# Information Security

## 1. PURPOSE

This policy establishes guidelines and responsibilities for Northern Pennsylvania Regional College ("NPRC" or "College) technology users regarding information security, protection of College information resources, and the parameters for the use and operation of NPRC computing systems, telecommunications, and network resources.

## 2. SCOPE AND APPLICABILITY

This policy applies to all technology users who have access to College information resources, including employees, guests, students, and external entities.

## 3. REFERENCES

3.1 INDX-1310-01: Master Policy Index
3.2 CLDR-1310: Policy Review Schedule
3.3 3.3INDX-1310-02: Document Naming
3.4 NPRC-2110: Employee Code of Conduct
3.5 NPRC 2120: Corrective Action
3.6 NPRC-3235: Behavioral Code of Conduct for Students
3.7 NPRC-3225: Academic Code of Conduct for Academic Students
3.8 NPRC-3240: Educational Rights and Privacy (FERPA)
3.9 NPRC-3311 Instructor Code of Conduct
3.10 NPRC-4010: Workforce Instructor Code of Conduct
3.11 STND-5010-01: Information Security Standards
3.12 STND-5010-02: Technology and Equipment Use Standards
3.13 PROC-5010-01: Reporting a Security Incident
3.14 FORM-5010-01: Security Incident Report
3.15 PROC-5010-02: Equipment Loan
3.16 FORM-5010-02: Equipment Loan Request
3.17 PROC-5010-03: Standards Exception Request

3.18 FORM-5010-03: Standards Exception Request

3.19 FORM-5010-04: Technology and Equipment Acceptable Use

3.20 State of Pennsylvania Information Technology Security policies, https://www.oa.pa.gov/Policies/Pages/itp.aspx.

3.21 Pennsylvania Right-to-Know Statute, (65 P.S. 67.101)

## 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 Confidential Information is defined as information disclosed to an individual employee or known to that employee because of the employee's employment at NPRC, and not generally known outside NPRC, or is protected by law. Examples of "Confidential Information" include but are not limited to – student grades; financial aid information; social security numbers; payroll and personnel records; health information; self-restricted personal data; credit card information; information relating to intellectual property such as an invention or patent; research data; passwords and other IT-related information; and NPRC financial and account information. Individual offices, units, divisions, or programs may have additional types or kinds of information that are considered "Confidential Information." "Confidential Information" may include written documents or records or electronic data.

4.3 A Contractor is anyone who has a contract with the College or one of its entities.

4.4 An Employee shall mean any individual who serves the College in a full-time or part-time capacity as an administrator, staff, or faculty.

4.5 Information Resources are any of the data, hardware, software, network, documentation, and personnel used to manage and process information, in all known formats.

4.6 Information Security Standards represent 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.

4.7 Technology and Equipment Use Standards represent the expectations and guidelines for acceptable use and operation of information technology.

4.8 Information Security Incident is an event characterized by unexpected and unwanted system behavior, breach, or unintended alteration of data.

4.9 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.

4.10 Security represents those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

4.11 Equipment shall refer to the computer, tablet, distance learning unit, power cord, charging brick, College-issue mobile phone, and, in some instances, protective case assigned or loaned to a User.

4.12 User shall include the following: faculty, staff, employees, students, contractors, subcontractors, employees of contractors, volunteers, business associates, and any other persons who are determined and notified by the College to be subject to this policy. This definition does not create any additional rights or duties.

## 5. POLICY

5.1 NPRC will maintain and enforce STND-5010-01: Information Security Standards to govern information technology practices and protection of information at the College.

5.2 All Information Resources, including hardware, software, and data are owned by the College, unless excepted by contractual agreement.

5.3 Access controls must be consistent with all state and federal laws and statutes and will be implemented in accordance with this policy.

5.4 All access to information resources will be granted on a need-to-use basis.

5.5 NPRC will maintain and enforce STND-5010-02: Technology and Equipment Use Standards.

5.6 The Department of Information Technology will provide users with access to Information Resources as required by the users' role at the College.

5.7 The Director of Information Technology or designee must assure that all users will receive sufficient training in policies and procedures, security requirements, correct use of information resources, and other administrative controls.

5.8 Information resource facilities will be physically secured by measures appropriate to their critical importance.

5.9 Security vulnerabilities will be identified, and controls will be established to detect and respond to threats to facilities and physical resources.

5.10 Procedures, guidelines, and mechanisms utilized during an information security incident, along with the roles and responsibilities of the incident management teams, will be established, documented, and periodically reviewed. This may include testing to make sure that all plans remain current, viable, and comprehensive.

5.10.1 Testing will be performed at intervals according to industry best practices. At a minimum, testing will occur every six (6) months.

5.11 Confidential Information handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

5.12 Equipment will be secured and protected from physical and environmental damage.

5.13 The NPRC computing, telecommunications and networking resources are provided for the support of the instructional, research, and administrative activities of the College. Use of these resources is a privilege granted by the College and it reserves the right to limit, restrict or extend access to these electronic resources.

5.14 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.

5.15 Violation(s) of this policy may result in the restriction or loss of access to technology resources or additional disciplinary action(s) per NPRC-2110: Employee Code of Conduct, NPRC-2120: Corrective Action, NPRC-3225: Academic Code of Conduct for Academic Students, NPRC-3235: Behavioral Code of Conduct for Students, NPRC-3311: Instructor Code of Conduct, NPRC-4010: Workforce Instructor Code of Conduct, and NPRC-3240: Educational Rights and Privacy (FERPA).

## 6. RESPONSIBILITIES AND TIMELINES

6.1 The Director of Information Technology, Safety, and Facilities or designee must perform, contract, or delegate the necessary functions and responsibilities of the position as defined in this policy. If necessary, duties may be delegated to one or more individuals whose main function will be to assist in the protection of information resources within their department or division including:

6.1.1 The Department of Information Technology, Safety, and Facilities will ensure that a risk management program will be implemented and documented, and that a risk analysis will be conducted periodically.

6.1.2 The Director of Information Technology, Safety, and Facilities or designee 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.

6.1.3 The Director of Information Technology, Safety, and Facilities is the person responsible for the maintenance and security of the College's information resources.

6.1.4 The Director of Information Technology, Safety, and Facilities or designee is the person responsible for responding to reports of suspicious or questionable activities associated with maintenance and security of the College's information resources.

6.2 The Registrar or designee is responsible for collecting student acknowledgement of receipt of the Security Information Standards upon registration.

6.3 The Director of Human Resources or designee is responsible for collecting employee acknowledgement of receipt of Security Information Standards upon hiring.

6.4 The Vice President of Finance and Operations is responsible for the administration of this policy.

## 7 REVIEW STATEMENT

Review of this policy will occur in alignment with CLDR-1310: Policy Review Schedule.

## SIGNATURES

*Signature on file*

_____ _____
Chairperson, Board of Trustees Date

*Signature on file*

_____ _____
President Date

Revision Notes: Policy in Revision