The University of Texas at El Paso
Information Security Office
Incident Response Plan

Notice to Readers

Incident Response Plan – Template for Breach of Personal Information[1] does not represent an official position of the *American Institute of Certified Public Accountants*, and it is distributed with the understanding that the author and the publisher are not rendering accounting, or other professional services in the publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

[1] Adapted from the "*Incident Response Plan Template for Breach of Personal Information*" (*http://www.datasecuritypolicies.com/category/security-policies/incident-response-policy/*), with permission from the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

Contents

Introduction

The University of Texas at El Paso (also referred to as "UTEP" or "the University") provides guidance and defines procedures for documenting and handling any potential threat to UTEP Information Resources, computers and data, as well as taking appropriate action when the source of an intrusion or incident at a third party is traced back to the University. This plan identifies and describes the roles and responsibilities of the Incident Response Team and the steps necessary for putting the plan into action. The increase in identity theft is a concern for all of us. As business systems and processes become increasingly more complex and sophisticated and more and more confidential information continues to be collected, laws and regulations continue to place requirements on the protection of confidential information.

To help organizations address these issues and implement good privacy practices, the *American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA*) introduced the *AICPA/CICA Privacy Framework* for protecting confidential information. The Framework can be used by CPAs/CAs[2] (both in industry and public practice) to guide and assist the organizations they serve in implementing good privacy programs. It incorporates concepts from significant domestic and international privacy laws, regulations and guidelines. You can download the Framework at www.aicpa.org/privacy or www.cica.ca/privacy .

Purpose

To assist in addressing these issues and implement good privacy practices, The University of Texas at El Paso will continue to strive towards thwarting these types of threats and implement sound privacy programs. While the privacy and protection of confidential information is not absolute, the University is committed to the aggressive pursuit in the protection of confidential information. In addition, credit card companies now require all merchants to implement an Incident Response Plan to deal with system breaches (refer to **Appendix A1**.).

An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of confidential information, and other events with serious information security implications. The Incident Response Team's mission is to prevent a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases. The Incident Response Team is responsible for putting the plan into action.

Objective

The objective of the Incident Response Plan (IRP) is to:

- Limit immediate incident impact to customers and business partners;
- Recover from the incident;
- Determine how the incident occurred;

[2] CPA/CA refers to a certified public accountant in the United States, and a chartered accountant in Canada, or their equivalent in other countries, whether in public practice, private industry, government or education.

- Find out how to avoid further exploitation of the same vulnerability;
- Avoid escalation and further incidents;
- Assess the impact and damage in terms of loss of image and financial impact;
- Update company policies, procedures, standards and guidelines as needed; and
- Determine who initiated the incident for possible criminal and/or civil prosecution.

Scope

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident involving Confidential data. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Chief Information Security Officer (CISO) will coordinate these investigations.

The Incident Response Team will subscribe to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents.

Roles and Responsibilities

Incident Response Team Members

Each of the following areas will have a primary and alternate member:

- Information Security Office (ISO)
- Information Resource Manager (IRM)/Chief Information Officer (CIO)
- Office of Institutional Compliance
- Telecommunications Infrastructure (TI)
- Enterprise Computing (EC)
    - Systems Support
    - Data Management
    - Development and Programming

Incident Response Team Roles and Responsibilities

Information Security Office (ISO)

- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice as needed
- Contacts members of the Incident Response Team
- Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken
- Central point of contact for all computer incidents
- Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach

Office of Institutional Compliance

- Coordinates activities with the ISO
- Documents the types of confidential information that may have been breached
- Provides guidance throughout the investigation on issues relating to privacy of student/faculty/staff/other confidential information
- Assists in developing appropriate communication to impacted parties

Telecommunications Infrastructure (TI)

- Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks
- Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers
- Looks for signs of a firewall breach
- Contacts external Internet Service Provider for assistance in handling the incident
- Takes action when requested by the CISO to block traffic from suspected intruder

Enterprise Computing (EC):

Systems Support

- Ensures all service packs and patches are current on mission-critical computers
- Ensures backups are in place for all critical systems
- Examines system logs of critical systems for unusual activity

Data Management

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Information Security Office with any information relating to a suspected breach
- Collects pertinent information regarding the incident at the request of the CISO

Development and Programming

- Monitors business applications and services for signs of attack
- Reviews audit logs of mission-critical servers for signs of suspicious activity
- Contacts the Information Security Office with any information relating to a suspected breach
- Collects pertinent information regarding the incident at the request of the CISO

General

This Incident Response Plan outlines steps the University will take upon discovery of unauthorized access to confidential and/or personally identifiable information (PII,) hereinafter referred to as confidential information, on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be a student, faculty, staff, or customer of the University.

In addition to the internal notification and reporting procedures outlined below, credit card companies require us to immediately report a security breach, and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Specific steps are outlined in **Appendix A2**. Selected laws and regulations require the organization to follow specified procedures in the event of a breach of confidential or PII as covered in **Appendix B**.

Confidential Information and/or **Personally Identifiable Information (PII)** is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the University collects about an individual is likely to be considered confidential information if it can be attributed to an individual. Additionally, data that must be protected due to a contractual agreement or grant is also considered Confidential information. This includes, but is not limited to, Controlled Unclassified Information (CUI) and other data as defined in the agreement. This classification of data may require additional safeguards. Please refer to the agreement/contract/grant/etc. for additional applicable requirements such as NIST SP 800-171, NIST SP 800-53, DFARS, etc.

For our purposes, confidential and PII is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security Number (SSN)
- UTEP ID Numbers (80/88 or 60)
- Race, Ethnicity, and/or Nationality
- Transcripts and/or Grade Report
- Driver's license number or Identification Card Number
- Date and/or Place of Birth
- Government Issued Identification Number
- Mother's Maiden Name
- Biometric Data (e.g., face, fingerprints, handwriting, retina, etc.)
- Vehicle Registration Plate Number
- Financial Account Number, credit or debit card number* with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account
- Home address or e-mail address
- Medical or health information (FERPA-covered information)
  * If the individual is a Visa, MasterCard, American Express, or Discover cardholder, follow additional procedures outlined in the **Appendix A2**.

NOTE: Confidential information must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements) in accordance with the Texas Administrative Code 202, FERPA, NIST 800-171, etc.

Incident Response Team Notification

The Information Security Office (ISO) will be the central point of contact for reporting information resource incidents or intrusions. The ISO will notify the Chief Information Security Officer (CISO).

