Northeastern Illinois University

NEIU POLICY

Volume I1: Information Technology	**I1.02.2** **Data Security Breach**	**Responsible Office:** University Technology Services
Chapter 02: Data Security	**Effective Date:** 04/01/2013 **Last Revision:** 10/01/2013	**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

State and federal laws require that NEIU have a policy in place that addresses breaches of security involving personal information.

PURPOSE OF THE POLICY

The purpose of this policy is to comply with both State of Illinois and Federal regulations related to breaches in data security as defined by the applicable State and Federal laws and regulations.

WHO IS AFFECTED BY THIS POLICY

University staff, faculty, contractors and students are affected by this policy.

DEFINITIONS

Data Subject To Security Breach: the definition is provided by the Illinois Personal Information Protection Act, and currently includes:

- Social Security number
- Driver's license number or State Identification card number
- Account number or credit or debit card number

Additionally, institutions of higher education are responsible for the privacy of data included in the Family Educational Rights and Privacy Act (FERPA), such as records that directly relate to a student and that are maintained by an educational agency or institution or by a party acting for the agency or institution.

Such records may include:

- Written documents; (including student advising folders)
- Computer media;
- Microfilm and microfiche;
- Video or audio tapes or CDs;
- Film;
- Photographs

Any record that contains personally identifiable information that is directly related to the student is an educational record under FERPA. This information can also include records kept by the school in the form of student files, student system databases kept in storage devices such as servers, or recordings or broadcasts which may include student projects.

Two Types of Educational Records

There are two types of educational records as defined under FERPA. Each type of educational record is afforded different disclosure protections.

DEFINITIONS (CONTINUED)

Directory Information
Some information in a student's educational record is defined as directory information under FERPA. Under a strict reading of FERPA, the school may disclose this type of information without the written consent of the student. However, the student can exercise the option to restrict the release of directory information by submitting a formal request to the school to limit disclosure. Directory information may include:

- Name
- Address
- Phone number and email address
- Dates of attendance
- Degree(s) awarded
- Enrollment status
- Major field of study

Non-directory Information
Non-directory information is any educational record not considered directory information. Non-directory information must not be released to anyone, including parents of the student, without the prior written consent of the student. Further, faculty and staff can access non-directory information only if they have a legitimate academic need to do so. Non-directory information may include:

- Social security numbers
- Student identification number
- Race, ethnicity, and/or nationality
- Gender
- Transcripts; grade reports

Transcripts are non-directory information and, therefore, are protected educational records under FERPA.

REGULATIONS

815 ILCS 530/ Personal Information Protection Act
Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102
Health Insurance Portability and Accountability Act (HIPAA), P.L. 104-191
5 ILCS 179/ Identity Protection Act
Illinois Social Security Number Protection Task Force Report
Family Educational Rights and Privacy Act, 20 U.S.C. §1232

PROCEDURES

It is the responsibility of each University staff, faculty, contractor and student to notify the office of the Chief Information Officer, University Technology Services (UTS), of any known or suspected data security breach as identified in this document.

It is the responsibility of the Chief Information Officer to facilitate an appropriate investigation of suspected breaches of security, to notify officials and affected individuals in accordance with applicable State and Federal regulations, and to assure maintenance of this document according to the policy stated herein.

Subject	Responsible	Contact	Phone Number
Report Data Security Breach immediately	Staff, Faculty, Student or Contractors and students with knowledge or reasonable suspicion of data security breach	Chief Information Officer, University Technology Services (UTS)	773-442-4190
Facilitate investigation of possible data security breach immediately.	Chief Information Officer, University Technology Services (UTS)	University Technology Services (UTS) Technical Staff	773-442-4190
Report on technical investigation and assessment immediately	University Technology Services (UTS) Technical Staff	Chief Information Officer, University Technology Services (UTS)	773-442-4190

PROCEDURES (CONTINUED)

Subject	Responsible	Contact	Phone Number
Report Data Security Breach to State of Illinois Social Security Number Task Force (breaches involving SSNs)	Chief Information Officer, University Technology Services (UTS)	Illinois Attorney General SSN Protection Task Force 100 W. Randolph, 12th Flr. Chicago, IL 60601	217-782-8198 Fax: 217-782-2906
Report Data Security Breach to General Assembly within 5 business days of discovery of the event	Chief Information Officer, University Technology Services (UTS)	State Representative, currently John D'Amico, jdamico@ilga.gov	217-782-8198 Fax: 217-782-2906
Notify affected or possibly affected individuals within 5 business days of discovery of the event	Chief Information Officer, University Technology Services (UTS)	Individuals impacted	n/a
Annual Report on Data Security Breach (if a breach has been discovered in that year)	Chief Information Officer, University Technology Services (UTS)	State Representative, currently John D'Amico, jdamico@ilga.gov	217-782-8198 Fax: 217-782-2906

GUIDELINES

State and Federal laws and regulations may change at any time. While this document refers the reader to applicable State and Federal laws or regulations for the most up-to-date information possible, in order to maintain relevancy, this Data Security Breach Policy shall be reviewed annually, beginning one year from the acceptance date.

RELATED POLICIES, DOCUMENTS AND LINKS

Application Access and Security Policy
Identity Protection Policy

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	E-Mail
Chief Information Officer	773-442-4374	k-tracy@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 a 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.