Approved 4/25/2011 – last updated May 2018

Security Incident Reporting and Response Policy

PURPOSE

Confidential personal information and data compromised by a security breach may lead to identity theft and invasion of privacy for affected individuals. The University is required to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure of any sensitive personal information collected or maintained in the regular course of business.

The purpose of this policy is to provide the basis of appropriate response to incidents that threaten the confidentiality, integrity, and availability of university digital assets, information systems, and the networks that deliver the information. The Incident Response Policy provides a process for documentation, appropriate reporting internally and externally, and communication to the community as part of an ongoing educational effort. Finally, the policy establishes responsibility and accountability for all steps in the process of addressing computer security incidents.

SCOPE

This policy applies to all members of the Texas Wesleyan University community. The Texas Wesleyan University community includes faculty and staff members, students, alumni, guests, and contractors. This Policy also includes computing or network devices owned, leased, or otherwise controlled by Texas Wesleyan University. Additionally, incidents involving confidential information apply to any computing or network device, regardless of ownership, on which confidential or restricted information is stored or by which access to confidential or restricted information might be gained.

POLICY

Intrusion attempts, security breaches, theft or loss of hardware and other security related incidents perpetrated against the University must be reported to the Office of Information Technology. Anyone with knowledge, or a reasonable suspicion, of an incident which violates the confidentiality, integrity, or availability of digital information, shall make an immediate report by phone to 817-333-1251 or 817-531-4428.

The Information Security Manager in collaboration with other appropriate staff, shall determine if a reported incident is or is not a confidential information security incident.

If the incident **is not** considered a confidential information Security incident, the incident shall be referred to a technician who shall insure that the incident is handled in accordance with approved procedures.

If the Information Security Manager, in collaboration with other appropriate staff, determines that the incident **is** a confidential information security incident, an Incident Response Team shall be formed. The purpose of the Incident Response Team will be to determine a course of action to appropriately address the incident. The Incident Response Team membership will include the Chief Information Officer, University Risk Manager, appropriate individuals from the Office of Information Technology, and director(s) of the office(s) with primary responsibility for the compromised data.

It is the responsibility of the Incident Response Team to assess the actual or potential damage to the University caused by the Confidential Data Security Incident, and to develop and execute a plan to mitigate that damage. Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

The Incident Response Team should review, assess, and respond to the incident for which it was formed according to the following factors, in decreasing order of priority:

1. Safety - If the system involved in the incident affects human life or safety, responding in an appropriate, rapid fashion is the most important priority.
2. Urgent concerns - Departments and offices may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Appropriate OIT staff shall be available for consultation in such cases.
3. Scope - Work to promptly establish the scope of the incident and to identify the extent of systems and data affected.
4. Containment - After life and safety issues have been resolved, identify and implement actions to mitigate the spread of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the network.
5. Preservation of evidence - Promptly develop a plan to identify and implement steps for the preservation of evidence, consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information. Preservation of evidence should be addressed as quickly as possible in order to restore availability of the affected systems as soon as practicable.
6. Investigation - Investigate the causes and circumstances of the incident and determine future preventative actions.
7. Incident-specific risk mitigation - Identify and recommend strategies to mitigate the risk of harm arising from this incident.

If, in the judgment of the Chief Information officer, the incident is indicative of a true security breech and might reasonably be expected to cause significant harm to the subjects of the data or to the university, the Chief Information Officer may recommend to the Vice President of Finance and Administration and Vice President of Marketing, Communications, and Enrollment that a Senior Response Team be established.

The Senior Response Team shall be comprised of Chief Information Officer, University Risk Manager and other senior-level administrators designated by the Vice President of Marketing, Communications, and Enrollment. The Senior Response Team will determine whether Texas Wesleyan University should make best efforts to notify individuals whose personally identifiable

information and data might have been at risk due to the incident. In making this determination, the following factors shall be considered:

- Legal duty to notify
- Length of compromise
- Human involvement
- Sensitivity of compromised data
- Existence of evidence that data were compromised
- Existence of evidence that affected systems were compromised for reasons other than accessing and acquiring data
- Additional factors recommended for consideration by members of the Incident Response Team or Senior Response Team

If a legal duty to notify exists, affected individuals shall be notified in a manner compliant with the State's Security Breach Notification Law or EU General Data Protection Rights act (for citizens of the EU only).

Personal information that is lawfully available to the public from a government record is not subject to this breach notification policy. In addition, personal information rendered unreadable to an unauthorized party through use of encryption is not subject to this breach notification policy. Accordingly, all computers and other electronic data storage devices where confidential personal information may reside must be protected in accordance with the Network Protection and Information Security Policy. Personnel who work with personal data also must follow the requirements set forth in the University's Records and Data Retention Policy.

TERMS AND DEFINITIONS

Confidential Personal Information – an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- Social Security Number;
- Driver license number or government-issued ID number; or
- Account number or credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Confidential Personal Information also includes information that identifies an individual and relates to:

- FERPA, HIPAA, and GDPR protected information

Confidential information does not include publicly available information that is lawfully made available to the general public from the federal government or a state or local government.

Security Breach - unauthorized acquisition of data that compromises the security, confidentiality, or integrity of confidential personal information maintained by the University, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

ENFORCEMENT

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the Office of the Dean of Students, the Office of Information Technology, the Office of Housing and Residential Life, and/or the Office of Human Resources.

RELATED DOCUMENTS

Network Protection and Information Security Policy
Texas Wesleyan University Privacy Policy