A preliminary analysis of the incident will take place by the CISO and that will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of Confidential or Personally Identifiable Information
- Breach of Card Holder Data (PCI DSS)
- Denial of Service / Distributed Denial of Service
- Excessive Port Scans
- Firewall Breach
- Virus Outbreak
- Compromised Systems or Webpages
- RedFlag Incidents

Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality, integrity, or availability of confidential information maintained by the University. Good faith acquisition of this type of information by an employee or agent of the University for business purposes is not a breach, provided that the information is not used or subject to further unauthorized disclosure. Please refer to UTEP Standard 9: Data Classification for more information

Requirements

Data owners and/or custodians must identify and document all systems and processes that store or utilize confidential information on individuals. Documentation must contain system name, device name, file name, location, database administrator and system administrator (primary and secondary contacts for each). The data owners, with the assistance of the Enterprise Computing teams, must maintain the contact list of database and system administrators.

Likewise, all authorized users who access or utilize confidential information on individuals should be identified and documented. Documentation must contain user name, department, device name (i.e., workstation or server), folder name, location, and system administrator (primary and secondary contacts).

Data Owner/Custodian Responsibilities

Data owners/custodians responsible for confidential information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between the University and any third-party involved with a privacy breach affecting University-held data.

All data owners/custodians must report any suspected or confirmed breach of confidential information to the **ISO or CISO immediately upon discovery**. This includes notification received from any third-party service providers or other business partners with whom the University shares confidential information. The CISO will notify the IRM/CIO, Executive Vice President, and data owners/custodians whenever a breach or suspected breach of confidential information affects their respective area.

Note: For ease of reporting, and to ensure a timely response 24-hours a day, seven-days a week, the Information Security Office (security@utep.edu) will act as a central point of contact for reaching the CISO, IRM/CIO, and Executive Vice President.

The CISO will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation (See "Incident Response" section.) The data owner will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the CISO, IRM/CIO, Office of Institutional Compliance, Office of Legal Affairs or other Incident Response Team members throughout the investigation.

Departmental Directors/Chief Administrative Officers (CAO) Responsibilities

Departmental Directors/Chief Administrative Officers (CAOs) are responsible for ensuring all employees in their group are aware of policies and procedures for protecting confidential information.

If a breach or suspected breach of confidential information occurs in their respective area or location, the Departmental Director/CAO must notify the Information Security Office immediately and open an incident report. (See the "Incident Management" Section, Information Security Policies.)

Note: Education and awareness communication will be directed to all employees informing them of the proper procedures for reporting a suspected breach of confidential information..

When Notification Is Required

The following incidents **may** require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (student, faculty, staff, contractor, or third-party provider) has obtained unauthorized access to confidential information maintained in any format, including paper and electronic form.
- An intruder has broken into a system or database(s) that contains confidential information.
- Computer equipment such as a workstation, laptop, CD-ROM, External Hard Drive, Thumb Drive, or other electronic media containing confidential information has been lost or stolen.
- A department or group has not properly disposed of records containing confidential information.
- A third-party service provider has experienced any of the incidents above, affecting the University's data containing confidential information.

The following incidents **may not** require individual notification under contractual commitments or applicable laws and regulations providing the University can reasonably conclude after investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

- The University is able to retrieve confidential information that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The University determines that confidential information was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.

- An intruder accessed files that contain only individuals' names and addresses.
- A laptop computer is lost or stolen, but the data is encrypted and may only be accessed with a secure token or similar access device.

Incident Response – Breach of Confidential Information

Incident Response Team members must maintain accurate notes of all actions taken, by whom, and the exact time and date (Who, What, When, Where, Why, How, etc.). Each person involved in the investigation must record his or her own actions.

CONTACT
Information Security Office – security@utep.edu or (915) 747-6324, (915) 490-3203 on-call

1. The ISO will serve as a central point of contact for reporting any suspected or confirmed breach of confidential information.

2. After documenting the facts presented by the caller and verifying that a privacy breach or suspected privacy breach occurred, the ISO will open a Priority Incident Request. The ISO will initiate notification of the CISO immediately.
3. The ISO will contct the CISO and advise that a breach or suspected breach of confidential information has occurred/been reported. After the CISO analyzes the facts and confirms that the incident warrants incident response team activation, the Incident Request will be updated to indicate **"Incident Response Team Activation – Critical Security Problem"**.
4. The ISO is responsible for documenting all details of an incident and facilitating communication to CISO and other auxiliary members as needed.
5. ISO may be assigned the responsibility of sending out communications/notifications.

CONTACT
Chief Information Security Officer – security@utep.edu or (915) 747-6324

1. When notified by the ISO, the CISO performs a preliminary analysis of the facts and assesses the situation to determine the nature and scope of the incident.
2. CISO informs the IRM/CIO, Executive Vice President, Office of Legal Affairs and others as deemed appropriate, that a possible privacy breach has been reported and provides an overview of the situation.
3. CISO will contact the individual who reported the problem.
4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of confidential information. Every breach may not require participation by all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
5. Reviews the preliminary details with the IRM/CIO, Executive Vice President, Office of Legal Affairs and others as may be deemed appropriate.
6. If a privacy breach affecting confidential information is confirmed, Incident Response Team activation is warranted. Contact the ISO and advise them to update the Incident Request with **"Incident Response Team Activation – Critical Security Problem".**

7. Update the IRM/CIO and Executive Vice President of the details of the investigation/breach on key findings as the investigation proceeds.
8. Contact all appropriate teams (e.g., database administrators, system administrators, etc.) to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
9. Contact appropriate Incident Response Team members and First-Level Escalation members.
10. Identify and contact the appropriate Data Owner(s) affected by the breach. In coordination with the IRM/CIO, Executive Vice President, Office of Legal Affairs, and others as deemed necessary, determine additional notification requirements (e.g., Data Owners/Custodians, Human Resources, external parties, etc.).
11. If the breach occurred at a third-party location, determine if a legal contract exists. Work with the IRM/CIO, Executive Vice President, and Office of Legal Affairs to review contract terms and determine next course of action.
12. Work with the appropriate parties to determine the extent of the potential breach. Identify system(s)/application(s) where data may have been affected (i.e., where data is stored and potentially compromised – whether on test, development and/or production systems) and the number of individuals potentially placed at risk.
13. Determine the type of confidential information that is potentially at risk, including but not limited to:

