UTIA IT0124 – INFORMATION TECHNOLOGY RISK ASSESSMENT POLICY

Effective: December 19, 2016
Last Reviewed: April 01, 2021 **Last Updated:** January 08, 2018

Objective:
This policy provides guidance for the risk assessment of information technology (IT) assets at the University of Tennessee Institute of Agriculture (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:
This policy applies to information systems (IT assets) that host or store Institute data classified as moderate or high, or that are designated as business critical. This includes IT assets that are 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.

Explanation:
Risk assessment of IT assets at the Institute will follow the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100. NIST SP 800-100 defines the Risk Assessment Process as being a six-step process. Those steps are:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis, Likelihood Determination, Impact Analysis, and Risk Determination
5. Control Recommendations
6. Results Documentation

The risk assessment process will be used in evaluating all risks as they relate to information technology according to the six steps outlined below.

The Institute will focus its risk assessment process, as it relates to business critical systems, using the following process. The Institute’s Chief Information Security Officer (CISO) will contact the following Institute leadership positions in determining and evaluating risks to the business critical systems at the Institute.

1. Chancellor
2. The Institute’s Chief Business Officer
3. AgResearch, College of Agricultural Sciences and Natural Resources, Extension, and the College of Veterinary Medicine Deans and associated budgetary staff
4. Institute Department Heads and associated budgetary staff
5. Institute Directors and associated budgetary staff

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 Policy (availability).

This step begins with the identification of the information system boundaries, IT assets, and information. At a minimum, the system characterization describes the following individual IT asset components:

- Hardware
- Software
- External interfaces to other IT assets
- Data
- People

Step 2 – Threat Identification

Threat identification consists of identifying threat sources with the potential to exploit weaknesses in the IT asset.

Step 3 – Vulnerability Identification

Vulnerabilities can be identified using a number of techniques and sources, such as vulnerability scanning. Please see the UTIA IT0124P2 – Vulnerability Assessment Procedures for details on this crucial step.

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

This step combines four parts of the risk assessment process. Controls must be in place and the results from the analysis of those controls are used to strengthen the determination of the likelihood that a specific threat might successfully exploit a particular vulnerability. Impact analysis is completed to consider the impact to the IT assets, data, and the mission of the Institute, as well as the criticality and sensitivity of the IT assets and data. Finally, once the ratings for likelihood and impact have been determined, the risk level can be calculated.

Step 5 – Control Recommendations

Control recommendations are made in an effort to reduce the level of risk to the IT asset and its data. Factors for recommending controls include the following:

- Effectiveness of recommended options
- Legislation and regulation
- Organization policy
- Operations impact
- Safety and reliability

Step 6 – Results Documentation

The risk assessment report is used to formally document the results of all risk assessment activities. It should, at a minimum, contain the following:

- Scope of the assessment based on the system characterization
- Methodology used to conduct the risk assessment; Individual observations resulting from conducting the risk assessment
- Estimation of the overall risk posture of the IT asset

Documentation:

Documentation for the risk assessment process will be handled in the following manner:

- Identify and document IT assets for risk assessment;
    - Moderate and high systems based on confidentiality, and availability
    - Business critical systems based on availability
- Conduct the risk assessment at least annually;
- Notify the Institute's CISO whenever there are significant changes to the IT asset or environment of operation, or other conditions that may impact the security of the IT asset; and
- Select and implement appropriate controls for each IT asset using the baseline established by the Institute IT Security Program and with the cooperation of the Institute's CISO.

Once the risk assessment is complete, the Institute's CISO will create the risk assessment report and distribute to the appropriate persons.

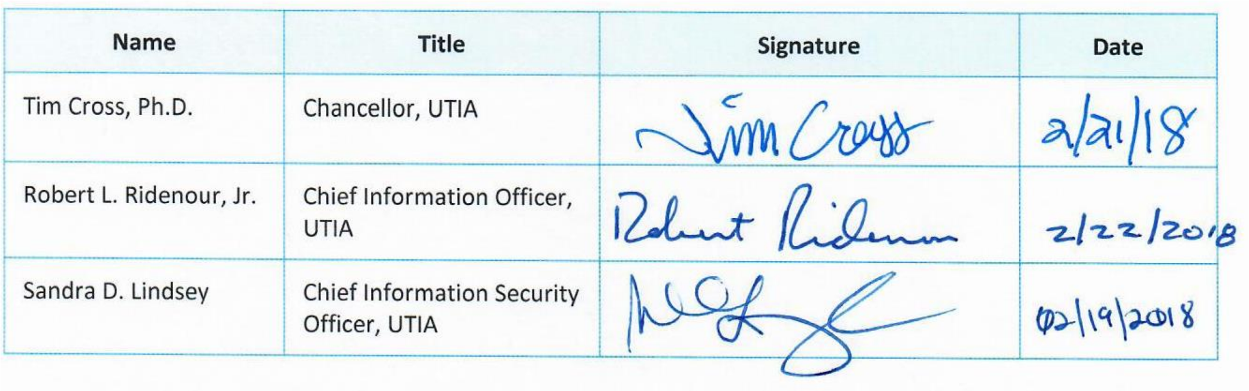
References:

UTIA Glossary of Information Technology Terms
UTIA IT0124P1 – Information Technology Risk Assessment Procedures
UTIA IT0124P2 – Vulnerability Assessment Procedures
UT Policy IT 0124 – Risk Assessment
UTIA IT0115 – Information and Computer System Classification Policy
UTIA IT0115P – Organizational Guidance for the Classification of Information and Systems
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 Policy

We approve UTIA IT0124 – Information Technology Risk Assessment Policy as described in this document.



Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA	Tim Cross	2/21/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA	Robert Ridenour	2/22/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		02/19/2018