THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT0130 - Personnel Security	
Version: 1	Effective Date: 10/01/2017

IT0130 - Personnel Security

Objective:

To establish policy for developing and maintaining a Personnel Security program to ensure compliance with minimally acceptable University requirements.

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 to ensure that individuals granted access to systems and data are vetted to ensure that information security objectives are maintained.

The program must ensure that individuals occupying Positions of Responsibility (including third-party providers) are trustworthy and meet established security criteria for those positions, and that the environment in which they function operates securely and does not constitute an unacceptable security risk.

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 are University-wide controls that are required to be consistently designed, implemented, monitored, and regularly assessed by all Campuses.

Each Campus must establish and maintain a Personnel Security Program for all information systems classified as Moderate, High, or Business Critical that includes:

1. **Personnel Screening** (PS-3): Appropriate background checks are complete before access to information systems is granted.
2. **Personnel Termination** (PS-4): Upon termination of an individual's employment, each Campus must:
   a. Retrieve all University security/system-related information and property;
   b. Disable information system access;
   c. Terminate/revoke any credentials associated with the individual.
3. **Third-Party Personnel Security** (PS-7): Each Campus must:
   a. Establish and document third-party personnel security requirements;
   b. Require third-party providers to comply with Campus personnel security procedures; and
   c. Monitor provider compliance.
4. **Personnel Sanctions** (PS-8): Non-compliance with information security policies is addressed appropriately as outlined in HR0525 - Disciplinary Action.

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.

Definitions:

1. **Position of Responsibility** – Individuals performing job functions that have, can grant, or can approve access to sensitive information or business critical systems.
2. **Sensitive information** - Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical,

privacy, or proprietary considerations. Sensitive information includes all data which contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies.

References:

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

Last Reviewed: January 11, 2017