University Policy

Volume I1: Information Technology	**I1.02.3** **Software Applications Security**	**Responsible Office:** University Technology Services
Chapter 02: Data Security	**Effective Date:** 04/01/2013 **Last Revision:** 12/01/2014	**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

In order to protect the integrity of its information systems, Northeastern Illinois University will establish procedures to authorize access to software containing Personally Identifiable Information (PII) used by employees. The University will work to ensure a secure office environment with regard to all University data systems.

PURPOSE OF THE POLICY

The purpose of this policy is to establish specific procedures to protect Personally Identifiable Information (PII) from misuse or unauthorized exposure.

WHO IS AFFECTED BY THIS POLICY

All University faculty and staff and authorized contractors.

DEFINITIONS

Authorized Contractors: Vendors that the University has entered into an agreement with through the procurement process to perform specific operations. These vendors are granted restricted server, database and/or application access to perform specific tasks.

Data Custodians: Individuals responsible for the accuracy and completeness of data files under their control including the maintenance and control of the various validation and rules tables. These tables, and processes related to their use, define how business is conducted at the University.

NEIUworks Enterprise Resource Planning (ERP) Applications: A compilation of software applications. Primarily the Ellucian Banner Application (Internet Native Banner (INB)) which comprises Financial Aid, Constituent Relationship Management (CRM), Student, Human Resources and Finance modules. Additional software applications within the NEIUworks ERP include Collegenet, Evisions, Cognos, NOLIJ, Touchnet, Xtender, and other software applications.

Applications outside the NEIUworks ERP: Other applications with access to sensitive Personally Identifiable Information (PII) data, such as, but not limited to, Razor's Edge, and Desire2Learn.

Personally Identifiable Information (PII): Information that can be used to specifically identify an individual. Data included within this definition includes but is not limited to social security number, last name, first name, date of birth, driver's license number, state identification number, university identification number, or information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

Security Audit: Process whereby University Technology Services (UTS) and/or Data Custodians periodically requires verification of the appropriate access to software applications.

REGULATIONS

5 ILCS 179/ Identity Protection Act
Health Insurance Portability and Accountability Act (HIPAA), P.L. 104-191
Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102
Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232

PROCEDURES

1. ACCESS

Only employees who are required to access PII in the course of performing their assigned duties will be permitted access by the appropriate Data Custodian.

Some employees, primarily faculty, will automatically receive restricted access to student data as they are teaching these students and their teaching assignments are recorded in the Ellucian Banner Application.

Access to data will not be approved for use outside a user's official University responsibility without review and approval by the employee's supervisor and the appropriate Data Custodian.

Access to NEIUworks ERP Applications: Employees who require access to any of the NEIUworks ERP Applications must submit a request to University Technology Services (UTS) Applications Department for access using one or all of the appropriate NEIUworks request forms.

Request forms must be complete and include:

- The employee's signature in the appropriate location(s)
- Signature of the employee's supervisor as authorization/confirmation that the employee's security access as identified is appropriate

Access to Applications outside the NEIUworks ERP: Employees who require access to any application containing PII outside of the NEIUworks ERP must contact the appropriate Data Custodian who is authorized to grant access.

2. AUDITING

NEIUworks ERP: All employees who have access to any of the applications within the NEIUworks ERP environment in the course of performing their assigned duties must participate in regularly scheduled NEIUworks security audits to protect the confidentiality of all data within the NEIUworks ERP environment.

Compliance with the security audit will include the receipt and detailed review of access by application, the acknowledgement of access and the written confirmation of familiarity with the related University policies as well as state and federal mandates and laws.

Any employee who fails to respond to the NEIUworks security audit or fails to act appropriately as defined by the guidelines referenced in this policy will have their access terminated.

In addition, a report of login access violations (locking of accounts, attempts to log into unassigned modules, etc) will be automatically produced on a regular basis and sent to the appropriate system and data administrators for review and follow-up. All login access violation entries will be actively assessed for unauthorized access attempts to the NEIUworks ERP application. Follow-up by the system and/or data administrators will include contacting the user(s) with access violations, determining the cause of the violation, scheduling additional training if needed, and recording of the disposition and resolution of the violation.

Applications outside the NEIUworks ERP: All employees who have access to any of the application outside of the NEIUworks ERP environment in the course of performing their assigned duties must participate in regularly scheduled security audits by the appropriate Data Custodian to protect the confidentiality of all data.

Compliance with the security audit will include the receipt and detailed review of access by application, the acknowledgement of access and the written confirmation of familiarity with the related University policies as well as state and federal mandates and laws.

Any employee who fails to respond to the security audit or fails to act appropriately as defined by the guidelines referenced in this policy will have their access terminated.

GUIDELINES

Data, and information derived from data, are vital assets owned by the University.

The University is required to protect the security and confidentiality of data while creating procedures that do not unduly interfere with the efficient conduct of University business.

The University will ensure a secure office environment with regard to all University data systems.

All University data and information, whether maintained in a central database or copied into other data systems (e.g. personal computers) remain the property of the University.

HISTORY

Formerly, Security Audit Interim Policy effective 4/1/2013

APPENDIX

UTS Request Forms (Found on the Technology Applications channel within the Employee tab on NEIUport)

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Acceptable Use
Release of Information Pertaining to Students
Data Standards Document
Data Security Breach

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
Chief Information Officer	773-442-4357	helpdesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.