have when in the office.
- **Password Use**: The use of a strong password and protection for the password (in accordance with the standards), is even more critical in the telecommuting environment. Remote workers must never share or write down their passwords.
- **Training**: All telecommute workers must complete the same annual security awareness and training as all other employees.
- **Contract Specific**: Additional requirements, as needed, are specified to the individual contracts for remote users.
- **Multifactor authentication**: Multifactor authentication is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.

Password Policy

Statement & Purpose

The Password policy establishes a set of rules to enhance security best practices by encouraging the creation of strong passwords, their protection, and the frequency of changing them.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Users accessing CNI College's systems must take appropriate steps to protect their passwords. Password-based authentication mechanisms are also vulnerable to compromise due to the following types of malicious activity:

- Password guessing using a dictionary attack or attributes known about the user.
- Social engineering (e.g., manipulating a user to obtain a password)
- Interception during password transmission

Controls must be in place to ensure a password remains secure for the protection of CNI College's systems and data. Passwords can be intercepted during transmission or

stolen while stored on a disk. CNI College implements practical standards and mechanisms to enforce secure password creation, protection, and management.

Multi-factor authentication (MFA) is implemented to securely protect CNI College's sensitive data, such as cardholder data.

All passwords have the following characteristics:

- Require a minimum length of at least 10 characters
- Contain at least two of the following:
    - Upper and lowercase characters
    - At least one number or one special character

The following requirements also apply to the management of passwords:

- Passwords are set to not expire but can be changed by the user as needed.
- After five unsuccessful login attempts, the user account will be locked.
- The account lockout is set for 30 minutes. The IT Department must be contacted to verify the user and unlock the account.
- If a session has been idle for 60 minutes for faculty members and 15 minutes for other employees, the user is required to re-authenticate.
- Newly issued passwords must be changed immediately after first use.
- System default accounts/passwords are manually disabled/changed immediately as part of the initial setup and configuration.
- CNI College uses a challenge/response process upon password reset requests to verify the identity of the staff member.
- All passwords are disabled/changed in test and development systems when promoted into the live environment.

Cryptography Policy

Statement & Purpose

The Cryptography policy aims to safeguard CNI College's assets by employing data encryption. It is key in protecting sensitive information from unauthorized access, control, and deletion.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College's academic, administrative, and business functions must employ approved encryption solutions to control access to and preserve the integrity and confidentiality of the processing, storing, and transmission of data classified as "covered data."

In general, the CNI College's cryptography policy ensures that encryption techniques are in place during the following processes and situations to protect the college's classified information from ever-growing potential threats.

The items are as follows:

- Storage of data in the cloud
- Protection of data on removable media
- E-commerce transactions over the internet
- Protection of passwords on systems
- All passwords are hashed.
- Email security
- Remote access
- Processing and/or transmitting cardholder data over a wireless network
- Strong cryptography under industry-recognized standards
- Accessing systems that store, process, or transmit cardholder data
- Strong cryptography per industry-recognized standards
- Use of HTTPS for web application transactions
- Securing wireless networks

A lifecycle approach must be taken to key management. It is vital that cryptographic keys are stored and protected from modification, loss, destruction, and unauthorized disclosure.

Change Management Policy

Statement & Purpose

CNI College understands that a formalization of proper change management and control is crucial for a more disciplined and efficient infrastructure that enables quality control of information systems.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

This policy provides management direction and high-level objectives for change management and control.

It ensures the implementation of change management and control strategies to mitigate associated risks such as:

- Corruption and/or destruction of information;
- Disruption and/or degradation of computer performance;
- Loss of productivity; and
- Reputational risk exposure.

Information resource and service changes are managed and executed according to a formal change control process. The control process ensures that changes proposed are reviewed, authorized, tested, implemented, and released in a controlled manner and that the status of each change is monitored and documented.

Malicious Code & Computer Compromise Policy

Statement & Purpose

The Malicious Code and Computer Compromise (MCCC) policy provides information to CNI College's IT Department and the entire College community to improve the resistance to, detection of, and recovery from the effects of malicious code.

