NORTHWESTERN STATE

Information Technology Policies and Standards

Computer Systems Security Breach Policy

Purpose:

Northwestern State University shall provide timely and appropriate notice to affected individuals when there is reasonable belief that a breach in the security of private information has occurred. A breach in security is defined as an unauthorized acquisition of information, typically maintained in an electronic format by the University.

Scope:

Attacks on University IT resources are infractions of the Acceptable Use Policy constituting misuse, or they may be vandalism or other criminal behavior. Reporting information security breaches occurring on University systems and/or on University networks to appropriate authorities is a requirement of all persons affiliated with the University in any capacity, including staff, students, faculty, contractors, visitors, and alumni.

Policy Statement:

Suspected or confirmed information security breaches must be reported to University authorities. This includes the affected department head of director, as well as the CIO.

The CIO will investigate the report, and if a security breach of private and/or highly sensitive information may have occurred, will inform the President and appropriate Vice-President(s), and/or law enforcement, as appropriate.

In the event that a public notification of the security breach may be warranted, the CIO will consult with the President, Vice President(s), Provost, and General Counsel to develop the response and make the final determination if a public notification of the event is warranted.

Procedures:

The entity responsible for support of the system or network under attack is expected to:

1. Report the attack to their management and to the Deputy CIO
2. Block or prevent escalation of the attack, if possible
3. Follow instructions communicated from the Deputy CIO in subsequent investigation of the incident and preservation of evidence

4. Repair the resultant damage to the system

Internal Notifications

The Deputy Chief Information Officer will report serious computer security breaches to the Chief Information Officer (CIO) in a timely manner. The CIO will consult the President and VP's as appropriate, and decide upon appropriate next steps. This determination may be made prior to completion of the investigation of the security breach. The CIO will report the incident to the Department of Public Safety, the appropriate Judicial Representative, and/or the University General Counsel when, based on preliminary investigation, criminal activity has taken place and/or when the incident originated from a University computer or network.

Determination of External Notification

To determine if unencrypted private or highly sensitive information has been acquired, or is reasonably believed to have been acquired by an unauthorized person, the (likelihood of the) following will be considered:

1. Physical possession (lost or stolen device?)
2. Credible evidence the information was copied/removed
3. Length of time between intrusion and detection
4. Purpose of the intrusion was acquisition of information
5. Credible evidence the information was in a useable format
6. Ability to reach the affected individuals
7. Applicable University policy, and/or local, state, or federal laws

External Notification

If it is determined that an external notification to the affected individuals is warranted, the following procedures will apply:

1. Written notice will be provided to the affected individuals using US Mail, unless the cost is excessive or insufficient contact information exists.
2. If written notice to the affected individuals is not feasible, the following methods will be considered for providing notice:

- Personal e-mail notices (provided addresses are available.
- A press release to media, to be written by Information Services and approved by the President, and other administrators as appropriate.
- An informational web site, developed and hosted by the department responsible for the system experiencing the breach, and approved by the CIO, External Affairs, and others as appropriate, with a conspicuous link in the University Home Page News area.

Definitions:

Private Information

If the information acquired includes a name (first and last name or first initial and last name) in combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

1. Social security number
2. Driver's license Number
3. Bank Account, Credit, or Debit Card Account number with security, access, PIN, or password that would permit access to the account
4. myNSU or other system passwords

Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address are not considered private information for the purposes of this policy.

Highly Sensitive Information

If the information acquired is of a very sensitive, confidential, or proprietary nature, the security breach will be investigated and University officials, including the CIO, General Counsel, and Vice Presidents will determine if a public notification is warranted. Examples of highly sensitive information include but are not limited to:

1. Name, Address, with Date of Birth
2. Records protected by FERPA, HIPAA, GLBA, or other applicable federal laws and regulations
3. Research data or results prior to publication or filing of a patent application
4. Information subject to contractual confidentiality provisions
5. Security codes, combinations, or passwords

** This policy is adapted from similar work created at the University of Iowa.*