HSCEP OP: Identification & Authentication (IA)

Policy Statement:

TTUHSC El Paso shall implement mechanisms are employed to properly identify system users, processes acting on behalf of users, or devices, and authenticate the identities of those users, processes, or devices.

Reason for Policy:

The overall policy addresses the Institutional stance as it applies to TTUHSC El Paso in the areas of identification and authentication, account management, device-to-device identification and authentication, identifier management, authenticator management, timely maintenance, and cryptographic module authentication.

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.

What is covered in this Policy?

The overall policy addresses the Institutional stance as it applies to internal use and information sharing with third parties.

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.

IA-01: Identification & Authentication Policy & Procedures

TTUHSC El Paso develops, disseminates, reviews & updates:

- A formal, documented identification and authentication 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 identification and authentication policy and associated identification and authentication controls.

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

- A formal, documented identification and authentication policy; and
- Processes to facilitate the implementation the identification and authentication policy, procedures, and associated controls.

IA-02: Account Management

Systems uniquely identify and authenticate organizational users or processes to:

- Allow the use of group authenticators only when used in conjunction with an individual/unique authenticator; and
- Require individuals to be authenticated with an individual authenticator prior to using a group authenticator.
- Verify the identity of a user, process or device as a prerequisite to granting access.

TTUHSC El Paso is required to assign all users a unique identification (ID) before allowing them to access systems. In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:

a. Something you know, such as a password or passphrase;
b. Something you have, such as a token device or smart card; or
c. Something you are, such as a biometric.

User Identification & Authentication Includes:

Network Access To Privileged Accounts
Where technically feasible, information systems must implement multifactor authentication for network access to privileged accounts.

Network Access To Non-Privileged Accounts
Where technically feasible, and a business justification exists, information systems must implement multifactor authentication for network access by non-privileged accounts.

Access To Privileged Accounts
Where technically feasible, and a business justification exists, asset custodians are required to incorporate two-factor authentication for local access to systems by employees, administrators, and third parties.

Group Authentication
Where technically feasible, individuals must be authenticated with an individual authenticator when a group authenticator is employed.

Network Access To Privileged Accounts - Replay Resistant
Where technically feasible and a business justification exists, information systems must implement replay-resistant authentication mechanisms for network access by privileged accounts.

Network Access To Non-Privileged Accounts - Replay Resistant
Where technically feasible and a business justification exists, information systems must implement replay-resistant authentication mechanisms for network access by non- privileged accounts.

Remote Access - Separate Device (Multifactor Authentication)
Asset custodians are required to secure all individual non-console administrative access and all remote access to sensitive networks using multi-factor authentication:4,5,6,7

a. Incorporate multi-factor authentication for all non-console access for personnel with administrative access.
b. Incorporate multi[factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside TTUHSC El Paso's network.

Acceptance Of PIV Credentials
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall configure information systems to accept and electronically verify Personal Identity Verification (PIV) credentials.

IA-03: Device-To-Device Identification & Authentication

Systems uniquely identify and authenticate devices before establishing a connection.

TTUHSC El Paso is required to use Active Directory (AD) to authenticate devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

IA-04: Identifier Management (User Names)

TTUHSC El Paso manages system identifiers for users and devices by:

- Receiving authorization from a designated organizational official to assign a user or device identifier;
- Selecting an identifier that uniquely identifies an individual or device;
- Assigning the user identifier to the intended party or the device identifier to the intended device; and
- Preventing reuse of user or device identifiers.

TTUHSC El Paso is required to ensure proper user identification and authentication management for all standard and privileged users on all systems, as follows:

a. Ensure that only authorized users are provided with user IDs'
b. Ensure that user names and service accounts are uniquely named and in a manner consistent with organizationally defined guidelines; and
c. Require written authorization by a supervisor or manager to receive a user ID.