    Name, Address, Social Security Number, Account number, Cardholder name, Cardholder address, Medical and Health Information (FERPA related), Unclassified Controlled Information (CUI), Other
14. If confidential information is involved, have the Data Owner(s), with the assistance of Data Custodian(s), determine who might be affected. Coordinate next steps with the IRM/CIO, Executive Vice President, Office of Legal Affairs, Institutional Compliance and University Relations (e.g., individual notification procedures).
15. Determine if an intruder has exported, or deleted any confidential information data.
16. Determine where and how the breach occurred.
    - Identify the source of compromise, and the timeframe involved.
    - Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal network, test and production environments, and virtual private networks. Look at appropriate system and audit logs for each type of system affected.
    - Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.
17. Take measures to contain and control the incident to prevent further unauthorized access to or use of confidential information, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls if necessary.
    - Change all applicable passwords for IDs that have access to confidential information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.
    - Do not access or alter the compromised system.
    - Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).
    - Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the wireless network if applicable.

18. Monitor systems and the network for signs of continued intruder access.
19. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

    Note: Credit Card processors like Visa have specific procedures that must be followed for evidence preservation. Likewise, a Contract/Grant/Purchase Order/Etc. will specify what procedures must be followed for evidence preservation when Controlled Unclassified Information (CUI) is involved.

20. Notify the IRM/CIO in coordination with the Executive Vice President and Office of Legal Affairs as appropriate. Provide a summary of confirmed findings, and of the steps taken to mitigate the situation.
21. If credit cardholder data is involved, follow additional steps outlined under **Appendix A**. Bankcard companies, specifically Visa and MasterCard, have detailed requirements for reporting security incidents and the suspected or confirmed compromise of cardholder data. Reporting is typically required within 24 hours of compromise.
22. If an internal user (authorized or unauthorized student, staff, faculty, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager or Dean of Students, if a student is involved, for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the University.

CONTACT
Data Owners/Data Custodians - Enterprise Computing
Systems Support – (915) 747-4357 or sysadmin@utep.edu
Data Management – (915) 747-4357 or DataManagement@utep.edu
Development and Programming – (915) 747-4357 or Programmers@utep.edu

Notification Steps
Enterprise Computing or Data Owner(s)/Data Custodian(s)

1. If the Enterprise Computing or Data Owner(s)/Data Custodian(s) hear of or identify a privacy breach, contact the ISO to ensure that the CISO and other primary contacts are notified.
2. The IT Enterprise Computing Group and Data Owner(s)/Data Custodian(s) will assist the CISO as needed in the investigation.

Process Steps

1. Monitor access to database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).
2. Identify individuals whose information may have been compromised. An assumption could be “all” if an entire table or file was compromised.

3. Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.
4. Upon request from the CISO, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

Evidence Preservation – Seek CISO Guidance

1. **Do not access or alter compromised system(s)**—i.e., don't log on **at all** to the compromised system(s) and change passwords; do not log in as ROOT. To avoid losing critical data, it is highly recommended the compromised system not be used.
2. Do not turn the compromised system(s) OFF. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
3. Preserve all evidence and logs—i.e., original evidence, security events, web, database, firewall, etc. Ensure the integrity of the evidence is not impacted by any tools used in the collection and analysis process.
4. Document all actions taken, including dates and individuals involved.

EC Systems Support, Development and Programming Groups

1. Systems Support, Development and Programming Groups will serve as the primary contact for the online sales or web applications. These groups are available 24x7 and should be contacted as shown above depending on affected systems and processes/applications.
2. When notified by the ISO that the privacy breach incident response plan has been activated, EC Groups or ISO Systems Administrator(s) will collect pertinent information regarding the incident from the CISO and determine the appropriate system(s) to be inspected. If notification of a possible breach of information on an individual comes from any other source (an individual outside the University), refer the caller to the ISO to begin the official incident response notification process.
3. EC Groups or ISO Systems Administrator(s), using the information gathered from the sources listed in item 2, will begin by inspecting web server logs and operating system logs (e.g. Windows event logs, UNIX syslogs, security logs, etc.). They will look for suspicious activity that may suggest which application interface to processing systems may have been compromised. From there they will look at the operating system level to ensure that servers were not compromised and used as a pass-through into the backend network. This will also be done by checking the systems Event logs, looking at the network for abnormal connections, inspecting the systems registry for non-standard entries, looking at the running process list for any abnormal executing processes, etc.
4. Due to the sensitivity of a security breach, Systems Support will only notify and communicate with the following individuals/teams:

   Chief Information Security Officer: security@utep.edu or (915) 747-6324
   Information Resource Manager/Chief Information Officer: (915) 747-4357
   Information Security Office: security@utep.edu or (915) 747-6324, (915) 490-3203 on-call Development and Programming Teams: (915) 747-4357 or Programmers@utep.edu
   Data Management Team: (915) 747-4357 or DataManagement@utep.edu

5. Systems Support Manager will keep these persons informed until it can be confirmed or denied that the Online Sales systems were compromised.

CONTACT
Credit Payment Systems

1. If notified of a privacy breach by a business area directly, open an incident request with the ISO to activate the incident response plan for a suspected privacy breach.
2. When notified by the ISO that the privacy breach Incident Response Plan has been activated, perform a preliminary analysis of the facts and assess the situation to determine the nature of incident.
   a. Determine the type of confidential information breached.
      i. Current credit card customers
      ii. Personal check authorizations
   b. Determine data sources and method of breach (hardcopy, electronic)
   c. Determine method of breach if possible.
   d. Identify additional resources needed to complete investigation
3. Determine the scope of the breach.
   a. Time Frame
   b. Specific Data Elements
   c. Specific Customers
4. Take necessary steps to prevent additional compromise of confidential information.
5. Report all findings to the Incident Response Plan Team.
6. Notification of an account number compromise, the CISO will contact the appropriate card companies:
   a. Visa Fraud Control Group
   b. MasterCard Compromised Account Team
   c. Discover Fraud Prevention
   d. American Express Merchant Services
7. Act as liaison between the card companies, CISO, Executive Vice President and Legal.
8. Ensure credit card companies' specific requirements for reporting suspected or confirmed breaches of cardholder data are followed. For detailed requirements, see **Appendix A2**.

