Information Security Policy

Union Centre Institute

4845 Rialto Road, West Chester, Ohio 45069

(513) 855-5100 | admissions@unioncentreinstitute.com

https://unioncentreinstitute.com

Effective Date: September 15, 2026

Policy Owner: Information Security Officer

Review Cycle: Annual

Classification: Internal Use. Distribute to all employees, contractors, and other authorized personnel.

Contents

Introduction

This policy document encompasses all aspects of security surrounding confidential Union Centre Institute information and must be distributed to all Union Centre Institute employees and applicable contractors. All employees must read this document in its entirety and sign the form in Appendix A confirming they have read and fully understand this policy. This document will be reviewed and updated by management on an annual basis, or sooner when newly developed security standards need to be incorporated, and re-distributed to all employees and contractors where applicable.

Union Centre Institute (also referred to in this document as "the Institute") is a career education provider located at 4845 Rialto Road, West Chester, Ohio 45069, offering hybrid hands-on programs in healthcare and technical fields. In the course of admissions, enrollment, and tuition processing, the Institute handles sensitive student, employee, and payment information. This policy sets the minimum standards for protecting that information.

Information Security Policy

Union Centre Institute handles sensitive information daily. Sensitive information must have adequate safeguards in place to protect account data, including cardholder data, cardholder privacy, and student and employee records, to ensure compliance with applicable regulations, and to guard the future of the organization.

Union Centre Institute commits to respecting the privacy of all its students, applicants, and customers and to protecting their data from outside parties. To this end, management is committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling sensitive cardholder data must:

- Handle Institute and account data in a manner that fits its sensitivity and classification.
- Limit personal use of Institute information and telecommunication systems and ensure it does not interfere with job performance.
- Understand that Union Centre Institute reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems, and network traffic for any purpose.
- Not use email, internet, or other Institute resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing, or illegal.
- Not disclose personnel or student information unless authorized.
- Protect sensitive account data, including cardholder information.
- Keep passwords and accounts secure.
- Request approval from management prior to establishing any new software, hardware, or third party connections.
- Not install unauthorized software or hardware, including modems and wireless access points, without explicit management approval.
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended.
- Report information security incidents without delay to the Information Security Officer.
- Attend security awareness training on an annual basis.

We each have a responsibility for ensuring the Institute's systems and data are protected from unauthorized access and improper use. If you are unclear about any of the policies detailed herein,

seek advice and guidance from your supervisor or the Information Security Officer.

1. Network Security

A high-level network diagram is maintained and reviewed on a yearly basis. The network diagram provides an overview of the cardholder data environment (CDE) and, at a minimum, shows the connections in and out of the CDE. Critical system components within the CDE, such as point of interaction (POI) and point of sale (POS) devices, databases, eCommerce web servers, redirection or iFrame servers, and any other necessary payment components, should also be illustrated as applicable.

Where applicable, external vulnerability scans must be performed and completed by a PCI SSC Approved Scanning Vendor (ASV) on a quarterly basis (every 90 to 92 days). Evidence of these scans will be maintained for a period of 18 months. For eCommerce payment pages, the scans must include the redirection or iFrame servers at a minimum.

Payment channel specific requirements:

- Standalone dial-up and P2PE terminals: see Appendix D (Standalone and P2PE POI Management Policy).
- eCommerce redirection or iFrame to a hosted payment page: see Appendix E (eCommerce Configuration and Hardening Policy).

2. Acceptable Use Policy

Management's intention in publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the Institute's established culture of openness, trust, and integrity. Management is committed to protecting employees, students, partners, and Union Centre Institute from illegal or damaging actions, whether committed knowingly or unknowingly. The Institute will maintain an approved list of technologies and devices and the personnel with access to such devices as detailed in Appendix B.

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.
- Employees must take all necessary steps to prevent unauthorized access to confidential data, which includes account data and cardholder data.
- Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
- All PCs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature enabled.
- All POS and POI or PIN entry devices must be appropriately protected and secured so they cannot be tampered with or altered.
- The List of Devices in Appendix B will be updated when devices are modified, added, or decommissioned. A stocktake of devices will be regularly performed and devices inspected to identify any potential tampering or substitution.
- Users will be trained to identify suspicious behavior indicating tampering or substitution. Any suspicious behavior must be reported to the Information Security Officer.
- Information contained on portable computers is especially vulnerable, and special care must be exercised.

- Postings by employees from an Institute email address to public forums or newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Union Centre Institute, unless the posting is in the course of business duties.
- Employees must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, Trojan horse code, or phishing attacks.