Identifier Management Includes:

Identity User Status
Where technically feasible, TTUHSC El Paso shall identify individuals with unique username characteristics that correspond to employment status.

Dynamic Management
Where technically feasible, information systems shall dynamically manage identifiers.

Cross-Organization Management
Where technically feasible, TTUHSC El Paso shall coordinate with external organizations for cross-organization management of identifiers.

Privileged Account Identifiers
TTUHSC El Paso requires privileged user accounts to be:

a. A unique account separate from a standard user account; and
b. Used only when necessary for running privileged functions.

IA-05: Authenticator Management (Passwords)

TTUHSC El Paso manages system authenticators for users and devices by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
- Ensuring that authenticators have sufficient strength of mechanism for their intended use;
- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
- Changing default content of authenticators upon system installation;
- Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate)'
- Changing/refreshing authenticators according to an organization-defined time period by authenticator type;
- Protecting authenticator content from unauthorized disclosure and modification; and
- Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

TTUHSC El Paso manages system accounts (authenticators) for users and devices by the following:

a. Verify, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b. Ensure that authenticators have sufficient strength of mechanism for their intended use;
c. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
d. Change default content of authenticators upon system installation;
e. Establish minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
f. Change/refresh authenticators according to an TTUHSC El Paso-defined time period by authenticator type;
g. Protect authenticator content from unauthorized disclosure and modification; and
h. Require users to take, and having devices implement, specific measures to safeguard authenticators.

Authenticator Management includes:

Password-Based Authentication
TTUHSC El Paso manages system accounts (authenticators) for users and devices by the following:

a. User Accounts:
   I. Password Length: Minimum of eight (8) characters
   II. Password Reuse: Ten (10) (users cannot use any of the last ten (10) password he or she have used)
   III. Password Life:
      1. Maximum: Ninety (90) days
      2. minimum: One (1) day
   IV. Password Complexity:
      1. Passwords are not a derivative of the user ID
      2. Passwords have at least one (1) lower alpha, one (1) upper alpha, one (1) number, and one (1) special character.
      3. Passwords cannot contain two identical, consecutive characters
b. Service Accounts:
   i. Password Length: Minimum of eight (8) characters
   ii. Password Reuse: Ten (10) (service accounts cannot use any of the last ten (10) password he or she have used)
   iii. Password Life:
      1. Maximum: Three hundred sixty-five (365) days
      2. Minimum: One(1) day
   iv. Password Complexity:
      1. Passwords are not a derivative of the user ID
      2. Passwords have at least one(1) lower alpha, one (1) upper alpha, one (1) upper alpha, one (1) number, and one (1) special character.
      3. Passwords cannot contain two identical, conservative characters
c. Password Protection:
   i. Do not use the same password for TTUHSC El Paso accounts as for other non-TTUHSC El Paso access (e.g., personal ISP account, online banking, benefits, etc.). Users must not use the same password for various TTUHSC El Paso access needs and are required to have unique passwords for each account they access.
   ii. Do not share TTUHSC El Paso passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as Restricted, Confidential TTUHSC El Paso information.
   iii. Prohibited password practices:
      1. Do not use default vendor passwords
      2. Do not reveal a password over the phone to anyone for any reason
      3. Do not reveal a password in an e-mail message
      4. Do not reveal a password to a co-worker or supervisor
      5. Do not talk about a password in front of others
      6. Do not hint at the format of a password (e.g., "my family name")

7. Do not reveal a password on questionnaires or security forms
8. Do not share a password with family members
9. Do not write passwords down and store them anywhere in the user's office
10. Do not store passwords in a file on any information asset without encryption

d. Compromise:
   i. If an account or password is suspected to have been compromised, report the incident to management and change all passwords immediately.

