HSCEP OP: 56.50 – Media Protection (MP)

Policy Statement:

TTUHSC El Paso shall protect system media, both hardcopy and digital, by limiting access to authorized users and sanitizing or destroying media so that unauthorized data recovery is technically infeasible.

Reason for Policy:

The purpose of the Media Protection (MP) policy is to ensure that access to both paper and digital media is limited to authorized individuals.

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 media protection & procedures, media access, media marking, media storage, media transportation, media sanitization, media use, and media downgrading.

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.

P-01: Media Protection Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates;1

- A formal, documented media protection 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 media protection policy and associated media protection controls.

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

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

MP-02: Media Access

TTUHSC El Paso restricts access to types of digital and non-digital media authorized individuals using organization-defined security measures.

Asset custodians and data/process owners are required to restrict access to digital and non-digital media to authorized individuals.

Auditable Events Include:

Automated Restricted Access
Asset custodians and data/process owners are required to assign Role-Based Access Control (RBAC) to the specific data that is under their care or line of business to limit access to authorized personnel.

Disclosure Of Information
TTUHSC El Paso personnel, including TTUHSC El Paso subcontractors, are prohibited from releasing any information, regardless of medium (e.g., film, tape, document), pertaining to any part of a contract or any program related to a contract to anyone outside the TTUHSC El Paso. The only exceptions are if:

- The project's contracting officer has given prior written approval; or
- The information is otherwise in the public domain before the date of release

MP-03: Media Marking

TTUHSC El Paso marks media in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings required, if any.

TTUHSC El Paso users are required to mark media in accordance with our Data Classification & Handling Guidelines listed in our Data Classification Policy.

MP-04: Media Storage

TTUHSC El Paso:

- Physically controls and securely stores digital and non-digital media within controlled areas using organization-defined security measures; and
- Protects system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.

TTUHSC El Paso users are required to:

a. Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility;
b. Review the location's security at least annually;
c. Physically secure all media;
d. Maintain strict control over the storage and accessibility of media; and
e. Maintain strict control over the internal or external distribution of any kind of media, including the following;
    I. Classify media so the sensitivity of the data can be determined.
    II. Send the media by secured courier or another delivery method that can be accurately tracked.

Media Storage Includes:

Cryptographic Protection (Encrypting Data At Rest)
TTUHSC El Paso users are required to render sensitive data unreadable anywhere it is stored by using strong cryptography with associated key-management processes and procedures.

Sensitive Data Inventories
Asset custodians and data/process owners of sensitive data are required to:

a. Maintain an inventory log of all media; and
b. Conduct media inventories at least annually

MP-05: Media Transportation

TTUHSC El Paso:

- Protects and controls digital and non-digital media during transport outside of controlled areas using organization-defined security measures;
- Maintains accountability for system media during transport outside of controlled areas; and
- Restricts the activities associated with transport of such media to authorized personnel.

TTUHSC El Paso users are required to ensure:

- Digital and non-digital media is protected during transport outside of TTUHSC El Paso-controlled areas using available security measures;
- Management must approve any sensitive media that is moved from a secured area;
- Accountability is maintained for system media during transport outside of TTUHSC El Paso-controlled areas; and
- Activities associated with transport of sensitive media are restricted to authorized personnel.

Media Transportation Includes:

Custodians
Data/process owners are required to ensure a dedicated custodian is identified throughout the transport of system media.

Cryptographic Protection (Encrypting Data In Storage Media)
Asset custodians and data/process owners are required to employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Ad-Hoc Transfers
Unscheduled, infrequent and one-time file transfers that contain sensitive data are required to be performed through encrypted transport protocols.

MP-06: Media Sanitization

TTUHSC El Paso:

- Sanitizes system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
- Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Media must be sanitized when it is no longer needed for business or legal reasons. TTUHSC El Paso asset custodians and data/process owners are required to destroy system media that cannot be sanitized, as follows:

- Shred, incinerate, or pulp hardcopy materials so that data cannot be reconstructed; or;
- Render data on electronic media unrecoverable so that data cannot be reconstructed.

Media Sanitation Includes:

Media Sanitation Documentation
Asset custodians and data/process owners are required to:

- Track, document, and verify media sanitization and disposal actions;
- Assign one individual or department responsible for coordinating data disposal and reuse of equipment; and

- Train staff members on the security risks associated with the reuse of equipment that stored or processed sensitive data.

Equipment Testing
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall test sanitization equipment and procedures, at least annually.

MP-07: Media Use

TTUHSC El Paso restricts the use of organization-defined types of digital and/or non-digital media on systems or system components using security safeguards.10

Asset custodians and data/process owners are required to employ technical and non-technical safeguards to restrict the insecure use of mobile computing and communications devices with information storage capability

Media Use Includes:

Prohibit Use Without Owner
TTUHSC El Paso prohibits the use of portable storage devices in TTUHSC El Paso-owned or managed systems when such devices have no identifiable owner.

Limitations On Use
To protect sensitive information, including, but not limited to Controlled Technical Information (CIT) and Covered Defense Information (CDI), TTUHSC El Paso personnel shall:

- Only access and use sensitive information for intended purposes;
- Protect against unauthorized release or disclosure; and
- Ensure applicable third parties implement mechanisms to restrict the use and distribution of sensitive data, in accordance with TTUHSC El Paso information security requirements.

To ensure sensitive data is not inadvertently released, management approval is required to downgrade the classification of media.

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

1) HIPAA 164.308(a)(4)(ii)(B) | MA201CMR17 17.03(2)(c)
2) HIPAA 164.308(a)(4)(ii)(C) | NIST CSF PR.PT-2
3) DFARS 252.204-7000
4) HIPAA 164.310(d)(b)(iv) | PCI DSS 9.5, 9.5.1, 9.6, 9.6.1, 9.6.2, 9.7 & 9.9 | MA201CMR17 17.03(2)(c) | OR646A.620 & ORS646A.622(2)(d)(C)(i) | NIST CSF PR.PT-2
5) PCI DSS 3.4, 3.4.1 & 9.8.2
6) PCI DSS 9.7.1
7) HIPAA 164.310(d)(a) | PCI DSS 9.6, 9.6.2, 9.6.3 & 9.7 | MA201CMR17 17.03(2)(c) | OR646A.620 | NIST CSF PR.PT-2
8) HIPAA 164.310(d)(b)(i) | PCI DSS 9.8, 9.8.1 & 9.8.2 | OR646A.622(2)(d)(C)(i) & OR646A.622(2)(d)(C)(iv) | NIST CSF PR.DS-3 & PR.IP-6
9) HIPAA 164.310(d)(b)(ii) | PCI DSS 9.7.1
10) NIST CSF PR.PT-2
11) DFARS 252.204-7009
12) TAC §202.74, §TAC 202.75