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.

Created: June 2009
Revised: June 2010
Revised: January 2012
Revised: November 8, 2013

\(^1\) 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 ........................................................................................................................................... 4  
Purpose .................................................................................................................................................. 4  
Scope ................................................................................................................................................... 4  
Roles and Responsibilities .................................................................................................................... 5  
General .................................................................................................................................................. 6  
Incident Response Team Notification .................................................................................................... 7  
Types of Incidents ................................................................................................................................ 7  
Definitions of a Security Breach ........................................................................................................... 8  
Requirements ........................................................................................................................................ 8  
Data Owner Responsibilities .................................................................................................................... 8  
Location Manager Responsibilities ......................................................................................................... 9  
When Notification Is Required ............................................................................................................. 9  
Incident Response – Breach of Confidential Information ...................................................................... 10  
Conclusion ............................................................................................................................................ 17  
Appendix A1 – Payment Card Industry Data Security Standard ............................................................. 18  
Appendix A2 – Cardholder Requirements ............................................................................................ 20  
Appendix B – U.S. Privacy Legislation .................................................................................................. 22  
Appendix C – Incident Response Notification ...................................................................................... 25  
Acknowledgments .................................................................................................................................. 27
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 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 mitigating 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.

Scope
The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. 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.

\(^2\) 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.
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
- Office of Auditing and Consulting (OACS)

**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

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
- Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach

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 necessary 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 Technology Department 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 Technology Department with any information relating to a suspected breach
• Collects pertinent information regarding the incident at the request of the CISO

**Office of Auditing and Consulting Services (OACS)**
• Reviews systems to ensure compliance with information security policy and controls
• Performs appropriate audit test work to ensure mission-critical systems are current with service packs and patches
• Reports any system control gaps to management for corrective action

**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 and [http://www.utep.edu/privacy.aspx](http://www.utep.edu/privacy.aspx).

**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.

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 Number (800/880)
- 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
  * If the individual is a Visa, MasterCard, American Express, or Discover cardholder, follow additional procedures outlined in the Appendix A2.
- Credit Card Numbers

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, etc.

**Incident Response Team Notification**

The Information Security Office (ISO) will be the central point of contact for reporting computer 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.

Requirements
Data owners 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 and 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 Responsibilities
Data owners 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 company and any third party involved with a privacy breach affecting the University’s data.

All data owners must report any suspected or confirmed breach of confidential information on individuals to the 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 on individuals. The CISO will notify the IRM/CIO, Executive Vice President, and data owners whenever a breach or suspected breach of confidential information on individuals 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 will act as a central point of contact for reaching the CISO, IRM/CIO, and Executive Vice President. (This should also be put in the Incident team notification section)

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.
Location Manager Responsibilities

Location managers 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 location, the location manager 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 on an individual.

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 either paper or electronic form.
- An intruder has broken into database(s) that contain confidential information on an individual.
- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing confidential information on an individual has been lost or stolen.
- A department or group has not properly disposed of records containing confidential information on an individual.
- 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 on an individual 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 on an individual 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 keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

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

1. The ISO will serve as a central point of contact for reporting any suspected or confirmed breach of confidential information on an individual.
   Information Security Office contact information: (915) 747-6324 or the Help Desk at extension 4357 (HELP) or 747-5257 from off-campus

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 and immediately notify the CISO.

3. The ISO will contact the CISO. The ISO advises that a breach or suspected breach of confidential information on an individual has occurred. 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 executive management and other auxiliary members as needed.

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

1. When notified by the ISO, the CISO performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.

2. Informs the IRM/CIO, Executive Vice President, Office of Legal affairs and the Office of Institutional Compliance office that a possible privacy breach has been reported and provides them an overview of the situation.

3. Contacts 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 about an individual. Every breach may not require participation of 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 the Institutional Compliance office.

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 database and system administrators 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, Office of Institutional Compliance and Data Owner(s), determine additional notification requirements (e.g., Human Resources, external parties).

11. If the breach occurred at a third party location, determine if a legal contract exists. Work with the IRM/CIO, Executive Vice President, Office of Legal Affairs, Office of Institutional Compliance, and Data Owner(s) 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 data stored and compromised on all test, development and production systems and the number of individuals at risk.

13. Determine the type of confidential information that is at risk, including but not limited to: Name, Address, Social Security Number, Account number, Cardholder name, Cardholder address, Medical and Health Information

14. If confidential information is involved, have the Data Owner(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 corporate network, test and production environments, virtual private networks, and modem connections. 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 on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.
   - 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 it 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 corporate wireless network.

