TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: Incident Response (IR)

Policy Statement:

TTUHSC El Paso shall establish an actionable IT security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities.

Reason for Policy:

The purpose of the Incident Response (I R) policy is to establish a protocol to guide TTUHSC El Paso's response to a cyber-security or other Information Security Incidents.

Entities Affected by this Policy are any and all users of Information Resources at TTUHSC El Paso.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of: policy & procedures, incident response training, incident response testing, incident handling, monitoring, reporting, reporting assistance, response plan, spillage response, and integrated information security analysis team.

It is the stance of TTUHSC El Paso to ensure that there are safeguards in place aligned with NIST 800-53 and TAC 202 to ensure the protection, integrity, and confidentiality of information resources at TTUHSC El Paso.

Who Should Read this Policy?

All individuals accessing, storing, viewing any TTUHSC El Paso information resources.

What happens if I violate this policy?

Any person(s) violating TTUHSC El Paso Information Technology policies are subject to penalty under federal, state, and local legislation. Disciplinary actions are further outlined in 56.50 Sanctions Policy.1

Incident Response Sanctions also include:

1. A failure to report a suspected or abnormal event by any employee, student, or vendor, may result in the disciplinary actions as defined in HSCEP Information Technology Policy 56.01.10. [7]
2. Disciplinary actions also include but are not limited to:
    1. In the event that a system user is found to be out of compliance with this policy or impede Information Security efforts, they are required to complete additional security awareness training within 30 days of incident.
    2. If the end user fails to comply with sanctions for policy violation, they are subject to additional sanctions that include, but are not limited to reduction in privileges, security monitoring, and access restrictions.
3. Incidents will be reported to Human Resources Department. For repeated incidents, additional disciplinary actions as aligned with Compliance and Human Resource disciplinary policies will apply.

IR-01: Incident Response Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

TTUHSC El Paso is required to document organization-wide response controls that, at a minimum, include:

- A formal, documented incident response policy; and
- Processes to facilitate the implementation of the incident response policy, procedures and associated controls.

The Information Security Office will conduct periodic reviews of detected abnormal events and will verify whether these events are being reported per this policy, by employees, students, and vendors at TTUHSC El Paso. The Information Security Officer will assess the CIRT's effectiveness to implement incident handling and response in two ways: lessons learned phase as established in the Incident Response Plan per incident, and conduct an annual test incident to determine gaps in the policy, handling procedures, and response plan

IR-02: Incident Response Training

TTUHSC El Paso:

- Trains personnel in their incident response roles and responsibilities with respect to systems; and
- Provides refresher training.

TTUHSC El Paso Information Security staff are required to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

IR-03: Incident Response Testing

TTUHSC El Paso tests and/or exercises the incident response capability for systems using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results.3

TTUHSC El Paso management and IT staff are required to perform annual tests and/or exercises of its incident response capability to formally determine incident response effectiveness and make corrections, based on any deficiencies.

Incident Response Testing includes:

Coordination with Related Plans
Process owners must ensure coordinated incident response testing is conducted with appropriate personnel responsible for related plans.

IR-04: Incident Handling

TTUHSC El Paso Information Security:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

TTUHSC El Paso Information Security staff are required to:

a. Identify the severity and classification of incidents; and
b. Define appropriate actions to take in response to ensure the continuation of business functions.

Incident Handling includes:

Automated Incident Handling Processes
Where technically feasible, TTUHSC El Paso shall employ automated mechanisms to support the incident handling process.

Identity Theft protection Program (ITPP)
TTUHSC El Paso is required to maintain an Identity Theft Protection Program (ITPP) that is focused on preventing identity theft incidents. TTUHSC El Paso shall take precautions to detect, prevent, and mitigate identity theft through the following means;

a. Identity relevant patterns, practices, and specific forms of activity that signal possible identity theft and incorporate those warnings into the ITPP:
   i. Alerts, notifications or warnings from a Consumer Reporting Agency;
   ii. Suspicious documents;
   iii. Suspicious personal identifying information;
   iv. Unusual use of, or suspicious activity related to, the covered account; and
   v. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.
b. Detect Red Flags that have been incorporated into the ITPP;
c. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
d. Ensure the ITPP is updated periodically to reflect changes in risks from identity theft

IR-05: Incident Monitoring

TTHUSC El Paso tracks and documents system security incidents.

TTUHSC El Paso Information Security staff are responsible for managing and documenting security incidents.

IR-06: Incident Reporting

TTUHSC El Paso:

- Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
- Reports security incident information to designated authorities.

Users are responsible for reporting system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to TTUHSC El Paso's IT security personnel. Please see reporting procedure in Table 1.

Incident Reporting includes:

Automated Reporting
Where technically feasible, TTUHSC El Paso shall employ automated mechanisms to assist in the reporting of security incidents.

Cyber Incident Reporting for Covered Defense Information (CDI)
Upon discovery of a cyber incident that affects a Covered Contractor Information System (CCIS) or the Covered Defense Information (CDI) residing therein, or that affects TTUHSC El Paso's ability to perform the requirements of the contract that are designated as operationally critical support, TTUHSC El Paso shall:

a. Conduct a review of evidence of compromise of CDI, including but not limited to, identifying compromised computers, servers, specific data, and user accounts.
    i. This review shall also include analyzing CCIS(s) that were part of the cyber incident, as well as other information systems on TTUHSC El Paso's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect TTUHSC El Paso's ability to provide operationally critical support; and
    ii. Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

b. The cyber incident report shall be treated as information created by or for Department of Defense (DoD) and shall include, at a minimum, the required elements at http://dibnet.dod.mil;

c. If applicable, submit identified and contained malicious software in accordance with instructions provided by the DoD Contracting Officer;

d. Preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least ninety (90) days from the submission of the cyber incident report to allow DoD to request the media or decline interest; and

e. Upon request by DoD, provideDoD with:
    i. Access to additional information or equipment that is necessary to conduct a forensic analysls; and
    ii. All of the damage assessment information gathered

IR-07: Security Concept Of Operations

TTUHSC El Paso provides an incident response support resource that offers advice and assistance to users of systems for the handling and reporting of security incidents.