Malicious code describes software designed to exploit, infiltrate, or damage a computer system without the informed consent of the computer user. It includes, but is not limited to, computer viruses, worms, Trojan horses, rootkits, spyware, and adware. Malicious code is typically distributed over the internet via email or web pages.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

The college utilizes a viable endpoint control solution to prevent information loss due to infection by and spread of malicious code and to ensure continued uninterrupted services for CNI College computers and networks.

Any device or system that may be affected by computer viruses, malware, phishing, mobile code, or email spam that connects to the CNI College network has the standard endpoint protection solution installed and always running, as configured or approved by IT.

Endpoint protection is configured to clean and remove an infected file automatically or to quarantine the infected file if automatic cleaning is not possible. The software is configured to update automatically on a regular basis.

Employees are prohibited from disabling or tampering with the installed software. Should malicious code be detected or a device suspected of being compromised be compromised, access to CNI College's resources will be removed, and CNI College will follow protective measures.

3rd Party Services Policy

Statement & Purpose

The 3rd Risk Management Policy is intended to accomplish the following key goals:

- Provide a framework through which CNI College adheres to a consistent, documented process of engaging and managing 3rd Parties;
- Maintain a reasonably complete and accurate 3rd Party Inventory;
- Assess the suitability of using a 3rd Party to provide a product or service consistent with CNI College's business strategies and objectives;
- Take reasonable steps to select and retain 3rd Party Relationships that are capable of maintaining appropriate safeguards for the Federal Student Aid, student, and CNI College's information;
- Require that 3rd Parties be governed by written contracts that clearly define the expectations and obligations of CNI College and each 3rd Party, and include provisions to protect the interests of CNI College and its constituents;
- Engage in ongoing risk-based management of CNI College's 3rd Party relationship to determine if expectations and obligations are being met, and, if performance errors or compliance infractions occur, determine whether penalties and/or remediation are warranted and/or if engagement with the 3rd Party should continue; and
- Disengage from 3rd Party relationships, when warranted.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College has established a college-wide program for managing 3rd Party relationships, which consists of two separate processes: (i) Standard and (ii) Alternative. Whether a 3rd Party relationship is managed through the standard process or an approved alternative program, the full scope of required risk management phases articulated in this policy must be employed.

Alternative programs involve department management of a group of 3rd Party relationships (that provide a common product, service, activity, or function) within an alternative program. Considerations for creating an alternative program may include, but are not limited to, the following:

- Whether managing the TPRs collectively provides added efficiency without creating additional risk
- Whether the 3rd Party relationship share similar risk characteristics to allow them to be risk-assessed as one
- The ease or difficulty of terminating or replacing a 3rd Party relationship
- Whether the 3rd Party relationship are mission critical to the College
- Whether the TPRs are subject to independent oversight (for example, professional license or certification)

In the course of conducting business, CNI College engages 3rd parties (as defined below) to:

- Provide products or services to the College or its students, alumni, and/or other relationships;
- Perform functions of the College's operations on behalf of the College (commonly referred to as "outsourcing"); and
- Conduct business on behalf of the College or franchising the College's attributes (e.g., using the College's brand, name, logo, etc.)

Although the use of 3rd parties can provide an effective and efficient means of accomplishing College objectives, such as increasing efficiency, revenues, offering specific knowledge or expertise, and/or providing technology, reliance on 3rd Party relationships can significantly increase the College's risk profile.

The College recognizes that increased risk often arises from poor planning, ineffective management control and/or oversight over the 3rd Party, and inferior performance or service on the part of the 3rd Party.

When engaging a 3rd Party, the College will conduct appropriate risk management activities, as provided in this policy, to manage the College's corresponding risks, including, but not limited to, reputational, financial, operational, strategic, and compliance risks. Accordingly, the decision of a College Department to engage a 3rd Party must be consistent with the College's business objectives and made only after due diligence and consideration of the risks involved.

