Overview

This document outlines procedures and protocols for notification of and response to a data security breach involving unencrypted sensitive personal information processed and/or maintained by the university and its auxiliary organizations in accordance with the UT Austin Information Resources Use and Security Policy, namely section 5.13, and with the Texas Identity Theft Enforcement and Protection Act. This plan does not attempt to address general system security breaches and breaches of contracts.

1. Security Incident Reporting & Investigation Protocol

1. Security Incident Reporting

Any individual, who believes that a security incident has occurred, shall immediately notify the Chief Information Security Officer at (512) 475-9242 or security@utexas.edu.

Upon notification, the Chief Information Security Officer shall promptly assess the situation, working with the university's Triage Group (e.g., Vice President for Legal Affairs, University Compliance Officer, Director of Internal Audit), to determine whether or not the event warrants notification to affected individuals.

If notification is required the Chief Information Security Officer will inform the Data Breach Response Planning Group. The group includes the President, Provost, Vice President for Legal Affairs, Vice President and Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, Deputy to the President, University Compliance Officer, Chief Communications Officer, and other university officials as required.

2. Security Incident Investigation

The Chief Information Security Officer will conduct an investigation into the security incident to determine whether there has been a data security breach. As part of the investigation, and when applicable, the appropriate system administrator shall require the data owner to complete and submit an Employee Identification of Stored Data statement to the Chief Information Security Officer. The Chief Information Security Officer may also require copies of systems and/or application logs in a timely fashion. It is possible that the Chief Information Security Officer may need to physically secure some systems or data as potential evidence should a criminal investigation be expected. All investigatory work will be documented within an Incident Report.

The Chief Information Security Officer will coordinate with the Vice President for Legal Affairs throughout the initial investigation. Upon completion of the investigation, the Chief Information Security Officer will inform the Data Breach Response Planning Group of the result of the investigation.

2. Security Breach Notification Protocol

1. Internal Notifications

If it is determined after investigation that a data security breach involving notice-triggering information has occurred, the Chief Information Security Officer shall notify the Vice President for Financial Affairs and the Vice President for Legal Affairs as soon as possible.

If it is determined that a breach is of the appropriate magnitude and may require a press release (See Exhibit-A, Sample Communications), the Chief Information Security Officer shall further notify the Data Breach Response Planning Group as soon as possible. The Chief Information Security Officer shall also notify the UT System Chief Information Security Officer and other state and federal entities, as required by law.

The Chief Information Security Officer will notify the responsible department(s), confirming the security breach of notice-triggering information and provide advice and guidance. The Chief Information Security Officer shall also initiate the campus breach notification process and work closely with the department head, or their designee, of the department responsible for controlling access to, and security of, the breached electronic equipment to ensure the appropriate handling of the breach response and inquiries. The Chief Information Security Officer will provide guidance to designated employees responsible for responding to breach notification inquiries.

2. External Notification

If it is determined after investigation that a security breach involving credit/debit card information has occurred, the Chief Information Security Officer will coordinate with the pre-negotiated data breach vendor (See Exhibit-B, Credit Monitoring Vendor Information) to direct notification to the appropriate merchant bank(s). Within three (3) business days of a confirmed breach, the Chief Information Security Officer shall ensure an Incident Report is provided to the appropriate merchant bank(s). Within ten (10) business days, the Chief Information Security Officer shall ensure a list of all potentially compromised accounts is provided to the appropriate merchant bank(s).

3. 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. In consultation with the Chief Information Security Officer, a list of individuals to notify shall be compiled based on the following criteria:

- Residents of Texas.
- All other individuals who are likely to have been affected, such as all whose information had been stored in the files involved, when identification of specific individuals cannot be made.

For all affected individuals, the Chief Information Security Officer shall work with the contracted data breach vendor, which is on retainer. The process for determining inclusion in the notification group shall be included in the Incident Report.

4. 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 data 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.

5. Content of Notice

The breach notification will provide a brief description of the data 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 Security Officer and the Data Breach Response Planning Group.