CONTACT
Executive Vice President or Office of Legal Affairs – (915) 747-5555 or 747-5056
Privacy Officer/CISO security@utep.edu or (915) 747-6324

Ongoing:

1. Monitor relevant privacy-related legislation, provide input as appropriate, and communicate to our community the effect that any enacted legislation may have on them.
2. Be cognizant of major contracts which the University enters that may have an impact or effect on our students, employees, and other data.
3. Be aware of other University privacy policies that may affect the institution and affiliates.

When a Privacy Breach Occurs:

1. After confirmation that a privacy breach has occurred, notify Privacy Officer/CISO. The Privacy Officer/CISO will in turn notify the IRM/CIO, Office of Institutional Compliance, and Office of Legal Affairs.
2. Coordinate activities between business area(s) and other departments (e.g., Human Resources, Business Affairs, etc. if necessary).

3. If necessary, notify the appropriate authorities (e.g., Federal Trade Commission (FTC)/RCMP, the relevant privacy commissioner's office, etc.).
4. Coordinate with the Office of Legal Affairs on the timing and content of notification to individuals.
5. If the Executive Vice President and Privacy Officer determine that the breach warrants law enforcement involvement, any notification to individuals may be delayed if law enforcement determines the notification will impede a criminal investigation. Notification will take place after law enforcement determines that it will not compromise the investigation.
6. Notification to individuals may be delayed until the Privacy Officer/CISO is assured that necessary measures have been taken to determine the scope of the breach and that it has been properly investigated.
7. Follow approved procedures for any notice of unauthorized access to confidential information.
8. Notification to individuals should be timely, conspicuous, and delivered in any manner that will ensure the individual receives it. Notice should be consistent with laws and regulations the University is subject to.

   Appropriate delivery methods include:
   - Written notice
   - Email notice
   - Substitute notice
     - Conspicuous posting of the notice on the University's website
     - Notification to major media

   Items to consider including in notification to individuals:
   - A general description of the incident and information to assist individuals in mitigating potential harm, including a customer service number, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.
   - Remind individuals of the need to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft.
   - Inform each individual about the availability of the Federal Trade Commission's (FTC's) online guidance regarding measures to protect against identity theft, and encourage the individual to report any suspected incidents of identity theft to the FTC. Provide the FTC's website address and telephone number for the purposes of obtaining the guidance and reporting suspected incidents of identity theft. At the time of this document's publication, the website address is http://www.ftc.gov/idtheft. The toll-free number for the identity theft hotline is 1-877-HELP (877-382-4357); TDD: 1-(866) 653-4261.

CONTACT
Human Resource Services – (915) 747-5202 or hrs@utep.edu

1. If notified of a privacy breach affecting employee confidential information, open an incident request with the ISO to activate the Incident Response Plan for suspected privacy breach.
2. When notified by the ISO that the privacy breach incident response plan has been activated for a breach of information, perform a preliminary analysis of the facts and assess the situation to determine the nature of the incident.

3. Work with the ISO, CISO, IRM/CIO and business area to identify the extent of the breach.
4. If approved by CISO, IRM/CIO, Executive Vice President, or Office of Legal Affairs, notify the business area(s) that a breach has been reported and is under investigation.
5. Work with the business area(s) to ensure there is no further exposure to privacy data.
6. Work with the CISO, IRM/CIO and Office of Legal Affairs to determine if the incident warrants further action.

CONTACT
Telecommunications Infrastructure (TI) – (915) 747-4356, TI@utep.edu or Networking@utep.edu

1. When notified by the CISO that the privacy breach Incident Response Plan is activated, provide assistance as determined by the details of the potential breach.
2. Review firewall logs for correlating evidence of unauthorized access.
3. Implement firewall rules as needed, or requested by CISO, to close any exposures identified during the investigation.

CONTACT
Office of Institutional Compliance – (915) 747-6478 or ComplianceOffice@utep.edu

Ongoing:

1. Monitor consumer privacy issues and practices of other organizations.
2. Monitor consumer privacy breaches of other organizations and how they respond.
3. Keep generic/situational talking points current.

When Privacy Breach Occurs:

1. After confirmation that a breach of confidential information has occurred, notify the CISO and Executive Vice President to determine which department will be assigned notification responsibilities.
2. Coordinate with the Executive Vice President, and Office of Legal Affairs on the timing, content and method of notification. Prepare and issue press release or statement, if needed.

   Vehicles for communicating include:

   a. News wire service.
   b. Online Sales web site – Post statement on home page or conspicuous location of web site.
   c. Internal Website – If appropriate for breach of employee information.
   d. E-mail.
   e. News conference – If privacy breach should reach a national and/or crisis level, coordinate brief news conference at headquarters or appropriate location.
   i. Appoint appropriate spokesperson.
   ii. Prepare statement and, if necessary, potential Q & A.
   iii. Coach spokesperson on statement and potential Q & A.
   iv. Invite select media to attend and cover organization's proactive message.
   v. Use conference as a platform for communicating who the breach involves, what the University is doing to correct breach, how it happened and the University's apology but reassurance of its privacy policies.

3. Prepare appropriate response to media, student, staff, faculty and/or customer; and have the Executive Vice President and Office of Legal Affairs approve prior to distribution.
4. Proactively respond to media inquiries, if necessary.
5. Monitor media coverage and circulate accordingly.

CONTACT **University Police Department – (915) 747-5611**

1. If the University Police Department (UTEP PD) becomes aware of or identifies a privacy breach, contact the ISO to ensure that the CISO and other primary contacts are notified.
2. The UTEP PD will secure the area of the breached information (e.g. computer room, data center, records room), if requested by CISO.
3. The UTEP PD will assist CISO as needed in the investigation.
4. The UTEP PD will keep CISO updated on appropriate investigation information gathered if applicable.

Conclusion

This document provides a useful template for developing an appropriate approach to handling the risks associated with a threat to the University due to a privacy breach, no matter how it may have occurred. This template provides an approach but the University will need to develop its strategy based on the nature of the incident and its organizational structure. The incident response plan developed should be constantly reviewed to ensure that it reflects current requirements and reflects experienced gained within the University.

Revision History

Version	Date	Author	Description of Change
1.0	June 2009	Information Security Office	Document was created
2.0	June 2010	ISO	Document was reviewed and updated
2.0	January 2012	ISO	Document links updated
3.0	July 5, 2018	ISO	Document reviewed and updated links, contact info, paragraph numbering, added protection of CUI
4.0	May 1, 2019	ISO	All credit card contact and procedures updated to reflect current data. Expanded on process for evidence preservation. Added revision and approval history.

