Security Incident Reporting and Response Policy

Policy
Personal information will be protected to the best of the University's ability from unauthorized acquisition.

Purpose
This document outlines procedures and protocols for notification of and response to a security breach involving unencrypted personal information processed and/or maintained by the university and its auxiliary organizations.

I. SECURITY INCIDENT REPORTING & INVESTIGATION PROTOCOL
   A. Security Incident Reporting

   An employee or data owner who believes that a security incident has occurred, shall immediately notify the Chief Information Officer (817) 531-6515. After business hours, notification shall be made to Campus Security (817) 531-4911.

   Upon notification by an employee, Information Technology, Campus Security, or a Law Enforcement agency of a suspected unauthorized acquisition of confidential information the Chief Information Officer shall promptly notify the Sr. Vice President of Administration and Finance.

   B. Security Incident Investigation

   The Chief Information Officer or his/her designee will conduct an investigation into the security incident to determine whether there has been a security breach. As part of the investigation, and when applicable, the appropriate administrator shall require the data owner to complete and submit a statement to the Chief Information Officer or his/her designee. All investigatory work will be documented within an Incident Report.

   Upon completion of the investigation, the Chief Information Officer shall inform the Sr. Vice President of Finance and Administration and the appropriate Division Executive of the result of the investigation.

II. SECURITY BREACH NOTIFICATION PROTOCOL
   A. Internal Notifications

   If it is determined after investigation that a breach has occurred involving notice-triggering information, the Chief Information Officer shall notify the Sr. Vice President of Administration and Finance who will seek appropriate legal counsel.
The Chief Information Officer or his/her designee will notify the responsible department, confirming the security breach and provide advice and guidance on minimize the impact of the current breach and preventing a future breach.

If it is determined that a breach is of the appropriate magnitude and may require a press release, the Chief Information Officer shall notify the Assistant Vice President of Marketing and Communications, who will be responsible for notifying members of Senior Staff. The Assistant Vice President of Marketing and Communications will work closely with the Division Executive or designee of the department responsible for controlling access to, and security of, the breached area or electronic equipment to ensure the appropriate handling of the breach response and inquiries.

B. Notification of Affected Individuals

The department or office responsible for controlling access to, and security of, the breached electronic equipment shall compile the list of the names of persons whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The Assistant Vice President of Marketing and Communications or his/her designee will compose and send out an appropriate notice to all listed individuals.

Notification Timing

Individuals whose notice-triggering information has been compromised shall be notified in the most expedient time possible, and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The information considered when determining the notification date shall be included within the Incident Report.

Content of Notice

The breach notification will provide a brief description of the security breach, a contact for inquiries, and helpful references to individuals regarding identity theft and fraud. The content of the breach notification, and when appropriate, the content of both the web site page and the press release will be reviewed and approved by the Chief Information Officer.

Communications with Outside Agencies

With the exception of the Office of Marketing and Communications, university personnel are not authorized to speak on behalf of the university to media personnel or representatives of other outside agencies. All media inquiries or other
public affairs inquiries should be directed to the Office of Marketing and Communications at (817) 531-4480.

**Method of Notification**

A letter shall be printed with official Texas Wesleyan University letterhead, addressed to the individual at the last recorded home address. Any notices returned with address forwarding information will be re-sent by the responsible department.

If less than 3,000 individuals were affected, or if the cost of disseminating individual notices is less than $3,000, notices shall be sent by mail.

If more than 3,000 individuals were affected or if the cost of giving individual notices to affected individuals is greater than $3,000 or if there is insufficient contact information, the following substitute notification procedures shall be followed:

- Notices by e-mail shall be sent to all affected individuals whose e-mails are known.
- A “Notice of Breach” shall be conspicuously posted on the campus web site for a period of three months.

**Breach Notification Inquiry Response**

Subsequent to a security breach notification, the University can expect several inquiries from notified users, their parents/spouse, and security vendors. The Assistant Vice President of Marketing and Communications will provide a written *Inquiry Response Guide* to be used to respond to any phone calls/emails/letters/walk in traffic with inquiries regarding the breach.

**Department Responsibility**

The department responsible for controlling access to, and security of, the breached information may be held responsible for financial and human resources used to notify and respond to the affected individuals.

**III. DEFINITIONS**

**Data Acquisition**

Unencrypted personal information/notice-triggering information will be considered to have been acquired, or reasonably believed to have been acquired, by an unauthorized person in any of the following situations.

**Equipment**

Lost or stolen electronic equipment (including laptops, desktop computers, and USB storage devices) containing unencrypted personal information.

**Hacking**
A successful intrusion of computer systems via the network where it is indicated that unencrypted personal information has been downloaded, copied, or otherwise accessed.

**Unauthorized Data Access**

Includes situations where someone has received unauthorized access to data, such as sending non public mail/e-mail to the wrong recipient, incorrect computer access settings, inadvertent posting of personal information in electronic format or other non-hacking incidents. Unauthorized data access also includes indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

**Documents**

Lost or stolen electronic or paper documents containing unencrypted personal information.

**Data Owner**

The individual with primary responsibility for determining the purpose and function of a record system.

**Incident Report**

An investigatory summation of a *Security Incident* completed by Chief Information Officer to determine if the university has incurred a *Security Breach*.

**Notice-Triggering Information**

Specific items of personal information limited to an individual’s name in combination with Social Security Number, driver’s license, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

**Security Breach**

An unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by Texas Wesleyan University or its auxiliary organizations.

**Security Incident**

A collection of related activities or events which provide evidence that confidential information could have been acquired by an unauthorized person.

**IV. LEGAL OR CIVIL ACTIONS**

Subsequent to a breach, the University may be reviewed by a governing state or federal agency or a civil action could be brought against the University. The Assistant Vice President of Marketing and Communications will address all complaints and agency inquiries submitted to the University as a result of the security breach. Legal counsel will be solicited as needed to respond to complaints or actions.