6. Use of Credit Monitoring Services

The university will make credit monitoring services available to all individuals affected by the data breach for 24-months. Once the university purchased subscription period has ended, the vendor providing credit monitoring services will provide ongoing identity repair and after care to all individuals who elect to pay for credit monitoring at their own expense. Note: It is estimated that approximately 20% of all individuals affected by a data breach will elect to take advantage of credit monitoring services.

In the event the data breach is associated with a decentralized Information Technology resource not managed or operated by Information Technology Services, the responsible unit may be required to pay for all or some portion of the noted credit monitoring services as the situation warrants.

7. Communications with Outside Agencies

With the exception of the Chief Communications Officer, the President's Office, University Police, and the Chief Information Officer, university personnel are not authorized to speak on behalf of the university to media personnel regarding the breach. All media inquiries or other public affairs inquiries should be directed to the Chief Communications Officer at (512) 471-6080. All other inquiries should be directed to:

Data Breach Hotline
local: (512) 475-9020
toll free: (866) 657-9400
e-mail: datatheft@its.utexas.edu

8. Method of Notification

A letter shall be printed with official University of Texas at Austin letterhead, addressed to the individual at the last recorded home address, or if only an e-mail address is known, the last recorded e-mail address with the university. Any notices returned with address forwarding information will be re-sent by the responsible department.

If less than 500,000 individuals were affected, or if the cost of disseminating individual notices is less than $250,000, notices shall be sent by first class mail or e-mail address. The university may also elect to take advantage of the contracted vendor's ability to initiate automated phone calls to all individuals affected by the data breach.

If more than 500,000 individuals were affected or if the cost of giving individual notices to affected individuals is greater than $250,000 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.
- The University shall issue a press release to the media as appropriate.
- A "Notice of Breach" shall be conspicuously posted on the campus web site. After a six month period of time the Office of Legal Affairs and the Chief Communications Officer will determine if additional website posting time is necessary.

9. 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 Chief Information Officer's ITS Help Desk operation will respond to any phone calls/emails/walk-in traffic with inquiries regarding the breach using a script approved by the Chief Communications Officer. The ITS Help Desk will escalate any serious issues to the Chief Communications Officer, as appropriate, who may need to also engage the Office of Legal Affairs or others campus units as needed. The Chief Communications Officer will create scripted language to be used as a reference by university leadership and will update the content as needed.

10. Department Responsibility

The department responsible for the breach event is also responsible for financial and human resources required to locally manage the event (e.g., gather data, collaborate with university administration to prepare public responses, build notification websites).

3. Definitions

Personally Identifying Information
Information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number (Note: this is not the UT EID), address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Texas Penal Code.

Sensitive Personal Information (or Confidential Personal Information)
An individual's first name or first initial and last name in combination with any one of more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number of government-issued identification number; or (iii) account number or credit 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; or information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

Confidential Information

Information maintained by state agencies and universities that is exempt from disclosure under the provisions of the Public Records Act or other applicable state and federal laws. The controlling factor for confidential information is dissemination.

Unauthorized Data Acquisition
Unencrypted electronic personal information or 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 but not limited to smartphones, laptop computer, desktop computers, other portable computing or storage devices) containing unencrypted personal information or notice-triggering information.
- Hacking: A successful intrusion of computer systems via the network where it is indicated that unencrypted personal information or notice-triggering 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 or application access settings, inadvertent posting of personal information in electronic format, or other non-hacking incidents. Unauthorized data access also includes indications that an unauthorized person used the personal information or notice-triggering information (e.g., fraudulent accounts opened, instances of identity theft reported).

Data Owner
The authoritative head of the respective college, school, or unit. The owner is responsible for the function that is supported by the resource or for carrying out the program that uses the resources. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Encryption
The process of converting data into a cipher or code in order to prevent unauthorized access. Encryption obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher or code. The keys are binary values that may be interpretable as the codes for text strings, or they may be arbitrary numbers. The purpose of encryption is to prevent unauthorized access to data while it is either in storage or being transmitted. All encryption algorithms, with the exception of trivial ciphers, meet the minimal campus requirements for encryption. If personal information stored on the compromised electronic equipment is encrypted, no university notification is required.