Approvals

Role	Date	Name	Title
Approval	May 1, 2019	Gerard D Cochrane Jr	Chief Information Security Officer

Appendix A1 – Payment Card Industry Data Security Standard

Background:
The PCI Data Security Standard, revised in April 2016, was the result of a joint initiative by VISA, MasterCard, American Express, Discover, Diners Club, and JCB to create a single security standard for storing and transmitting sensitive customer information initially released on December 15, 2004.

Requirements
The PCI Data Security Standard applies to all members, merchants, and service providers that store, process or transmit cardholder data. The standard consists of the following 12 requirements:

1. Install and maintain a firewall configuration to protect data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored data;
4. Encrypt transmission of cardholder data and sensitive information across public networks;
5. Use and regularly update anti-virus software;
6. Develop and maintain secure systems and applications;
7. Restrict access to data by business need to know;
8. Assign a unique ID to each person with computer access;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes;
12. Maintain a policy that addresses information security.

Included in Requirement 12 is the implementation of an Incident Response Plan[3] (see next page).

For a complete copy of the Payment Card Industry Data Security Specifications, see https://www.pcisecuritystandards.org/document_library

Compliance
Failure to comply with the new standards could result in a merchant being subjected to a fine or the loss of access to the credit card networks.

On-site reviews
Merchants, including e-commerce merchants, with more than 6 million total transactions annually, or merchants who have already experienced an account compromise are required to have an onsite review carried out annually. Any other merchant can also be subjected to an onsite review at the discretion of the payment card institution. The review can be carried out either by the merchant's internal audit function or an independent assessor acceptable to the payment card institution.

Self-Assessments
Merchants with e-commerce transactions between 20,000 and 6 million total transactions annually are required to carry out a Self-Assessment annually. For all other merchants, the credit card companies recommend that the Self-Assessment be carried out on an annual basis. For a copy of the Payment Card

[3] See 12-10: "Implement an incident response plan." *Payment Card Industry Data Security Standard Version 3.2*

Industry Self-Assessment Questionnaire, see https://www.pcisecuritystandards.org/document_library?category=saqs#results.

PCI Data Security Standard Incident Response Plan Details[4]

12.10 Incident Response (IR) team is required to:

(a) Implement an IR plan that is prepared to respond immediately to potential cybersecurity incident.

(b) Create an IR plan to be used in the event of system breach. Ensure the plan addresses, at a minimum:

1. specific incident response procedures;
2. business recovery and continuity procedures;
3. data backup processes;
4. roles, responsibilities, and communication and contact strategies (for example, notifying payment brands, at a minimum);
5. Analysis of legal requirements for reporting compromises;
6. Coverage and responses of all critical system components; and
7. Reference or inclusion of incident response procedures from the payment brands.

(c) Test the IR plan at least annually.

(d) Designate IR personnel to be available on a 24/7 basis to respond to alerts.

(e) Provide appropriate training to staff with security breach response responsibilities.

(f) Include alerts from security monitoring systems, including but not limited to:

1. intrusion detection systems (IDS);
2. intrusion prevention systems (IPS);
3. firewalls; and
4. file integrity monitoring (FIM) systems; and

(g) Have a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

[4] *Payment Card Industry Data Security Standard – Version 3.2 Requirements 12.10-12.10.6*

Appendix A2 – Cardholder Requirements

Specific requirements for reporting suspected or confirmed breaches of cardholder data – notify PCI SSC as well as payment card companies. Contact and other information is provided herein; however, please review each specific credit card company's web page for up-to-date information.

Payment Card Industry Security Standards Council (PCI SSC)[5]
Notification any other legal obligations the Vendor (University) must promptly notify PCI SSC of any Security Issue relating to any of the Vendor's listed Payment Applications. Notification to PCI SSC must be in writing in accordance with the *Vendor Release Agreement*, and should be preceded by a phone call to the PCI PA-DSS Program Manager at (781) 876-8855. As part of the Vendor's initial notification to PCI SSC, the Vendor must supply at a minimum the following:

- The name, PCI SSC reference number, and any other relevant identifiers of the Payment Application;
- A description of the general nature of the Security Issue;
- The Vendor's good-faith assessment, to it knowledge at the time, as to the scope and severity of the vulnerability or vulnerabilities associated with the Security Issue (using CVSS or other industry accepted standard scoring);
- Assurance that the Vendor is following their Incident Response Plan and/or Vulnerability Handling Policies.

MasterCard Account Data Compromise (ADC) Reporting Steps: (Excerpts from MasterCard Security Rules and Procedures, Merchant Edition, February 14, 2019[6])

ADC Event Reporting
When you are informed, receive notification from MasterCard, become aware or discover a Account Data Compromise (ADC) event, you must notify MasterCard immediately and the following actions must be taken:

- Immediately commence a thorough investigation into the ADC Event or Potential ADC Event, hereafter referred to as Event.
- Immediately, and no later than within twenty-four (24) hours, identify, contain, and mitigate the ADC Event; secure account data; and preserve all information in all media including:
  - preserve and safeguard all potential evidence pertinent to a forensic examination of an ADC Event using industry best practices;
  - isolate compromised systems and media from network;
  - preserve all Intrusion Detection System, Intrusion Prevention System logs, all firewall, Web, database, and event logs;
  - document all incident response actions thoroughly; and

[5] Portions reproduced from the Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS), *"Notification Following a Security Breach, Compromise, or Known Vulnerability", (https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss),* Version 3.2 – April 2016.

[6] Portions reproduced from the "MasterCard Security Rules and Procedures, Merchant Edition", February 14, 2019 © (*https://www.MasterCard.us/content/dam/mccom/en-us/documents/rules/SPME-Manual-February-2019.pdf*)

- refrain from restarting or rebooting any compromised or potentially compromised system or taking equivalent or other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC event.

- Within **twenty four (24) hours,** and on an ongoing basis thereafter, submit to MasterCard all known or suspected facts to the cause and source concerning the ADC Event.
- Within **twenty-four (24) hours** and continuing throughout the investigation and thereafter, provide to MasterCard in the required format all primary account numbers (PANs) associated with Account data that were actually or potentially accessed or disclosed.
- Within **seventy-two (72) hours**, engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event. ***NOTE:*** Prior to engaging the services of a PFI, notify MasterCard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal to MS, or if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard.
- Within two (2) business days from date PFI was engaged, identify to MasterCard the engaged PFI and confirm that PFI has commenced it investigation.
- Within five (5) business days from start of forensic investigation, ensure that the PFI submits a preliminary forensic report detailing all findings to date.
- Within twenty (20) business days from start of forensic investigation, provide MasterCard a final forensic report detaining all findings, conclusion, and recommendations of the PFI.