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: Visa has specific procedures that must be followed for evidence preservation.
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

<table>
<thead>
<tr>
<th>Data Owners / Enterprise Computing</th>
<th>(915) 747-5257</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems Support</td>
<td>(915) 747-5070 or <a href="mailto:sysadmin@utep.edu">sysadmin@utep.edu</a></td>
</tr>
<tr>
<td>Data Management</td>
<td>(915) 490-3206 or <a href="mailto:DataManagement@utep.edu">DataManagement@utep.edu</a></td>
</tr>
<tr>
<td>Development</td>
<td>(915) 490-3243</td>
</tr>
<tr>
<td>Programming</td>
<td>(915) 490-3201 or <a href="mailto:Programmers@utep.edu">Programmers@utep.edu</a></td>
</tr>
</tbody>
</table>

### Notification Steps

**Enterprise Computing or Data Owner(s)**

1. If the Enterprise Computing or Data Owner(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) 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.).
**Development and Programming Groups**

1. Development and Programming Groups will serve as the primary contact for the online sales or web applications. Development and Programming, and Systems Support Groups are available 24x7 and should be contacted as shown above.

2. When notified by the ISO that the privacy breach incident response plan has been activated, Systems Operations will collect pertinent information regarding the incident from the CISO and determine the appropriate systems in which to begin inspecting. 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. Systems Operations, 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, etc.). They will look for suspicious activity that may suggest the application interface to processing systems was 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: (915) 747-6324 or security@utep.edu
   - Information Resource Manager/Chief Information Officer: (915) 747-5216
   - Information Security Office: (915) 747-6324 or security@utep.edu
   - Development Teams: (915) 490-3243
   - Programming Teams: (915) 490-3201 or Programmers@utep.edu
   - Data Management Team: (915) 490-3206 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. New credit card applications
      iii. 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 about individuals.

5. Report all findings to the Incident Response Plan Team.

6. Within 24 hours of notification of an account number compromise, 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

---

**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 organization enters that may have an impact or effect on our customers, employees, and other data.

3. Be aware of other companies’ privacy policies that may affect our organization and affiliates.

**When a Privacy Breach Occurs:**

1. After confirmation that a breach of confidential information on individuals has occurred, notify the IRM/CIO, Office of Institutional Compliance, and Office of Legal Affairs.

2. Coordinate activities between business area and other departments (e.g., HRS, 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 University Relations on the timing and content of notification to individuals.

5. If the ISO determines 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 CISO is assured that necessary measures have been taken to determine the scope of the breach and properly investigated.

7. Follow approved procedures for any notice of unauthorized access to confidential information about individuals.

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](http://www.ftc.gov/idtheft). The toll-free number for the identity theft hotline is 1-877-IDTHEFT.

**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 on an individual, 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 appropriate, notify the business area that a breach has been reported and is under investigation.
5. Work with the business area to ensure there is no further exposure to privacy breaches.
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) 747-8719 or TI@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 to close any exposures identified during the investigation.
Ongoing:
1. Monitor consumer privacy issues and practices of other companies.
2. Monitor consumer privacy breaches of other companies and how they respond.

When Privacy Breach Occurs:
1. After confirmation that a breach of confidential information about individuals has occurred, notify the University Relations Director and ISO.
2. Coordinate with the Executive Vice President, University Communications 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 organization is doing to correct breach, how it happened and the organization’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.

1. If the Location Manager becomes aware of or identifies a privacy breach, contact the ISO to ensure that the CISO and other primary contacts are notified.
2. The Location Manager will secure the area of the breached information (e.g. computer room, data center, records room).
3. The Location Manager will assist CISO as needed in the investigation.
4. The Location Manager will keep CISO updated on appropriate investigation information gathered.
Conclusion
This document provides a useful template for developing an appropriate approach to handling the risks associated with a threat to an organization because of a privacy breach, no matter how caused. 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.
Appendix A1 – Payment Card Industry Data Security Standard

Background:
The PCI Data Security Standard, revised in October 2010, 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.

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 Plan3 (see next page).

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

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 Industry Self-Assessment Questionnaire, see https://www.pcisecuritystandards.org/saq/index.shtml.

PCI Data Security Standard Incident Response Plan Details

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create an incident response plan to be used in the event of system compromise. Ensure the plan addresses, at a minimum, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies (for example, informing Acquirers and credit card associations).

12.9.2 Test the plan at least annually.

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.

