THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0132 - Identification and Authentication	
Version: 1	**Effective Date: 10/01/2017**

IT0132 - Identification and Authentication

Objective:

To establish a policy for managing risks from user access and authentication into the University's critical information systems and provide the minimum requirements for the control of that risk.

Scope:

This policy applies to all users of and information technology (IT) resources owned, operated, or provided by the University of Tennessee including its campuses, institutes, and administration (University and/or Campuses).

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling the University's information technology resources.

Information transmitted or stored on University IT resources is the property of the University unless it is specifically identified as the property of other parties.

Principles:

The University has chosen to adopt the policy principles established in the National Institute of Standards (NIST) 800 series of publications, and this policy is based on those guidelines.

The Chancellor or equivalent at each Campus must designate an individual or functional position responsible for information security at their Campus (Position of Authority and/or Campus Authority). The Position of Authority should be at a high enough organizational level to allow him/her to speak with authority on and for the Campus.

Each Campus must develop or adopt and adhere to a program that demonstrates compliance with this policy and related standards. This program is the responsibility of the Position of Authority.

A Campus may apply more stringent requirements than those documented in this policy provided they do not conflict with or lower the standards or requirements established by this or any other University policy.

Each User of University resources is required to be familiar and comply with University policies. Acceptance of this policy is assumed if a User accesses, uses, or handles University IT resources.

Policy:

Each of the University's Campuses must develop or adopt and adhere to a formal, documented program that protects critical information systems and assets from unauthorized modification, disclosure, or destruction, and ensures that information is accurate, remains confidential, and is available when needed.

The program must identify critical information system users, processes, and devices and authenticate those identities before allowing access to information, applications, or information systems.

All policy related standards and procedures must be consistent with applicable laws, regulations, and guidance. This policy and all associated standards and procedures as well as their implementation effectiveness must be reviewed periodically and updated as needed.

Mandatory Controls:

Mandatory security controls for information systems are University-wide controls that are required to be consistently designed, implemented, monitored, and assessed by all Campuses.

1. **Policy and Procedures** (IA-1): Each Campus must develop or adopt and maintain an identification and authentication program that includes the implementation of this policy and associated controls, and an annual review of that program.
2. **Identifier Management** (IA-4): Each Campus must establish, document, and follow processes and standards to appropriately manage user identifiers used to access critical information systems including:
   a. Uniquely identifying each user;
   b. Ensure each user identifier is appropriately authorized before creation;
   c. Define a period of inactivity after which a user identifier is disabled;
   d. Establish appropriate management guidance for shared information system accounts (e.g. service, guest, and anonymous accounts).
3. **Authenticator Management** (IA-5): Each Campus must establish and document processes and standards to appropriately manage system authenticators (e.g. tokens, PKI certificates, passwords, etc.) by:
   a. Defining initial/default authenticator content;
   b. Establishing administrative procedures for initial authenticator distribution, lost or compromised authenticators, and for revoking authenticators;
   c. Changing default authenticators upon information system installation;
   d. Changing/refreshing authenticators periodically as appropriate.
4. **Authenticator Feedback** (IA-6): Critical information systems must obscure feedback of authentication information during the authentication process to protect the information from possible unauthorized use.

Discretionary Controls:

Discretionary Controls are security controls whose scope is limited to a specific campus, institution, or other designated organizational component. Discretionary Controls are designed, implemented, monitored, and assessed within that organizational component. Discretionary controls must not conflict with or lower the standards established by Mandatory Controls.

References:

1. NIST 800-53 "*Recommended Security Controls for Federal Information Systems and Organizations*"

Definitions: n/a

Last Reviewed: July 17, 2017