NORTHERN PENNSYLVANIA REGIONAL COLLEGE

STND-5010-01: Information Security Standards
Origination: 05-10-2024
Effective: 07-09-2024
Reviewed: 07-09-2024
Last Updated: 06-06-2024

Information Security Standards

1. INTRODUCTION OF STANDARDS

1.1 Information Security Standards support the security posture of the Northern Pennsylvania Regional College (“NPRC” or “the College”). These Standards specify a required level of attainment of the College security controls and prescribe ways in which the College will enforce the Information Security Policy (NPRC-5010).

1.2 College entities may adopt supplemental standards, so long as they do not lessen or contradict NPRC-5010: Information Security and these Standards.

1.3 Standards are consistent with, and derived from, recognized standards organizations, including but not limited to, the National Institute of Standards (NIST), International Organization for Standards (ISO), and Federal Information Processing Standards (FIPS).

2. SECURITY OBJECTIVES

2.1 **CONFIDENTIALITY**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

2.2 **INTEGRITY**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

2.3 **AVAILABILITY**: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

3. INFORMATION TECHNOLOGY SECURITY STANDARDS

3.1 Access Control

3.1.1 System access is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

3.1.1.1 Authorized users are identified through a process that verifies the identity of the user when requesting a new account or system access with approval by the User’s supervisor or department head.

3.1.1.2 Active accounts are reviewed on a minimum of a quarterly basis.

3.1.2 The principle of least privilege is employed for provisioning user accounts, systems administration and/or privileged accounts, and security functions.

3.1.2.1 The goal of least privilege is that privileges no higher than necessary are authorized.

3.1.2.2 Allocation of privileges is limited to the minimum necessary.

3.1.2.3 Privileged accounts include superuser user accounts, superuser systems administrator accounts, and for development and implementation accounts.

3.1.2.4 User activity logging may be employed to monitor use of privileged accounts, and access authorizations may be configured to limit functions that are executable by accounts.

3.1.3 System access is limited to the types of functions that authorized users are permitted to execute.

3.1.3.1 Access privileges are defined by account, type of account, or both; i.e., through individual, shared, group, system, guest, emergency, developer, vendor, or temporary accounts. Other account attributes may be restrictions on time-of-day, point-of-origin.

3.1.4 Information posted or processed on publicly accessible systems is controlled and monitored.

3.1.4.1 Identify individuals authorized to post information on publicly accessible sites, and ensure procedures to review content prior to posting, and to remove content if posted inappropriately.

3.1.5 Unsuccessful logon attempts are limited to three (3).

3.1.6 Computer workstation screens will automatically lock after a period of thirty (30) minutes of inactivity.

3.1.7 Remote access sessions, via secure access channels, are limited to support functions unless specifically required.

3.1.8 Where possible, separate operational functions, system support functions (including management, programming, quality assurance, testing, security, etc.), and administration of audit functions to reduce the risk of malevolent activity without collusion.

3.1.9 Authorization is required for remote execution of privileged commands, and remote access to security-relevant information.

3.1.9.1 Identify and document commands and security-relevant information.

3.1.10 Protect wireless access using authentication and encryption.

3.1.11 Encrypt information on mobile devices and mobile computing platforms.

3.2 Cybersecurity Awareness and Training

3.2.1 Ensure that all users of organizational systems are made aware of the security risks associated with their activities; and of the applicable policies, standards, and procedures related to the security of those systems.

3.2.2 Provide training that will include an understanding of information security, necessity, and user actions to maintain security and respond to suspected incidents, and awareness of operations security.

3.2.3 Training will include email advisories, logon screen messages, awareness events, recognizing and reporting potential incidents introduced by staff and trusted partners (“insider threat”), and other methods.

3.2.3.1 Insider threat is a term describing vulnerabilities introduced by employees and trusted partners. It may include mistaken, negligent or malicious action that compromise security controls, for example, sending sensitive information to an unintended recipient via email, being unaware of or not following security policy and procedures, or deliberate unauthorized disclosure of information or bypass of security controls**.**

3.3 Audit and Accountability

3.3.1 Required for all College data/systems.

3.3.2 System audit logs are retained to enable monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

3.3.3 Ensure that the actions of individual system users can be uniquely traced to those users.

3.3.4 Re-evaluate the applicability of the types of logged events annually and adjust if warranted.

3.3.5 Ensure all internal system clocks are synchronized with an authoritative source to ensure the integrity of time stamps for audit records.

3.3.6 Failure of the audit logging process will trigger an alert to the Information Technology Department.

3.3.6.1 Alerts will be addressed by the Information Technology Department within 24 hours of the generation of the alert.

3.3.7 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

3.3.8 Limit management of audit logging functionality to a subset of privileged users.

3.4 Configuration Management

3.4.1 Required for all College data/systems.

3.4.2 Establish and maintain baseline configurations and inventories of College systems (including hardware, software, firmware, and documentation) throughout the system development life cycles.

3.4.3 Establish and enforce security configuration settings for information technology products employed in College systems.

3.4.4 Track, review, approve or disapprove, and log configuration changes to NPRC systems.

3.4.4.1 Change control includes proposal, justification, implementation, testing, review, and disposition of changes, including upgrades and modifications.