TTUHSC El Paso management and IT staff are required to establish a direct, cooperative relationship between its incident response capability and stakeholders (internal & external).

Incident Reporting Assistance includes:

Automation Support of Availability of Information/Support
Where technically feasible, TTUHSC El Paso shall employ automated mechanisms to increase the availability of incident response-related information and support.

Coordination With External Providers
The Cyber Security Incident Response Team (CIRT):

a. Is TTUHSC El Paso's integrated digital security analysis team; and

b. Designates incident response personnel to:
    i. Be available on a 24/7 basis to respond to potential incidents; and
    ii. Assign personnel to establish and maintain direct, cooperative relationships with applicable external providers.

IR-08: Incident Response Plan (IRP)

TTUHSC El Paso Information Security:

Develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;
- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by designated officials within the organization;
- Distributes copies of the incident response plan to incident response personnel (identified by name and/or

by role) and organizational elements;

- Reviews the incident response plan on an organization-defined frequency;
- Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
- Communicates incident response plan changes to incident response personnel (identified by name and/or by role) and organizational elements.

TTUHSC El Paso Information Security staff are required to:

a. Be prepared to respond immediately to information security-related incidents;
b. Create the Incident Response Plan (IRP) to be implemented in the event of a system breach.
c. Test the IRP at least annually;
d. Designate specific personnel to be available on a 24/7 basis to respond to alerts;
e. Provide appropriate training to staff with security breach responsibilities;
f. Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems;
g. Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments; and
h. Ensure the plan addresses the following, at a minimum;
   i. Roles, responsibilities, and communication and contact strategies in the event of a compromise;
   ii. Specific incident response procedures;
   iii. Business recovery and continuity procedures;
   iv. Data backup processes;
   v. Analysis of legal requirements for reporting compromises;
   vi. Coverage and responses of all critical system components; and
   vii. Reference or inclusion of incident response procedures from legal or contractual sources, if applicable.

In the event of a "large incident", the Institution Head of TTUHSC El Paso, the information Resource Manager, and other executive level management, will provide support and the necessary resources (financial, staff, etc.) to the Information Security Officer, the Information Security Office, Computer Incident Response Team, and Information Technology to mitigate exposure and loss.4,5,6

The activities of the TTUHSC El Paso Information Security Office, in collaboration with other IT and non-IT personnel, are performed in response to any situation determined to be either a potential or actual incident.

Table 1

Action by:	Action:
System User	1. Reports abnormal event to the IT Helpdesk via phone call at 915-215-4111 or if possible via email to ELP.HelpDesk@ttuhsc.edu.
IT Helpdesk Personnel	2. Receives report from System User and immediately notifies the Information Security Office.
CIRT (First Responder)	3. Validates abnormal event as an incident or not. a. If event is determined an incident, reports to the Information Security Officer
Information Security Officer	4. Determines level of incident as either small, medium, or large.

	5. Assigns CIRT Lead if incident is classified as medium or higher. 6. Activates Incident Response Plan. [4] 7. Notifies the Chief Information Officer/Information Resources Manager when incident is classified medium or higher.
CIRT (Lead & Team)	8. Implements remaining phases to handle incident as defined in the Incident Response Plan. [4] 9. Tracks and documents the incident as per the Incident Response Plan. [4] 10. Reports back on incident resolution and results to the Information Security Officer.
Information Security Officer	11. Reports incident resolution and results to the Chief Information/Information Resources Manager, other executive level management, and the Department of Information Resources.

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

1. 56.50 Sanctions Policy
2. HIPAA 164.308(a)(6)(i)
3. NIST CSF PR.IP-10 & RS.CO-1 | PCI DSS 12.10.2
4. 4. PCI DSS 12.5.3 | NIST CSF DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.CO-3, RS.CO-4, RS.IM-1, RS>IM-2, RS.MI-1, RM.MI-2, RS.RP-1, RC.RP-1, RC.IM-1, RC.IM-2 & RC.CO-3
5. Fair and Accurate Credit Transactions Act (FACTA)
6. PCI DSS 12.5.2 | NIST CSF DE.AE-3, DE.AE-5, RS.AN-1 & RS.AN-4
7. HIPAA 164.308(a)(6)(ii) | PCI DSS 12.8.3 | MA201CMR17 17.03(2)(j0 | OR646A.604(1)-(5) | CA SB 1386 SEC2-Section 1798.29 | NIST CSF RS.CO-2
8. DFARS 252.204-7012
9. HIPAA 164.308(a)(6)(ii) | PCI DSS 12.8.3, 12.10, 12.10.1-12.10.6 | OR646A.622(2)(d)(B)(iii) | NIST CSF PR.IP-7, PR.IP-9, DE.AE-3, DE.AE-5, RS.AN-4, RS.CO-1, RS.CO-2, RS.CO-3, RS.CO-4, RS.IM-1, RS.IM-2, RS.RP-1, RC.RP-1, RC.IM-1 & RC.IM-2
10. PCI DSS 12.10.3
11. 45 CFR 164.308(a)(6)
12. HSCEP OP 56.01 – Acceptable Use of Information Technology Resources
13. TAC §202.70, §202.71, §202.74, §202.75

Revised May 2018