



**NORTHERN
PENNSYLVANIA**
REGIONAL COLLEGE

Policy: NPRC-5010: Security of Information
Technology

Origination: 3-4-2019

Approved: 04-12-2019

Effective: 04-12-2019

Reviewed:

Last Updated:

Subject: Security of Information Technology

1. PURPOSE

This policy establishes guidelines and responsibilities for Northern Pennsylvania Regional College Employees regarding information security and the protection of agency information resources.

2. SCOPE AND APPLICABILITY

This policy applies to all Users who have access to College information and to systems that store, access, or process the information, including, without limitation, Employees as defined herein.

The intent of this policy is to explain the range of acceptable and unacceptable uses of NPRC provided Information Technology (IT) resources and is not necessarily all-inclusive. IT resources may include anything with a processor, communications capability, or data storage. (Please refer to NPRC-5015, Technology Resources Acceptable Use, for a list of examples).

3. REFERENCES

- 3.1 INDX-0010 Master Policy Index
- 3.2 NPRC-5015 Technology Resources Acceptable Use
- 3.3 State of Pennsylvania Information Technology Security policies,
<https://www.oa.pa.gov/Policies/Pages/itp.aspx>.

4. DEFINITIONS

- 4.1 **Access** is the ability to locate, gain entry to, and use a directory, file, or device on a computer system or over a network.
- 4.2 **Access Control** is the enforcement of specified authorization rules based on positive identification of Users and the systems or data they are permitted to access.
- 4.3 **Authentication** is the process of verifying the identity of a User.
- 4.4 The **College** is the Northern Pennsylvania Regional College.
- 4.5 **Confidential Data** is information that is legally protected (i.e., student records) or otherwise deemed by a qualified expert to be unsuitable for open access.

- 4.6 A **Contractor** is anyone who has a contract with the College or one of its entities.
- 4.7 The **Director of Information Technology** is the person responsible for the College's information resources.
- 4.8 For the purposes of information technology and security policies, the term "**Employee**" shall include the following: staff, students, faculty, business associates, contractors, contractor's employees, subcontractors, volunteers, and individuals who are determined and notified by the institution to be subject to this policy. This definition does not create any additional rights or duties.
- 4.9 **Information Assets** are any of the data, hardware, software, network, documentation, and personnel used to manage and process information.
- 4.10 **Information Resources** are all information assets in all known formats.
- 4.11 **Information Security** represents the measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.
- 4.12 The **Information Security Administrator (ISA)** is the person designated by the Director of Information Technology to administer the agency's internal and external point of contact for all information security matters.
- 4.13 **Information Security Liaison(s) (ISL)** are Employees assigned by the ISA to assist in the protection of information resources.
- 4.14 An **Information Security Incident** is an event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.
- 4.15 **Information Technology (IT)** is the technology involved with the transmission and storage of information, especially the development, installation, implementation, and management of computer systems and applications.
- 4.16 **Medium** is any repository, including paper, used to record, maintain, or install information or data.
- 4.17 **Owner of Information** is the person(s) ultimately responsible for an application and its data viability.
- 4.18 A **Password** is a string of characters known to a computer system or network and to a User who must enter the password in order to gain access to an Information Resource.
- 4.19 **Personally Identifiable Information (PII)** includes all protected and non-protected information that identifies or can be used to identify, locate, or contact an individual.
- 4.20 **Risk Analysis** is the evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.
- 4.21 **Threat** – Includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.
- 4.22 For the purposes of this policy a **User** is a person authorized to access an information resource.