PKI-Based Authentication
Where technically feasible, asset custodians must configure assets for PKI-based authentication by:

a. Validating certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b. Enforcing authorized access to the corresponding private key;
c. Mapping the authenticated identity to the account of the individual or group; and
d. Implementing a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

In-Person or Trusted Third-Party Registration
TTUHSC El Paso's Human Resources (HR) department, in conjunction with the Identity and Access Management (IAM) team, must develop and implement mechanisms to enforce authenticators are only issued by:

a. An in-person process that is managed by HR-designated personnel/roles; or
b. An outsourced process that is managed by a trusted third party.

Automated Support For Password Strength
TTUHSC El Paso Identity and Access Management (IAM) team may perform password cracking on a periodic or random basis determine if password authenticators are sufficiently strong to satisfy TTUHSC El Paso-defined requirements.

Protection of Authenticators
Users are required to follow TTUHSC El Paso's practices in

a. The use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.); and
b. Protecting authenticators commensurate with the risk posed to TTUHSC El Paso that use of the authenticator permits access.

No Embedded Unencrypted Static Authenticators
TTUHSC El Paso prohibits unencrypted static authenticators from being;

a. Embedded in applications or access scripts; or
b. Stored on function keys.

Hardware Token-Based Authentication
Where applicable, asset custodians must employ mechanisms for hardware token-based authentication that satisfy TTUHSC El Paso's token quality requirements.

Vendor-Supplied Defaults
Asset custodians and data/process owners are required to change vendor-supplied defaults before installing a system on the network, including but not limited to

a. Passwords;
b. Encryption keys;
c. Simple Network Management Protocol (SNMP) strings; and
d. Removing unnecessary, default accounts.

IA-06: Timely Maintenance

TTUHSC El Paso systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Asset custodians and data/process owners are required to ensure all systems and applications obscure the visible feedback of authentication information (e.g., passwords) during the authentication process to protect the information from possible exploitation by unauthorized individuals.

IA-07: Cryptographic Module Authentication

Systems use mechanisms for authentication to a cryptographic module that meet the requirements of applicable local, state, and federal laws, as well as non-regulatory requirements that the organization is contractually bound toaddress.

The minimum allowed encryption standard is AES 128 but the recommended standard for compliance is AES 256.

IA-08: Identification & Authentication (Non-Organizational Users)

Systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

Where technically feasible, asset custodians are required to assign non-TTUHSC El Paso users with unique identifiers in both usernames and email addresses to clarify the user is not directly employed by TTUHSC El Paso.

Identification & Authentication (non-organizational users) includes:

Acceptance of PIV Credentials from other organizations
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall configure information systems to accept and electronically verify Personal Identity Verification (PIV) credentials from US federal agencies.

Acceptance of Third-Party Credentials
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall configure information systems to accept only FICAM-approved third-party credentials.

Use of FICAM-Approved products
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall employ only FICAM-approved information system components to accept third-party credentials.

Use of FICAM-Issued profiles
Where technically feasible and justified by a valid business case, TTUHSC El Paso shall configure information systems to conform to FICAM-issued profiles.

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

56.50 Sanctions Policy (SN)
PCI DSS 8.1
PCI DSS 8.1.1 & 8.2 | MA201CMR17 17.04(1)(c) & 17.04(2)(b)
PCI DSS 8.3
PCI DSS version 3.2 Requirement 8.3
PCI DSS version 3.2 Requirement 8.3.1
PCI DSS version 3.2 Requirement 8.3.2

HIPAA 164.312(a)(b)(i) | MA201CMR17 17.04(1)(d)
HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)
HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)
HIPAA 164.308(a)(5)(ii)(D) | PCI DSS 8.1.2, 8.2.3, 8.2.4 & 8.2.5 | MA201CMR17 17.04(1)(b)-(e) & 17.04(2)(b)
NIST 800-53 IA-5(6) | ISO 27002 9.3.1 | FedRAMP | PCI DSS 8.6
PCI DSS 2.1, 2.1.1 & 8.3
PCI DSS 8.2.1
PCI DSS 8.1.8

Revised May 2018