UTIA IT0115 - Information and Computer System Classification Policy

Effective: February 20, 2017
Last Reviewed: March 29, 2019 **Last Updated:** January 09, 2018

Objective:
This plan provides guidance and procedures for the classification of information technology (IT) assets at the University of Tennessee Institute of Agriculture (the Institute). Classification of IT assets is critical for being able to protect data by putting the appropriate security controls in place, as well as being able to respond in the most efficient and accurate method when certain assets are compromised.

Scope:
This plan applies to all IT assets owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users, while accessing, using, or handing the Institute's IT assets. Users of the Institute's IT assets are accountable for giving timely and accurate information. The Institute's IT representatives are responsible for assisting users with the classification process.

Plan:
All IT assets are classified as low, moderate, or high for the information they store, transmit, or process (confidentiality and integrity) based on UT Policy IT0115 – *Information and Computer System Classification*. All IT assets are also classified based on and the criticality of the system (availability) as defined below:

- *Business Critical* – The department cannot operate without this IT asset.
- *Normal* – The department, as a whole, can operate without this IT asset for an extended period of time during which particular units or individuals may be inconvenienced and/or need to identify alternatives.

The risk assessment process will be used to determine the criticality of the IT asset. Please review *UTIA IT0124 – Information Technology Risk Assessment Policy* for more information.

The Institute will use the UT Knoxville's classification methods through their network registration (NetReg) system as a reference point for determining low, moderate and high. All IT assets using the Knoxville network must go through the NetReg process before network access is given, using the UT Self Classification application (https://classify.utk.edu).

Once a "new" IT asset has been registered, the Primary User (the person who will regularly use the asset) will get an email stating that he/she will have 30 days to classify the asset. The Primary User will then go to the self-classification site to complete the classification process. If an IT representative for someone else registers an IT asset, it is important to put the actual user

in the Primary User field, as this is the only person who will be notified for classification purposes.

It is important to closely read the guidelines on this website and think carefully about the numerous options. These options do NOT include data that belongs to you or your family that you may be storing on your computer. Your own personal information should not be stored on your IT assets, but if it is, you should not count it when completing the classification process. Classification of data refers only to that information belonging to other Institute or University faculty, staff, students, clients, customers, etc.

The Institute will review the classifications in NetReg and evaluate each IT asset separately for a final determination of its classification. The final classification of each system based on the data that it stores or processes will be determine based on communications between the information owner and the UTIA Chief Information Security Officer (CISO) or their designee.

The classification of the IT asset is important for choosing the appropriate incident response procedures used in the event of a possible compromise or data breach. IT assets storing or processing moderate or high data or IT assets that are business critical may require additional steps, including contacting external entities, before any kind of internal incident response can be considered.

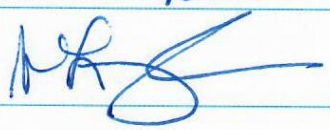
References:

UTIA Glossary of Information Technology Terms
UTIA IT0115P – *Organizational Guidance for the Classification of Information and Systems*
UT Policy IT0115 – *Information and Computer System Classification*
UTIA IT0122P – *Information Security Incident Response and Reporting Procedures*
UTIA IT0124 – *Information Technology Risk Assessment Policy*
UTIA IT0124P1 – *Information Technology Risk Assessment Procedures*

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

Approval of Policy

We approve UTIA IT0115 – *Information and Computer System Classification Policy* as described in this document.

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