Health Insurance Information
An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

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

Medical Information
Information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Notice-Triggering Information
Specific items of personal information identified in Texas Business and Commerce Code, Title 11, Subtitle B, Chapter 521, which is also known as the Texas Identity Theft Enforcement and Protection Act. This information includes an individual's name in combination with Social Security Number, driver's license/Texas identification card number, 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.

Data Breach
Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive 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. Good faith acquisition of sensitive personal information by a university employee for the purposes of university business is not a breach of system security unless the employee uses or discloses the sensitive personal information in an unauthorized manner.

Data Breach Response Planning Group
Individuals designated by the university to address high-profile information security issues. The group includes the President, Provost, Vice President for Legal Affairs, Vice President and Chief Financial Officer, Chief Information Officer, Chief Information Security Officer, Deputy to the President, University Compliance Officer, Chief Communications Officer, and other university officials as required.

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

Victim
A person whose identifying information is used by an unauthorized person.

4. 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 Chief Information Security Officer will work with the Vice President of Legal Affairs on all complaints and agency inquiries submitted to the university as a result of the data breach.

Exhibit A: Sample Communications

[DRAFT: Initial Press Release]

Unauthorized access of computer records discovered at The University of Texas at Austin

AUSTIN, Texas –The University of Texas at Austin officials announced today (April 23) that an unknown person or persons has gained unauthorized access to a large number of electronic records at the School of XYZ.

The security violation was discovered Friday, April 21, and the university has devoted all available resources to identify the source of the breach. An estimated 197,000 records were accessed.

"It is our highest priority to notify those who may be affected by this security breach," said university President William Powers Jr. "We have notified the proper law enforcement agencies and are doing everything we can to aid those whose information has been accessed unlawfully."

An investigation has determined that information from the school's computer system was obtained as recently as April 11, including Social Security numbers and other data related to alumni, faculty, staff and students of the school. Records of student applications, recruiters and job applicants were also accessed.

The school has created a Web page accessible at http://www.xyz.utexas.edu/datatheft to help people potentially affected by the theft of information. Letters and e-mails will be mailed to individuals who were directly affected, with detailed information about their records and recommendations on how to protect themselves from identity theft. Notification will also be sent to those whose information was stored on the same system, even though their Social Security numbers were not accessed. In its communications, the university will not request personal information. A call center is being established and that telephone number will be made available as soon as it is operational.

Powers said the university regrets the incident and is committed to ensuring the integrity of its data systems. University officials will release updates to affected parties and the news media as further information develops.

[DRAFT: Bulk Notice to Affected Users]

From: Dean, George Oak
Subject: School of XYZ security breach
Date: April 32, 2025

Dear Friend of the School of XYZ:

A serious breach of security has been discovered in the primary administrative information server at the School of XYZ at UT Austin. This server contains 197,000 individual records, and many, but not all, contain Social Security Numbers. I regret to advise you that your record is contained in the XYZ database(s).

At least 106,000 of these records were accessed (downloaded) by the intruder -- and we are unable to determine at this time if your record is included. Rather than wait to perform further analysis to determine the extent of your risk, we are advising you today to take precautions immediately to protect your credit. Specifically the University strongly recommends that you place a "fraud alert" on your file with the three major credit bureaus. Instructions for placing the no-charge fraud alerts, and other information about the security breach can be found on the special website, www.xyz.utexas.edu/datatheft

You will be receiving additional information from the University providing more specificity about information about you, if any, obtained by the intruder. Please do not wait for our follow-up communication, however, to take action. If you have questions or concerns not covered in the above website, please contact the University, via email to datatheft@xyz.utexas.edu or by calling 512 475-9020 (local Austin number) or 866-657-9400 (toll-free). Our help desk is open 8 a.m. to 6 p.m., Monday through Friday.

The University regrets that this incident has impacted you personally. Please know that the University is committed to doing everything it can to ensure the security of any personal information received from you, and to working vigorously with law enforcement authorities to identify and prosecute those responsible for this intrusion.

[DRAFT: Letter to Affected Users RE: Stolen Laptop]

Dear XXXXXXX: September 16, 2010

On Wednesday, August 25, 2010, a university-owned laptop computer was stolen from the home of an employee working for the ABC Research Center at The University of Texas at Austin. The Information Security Office at The University of Texas at Austin confirmed the existence of sensitive information contained in five Payee Information Forms, which were used to report income paid to an individual working for the ABC Research Center. These files included name, address, Social Security numbers, and citizenship information.