4.23 A **User ID** is a unique “name” by which each User is identified to a computer system.

5. POLICY

- 5.1 All Information Technology assets, including hardware, software, and data are owned by the College, unless excepted by contractual agreement.
- 5.2 Users are required to comply with legal protection granted to programs and data by copyright and license. No unauthorized software will be installed on College systems without the permission of the Information Technology Department.
- 5.3 Users will utilize, maintain, disclose, and dispose of all Information Resources, regardless of medium, according to law, regulation, and/or policy.
- 5.4 Employees must have no expectation of privacy while using NPRC provided Information Resources (i.e., cell phones, Internet, etc.).
- 5.5 The College reserves the right to filter Internet site availability, and to monitor and review Employee use as required for legal, audit, or legitimate authorized College operational or management purposes. By logging into their College-provided account, Users are acknowledging that they have read the document and agree to follow its provisions.
- 5.6 All Users must adhere to rules regarding unacceptable use of technology resources. (For a detailed list of unacceptable uses, see NPRC-5015, Technology Resources Acceptable Use).
 - 5.6.1 Users must not download, attach, change, distribute, or install any software or inappropriate files, including streaming content, for non-business functions (i.e., downloading MP3 files and/or broadcast audio or video files).
 - 5.6.2 User must not intentionally introduce a virus into a College-provided computer or withhold information necessary for effective virus control procedures.
 - 5.6.3 Users must not send or share Confidential information for unauthorized purposes.
 - 5.6.4 Users must not attach or use devices on the College network that are not owned or authorized by the College.
 - 5.6.5 Employees must not redirect Confidential or privileged College data to a non-College owned computing device without proper authorization.
 - 5.6.6 Users must not use unauthorized peer-to-peer networking or peer-to-peer file sharing.
 - 5.6.7 Employees must never execute programs or open e-mail attachments that have not been requested or come from an unknown source. If in doubt and lacking assurance from the sender, Employees should contact the Information Technology Department for assistance.
 - 5.6.8 Users must never attempt to disable, defeat, or circumvent any security firewall, proxies, web filtering programs, or other security controls.

- 5.6.9 Users must not use technology resources to promote harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability.
- 5.7 The Director of Information Technology, working with designated individuals, will develop procedures to protect information resources from accidental, unauthorized, or malicious access, disclosure, modification, or destruction.
- 5.8 Users must report any observation of attempted security or privacy violations to the Information Technology Department
 - 5.8.1 An Information Security Incident is any event that involves misuse of computing resources or is disruptive to normal system or data processing operations. Examples include, but are not limited to the following:
 - 5.8.1.1 Lost or stolen computers or other portable devices;
 - 5.8.1.2 Lost or stolen media that contains sensitive data;
 - 5.8.1.3 Rampant computer virus infections within the NPRC network;
 - 5.8.1.4 Loss of system or network functionality;
 - 5.8.1.5 A disaster scenario or act of terrorism;
 - 5.8.1.6 A prolonged power outage;
 - 5.8.1.7 A compromised (hacked) computer or server;
 - 5.8.1.8 A defaced Web page; and
 - 5.8.1.9 An information security policy violation.
- 5.9 Users should immediately report all Information Security Incidents to the Information Technology Department. Users must provide the following information to the extent possible:
 - 5.9.1 Point of contact (name, phone, e-mail);
 - 5.9.2 Characteristics of incident;
 - 5.9.3 Date and time the incident was detected;
 - 5.9.4 Extent of impact;
 - 5.9.5 Nature of incident, if known (i.e., unauthorized access, system breach or malfunction, data loss or exposure, defacement, other); and
 - 5.9.6 Any actions took in response to the incident.
- 5.10 Confidential, private, personally identifiable information (PII), Federal Tax Information (FTI), or other sensitive data (i.e., credit card numbers, calling card numbers, logon passwords, health information, or other protected information), must be encrypted or dissociated from any individual prior to transmission through any public data communications infrastructure, such as a network or the Internet.
- 5.11 Employees must immediately contact the Information Technology Department upon receiving or obtaining Confidential information to which the Employee is not entitled

or becoming aware of any inappropriate use of College-provided technology resource (Note: The owner or sender of such information must also be notified).

