UTIA IT0124P1 – INFORMATION TECHNOLOGY RISK ASSESSMENT PROCEDURES

Effective: February 16, 2018
Last Reviewed: January 08, 2018 **Last Updated:** January 09, 2018

Objective:
These procedures provide guidance for the risk assessment of all moderate, high, and business critical information technology (IT) resources at the University of Tennessee Institute of Agriculture (the Institute). A risk assessment of IT assets allows for determination of the level of risk to disclosure, alteration, and/or destruction of the information and the impact to the Institute.

Scope:
These procedures apply to moderate, high, and business critical IT assets owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users, while accessing, using, or handling the Institute's IT assets.

Moderate, high, and business critical (based on availability) IT assets, in the context of this process, are defined as any hardware, software, systems, services, and related technology assets that are used by the department, unit, and or Institute. These assets are identified at an appropriate level of granularity and in a manner such that overlap among information assets is minimized.

Procedures:
Step 1 – System Characterization
All IT assets are categorized for the information they store, transit, or process (based on confidentiality and integrity) and are classified based on and the criticality of the system according the UTIA IT0115 – *Information and Computer System Classification Plan* (availability).

A database of each system defined as moderate, high, or business critical will maintained by the Institute's Chief Information Security Officer (CISO) with access given to only those who have a clearly defined and approved need to know.

Step 2 – Threat Identification
The threats to the IT asset defined moderate, high, or business critical includes a review of all access, both physical and logical. The threats are evaluated on an individual and accumulative basis. The threat is the potential for a threat-source to exploit a vulnerability. A vulnerability is a weakness in an IT asset that is open for exploitation.

The threat-source is any event that could cause damage to an IT asset. There are multiple threats sources including:

- Natural – Floods, earthquake, tornado, etc.
- Human
- Unintentional – inadvertent data entry, inadvertent power changes
- Intentional – deliberate acts of sabotage

Once the threat-sources are identified, the motivation, resources available, and capabilities of the threat-source are evaluated. These factors provide the threat likelihood value of each threat-source.

The threat, including threat-sources, shall be identified as low, medium, or high.

Step 3 – Vulnerability Identification

Vulnerabilities are any weakness in an IT asset that leaves it vulnerable that could lead to a breach of a system or affect the security protections of the IT asset. Examples of vulnerabilities include termination of employees for disciplinary action, direct access from the Internet of IT assets, patches to flaws in an IT asset have not been created, and lack of backups for information on IT assets.

There are two types of vulnerability assessment. Passive vulnerability assessment includes research and visual inspection of the IT asset. Proactive vulnerability assessment includes actions such as vulnerability scanning. Please see the UTIA IT0124P2 – *Vulnerability Assessment Procedures* for more information.

All systems classified as moderate or high shall receive a yearly passive and proactive assessment and all systems categorized as business critical shall receive a yearly passive assessment.

The vulnerability, including passive and proactive vulnerability assessment, shall be identified as low, medium, or high.

Step 4 – Control Analysis, Likelihood Determination, Impact Analysis, and Risk Determination

The institute will use a three-step process for determining the overall likelihood of threat events occurring, and thus the risk to the IT asset.

The first step is to assess the likelihood that threat events will be initiated or will occur.

Likelihood Level Likelihood Definition

- High – The threat vulnerability is high and the threat identification is medium or high.
- Medium – The threat vulnerability is medium and the threat identification is medium, high, or low.

- Low – The threat vulnerability is low and the threat identification is low, medium, or high, or the threat vulnerability is medium and the threat identification is low.

Magnitude of Impact – Impact Definition

- High Exercise of the vulnerability
  (1) May result in the highly costly loss of major tangible assets or resources;
  (2) May significantly violate, harm, or impede an organization's mission, reputation, or interest; or
  (3) May result in human death or serious injury.
- Medium Exercise of the vulnerability
  (1) May result in the costly loss of tangible assets or resources;
  (2) May violate, harm, or impede an organization's mission, reputation, or interest; or
  (3) May result in human injury.
- Low Exercise of the vulnerability
  (1) May result in the loss of some tangible assets or resources or
  (2) May noticeably affect an organization's mission, reputation, or interest.

Risk Definition

The third step is to assess the overall risk of a combination of the first two steps.

- High – The impact is high and the likelihood is medium or high.
- Medium – The impact is medium and the likelihood is medium, high, or low.
- Low – The impact is low and the likelihood is low, medium, or high or the impact is medium and the likelihood is low.

Step 5 – Control Recommendations

The Institute will follow NIST SP 800-53 for determination of the appropriate controls. The implemented controls must mitigate and/or eliminate the identified risk. The controls are defined in each respective UTIA plan and procedure.

Step 6 – Results Documentation

All risks, threats identified, vulnerabilities identified, and the controls implemented must be documented for each moderate, high, or business critical IT asset. The documentation can be in the form of comprehensive information for low systems, but must be documented individually for all moderate, high, or business critical system.

References:

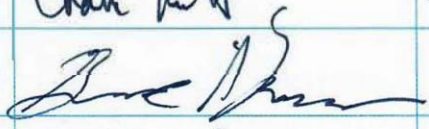
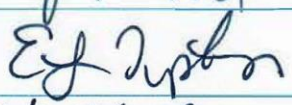
UTIA Glossary of Information Technology Terms
UTIA IT0124 – *Information Technology Risk Assessment Plan*
UTIA IT0124P2 – *Vulnerability Assessment Procedures*
UT Policy IT0124 – *Risk Assessment*
UTIA IT0115 – *Information and Computer System Classification Plan*
UTIA IT0115P - *Organizational Guidance for the Classification of Information and Systems*

UT Policy IT0115 – *Information and Computer System Classification*
NIST SP 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*
NIST SP 800-100 – *Information Security Handbook: A Guide for Managers*

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.

APPROVAL OF PROCEDURES

We approve UTIA IT0124P1 – *Information Technology Risk Assessment Procedures* as described in this document.

Name	Title	Signature	Date
Sandra D. Lindsey	Chief Information Security Officer, UTIA		02/16/2018
Charles Lambrecht	Computer Operations Manager, UTCVM		2/16/18
Brent Lamons	Director of Advising, Herbert College of Agriculture		2-16-18
Joel Lown	Coordinator, AgResearch		2/16/18
Emily Tipton	IT Coordinator, Extension		2-16-18
Kristy Keel-Blackmon	Communications Specialist, Forestry, Wildlife and Fisheries		2/16/18
Joanne Logan	Associate Professor, Biosystems Engineering and Soil Science		2/22/18