3. Protect Stored Data

- Union Centre Institute and its employees will not store cardholder data in the form of a full primary account number (PAN) or sensitive authentication data in electronic format at all.
- All sensitive account data, including cardholder data stored and handled in hard copy, must be securely protected against unauthorized use at all times. Any sensitive card data no longer required for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN, it must be masked when displayed, showing at most the first six and last four digits.
- PANs that are not protected as stated above must not be sent outside the network via end user messaging technologies such as email, chat, or instant messaging.

It is strictly prohibited to store:

1. The contents of the payment card magnetic stripe (track data) or chip equivalent track data on any media whatsoever.
2. The CVV2, CVC2, CAV2, or CID (the three or four digit number on the signature panel or front of the payment card) on any media whatsoever.
3. The PIN or the encrypted PIN block under any circumstance.

4. Information Classification

Data and media containing data must always be labeled to indicate sensitivity level.

- **Confidential** data includes information assets for which there are legal requirements preventing disclosure or financial penalties for disclosure, or data that would cause severe damage to Union Centre Institute if disclosed or modified. Confidential data includes account data and cardholder data, student education records, and employee personnel records.
- **Internal Use** data includes information that the data owner feels should be protected to prevent unauthorized disclosure.
- **Public** data is information that may be freely disseminated, such as program descriptions and published tuition information.

5. Access to Sensitive Cardholder Data

All access to sensitive cardholder data must be controlled and authorized. Any job functions that require access to cardholder data must be clearly defined.

- Any display of account data or cardholder data must be restricted, at a minimum, to the first six and last four digits of the PAN.
- Access to sensitive cardholder information such as PANs, personal information, and business data is restricted to employees who have a legitimate need to view such information.

- No other employees may access this confidential data unless they have a genuine business need.
- If cardholder data is shared with a third party service provider (TPSP), a list of such providers will be maintained as detailed in Appendix C.
- The Institute will ensure a written agreement is in place that includes an acknowledgement that the TPSP is responsible for the security of the cardholder data it possesses.
- The Institute will ensure an established process, including proper due diligence, is in place before engaging a TPSP.
- The Institute will have a process in place to monitor the PCI DSS compliance status of each TPSP.
- The Institute will ensure the responsibilities for securing account data are defined between the Institute and each TPSP and documented in a responsibility matrix.

6. Physical Security

Access to sensitive information in both hard and soft media format must be physically restricted to prevent unauthorized individuals from obtaining sensitive data.

- Media is defined as any printed or handwritten paper, received faxes, removable storage, back-up media, computer hard drives, and similar items.
- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- Procedures must be in place to help all personnel easily distinguish between employees and visitors, especially in areas where account data is accessible. "Employee" refers to full-time and part-time employees, temporary employees and personnel, instructors, and consultants who are resident on Institute sites. A "visitor" is a vendor, student guest, service personnel, or anyone who needs to physically enter the premises for a short duration, usually not more than one day.
- A list of devices, including POI terminals that accept payment card data, will be maintained. The list will include the make, model, location, and serial number or unique identifier of each device, and will be updated when devices are added, removed, or relocated.
- POS and POI device surfaces are periodically inspected to detect tampering or substitution.
- Personnel using the devices will be trained and aware of proper handling of POI devices.
- Personnel using the devices must verify the identity of any third party personnel claiming to repair, maintain, install, or replace devices.
- Personnel using the devices will be trained to report suspicious behavior and indications of tampering to the Information Security Officer.
- Strict control is maintained over the external or internal distribution of any media containing cardholder data, and distribution must be approved by management.
- Strict control is maintained over the storage and accessibility of media.
- All computers that store or access sensitive cardholder data must have a password-protected screensaver enabled to prevent unauthorized use.

7. Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

- Cardholder data (PAN, track data, etc.) must never be sent over the internet via email, instant chat, or any other end user messaging technology.
- If there is a business justification to send cardholder data via email or any other mode, it must be done only after authorization and by using a strong encryption mechanism (for example AES encryption, PGP encryption, or IPSEC).
- The transportation of media containing sensitive cardholder data to another location must be authorized by management, logged, and inventoried before leaving the premises. Only secure courier services may be used. The status of the shipment must be monitored until it has been delivered.

8. Disposal of Stored Data

- All data must be securely disposed of when no longer required by Union Centre Institute, regardless of the media or application type on which it is stored.
- An automatic process must exist to permanently delete online data when no longer required.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A quarterly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- The Institute will maintain procedures for the destruction of hard copy (paper) materials. These require that all hard copy materials are cross-cut shredded, incinerated, or pulped so they cannot be reconstructed.
- The Institute will maintain documented procedures for the destruction of electronic media. All cardholder data on electronic media must be rendered unrecoverable when deleted, for example through degaussing, secure wiping using industry accepted secure deletion standards, or physical destruction of the media. If secure wipe programs are used, the process must define the industry accepted standard followed.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked "To Be Shredded." Access to these containers must be restricted.

9. Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into Institute practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day to day practice.
- Distribute this security policy document to all employees to read. All employees must confirm that they understand the content of this document by signing the acknowledgement form in Appendix A.
- All employees who handle sensitive information will undergo background checks (such as criminal and credit record checks, within the limits of applicable law) before they commence employment with the Institute.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI DSS).
- Institute security policies must be reviewed annually and updated as needed.

10. Credit Card (PCI) Security Incident Response Plan

The Union Centre Institute PCI Security Incident Response Team (PCI Response Team) is comprised of the Information Security Officer and the staff responsible for tuition and payment processing. The Institute's PCI security incident response plan is as follows:

1. Each department must report an incident to the Information Security Officer (preferably) or to another member of the PCI Response Team.
2. The team member receiving the report will advise the full PCI Response Team of the incident.
3. The PCI Response Team will investigate the incident and assist the potentially compromised department in limiting the exposure of cardholder data and mitigating the risks associated with the incident.
4. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (card brands, payment processors, etc.) as necessary.
5. The PCI Response Team will determine whether policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred or for the Institute as a whole.

PCI Security Incident Response Team (roles, or their equivalent at the Institute):

- Executive Director / President
- Information Security Officer
- Compliance Officer
- Legal Counsel
- Finance / Bursar (Tuition and Payment Processing)
- Communications Lead
- Risk Manager

Incident Response Procedures

A department that reasonably believes it may have an account breach, or a breach of cardholder information or of systems related to the PCI environment in general, must inform the PCI Response Team immediately. After being notified of a compromise, the PCI Response Team, along with other designated staff, will implement the PCI Incident Response Plan to assist and augment the department's response.

Escalation Members

First level: Information Security Officer, Controller or Finance Lead, Director responsible for Tuition and Payment Processing, Legal Counsel, Risk Manager, Communications Lead.

Second level: Executive Director / President, Executive Leadership Team, Internal Audit, auxiliary members as needed.

External contacts (as needed): Merchant provider, card brands, internet service provider, internet service provider of the intruder (if applicable), communication carriers, business partners, insurance carrier, external response team (such as the CERT Coordination Center), and law enforcement agencies as applicable in the local jurisdiction.

In response to a systems compromise, the PCI Response Team and designees will:

1. Ensure the compromised system or systems are isolated from the network.
2. Gather, review, and analyze logs and related information from central and local safeguards and security controls.
3. Conduct appropriate forensic analysis of the compromised system.
4. Contact internal and external departments and entities as appropriate.
5. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required.
6. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions.

The card brands have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. These are outlined below.

Incident Response Notifications to Card Schemes

1. In the event of a suspected security breach, alert the Information Security Officer or your supervisor immediately.
2. The Information Security Officer will carry out an initial investigation of the suspected breach.
3. Upon confirmation that a breach has occurred, the Information Security Officer will alert management and begin informing all relevant parties that may be affected by the compromise.

Visa Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent and prevent further exposure.
- Alert all affected parties and authorities, including the merchant bank, Visa Fraud Control, and law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours.
- Consult the current Visa "What To Do If Compromised" guidance at visa.com for additional requirements.

Visa Incident Report Template

This report must be provided to Visa within 14 days after the initial report of the incident. The report must be securely distributed to Visa and the merchant bank. Visa will classify the report as "Visa Secret," the classification applied to Visa's most sensitive business information. The report must include:

1. **Executive Summary:** overview of the incident, risk level (High, Medium, Low), and whether the compromise has been contained.
2. **Background**
3. **Initial Analysis**
4. **Investigative Procedures:** including forensic tools used during the investigation.
5. **Findings:** number of accounts at risk and those compromised; type of account information at risk; identification of all systems analyzed and all compromised systems (DNS names, IP addresses, OS version, and function); timeframe of compromise; any data exported by the intruder; how and from

where the compromise originated; confirmation that all potential database locations (including backup, development, staging, and test environments and engineers' machines) have been checked to ensure no CVV2, Track 1, or Track 2 data is stored anywhere, encrypted or unencrypted; and, if applicable, a review of VisaNet endpoint security and risk.

6 **Compromised Entity Action**

7 **Recommendations**

8 **Contacts** at the Institute and the security assessor performing the investigation.