The system storing this information was not encrypted, but was password protected. The university is currently working with local law enforcement to recover this device.

In accordance with the Texas Identity Theft Enforcement and Protection Act, The University of Texas at Austin is notifying each of the individuals whose names and Social Security numbers were stored in these files. We wanted to make you aware of the situation so you can monitor your records for any unauthorized activity over the next several months.

The following resources may assist you in monitoring your records:

> Credit and Identity Protection Resources
> https://www.utexas.edu/datatheft/resources.html

We regret that this matter has impacted you personally. Please know that the university is doing everything it can to ensure the security of any personal information it maintains for you.

Please call the University of Texas at Austin Help Desk at 512-475-9400 or 866-657-9400 if you have any questions or concerns.

Sincerely,

Judy Pecan
Dean, School of ABC
University of Texas at Austin

[DRAFT: Letter to Affected Users RE: Publicly Posted Sensitive Data]

February 4, 2008

Dear XXXXX:

On Saturday evening, January 26, 2008, the Information Security Office at The University of Texas at Austin confirmed the existence of unauthorized student information that had been inadvertently posted to a public web server used by the College of 123. The files in question were associated with a College of 123's Graduate Application Review Form, which included applicant names, date of births, Social Security numbers, and academic transcript data.

The system storing this information was promptly assessed and the respective files have since been deleted.

In accordance with the Texas Identity Theft Enforcement and Protection Act, The University of Texas at Austin is notifying each of the individuals whose names and Social Security numbers were stored in these files. We wanted to make you aware of the situation so you can monitor your records for any unauthorized activity over the next several months.

The following resources may assist you in monitoring your records:

> Credit and Identity Protection Resources
> https://www.utexas.edu/datatheft/resources.html

We regret that this matter has impacted you personally. Please know that the University is doing everything it can to ensure the security of any personal information it maintains for you. Please call the University of Texas at Austin Help Desk at 866-657-9400 if you have any questions about this letter.

Sincerely,

Mary Cottonwood
Dean, College of 123
University of Texas at Austin

Exhibit B: Credit Monitoring Vendor Information

The data breach vendor, Debix, can provide the following services as needed:

- Credit monitoring services across all three credit bureaus
- Data breach notification services
- Call center services
- Data lookup services (e.g., address lookup, deceased lookup, SSN/DOB verification)

A master agreement between the university and Debix currently exists and has been approved by the Office of Accounting. The university's point of contact with this vendor is:

Erich Lambert
erich.lambert@debix.com
(512) 788.1940
(877) 441-3009

Costs for credit monitoring services will vary based on the size of the data breach, but aren't expected to exceed $30.50 per individual for twelve months of coverage. This rate assumes the smallest possible data breach. Larger breaches will leverage economies of scale, which will result in a much lower cost per individual. Costs for notifications and call center services will also vary based on size of the data breach, but should not exceed $3.05 per affected individual. Costs for data lookup services will also vary based on size of the data breach, but should not exceed $2.00 per affected individual. Given these costs, the estimated cost of services for a data breach involving 1000 affected users might be:

1000 x 20% = 200 users (the number expected to request credit services)

200 x $30.50 x 2 years = $12,200 (credit monitoring services)
1000 x $3.50 x 2 years = $7,000 (notification and call center services)
1000 x $2.00 x 2 years = $4,000 (data lookup services)

ESTIMATED TOTAL = $23,200

The estimated cost of services for a data breach involving 500,000 affected users would be:

500,000 x 20% = 100,000 users (the number expected to request credit services)

100,000 x $20.10 x 2 years = $4,020,000 (credit monitoring services)
500,000 x $1.89 x 2 years = $1,890,000 (notification and call center services)
500,000 x $1.50 x 2 years = $1,500,000 (data lookup services)

ESTIMATED TOTAL = $7,410,000

FURTHER INFORMATION

UT Austin Information Security Office
security@utexas.edu | (512) 475-9242