- 5.12 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any College-provided Technology Resource, or if questions arise regarding acceptable or unacceptable uses. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.
- 5.13 Access controls must be consistent with all state and federal laws and statutes and will be implemented in accordance with this policy.
- 5.14 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.
 - 5.14.1 All passwords are Confidential and must not be shared under any circumstances.
 - 5.14.2 Employees are expected to use strong passwords, which must conform to established standards and will be changed at intervals designated by the Director of Information Technology.
- 5.15 All access to computing resources will be granted on a need-to-use basis.
- 5.16 Individual Users will be assigned unique User ID's.
- 5.17 Each User must be accountable for securing his or her computer, and for any actions that can be identified to have originated from it.
- 5.18 The Information Technology Department will provide network User accounts by adding, modifying, and deleting User access.
 - 5.18.1 When an Employee is terminated, the unit's designated approval authority must contact the Information Technology Department immediately to disable all access, unless otherwise approved in writing by appropriate management.
- 5.19 All employees may be required to complete information security awareness as part of job orientation.
- 5.20 The authorized head of each department must assure that all Employees read this policy and understand that logging in to any system with College-provided credentials is an acknowledgment that the Employee has read, fully comprehends, and will abide by College policies and procedures regarding privacy and information security.
- 5.21 The department head must assure that all Employees, and others who access computer systems, will receive sufficient training in policies and procedures, security requirements, correct use of Information Resources, and other administrative controls.
- 5.22 Background checks may be conducted by the College's Human Resources department consistent with other College policies.
- 5.23 Information Resources are designated for authorized purposes. The College has a right and a duty to review questionable Employee activity. This must not include any unauthorized uses (See NPRC-5015, Technology Resources Acceptable Use), and must not interfere with the legitimate business of the College.

- 5.24 All information assets must be accounted for and have assigned owners. Owners, custodians, and users of information resources must be identified, and their responsibilities defined and documented.
- 5.25 Each owner or custodian of information will determine and document classification based on the circumstances and the nature of the information. Classification should consider legal protections, privacy, sensitivity, and criticality to the functions of the business.
- 5.26 The owner or custodian will determine and document the data classification, and the Information Technology Director will ensure the protective guidelines that apply for each level of information. They include, but are not limited to the following:
- 5.26.1 Access;
 - 5.26.2 Use within the College;
 - 5.26.3 Disclosure outside the College,
 - 5.26.4 Electronic distribution; and/or
 - 5.26.5 Disposal / Destruction.
- 5.27 If at any time equipment or Media changes ownership or is ready for disposal, the User must alert the responsible technical staff to the potential presence of any Confidential and/or sensitive data on said equipment or Media.
- 5.28 Information resource facilities will be physically secured by measures appropriate to their critical importance.
- 5.29 Security vulnerabilities will be determined, and controls will be established to detect and respond to threats to facilities and physical resources.
- 5.30 Employees must guard against access to files and take precautions to protect technology devices when away from the workstation. This includes but is not limited to the following:
- 5.30.1 Logging off the computer;
 - 5.30.2 Locking the computer; and/or
 - 5.30.3 Locking the file cabinets and drawers.
- 5.31 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.
- 5.32 Equipment will be secured and protected from physical and environmental damage.

6. RESPONSIBILITIES AND TIMELINES

- 6.1 The Director of Information Technology is assigned the role of Information Security Administrator (ISA). The ISA must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy. If necessary, the ISA may delegate duties to one or more individuals (i.e., ISL's) whose main function will be to assist in the protection of information resources within their agency.

- 6.2 The ISA will ensure that a risk management program will be implemented and documented, and that a risk analysis will be conducted periodically.
- 6.3 The ISA will oversee and ensure that cost effective contingency response and recovery plans will be maintained, providing for prompt and effective restoration of critical business functions in the event of any disruptive incident.
- 6.4 Procedures, guidelines, and mechanisms utilized during an Information Security Incident, along with the roles and responsibilities of the incident management teams, must be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.
- 6.5 Testing will be performed at intervals according to industry best practices.

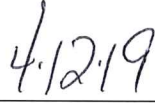
7. REVIEW STATEMENT

This policy shall be reviewed on a regular basis at least once every five years per the Policy Review Schedule established by the President or his designee. A review of the policy may be requested prior to the timeframe outlined by the policy review schedule by any student, faculty, staff, administrator, or board member. Such a request must be submitted in writing to the office of the President and must address specific concerns. Upon receipt of such a request, a complete review of the policy will be conducted within three months. Upon review, the President or President's designee may recommend to the Board of Trustees that the policy be amended or repealed.

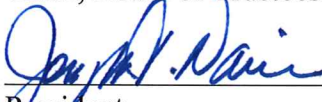
8. SIGNATURES



Chair, Board of Trustees



Date



President



Date

Attachments: None

Distribution: Board of Trustees; regionalcollegepa.org

Revision Notes: Policy in Origination