Please refer to 10.2.2.2 Ongoing Procedures for ADC Events and Potential ADC Events for reporting requirements.

Additionally, see 10.2.4 Alternative Standards Applicable to Certain Merchants or Other Agents. In the event of an ADC Event for which you fall under a Level 2, Level 3, or Level 4 Merchant (per 10.3.4), in lieu of complying with the responsible Customer obligations per 10.2.2.1, the first bullet point of section 10.2.2.2, and 10.2.3 of the document (Chapter 10), a responsible Customer may comply with the Standards set forth in Section 10.2.4 provided all of the following criteria are satisfied: Criteria A – MasterCard determines that fewer than 30,000 Accounts are potentially at risk of unauthorized disclosure as a result of the Event; and Criterion B – MasterCard determines that the Merchant has not been the subject of an ADC Event for the thirty-six (36) consecutive months immediately preceding the date that MasterCard determines likely to be the earliest possible date of the Event; and Criterion C – The responsible Customer determines that the Merchant uses a payment acceptance system that does not share connectivity with another Merchant/Merchant's system and that it is not operated by the Service Provider.

Visa U.S.A. Specific Steps:

Please refer to Visa Core Rules and Visa Product and Services Rules[7] and Visa Bulletin – Member and Entity Obligation to Report Suspected or Confirmed Account Data Compromises[8] for detailed information.

Below are excerpted from Visa U.S.A. Cardholder Information Security Program (CISP), What To Do If Compromised, Version 5.0 (Global), Effective August 2016 Visa Public (https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf[9]. Please refer to the documentation for detailed information and requirements.

In the event of a security breach, the **Visa U.S.A. Operating Regulations** require entities to immediately report the breach and the suspected or confirmed loss, theft, or compromise of Visa account or cardholder information involving either their own network environment or that of their merchant(s) or agent(s).

Preserve Evidence

Identify the root cause and facilitate investigations. Ensure the integrity of the system components and environment by preserving all evidence.

- Do not access or alter compromised system; instead take the system offline
- Do not turn off, restart, or reboot the compromised system; instead isolate it and unplug network cables or through other means
- Identify and document all suspected compromised components
- Document containment and remediation actions taken; use very detailed dates/times, etc.
- Preserve all evidence and logs

Provide Visa Initial Investigation Report

Within three (3) business days of a suspected or confirmed account data compromise, provide the Visa Initial Investigation Report—to the acquiring bank or directly to Visa.

Execute Notification Plan

Immediately notify all relevant parties, including your:

- Internal incident response team and information security group
- Merchant bank (also known as your acquirer or acquiring bank) – If you do not know the name and/or contact information for your merchant bank, contact the Visa Risk team for assistance:
  U.S. – +1 (650) 432-2978 or ***USFraudControl@visa.com***
  Canada – +1 (416) 860-3872 or ***CanadaInvestigations@visa.com***
  Latin America & Caribbean – +1 (305) 328-1593 or ***LACFraudInvestigations@visa.com***
  Asia Pacific (AP) and Central and Eastern Europe, Middle East and Africa (CEMEA) – ***VIFraudControl@visa.com***
- Manufacturer of the impacted payment device if you have determined that the incident involves the compromise of a PIN Entry Device (PED), specifically if it is a PCI PTS-approved device.
- Legal department to determine if laws mandating customer notification are applicable.

---

[7] Visa Core Rules and Visa Product and Service Rules, October 13, 2018, (*https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf*)

[8] Visa Bulletin: Member and Entity Obligation to Report Suspected or Confirmed Account Data Compromises, July 2017 (*https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-bulletin-data-compromise-reporting-requirements.pdf*)

[9] Visa U.S.A. August 2016

It is strongly recommended that you also immediately notify:

- The appropriate law enforcement agency in the event of an account data compromise.
- Federal law enforcement if the compromise is in the United States. The United States Secret Service Electronic Crimes Task Forces (ECTF) focuses on investigating financial crimes and can assist with incident response and mitigation of an account data compromise.

Visit ***www.secretservice.gov/investigation*** for ECTF field office contact information.

1. Perform Forensic Investigation
   - Visa may require you to engage a PCI Forensics Investigator (PFI) to perform an independent forensic investigation. If this is the case: engage a PFI (or sign a contract) within five (5) business days; provide Visa an initial forensic preliminary report within ten (10) business days from when contract is signed; provide Visa a final forensic report within ten (10) business days of completion of the review.

   For a list of approved PFI organizations please visit: https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators
2. Provide Exposed Accounts
   - Upload the compromised Visa account(s), known or suspected, to Visa's Compromised Account Management System (CAMS) within five (5) business days from the first to occur of the following events:
     - work with acquiring bank to upload accounts
     - for more information or assistance contact Visa at: CAMS@Visa.com.
3. Visa Initial Investigation Report
   - Upon notification of suspected or confirmed account data compromise, initial a preliminary investigation of all potentially impacted systems and those of 3rd-party service provides. Submit the following information via encryption, PGP encryption, Visa Online Secure Email, etc. the following:

Visa Investigation Report	
Name of entity:	
Type of entity:	
Acquirer BIN(s): (List all that are applicable.)	
Does the entity send transactions to a payment processor?	☐ Yes ☐ No *(If yes, attach a list of processor(s) and provide name and contact information. If reporting entity is a Processor, please provide a list of all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)*
Entity PCI DSS Level *(e.g. Level 1-4):*	
Entity PCI DSS Compliance Status:	*(If compliant, please attach proof of PCI DSS compliance documentation.)*
Approximate number of Visa transactions processed per year	• ATM • POS PIN/Debit • Credit
Is merchant entity corporate-owned or an individual franchise?	*(If merchant has other locations, please attach a list.)*
Name of payment application(s) and version(s):	• • • •