3.4.4.2 Changes include scheduled, unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

3.4.4.3 Analyze the security impact of changes prior to implementation.

3.4.5 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

3.4.6 Monitor installation of software by users and ensure compliance with NPRC-5010: Information Security and STND-5010-02: Technology and Equipment Use Standards.

3.5 Incident Response

3.5.1 Establish an operational incident-handling capability for College systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

3.5.2 Incident-related information can be obtained from sources including but limited to audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events.

3.5.3 Incident Response training will be provided by NPRC that links directly to assigned roles and responsibilities.

3.5.3.1 User training will include but not limited to identification and reporting of suspicious activity from external and internal sources.

3.5.3.2 System Administrator training will include but not limited to how to handle and remedy incidents, system recovery, and restoration.

3.5.4 Additionally, required for all users, entities, and data/systems with a College classification of Restricted:

3.5.5 Track, document, and report incidents to designated officials and/or authorities both internal and external to the College.

3.5.5.1 Incidents will be reported using FORM-5010-Security Incident Form.

3.5.6 Test the organizational incident response capability annually.

3.5.6.1 Incident response testing includes, for example, the use of checklists, walk-through or tabletop exercises, simulations (parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

3.6 Maintenance

3.6.1 Required for all College data/systems.

3.6.2 Perform maintenance on organizational systems including, but not limited to, installing patches, virus scans, and security scans.

3.6.3 Ensure equipment removed for off-site maintenance is sanitized of any sensitive information.

3.6.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

3.6.4.1 If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

3.6.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections; and terminate such connections when nonlocal maintenance is complete.

3.6.6 Supervise the maintenance activities of maintenance personnel without required access authorization (e.g., contractors, vendors, or consultants).

3.7 Media Protection

3.7.1 Sanitize or destroy system media before disposal or release for reuse; ensuring that any licensed software and data have been removed prior to reallocation or disposal. Attention will be taken to sanitize or destroy removable media.

3.7.2 Limit access to sensitive information on system media to authorized users, e.g. through physical controls or secure storage.

3.7.3 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8 Personnel Security

3.8.1 Required for all personnel with access to College data/systems.

3.8.2 Screen individuals prior to authorizing access to organizational systems containing sensitive information.

3.8.3 Ensure, through policy and procedures, that organizational systems containing sensitive information are protected during and after personnel actions such as terminations and transfers.

3.9 Risk Assessment

3.9.1 Annually assess the risk to College assets and operations (including mission, functions, image, or reputation); and to individuals resulting from the operation of College systems and the associated processing, storage, or transmission of sensitive information.

3.9.2 Continually, via cybersecurity tools, scan for vulnerabilities in College systems and applications, and address newly identified vulnerabilities.

3.9.3 Remediate vulnerabilities in accordance with risk assessments.

3.10 Security Assessment

3.10.1 Continually, via cybersecurity tools, assess the security controls in College systems to determine if the controls are effective in their application.

3.10.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

3.10.3 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.11 Systems and Communications Protection

3.11.1 Separate user functionality from system management functionality.

3.11.2 Prevent unauthorized and unintended information transfer via shared system resources.

3.11.2.1 Implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission; or otherwise protect by alternative physical safeguards.

3.11.3 Deny network communications traffic by default unless an exception is necessary for business needs.

3.11.4 Ensure that only connections that are essential and approved are allowed.

3.11.5 Terminate network connections associated with communication sessions at the end of the session(s) or after a defined period of inactivity.

3.11.6 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies by the implementation of guidelines based on the potential to cause damage to the system if used maliciously.

3.12 System and Information Integrity

3.12.1 Identify, report, and correct system flaws in a timely manner.

1.1 Monitor for security-relevant updates, i.e., patches, service packs, hot fixes, anti-virus signatures. Remediate in a timely manner noting the timeframe and remediation result documentation.

3.12.2 Provide protection from malicious code within College systems.

3.12.3 Update malicious code protection mechanisms when new releases are available.

3.12.4 Perform periodic scans of College systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

2.1 Monitor system security alerts and advisories and take action in response.

3.1 Monitor College systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.12.5 Identify unauthorized use of College systems as defined in STDN-5010-02: Technology and Equipment Use Standards.

4. EXCEPTIONS TO STANDARDS

4.1 Standard Exceptions may be considered when there is justifiable business case(s), resources are sufficient to implement and maintain the alternate configuration, and all NPRC policies and procedures are followed and upheld.

4.2 To request a Standards Exception, users will submit FORM-5010-03: Standards Exception Request to their supervisor in accordance with PROC-5010-03: Standards Exception Request.

5. USER VIOLATION

5.1 Users found to be in violation of these standards or NPRC-5010 Information Security may be subject to disciplinary action including, but not limited to, suspension of access to technology resources and/or any action defined in NPRC-3235: Behavioral Code of Conduct for Students and NPRC-2110: Employee Code of Conduct.

6. USER ACKNOWLEDGEMENT

6.1 All Users must acknowledge receipt of the Technology & Equipment Use Standards and the Information Security Standards by completing FORM-5010-04: Technology and Equipment Acceptable Use.

7. REVIEW STATEMENT

7.1 Standards are reviewed as needed or when the related policy is reviewed in accordance with CLDR-1310: Policy Review Schedule.

8. APPROVAL

______________________	___________________________	________
Name	Title	Date

Revision Notes: Standards in Origination