University Policy

Volume I1: Information Technology	I1.02.2 **Information Security Incident Management** **Interim Policy** **Effective Date:** 04/01/2013 **Last Revised:** 06/30/2022	**Responsible Office:** University Technology Services
Chapter 02: Data Security		**Responsible Officer:** Information Security Officer

POLICY STATEMENT

Northeastern Illinois University is committed to ensuring that information security incidents (including data breaches) are managed promptly and appropriately to limit the University's and individuals' exposure to risks resulting from these incidents.

PURPOSE OF THE POLICY

The purpose of this policy is to establish a consistent and effective approach for responding to and recovering from information/cyber security incidents (including data breach) promptly and appropriately, and to ensure the University complies with both the State of Illinois and Federal regulations that govern personal data breach incidents.

WHO IS AFFECTED BY THIS POLICY

Students, faculty, staff and other users of the University's information and IT Resources (ITR)

DEFINITIONS

Information Security Incidents: Information security incidents are events that have resulted or may result in unauthorized disclosure of, damage to, loss or unavailability of personal data (held by the University) or University information and/or ITR. Not all information security incidents are necessarily personal data breaches. Some may result in a breach of personally identifiable information. Examples include:

- Loss or theft of sensitive or personal information or a media that holds such information
- Unauthorized or accidental access, modification or handling of information or information systems (including inappropriate access privileges to information systems leading to inappropriate disclosure of information)
- Unauthorized or accidental disclosure of sensitive or personal information
- Damage to, destruction or loss of sensitive or personal information
- Compromised user accounts (e.g. disclosure of user login details through phishing, sharing, public display or as a result of a compromised IT system)
- Failed or successful attempts to gain unauthorized access to University information or information systems through any means
- Disruption to or denial of IT service, or system failure resulting in unavailability of IT services and/or information
- Malware infection
- Unauthorized system or file encryption

- Inappropriate disposal of sensitive or personal information or IT equipment that holds such information

Data Breach: This is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personally identifiable information.

Personally Identifiable Information (PII): This is any type of data that can be used to identify an individual directly or indirectly. This includes but is not limited to social security numbers, contact details such as phone numbers, physical address, email, address, employee or student ID, etc.

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 but are not limited to:

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

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.

Educational Records Types
There are two types of educational records as defined under FERPA; directory and non-directory information. Each type of educational record is afforded different disclosure protections.

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 the 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 the 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 or NetID
- 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

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 security incident.

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.

PROCEDURES

University Internal Incident Reporting

Subject	Responsible	Who to Contact
Report a suspected or actual incident immediately or as soon as practicable	Student, faculty, staff or contractors with the knowledge or reasonable suspicion of a security incident	University Technology Services helpdesk@neiu.edu
Facilitate investigation of the incident	Chief Information Officer, University Technology Services (UTS)	University Technology Services Technical Team
Investigate the incident and report on the assessment, findings and mitigation steps taken.	University Technology Services Relevant Technical Team	Chief Information Officer, University Technology Services

Incident Reporting and Communication to External Parties

Subject	Responsible	Who to Contact
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
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, 15th District, Michael Kelly mike@repkelly.com
Report to State and Federal agencies		
Notify affected or possibly affected individuals within 5 business days of discovery of the event	Chief Information Officer, University Technology Services (UTS)	Individuals impacted
Annual Report on Data Security Breach (if a breach has been discovered in that year)	Chief Information Officer, University Technology Services (UTS)	State Representative, 15th District, Michael Kelly mike@repkelly.com

Incident Response and Management

The CIO will initiate an investigation which will be carried out by the relevant team responsible for the area where the incident occurred. If the incident relates to a breach of personally identifiable information, University General Counsel and the Risk Management Officer will lead the investigation and will work with the CIO to ensure proper management of the incident and make an insurance claim as applicable.

Investigation of an incident should start within 24 hours of the incident being discovered, where possible. The investigation should establish the nature of the incident, and the type of data involved and will consider the extent of a system compromise or the sensitivity of the data. A risk assessment should be performed as to what might be the consequences of the incident, for instance, whether access to data or IT services could become disrupted or unavailable.

Where personally identifiable information is breached, the risk assessment will consider whether there is a risk to individuals and to what extent by taking into account the likelihood of the risk occurring, its impact and consequences. The risk assessment will help determine whether the incident should be reported to the State and Federal agencies and whether data subjects should be informed.

Evidence to support an investigation will be collected as soon as possible and safeguarded to ensure the integrity of the evidence is preserved for forensics and legal admissibility if applicable.

The incident management team will determine the appropriate course of action and the required resources needed to contain the incident and limit its impact. This might require isolating a compromised section of the network, alerting relevant staff or shutting down critical equipment or IT service.

Appropriate steps will be taken to recover system or data losses and resume normal business operations. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords or disabling a user account for an extended period during an investigation.

University Technology Services will lead all investigations relating to a cybersecurity incident and will work with internal teams and external investigators as assessed necessary to appropriately respond to and manage such incidents.

HISTORY

Revised: 06/00/2022; formerly Data Security Breach
Revised: 10/01/2013
Effective date: 04/01/2013

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Information Security Policy
Acceptable Use of Information Technology Resources
University Email

CONTACT INFORMATION

Please direct questions or concerns about this policy to

Contact	Phone	Email
Help Desk	(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.