<table>
<tr><td rowspan="5">Identify responsible party(s) for the configuration and support of the Point of Sale (POS) solution
(e.g. Integrator, Reseller, or Agent).</td><td>NAME</td><td>TITLE</td><td>CONTACT</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="3">(If entity is an Integrator or Reseller, please attach a list all Acquirer BINs and all Merchant Names, Merchant Card Acceptor IDs, City and State.)</td></tr>
<tr><td>Is this a corporate or franchise mandated payment application and version?</td><td colspan="3"></td></tr>
<tr><td>Is the terminal PC-based or is it connected to a PC-based environment?</td><td colspan="3"></td></tr>
<tr><td>Is there remote access connectivity to the entity's environment?</td><td colspan="3">☐ Yes ☐ No
If yes, which organizations have remote access?
•
•
•</td></tr>
<tr><td>What type of remote access solution is used?</td><td colspan="3"></td></tr>
<tr><td>Is remote access always on or is it enabled upon request?</td><td colspan="3"></td></tr>
<tr><td>Is the Point of Sale device EMV enabled?</td><td colspan="3">☐ Yes ☐ No
If yes, provide name and model number.</td></tr>
<tr><td>Is the POS solution enabled with point-to-point encryption?</td><td colspan="3">☐ Yes ☐ No
If yes, provide details.</td></tr>
<tr><td>Does the entity accept PIN?</td><td colspan="3">☐ Yes ☐ No</td></tr>
<tr><td>Is the entity's PIN entry device (PED), PCI PTS approved and listed on the PCI SSC website?</td><td colspan="3">☐ Yes ☐ No
Provide the PED model, hardware, firmware and application and version numbers. Visit www.pcisecuritystandards.org/pin for the list of PCI-approved PIN entry devices.</td></tr>
</table>

Is the entity co-located or hosted?	If hosted, provide name and contact information of the hosting provider.
Provide the shopping cart application and version information, if applicable.	
Describe any recent changes to the network and/or systems.	• Payment application upgrades ☐ Yes ☐ No • Installation of a firewall ☐ Yes ☐ No • Installation of an anti-virus program ☐ Yes ☐ No • Changes to remote access authentication ☐ Yes ☐ No OTHER: • • •
Has the entity received complaints regarding fraudulent transactions from their customers?	☐ Yes ☐ No Is yes, please describe.
Has entity been contacted by law enforcement regarding fraudulent transactions?	☐ Yes ☐ No If yes, list date(s) and by which law enforcement agency. • • •
If Account Data Compromise is Confirmed Provide the Following	
How and when was the incident identified?	
How did the compromise take place?	Attach documentation of the following, if known: • List of vulnerabilities that caused or contributed to the compromise • Sample of any phishing emails • Details of unauthorized activity • List of malicious IPs • Malware information, if applicable

Did entity notify law enforcement?	☐ Yes ☐ No If yes, which agency and when were they notified? Provide contact information if applicable.
If known, how many Visa cards were compromised (accounts made vulnerable as a result of a data security breach)?	
Have the impacted accounts been uploaded to CAMS?	
What data elements were compromised and/or exposed?	☐ Primary Account Number (PAN) ☐ Expiration Date ☐ Full Track 1 and/or 2 ☐ PIN ☐ CVV2 Cardholder personally-identifiable information (PII) ☐ Cardholder Name ☐ Social Security Number ☐ Date of Birth ☐ Other:
Has the compromise been contained? If yes, how?	☐ Yes ☐ No If yes, how?

Discover Card Specific Steps:

1. Within 24 hours of a data compromise or breach, notify Discover Fraud Prevention at (800) 347-3083. If an application has been submitted and access to the Discover *Account Incident Manager (AIM)* web portal has been provided, please log in and use Discover's reporting tool to report incidents[10].
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from Discover Card.

[10] Discover Global Network, Securing payments at home and abroad, Management Tools Tab, "*Fraud management tools for issuers and acquirers*", (*https://www.discoverglobalnetwork.com/en-us/business-resources/fraud-security/products-tools/*)

American Express Specific Steps[11]:

1. Notify American Express immediately and in case later than 24 hours after the discovery of data incident. To notify American Express Enterprise Incident Response Program (EIRP) at (888) 732-3750 in the U.S or email at EIRP@aexp.com.
2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
3. Prepare a list of all known compromised account numbers.
4. Obtain additional specific requirements from American Express.

SUMMARY

MasterCard

Contacts	***Office Phone***	***E-Mail***
MasterCard	(636) 722-6636 or (800) 999-0363-MC Connect; OR (800) 307-7309	compromised_account_team@MasterCard.com
MasterCard Merchant Fraud Control Department		
Use the ADC Reporting Form (ARF) located within the Manage My Fraud and Risk Programs application on MasterCard Connect™. ***www.MasterCardconnect.com***		

Visa Fraud USA

Contacts	***Office Phone***	***E-Mail***
Visa Fraud Control Group	(650) 432-2978	USFraudControl@visa.com CAMS@Visa.com (Visa Compromised Account management System)

American Express USA

Contacts	***Office Phone***	***E-Mail***
American Express Merchant Services	(888) 732-3750	EIRP@aexp.com

Discover

Contacts	***Office Phone***
Discover Fraud Prevention	(800) 347-3083

[11] American Express Merchant Reference Guide – U.S., October 2018, (*https://www.americanexpress.com/content/dam/amex/us/merchant/merchant-channel/US_RefGuide_October_2018-Final.pdf*)

Appendix B – U.S. Privacy Legislation

The following are selected United States laws and regulations relating to the breach of confidential and/or personal information about an individual. This Appendix should not be considered a complete list.

The Privacy Act of 1974, 2015 Edition (Department of Justice's Office of Privacy and Civil Liberties)

The "Overview of the Privacy Act of 1974, 5 U.S.C. § 552a," establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies and was prepared by the Department of Justice's Office of Privacy and Civil Liberties (OPCL). The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements. The Overview is a comprehensive treatise of existing Privacy Act case law, however the policy guidance role statutorily rests with the Office of Management and Budget (OMB), 5 U.S.C. § 552a(v).[12].

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191

The primary focus of HIPAA was to improve the health insurance accessibility to people changing employers or leaving the workforce. It also addressed issues relating to electronic transmission of health-related data in Title II, Subtitle F of the Act entitled "Administrative Simplification". The administrative simplification provisions include four key areas:

- National standards for electronic transmission, transactions and code sets
- Unique health identifiers for providers, employers, health plans and individuals
- Security Standards
- Privacy Standards

The HIPAA Security Standards require a covered entity to implement policies and procedures to ensure:

- the confidentiality, integrity, and availability of all electronic protected health information
- protect against any reasonably anticipated threats or hazards to the security of such information
- protect against any reasonably anticipated uses or disclosures that are not permitted

Within this context, HIPAA requires a covered entity to implement policies and procedures to address security incidents. A security incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system (164.304). Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

[12] The United States Department of Justice, "Overview of the Privacy Act of 1974, 2015 Edition" (*https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition*), Washington, DC 20530-0001.