12.9.4 Provide appropriate training to staff with security breach response responsibilities.

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.

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

---

Appendix A2 – Cardholder Requirements

Specific requirements for reporting suspected or confirmed breaches of cardholder data – notify PCI SSC as well as payment card companies.

Payment Card Industry Security Standards Council (PCI SSC)\(^5\)
Notification must take place no later than 24 hours after the vendor first discovers the security breach or compromise by phone call to the PCI SSC PA-DSS Coordinator (781-876-8855), followed by an e-mail, fax, or letter providing full details of the security breach or compromise. Notwithstanding any other legal obligations the vendor (University) may have, the vendor must immediately notify PCI SSC of any security breach, compromise, or known vulnerability relating to any vendor’s payment application listed by PCI SSC. The vendor must also provide immediate feedback about any potential impact (possible or actual) breach or vulnerability has had, may have, or will have.


To comply with MasterCard Security Rules and Procedures section 10.2.2, the University must contact MasterCard immediately when they become aware of a Potential Account Data Compromise Event or an ADC Event.

Visa U.S.A. Requirements: Please refer to the VISA What To Do If Compromised, Version 3.0 dated May 2011 and VISA Responding to a Data Breach: Communications Guidelines for Merchants for detailed information.

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 or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the Visa U.S.A. Cardholder Information Security Program. If Visa U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating the loss of this information, Visa U.S.A. may require immediate corrective action\(^6\).

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, Visa may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, or
- Permanently prohibit the merchant or its agent from participating in Visa programs.\(^7\)

---


\(^6\) Visa U.S.A. November 2003 Operating Regulations 2.3.F.5

\(^7\) Visa U.S.A. November 2003 Operating Regulations 2.3.F.7
**Discover Card Specific Steps:** Please refer to the following website for detailed information

1. In the event of an account compromise event, notify Discover Fraud Prevention immediately at (800) 347-3102 or 3083.
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.

**American Express:** Please refer to the American Express Data Security Operating Policy – U.S. for detailed information.

1. In the event of an account compromise event, notify American Express Merchant Services immediately and in no case later than 24-hours after discovery of a Data Incident at (888) 732-3750 or by email at EIRP@aexp.com in the U.S.
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**

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Office Phone</th>
<th>Encrypted E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>MasterCard Compromised Account Team</td>
<td>636-722-4100</td>
<td><a href="mailto:compromised_account_team@mastercard.com">compromised_account_team@mastercard.com</a></td>
</tr>
<tr>
<td>MasterCard Merchant Fraud Control Department</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Visa Fraud USA**

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Office Phone</th>
<th>Encrypted E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa Fraud Control Group</td>
<td>650-432-2978</td>
<td><a href="mailto:usfraudcontrol@visa.com">usfraudcontrol@visa.com</a></td>
</tr>
</tbody>
</table>

**American Express USA**

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Office Phone</th>
<th>Encrypted E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Express Merchant Services</td>
<td>888 732-3750</td>
<td><a href="mailto:EIRP@aexp.com">EIRP@aexp.com</a></td>
</tr>
</tbody>
</table>

**Discover**

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Office Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discover Fraud Prevention</td>
<td>800-347-3102 or 800-347-3083</td>
</tr>
</tbody>
</table>
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, 2010 Edition (Department of Justice’s Office of Privacy and Civil Liberties)

The "Overview of the Privacy Act of 1974," prepared by the Department of Justice's Office of Privacy and Civil Liberties (OPCL), is a discussion of the Privacy Act's disclosure prohibition, its access and amendment provisions, and its agency recordkeeping requirements. Tracking the provisions of the Act itself, the Overview provides reference to, and legal analysis of, court decisions interpreting the Act's provisions. The Overview is not intended to provide policy guidance, as that role statutorily rests with the Office of Management and Budget (OMB), 5 U.S.C. § 552a(y). However, where OMB has issued policy guidance on particular provisions of the Act, citation to such guidance is provided in the Overview. The 2010 edition of the Overview was issued electronically and sent for publication in February 2010 and includes cases through November 2009. The Overview is scheduled to be revised again in 2012.

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.

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 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. It requires financial institutions to provide customers with a privacy notice when a relationship is established and yearly thereafter.

The Safeguards Rule requires all financial institutions to design, implement and maintain 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 managing system failures. Effective security includes 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 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”.

The Privacy Rule took effect on November 13, 2000 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.9 & 10

---

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\textsuperscript{11}, 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

\textsuperscript{11} 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 (HRS)
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