It is the college's policy to establish and maintain comprehensive standards, procedures, and internal controls to assess, monitor, and manage third-party relationships and their associated risks. This policy and its related and supporting documents (collectively, the "Program") outline the risk-based framework and management processes the College has adopted to ensure the effective oversight and risk management of third-party relationships.

The Program outlines the risk management process throughout the 3rd Party relationship's life cycle, including planning, due diligence, contracting, ongoing monitoring and management, periodic reevaluation, and termination. The Program enables the College to outline the roles and responsibilities of parties involved with 3rd Party relationships. It also allows the College to properly identify 3rd Parties that present risk, measure the identified risks, perform thorough due diligence, provide ongoing oversight of 3rd Party relationships and activities, drive consistency for management and reporting of 3rd Party relationships, and manage the 3rd Party relationship, up to and including termination.

Physical & Environmental Security Policy

Statement & Purpose

The protection of the physical environment is one of the most obvious and yet most important tasks within the area of information security. A lack of physical access control can undo the most careful technical precautions, potentially risking lives.

CNI College is committed to ensuring the safety of its employees, contractors and assets and takes the issue of physical security very seriously. This policy sets out the main precautions that must be taken.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Sensitive information is stored securely. Appropriate security controls are in place to protect CNI College's information assets from unauthorized physical access and safeguard them against reasonable environmental hazards, active and passive electronic penetration, and to prevent unauthorized physical access, damage, and

interference. A risk assessment is carried out to identify the appropriate level of protection to secure the information being stored.

Physical security begins with the building itself; and perimeter vulnerability must be assessed. Appropriate control mechanisms are in place for the classification of information and equipment that is stored within it, which may include:

- Alarms activated outside working hours
- Window and door locks
- Access control mechanisms fitted to all accessible doors (if codes are utilized, they need to be changed regularly and known only to those people authorized to access the area/building)
- CCTV cameras (recordings need to be kept for at least 30 days)
- Protection against damage (e.g. fire, flood, vandalism)
- Identification and access tools/passes (e.g. badges, keys, entry codes etc.)
- Centralized protection of keys to all secure or public areas housing IT equipment (including wireless access points, gateways, and more)
- Offsite backup locations are reviewed at least annually to ensure these locations are physically secure for the backups

All internal or third-party vendor storage location security is reviewed at least annually to confirm that backup media storage is secure.

When media is no longer needed for business or legal reasons, it is destroyed using industry-standard security methods.

Media classification is implemented so that the sensitivity of data can be determined, and appropriate physical security is in place. All media inventory logs are properly maintained, and media inventories are to be performed at least annually.

Devices that capture payment card data via direct physical interaction with cards are protected from tampering and substitution by:

- Maintaining a list of devices
- Periodically inspecting devices to look for tampering or substitution
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

Risk Assessment & Management Policy

Statement & Purpose

The Risk Assessment and Management policy ensures that CNI College manages the risk associated with assets, information leakage, and network vulnerabilities. It is a formal acknowledgment of the commitment of CNI College to risk management. The Risk Assessment and Management Policy and associated plans augment the Information Security Program by proactively identifying threats and vulnerabilities, which can result in consequences (impact).

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Institutional data and computing resources have appropriate security controls in place commensurate with the resource's value to CNI College, as determined by the results of a formal risk assessment to ensure the identification and treatment of security risks using a comprehensive and methodical manner capable of producing comparable and reproducible results.

Risk management is addressed across CNI College through a formal risk management program. The IT Department is responsible for implementing and maintaining the IT risk management program.

An IT risk assessment of the systems is conducted at least biannually, either internally or by an independent contractor, to assess the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support CNI College's operations.

In support of this risk assessment process, vulnerability assessment and penetration testing are conducted biannually on all CNI College systems.