The HIPAA security standards were effective on April 21, 2003. The compliance date for covered entities is by April 21, 2005 and April 21, 2006 for small health plans.

Gramm-Leach-Bliley Act (GLBA), Public Law 106-102

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and Pretexting provisions.

The GLB Act gives authority to eight federal agencies and the states to administer and enforce the Financial Privacy Rule and the Safeguards Rule. These two regulations apply to "financial institutions", which include not only banks, securities firms and insurance companies, but also companies providing many other types of financial products and services to consumers. Among these services are lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities. Such non-traditional "financial institutions" are regulated by the FTC.

The Financial Privacy Rule (Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. §§ 6801, 6809) governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they are financial institutions, who receive such information. The Privacy Rule protects nonpublic personal information (MPI) and requires financial institutions to provide customers with a privacy notice when a relationship is established and yearly thereafter.

The Safeguards Rule (Subtitle A: Disclosure of Nonpublic Personal Information, codified at 15 U.S.C. §§ 6801, 6809) requires all financial institutions to conduct a thorough risk assessment of its security measures and design, implement and maintain a comprehensive information security program and safeguards to protect customer information. Additionally, financial institutions are required to develop a written security plan detailing procedures for protection of consumer personal financial information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions – such as credit reporting agencies – that receive customer information from other financial institutions. **The Rule requires the organization to consider all areas of its operations including employee management and training; information systems; and detecting and managing system failures. Effective security includes, but is not limited to, the prevention, detection and response to attacks, intrusions or other system failures. Specific considerations include maintaining up-to-date and appropriate programs and controls by following a written contingency plan to address any breaches of nonpublic confidential information and notify customers if their confidential information is subject to loss, damage, or unauthorized access.**

The Pretexting provisions (Subtitle B: Fraudulent Access to Financial Information, codified at 15 U.S.C. §§ 6821, 6827) of the GLB Act protect consumers from individuals and companies that obtain their personal financial information under false pretenses, a practice known as "pretexting" or "social engineering". It is illegal for any person to obtain/attempt to obtain, or attempt to disclose/cause to disclose customer information of a financial institution by false pretenses or deception (e.g., phishing, social engineering, fake websites, etc.) according to the GLB Act.

The Privacy Rule was enacted on November 12, 1999 and compliance on July 1, 2001. The Safeguard Rule was effective on May 23, 2003.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and
    - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.[13 & 14]

[13] U.S. Department of Education, *"Family Educational Rights and Privacy Act (FERPA)", (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html),* Washington, DC 20202-8520.
[14] U.S. Department of Education, "December 2011 – Revised FERPA Regulations: An Overview for SEAS and LEAS", (*http://www2.ed.gov/policy/gen/guid/fpco/pdf/sealea_overview.pdf*).

Appendix C – Incident Response Notification

Escalation Members (VP Level of Management)

Escalation - First Level
- Chief Information Security Officer (CISO)
- Enterprise Computing (EC)
- Office of Institutional Compliance
- Telecommunications Infrastructure (TI)

Escalation - Second Level
- Information Resource Manager (IRM)/Chief Information Officer (CIO)
- Executive Vice President
- Director, Office of Auditing and Consulting Services (OACS)
- Office of Legal Affairs

Auxiliary Members (as needed)

- Business Client Systems Manager
- Management of Client Department Affected by Incident
- Risk Management
- Office of Legal Affairs
- Loss Prevention
- University Communications

External Contacts (as needed)

- Internet Service Provider (if applicable)
- Internet Service Provider of Intruder (if applicable)
- Communications Carriers (local and long distance)
- Business Partners
- Insurance Carrier
- External Response Teams as applicable (CERT Coordination Center[15], etc.)
- Law Enforcement
  - Local Police Force (jurisdiction determined by crime)
  - Federal Bureau of Investigation (FBI) (especially if a federal interest computer or a federal crime is involved)
  - Secret Service

[15] The CERT/CC is a major reporting center for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. For more detailed information about the CERT/CC, see *http://www.cert.org*.

Notification Order

Information Security Office (central point of contact)
Chief Information Security Officer
Information Resource Manager/CIO (When nature and impact of incident has been determined)
Executive Vice President
Enterprise Computing/Data Owners
Appropriate Client Systems Managers:
Systems/Server Support
Data Management Team
- Reporting Team
- Database/Goldmine/Oracle Team
- SQL Team

Development and Programming Teams
- Programming
- Web Development

Construction and Infrastructure Manager
Office of Institutional Compliance
Office of Auditing and Consulting Services (OACS)
Vice President for Business Affairs (VPBA)
Office of Legal Affairs
University Communications
Business Partners (if connection/data has been compromised; avoid downstream liability)
Human Resource Services

Acknowledgments

The University of Texas at El Paso expresses appreciation to the *AICPA/CICA Task Force* for granting permission to copy, download, tailor, and disseminate the Incident Response Plan.

AICPA/CICA Privacy Task Force
Chair
Everett C. Johnson, CPA
Deloitte & Touche LLP (retired)
Vice Chair
Kenneth D. Askelson, CPA/CITP, CIA
JCPenney Company
Mary Grace Davenport, CPA
PricewaterhouseCoopers
Eric K. Federing
KPMG LLP
Marilyn Greenstein, Ph.D.
Accounting & Information Systems
Arizona State University—West
Don H. Hansen, CPA
Moss Adams LLP
Philip M. Juravel, CPA
Juravel & Company, LLC
Sagi Leizerov, Ph.D.
Ernst & Young LLP
Doron M. Rotman, CPA (Israel), CISA, CIA, CISM
KPMG LLP
Kerry Shackelford, CPA
KLS Consulting LLC
Donald E. Sheehy, CA, CISA
Deloitte & Touche LLP
AICPA Staff
Nancy A. Cohen, CPA, Senior Technical Manager, Business Reporting, Assurance and Advisory Services
Paul Herring, Director, Business Reporting, Assurance and Advisory Services