Mastercard Steps

1 Within 24 hours of an account compromise event, notify the Mastercard Compromised Account Team by phone at 1-636-722-4100.

2 Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured email to compromised_account_team@mastercard.com.

3 Provide the Mastercard Merchant Fraud Control Department with a complete list of all known compromised account numbers.

4 Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to Mastercard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).

5 Provide weekly written status reports to Mastercard, addressing open questions and issues, until the audit is complete to the satisfaction of Mastercard.

6 Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that Mastercard may request.

7 Provide findings of all audits and investigations to the Mastercard Merchant Fraud Control Department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of Mastercard.

Once Mastercard obtains the details of the account data compromise and the list of compromised account numbers, Mastercard will identify the issuers of the affected accounts, group all known accounts under the respective parent member IDs, and distribute the account number data to the respective issuers.

Discover Card Steps

1 Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102.

2 Prepare a detailed written statement of fact about the account compromise, including the contributing circumstances.

3 Prepare a list of all known compromised account numbers.

4 Obtain additional specific requirements from Discover.

American Express Steps

1 Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.

2 Prepare a detailed written statement of fact about the account compromise, including the contributing circumstances.

3 Prepare a list of all known compromised account numbers.

4 Obtain additional specific requirements from American Express.

Role of the Information Security Officer

Employees are expected to report any security related issue to the Information Security Officer. The role of the Information Security Officer is to effectively communicate all security policies and procedures to employees and contractors, oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in this document and at training sessions, and oversee the implementation of the incident response plan in the event of a sensitive data compromise.

11. Transfer of Sensitive Information Policy

- All third party companies providing critical services to Union Centre Institute must provide an agreed Service Level Agreement.
- All third party companies providing hosting facilities must comply with the Institute's Physical Security and Access Control Policy.
- All third party companies that have access to cardholder information must:

1. Adhere to the PCI DSS security requirements.
2. Acknowledge their responsibility for securing the cardholder data.
3. Acknowledge that the cardholder data must only be used for assisting the completion of a transaction, supporting a loyalty program, providing a fraud control service, or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster, or failure.
5. Provide full cooperation and access to conduct a thorough security review after a security intrusion by a payment card industry representative or a payment card industry approved third party.

12. User Access Management

- Access to Institute systems is controlled through a formal user registration process beginning with a formal notification from Human Resources or a supervisor.
- Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where suitable for the work carried out.
- There is a standard level of access; other services can be accessed when specifically authorized by Human Resources or line management.
- The job function of the user determines the level of access the employee has to cardholder data.
- A request for service must be made in writing (email or hard copy) by the newcomer's supervisor or by Human Resources. The request must state the name of the person making the request, the job title and workgroup of the newcomer, the start date, and the services required (default services are email, office productivity software, and internet access).
- Each user will be given a copy of their new user form to provide a written statement of their access rights, signed by an IT representative after their induction procedure. The user signs the form indicating that they understand the conditions of access.
- Access to all Institute systems is provided by IT and can only be started after proper procedures are completed.
- As soon as an individual leaves the Institute's employment, all of their system logons must be immediately revoked and their accounts disabled and removed.

- As part of the employee termination process, Human Resources (or supervisors in the case of contractors) will inform IT operations of all leavers and their date of leaving.

13. Access Control Policy

- Access control systems are in place to protect the interests of all users of Institute computer systems by providing a safe, secure, and readily accessible environment in which to work.
- The Institute will provide all employees and other users with the information they need to carry out their responsibilities as effectively and efficiently as possible.
- Generic or group IDs shall not normally be permitted, but may be granted under exceptional circumstances if sufficient other controls on access are in place.
- The allocation of privileged rights (for example local administrator, domain administrator, super-user, or root access) shall be restricted and controlled, and authorization provided jointly by the system owner and IT. Technical teams shall guard against issuing privileged rights to entire teams to prevent loss of confidentiality.
- Access rights will be granted following the principles of least privilege and need to know.
- Every user should attempt to maintain the security of data at its classified level even if technical security mechanisms fail or are absent.
- Users electing to place information on digital media or storage devices or to maintain a separate database must only do so where such an action is in accord with the data's classification.
- Users are obligated to report instances of non-compliance to the Information Security Officer.
- Access to Institute IT resources and services will be given through the provision of a unique user account and complex password.
- No access to any Institute IT resources and services will be provided without prior authentication and authorization of the user's account.
- Password issuing, strength requirements, changing, and control will be managed through formal processes. Password length, complexity, and expiration will be enforced through directory or identity management policy. Minimum standard: at least 12 characters, complex, unique, changed at first use, not reusable, and multi-factor authentication required for remote and administrative access.
- Access to Confidential, Restricted, and Protected information will be limited to authorized persons whose job responsibilities require it, as determined by the data owner or their designated representative. Requests for access permission to be granted, changed, or revoked must be made in writing.
- Users are expected to become familiar with and abide by Institute policies, standards, and guidelines for appropriate and acceptable usage of networks and systems.
- Access for remote users shall be subject to authorization by IT and be provided in accordance with this Information Security Policy. No uncontrolled external access shall be permitted to any network device or networked system.
- Access to data is controlled according to the data classification levels described in this policy.
- Access control methods include logon access rights, file share and NTFS permissions, user account privileges, server and workstation access rights, firewall permissions, web application authentication, database rights, isolated networks, and other methods as necessary.
- A formal process shall be conducted at regular intervals by system owners and data owners in conjunction with IT to review users' access rights. The review shall be logged and IT shall sign off the review to give authority for users' continued access rights.