Information & Cybersecurity Incident Response Policy

Statement & Purpose

An incident is defined as "any adverse event that compromises some aspect of a computer or network security." Incidents are grouped into the following categories:

- Loss of confidentiality of information
- Compromise of the integrity of information
- Misuse of service, systems, or information
- Damage to property, systems, or CNI College's assets

This policy provides a well-defined, organized approach for handling any potential threat to computers and data and taking appropriate action when the source of the intrusion or incident at a third party is traced back to the institution.

This policy facilitates the development of an incident response plan, process, and procedure that:

- Helps personnel identify, react, categorize, and classify a cyber and/or security incident quickly and effectively
- Minimizes loss of information or disruption of services due to an incident
- Ensures that post-event recovery is correct and complete
- Protects computing systems and corresponding data
- Uses technical and managerial personnel efficiently and effectively while responding to an incident

- Communicates incident response measures to appropriate internal and external parties
- Properly handles legal issues.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Institutional data and computing resources must be monitored to detect system, security, and operational events compromising confidentiality, integrity, or availability. Formalized incident response and investigation procedures are in place. Events are logged to ensure a timely response to information security incidents and to communicate information security events and vulnerabilities associated with information systems in a manner that allows appropriate and timely corrective action.
While preventing every incident from occurring is not feasible, two key aspects are established to manage the impact of an incident:

- A formalized plan detailing procedures for incident prevention, detection, assessment, forensics, containment, and recovery activities to mitigate computer security risks.
- Designated team(s) to respond to an incident and a list of person(s) responsible for following the procedures set forth in the plan.

Asset Management Policy

Statement & Purpose

Adherence to this policy ensures that all known systems, software, hardware, and information assets are protected according to their value and sensitivity to CNI College.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College's computing resources are formally acknowledged, and ownership is assigned to maintain accountability to ensure a formal accounting of all known systems, software, hardware, and information assets and facilitate the protection of these assets according to their value and sensitivity to CNI College. The confidentiality, integrity and availability of CNI College's physical and electronic information assets are safeguarded according to defined classifications.

CNI College has an inventory of and manages all hardware and software systems:

- **Hardware Assets**: Actively manages hardware systems, workstations, and devices on CNI College's network. Only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from accessing CNI College's network.
- **Software Assets**: Actively manages software systems on CNI College's network so that only authorized software is installed/executed and unmanaged software is found and prevented from installation and execution.

Configuration Management Policy

Statement & Purpose

The Configuration Management policy sets practices for establishing the mandatory requirements for installing, configuring, and implementing information technology systems throughout CNI College.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Configuration management focuses on establishing and maintaining consistency between a system's functional attributes and its requirements throughout its life cycle. This policy sets the guidance for CNI College to ensure that configurations are properly controlled and maintained accurately for the successful delivery of services.

Adherence to this policy ensures that the following aspects are properly addressed:

- System Configuration Baselines
- Configuration Monitoring
- Communication Requirements
    - Network Connectivity
    - Location
    - Equipment
    - Application/OS Requirements
- Security
    - Authentication
    - Encryption
    - Posts/Services/Protocols
- Applications
    - Installation
    - Configuration
    - Security

Audit Logging & Reporting Policy

Statement & Purpose

The purpose of this policy is to establish practices for the monitoring and secure logging of all system events throughout CNI College. To ensure that CNI College's information assets are secure, it is necessary to monitor the activities of both authorized and unauthorized users to identify any actions that do not present a secure use of CNI College's information systems and ensure immediate response should any suspicious incident occurs.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Audit Logging

When there is an incident of any system/service failures and/or security breaches, logs are a crucial factor in providing the source of information to track the trails of the incidents. Therefore, logs must be captured and be accessible for all CNI College systems.

CNI College ensures that all clients, servers, and other equipment (such as network routers and switches) involved in hosting the storage or processing of classified information have the available audit logging facilities activated to allow the recording and monitoring of activities.

Monitoring System Use

A Security Incident and Event Management (SIEM) tool identifies and alerts operations staff to events worth immediate investigation and finds potential links between events on multiple systems.

