HSCEP OP: 56.50 – Contingency Planning (CP)

Policy Statement:

The purpose of the Contingency Planning (CP) policy is to establish procedures that will help TTUHSC El Paso management to quickly determine the appropriate actions to be taken due to an interruption of service or disaster.

Reason for Policy:

The purpose of Configuration Management (CM) policy is to establish and maintain the integrity of systems.

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: contingency planning, capacity planning, business functions, critical asset, training, testing, sites, telecommunications, backups, reconstitution and timely recovery.

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 HSCEP OP 56.50, Sanctions Policy.

CP-01: Contingency Planning Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- a formal, documented contingency planning 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 contingency planning policy and associated contingency planning controls.

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

a. A formal, documented IT-specific contingency plan; and
b. Processes to facilitate the implementation of the contingency plan, procedures and associated controls.

CP-02: Contingency Plan

TTUHSC El Paso:

- Develops a contingency plan for systems that:
  - Identifies essential missions and business functions and associated contingency requirements;

- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, assigned individuals with contact information;
- Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure;
- Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented; and
- Is reviewed and approved by designated officials within the organization;

- Distributes copies of the contingency plan to key contingency personnel;
- Coordinates contingency planning activities with incident handling activities;
- Reviews the contingency plan as required by the organization-defined frequency;
- Revises the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and
- Communicates contingency plan changes to key contingency personnel.

TTUHSC El Paso is required to establish, and implement as needed, procedures to enable the continuation of critical business processes while operating in the other-than-normal conditions, that includes:

a. Developing a contingency plan that:
   i. Identifies essential missions and business functions and associated contingency requirements;
   ii. Provides recovery objectives, restoration priorities, and metrics;
   iii. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   iv. Addresses eventual, full system restoration without deterioration of the security measures originally planned and implemented; and
   v. Is reviewed and approved by company management.
b. Distributing copies of the contingency plan to key contingency personnel;
c. Coordinating contingency planning activities with incident handling activities;
d. Reviewing the contingency plan at least annually;
e. Revising the contingency plan to address necessary changes;
f. Communicating contingency plan changes to key contingency personnel; and
g. Establishing procedures for obtaining access to sensitive data during other-than-normal or emergency conditions.

CP-03: Contingency Training

TTUHSC El Paso trains personnel in their contingency roles and responsibilities.4

Asset custodians and data/process owners are required to be trained in their contingency roles and responsibilities with respect to systems.

CP-04: Contingency Plan Testing

TTUHSC El Paso tests the contingency plan for the information using organization-defined tests and/or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.5

Information Technology personnel are required to perform a full recovery and reconstitution of critical systems to a known state as part of contingency plan testing, at least once a year.

Contingency Plan Testing includes:

Coordinate with Related Plans
Process owners must ensure coordinated contingency plan testing with appropriate personnel responsible for related plans.

CP-05: Contingency Plan Update

TTUHSC El Paso reviews the contingency plan and any test/exercise results to initiate corrective actions.6

Asset custodians and data/process owners are required to:

a. Review the entire contingency plan at least once a year;
b. Review any test/exercise results; and
c. Initiate corrective actions, as necessary.

CP-06: Alternate Storage Site

TTUHSC El Paso establishes an alternate storage site including necessary agreements to permit the storage and recovery of system backup information.7

The responsible party for TTUHSC El Paso's technology infrastructure is required to identify an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards, in the event of an area-wide disruption or disaster.

Alternate Storage Site includes:

Separation from Primary Site
Asset and process owners must identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

Accessibility
Asset and process owners must identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

CP-07: Alternate Processing Site

TTUHSC El Paso:

- Identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards; and
- Ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

The responsible party for TTUHSC El Paso's technology infrastructure is required to identify an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards, in the event of an area-wide disruption or disaster.

Alternate Processing includes:

Separation from Primary Site
Asset and process owners must identify an alternate processing site that is separate from the primary processing site to reduce susceptibility to the same threats.

Accessibility
Asset and process owners must identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Priority of Service
TTUHSC El Paso must develop alternate processing site agreements that contain priority-or-service provisions in accordance with availability requirements.

CP-08: Telecommunications Services

TTUHSC El Paso establishes alternate telecommunications services including necessary agreements to permit the resumption of information for essential missions and business functions within the organization's defined time period when the primary telecommunications capabilities system operations are unavailable.8

The responsible party for TTUHSC El Paso's technology infrastructure is required to establish alternate telecommunications services, including necessary Service Level Agreement (SLA) to permit the resumption

essential communication functions within an acceptable time period when the primary telecommunications capability is unavailable.

Telecommunications services includes:

Priority of service provisions
The responsible party for TTUHSC El Paso's technology infrastructure is required to develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the business operations availability requirements.

Single Points of Failure
TTUHSC El Paso must obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

CP-09: Information System Backup

If TTUHSC El Paso outsources IT-related activities, the organization:

- Conducts backups of user-level information contained in the systems;
- Conducts backups of system-level information contained in the systems;
- Conducts backups of system documentation including security-related documentation; and
- Protects the confidentiality and integrity of backup information at the storage location.

Asset custodians and data/process owners are responsible for:

a. Conducting backups of user-level information contained in systems;
b. Conducting backups of system-level information contained in systems;
c. Conducting backups of system documentation including security-related documentation; and
d. Protecting the confidentiality and integrity of backup information at the storage location.

Information System Backups include:

Testing for Reliability & Integrity
At least annually, asset owners and custodians must test backup information to verify media reliability and information integrity.

Separate Storage for Critical Information
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall store backup copies of critical information system software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the operational system.

CP-10: Information System Recovery & Reconstitution

TTUHSC El Paso provides for the recovery and reconstitution of systems to a known state after a disruption, compromise, or failure.

TTUHSC El Paso's IT department is required to provide for the recovery and reconstitution of systems to a known state after a disruption, compromise, or failure. This includes but is not limited to:

a. Conducting backups;
b. Maintaining backup solutions and media; and
c. Periodically testing backup solutions to validate that successful recovery is possible.

Information System Recovery & Reconstitution includes:

Transaction Recovery
For critical systems, asset custodians and data/process owners are required to provide for transaction recovery of systems that are transaction-based.

Failover Capability
For critical systems, asset custodians and data/process owners are required to provide real-time or near-real-time failover capability for critical systems.

Backup & Restoration Hardware Protection
For critical systems, asset custodians and data/process owners are required to provide for backup and restoration hardware and software.

Electronic Discovery (eDiscovery)
TTUHSC El Paso's IT department is required to provide for electronic discovery (eDiscovery) for communication transactions, covering both active and archived communications data.

Information System Imaging
TTUHSC El Paso's IT department is required to provide the capability to re-image systems from configuration-controlled and integrity-protected disk images representing a secure, operational state for the system.

Revised May 2018