Appendix A: Agreement to Comply With Information Security Policies

Union Centre Institute

Employee Name (printed) Department

I agree to take all reasonable precautions to assure that Union Centre Institute internal information, or information that has been entrusted to the Institute by third parties such as students, applicants, and customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the Institute, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policy, I have read and understand this policy, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Institute's security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and possibly criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the Information Security Officer.

Employee Signature Date

Appendix B: List of Devices

Approved technologies and devices, and the personnel with access to them. Update when devices are added, modified, relocated, or decommissioned.

Asset / Device Name	Description (make, model, serial)	Owner / Approved User	Location

Appendix C: List of Third Party Service Providers

Service providers with access to cardholder data, including payment processors, hosting providers, and student information or tuition platforms.

Service Provider	Contact Details	Services Provided	PCI DSS Compliant	PCI DSS Validation Date

Appendix D: Standalone and P2PE POI Management Policy

Where Union Centre Institute utilizes standalone or P2PE point of interaction (POI) devices, the following policies apply:

POI Device Inventory and Management

- Maintain an up-to-date inventory of all POI devices, including make, model, location, and serial number.
- Establish procedures for securely adding, relocating, and decommissioning POI devices.

Physical Security Measures

- Secure POI devices to prevent tampering or substitution, including the use of tamper-evident seals or enclosures.
- Regularly inspect devices for signs of tampering or substitution.
- Implement secure storage for devices not in use.

Device Inspection and Maintenance

- Conduct regular inspections and maintenance of POI devices to ensure they are functioning correctly and have not been compromised.
- Document and maintain a record of all inspections and maintenance activities.

Secure Configuration and Software Management

- Ensure that POI devices are configured securely and in compliance with PCI DSS requirements.
- Implement measures to prevent unauthorized changes to software and configuration settings.
- Regularly update POI device software, including patches for known vulnerabilities.

Access Controls

- Restrict access to POI devices to authorized personnel only.
- Use strong authentication methods for administrative access to POI devices.
- Implement role-based access controls and segregate duties to minimize the risk of unauthorized access or changes.

Appendix E: eCommerce Configuration and Hardening Policy

Where Union Centre Institute utilizes redirect or iFrame solutions to take payments online (for example tuition payments or enrollment deposits through the Institute website), the Institute must apply system configuration and hardening of these systems as follows:

Establish a Standard eCommerce Server Configuration

- Define a standard configuration for servers that includes necessary services, protocols, and settings.
- Ensure that vendor default accounts are changed, removed, or disabled.
- Disable unnecessary services and protocols to minimize vulnerabilities.
- Ensure that all security settings are aligned with industry best practices.

Implement Hardening Procedures

- Implement strong authentication and authorization mechanisms.
- Use file integrity monitoring tools to detect unauthorized changes.
- Enforce the use of antivirus and anti-malware solutions.

Control Administrative Access

- Limit access to server configurations to authorized personnel only.
- Use multi-factor authentication for administrative access.
- Maintain an audit trail of all access and changes made to server configurations.

Regularly Review and Update Configurations

- Periodically review server configurations against the established standard.
- Update the configurations in response to new threats, vulnerabilities, or changes in organizational needs.

Maintain a Vulnerability Management Program

- Regularly scan for vulnerabilities and address identified weaknesses.
- Include both software and physical components in vulnerability assessments.
- Establish a process to check for new security vulnerabilities using industry recognized sources and a risk ranking process based on industry best practices that identifies high risk vulnerabilities.
- Regularly update and patch operating systems and software to fix vulnerabilities.
- Apply applicable security patches within one month of release.

Document Control: Information Security Policy, Union Centre Institute. Effective September 15, 2026. Owner: Information Security Officer. Next scheduled review: September 2027.