Protection of Log Information

Log information is maintained in accordance with standards and must be readily accessible. Strict access permissions are used to ensure that the confidentiality, integrity, and availability of the log contents are secured. Logs are securely stored to protect them from unauthorized access. Appropriate access controls are in place to prevent log data from being used for unauthorized purposes.

Record Retention & Data Disposal Policy

Statement & Purpose

The purpose of the Record Retention and Data Disposal Policy is to establish mandatory records retention and disposal plans as part of an overall records management program that applies to all departments and authorized users at CNI College. This policy outlines the practices for managing, maintaining, and disposing of records in an orderly, reasonable, and lawful manner.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

Record Retention

Records are classified as follows:

- Active
- Archived for Retention
- Prepared for Disposal

Active records are those that are currently being used in the operations and transactions of the business or are otherwise part of current activities such that they need to be organized, classified, and maintained in a form suitable for fast and reliable access for individuals authorized to use the records.

Use of Cryptography

Encryption keys used to encrypt data must be securely stored for the life of the relevant data.

Disposition

The record is reviewed after the expiry of the retention period, or if that is not feasible, the record is retained, and a later review date is set. The review is conducted by the appropriate personnel in consultation with relevant stakeholders. Decisions must not be made with the intent of denying access or destroying evidence.

Data Disposal

Once a record is no longer active, it may be archived for a period. To reduce records storage requirements and associated costs, all records that have no such value to CNI College are destroyed on a regular basis. If a class of records is considered as having no value for retention and is destroyed once the record's immediate purpose is completed. Such records may include the following:

- Extra copies of records that have no value
- Publications, trade journals, and magazines that require no action and have no value as defined above

- Correspondence, memos, and interoffice communications that have been completed and have no further value as defined above
- Drafts of documents on which no action was taken and that require no follow-up.
- Personal email messages and other documents not relating to CNI College's business

Disposal of Electronic Media: All external media are sanitized or destroyed in accordance with industry standard compliant procedures.

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor.
- External media must be wiped clean of all data. The IT Department has very definitive procedures for doing this so all external media must be sent to them.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

Disposal of IT Assets: Department managers coordinate with the IT Department on the disposal of surplus property that is no longer needed for business activities.

PCI DSS compliance requires that cardholder data is handled uniquely and independently of other data classifications.

For cardholder data, the following requirements must be fulfilled:

- Sensitive Authentication Data (SAD) are rendered unrecoverable upon completion of the authorization stage of the payment process.
    - SAD is the following information on credit/debit cards:
        - Full Track Data – Magnetic strip on the back of the card or the chip on the front of the card.

- CAV2/CVC2/CVV2/CID – The three- or four-digit value typically on the back of the card next to the signature section.
- PIN/PIN BLOCK – Personal identification number entered by the cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
- Primary Account Number (PAN) should only be stored if explicit authorization has been granted by the COO. If the PAN is stored, the following requirements must be met:

  - The PAN is masked when displayed. The maximum number of digits permitted to be displayed are the first six and last six digits.
  - Access to the full 16 digits of the PAN is only available to roles that require it for legitimate business reasons.
  - The PAN is rendered unreadable anywhere it is stored.
  - PANs are never sent via end-to-end user messaging.

End User Computing Policy

Statement & Purpose

End User Computing (EUC) policy consists of but is not limited to programs, spreadsheets, databases, report writers, and applications created and used by end users. EUC is used to extract, store, sort, calculate and compile CNI College data to perform queries, analyze trends, make business decisions, or summarize operational and financial data and reporting results. EUC involves technology used by end users, outside of administrative systems and systems not managed by the IT Department. Any cloud computing solution the end users use also forms part of the EUC.

EUC is the primary gateway to the organization's sensitive information and business applications. Implementing appropriate information security controls for EUC can mitigate the data and IT systems risk. Consequently, end-user protection is critical to ensuring a robust, reliable, and secure IT environment.

The purpose of this policy is to:

- set out the rules for effectively managing EUC
- place safeguards regarding access to EUC
- mitigate potential risks associated with the use of EUC.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and

protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

CNI College relies on EUC during its normal course of business and intends to protect the confidentiality, availability, and integrity of information created during its business, education, research, and other activities.

In using EUC-related resources, the end user (extracting, manipulating, summarizing, and analyzing their EUC data) must take appropriate risk management actions, including but not limited to, inventory and risk ranking to minimize risks.

The IT Department develops, maintains, and communicates EUC standards and trains users to comply with them.

End users must certify to the COO and Director of IT their compliance with the policy and standards annually. The COO and Director of IT also monitor and certify CNI College's compliance with the policy and standards to the Chief Financial Officer (CFO) annually.

Network Security Policy

Statement & Purpose

This policy sets out guidance for implementing security measures for CNI College's network systems. The established rules for network protection enable the IT Department to create and maintain a secure network for its IT infrastructure.

Scope

This policy applies to the CNI College community. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the college's assets, and protects the interest of CNI College, its students, faculty and staff, and any third party vendors.

Policy

The use of networks is an essential part of CNI College's day-to-day business. Networks not only connect many of the components of business processes together internally but also link the organization with its suppliers, customers, stakeholders, and the outside world. These networks need to be protected to ensure that the confidentiality, integrity, and availability of CNI College's vital information are always secure.

CNI College sets out appropriate security requirements to protect its information assets within its network and implements the following controls:

- Network segregation
- Perimeter security
- Remote access
- Public/untrusted networks
- Network configurations
- Firewalls and routers
- Wireless network
- Intrusion detection system and intrusion prevention system
- Defined roles and responsibilities
- File-integrity monitoring
- System hardening

Vulnerability & Patch Management Policy

Statement & Purpose

This policy sets out how CNI College assesses and manages technical vulnerabilities within the Information Technology environment, which includes cloud services. Adherence to this policy increases the security posture of CNI College and mitigates threats posed by vulnerabilities within CNI College's information systems.

Scope

This policy only applied to CNI College's IT Department. Therefore, all College information systems may not be covered by this policy. Adherence to this policy helps safeguard the confidentiality, integrity, and availability of the College's information assets, and protects the interest of CNI College, its customers, personnel, and business partners.

Policy

Vulnerability and patch management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities within organizations and their systems. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively and continuously managing vulnerabilities of systems reduces or eliminates the potential for exploitation and

involves considerably less time and effort than responding after exploitation has occurred.

Assigning Risk Ratings

A process is established to review new security vulnerabilities and assign a risk rating in accordance with the Risk Assessment and Management Policy and standards. A simple scoring mechanism is implemented to place the vulnerabilities into three categories of "Critical," "High," or "Medium." The risk rating depends on:

- Industry best practices on classifying vulnerability risk ratings
- Potential impact on CNI College
- Classification by the vendor
- Systems affected and data it may hold.

Patches and Updates

Procedures are in place to obtain copies of software updates electronically when they are issued by the vendor. Updates are applied to systems based on their criticality and CNI College's standards and procedures.

Vulnerability Assessment and Penetration Testing

Proactive measures to test the strength of CNI College's security controls are in place and are as follows:

- Vulnerability scanning of applications, systems, devices, and cloud environment
- Network security testing and scanning
- Penetration testing
- Database assessment

Test results are recorded, and the risk is assessed and ranked (usually as critical, high, or medium) and sent through the treatment process to remediate any vulnerabilities found.

Internal and external targets for testing include but are not limited to:

- Internal systems, applications, networks, and devices
- Databases
- Cardholder Data Environment (CDE)
- Demilitarized Zone (DMZ)
- Cloud environments

Internal and external vulnerability scans are performed at least weekly and after any significant change to the network. If required to fulfill CNI College's PCI DSS compliance requirements, external scans are performed via an Approved Scanning Vendor (ASV) designated by the PCI Security Standards Council (SSC).