UTIA IT0132 – IDENTIFICATION AND AUTHENTICATION PLAN

Effective: April 17, 2018
Last Reviewed: February 16, 2018 **Last Updated:** February 19, 2018

Objective:
This plan is created to establish a policy for managing risks from user access and authentication into all University of Tennessee Institute of Agriculture's (the Institute) information technology (IT) assets and for providing the minimum requirements for the control of that risk.

Scope:
This plan applies to all IT assets owned, operated, or provided by the Institute, as well as all students, faculty, staff, and users who access, use, or handle the Institute's assets. The plan also applies to all visitors, volunteers, county-paid employees, and Tennessee State University employees accessing Institute-owned IT assets.

Plan:
All Institute-owned IT assets must be protected from unauthorized access potentially leading to modification, disclosure, or destruction of the asset and the data contained on the asset. The Institute has multiple security plans (policies) and procedures that explain the requirements for using unique identification and authentication methods (see UTIA IT0110 – *Acceptable Use of Information Technology Resources (AUP)*, UTIA IT01xx – *Media Protection Plan*, UTIA UT01xx – *Information Technology Access Control Plan*). In addition, this plan defines policies and procedures for accessing Institute-owned IT assets. This plan will be reviewed at least annually and will be updated as necessary.

Access to Institute-owned IT assets is authorized based on the principle of least privilege. This means that an individual is given the minimum access level to a given asset or system in order to perform his/her job duties.

Each user must use his/her own unique account to access any Institute-owned IT asset. Systems may be audited for appropriate login data. Should an Institute-owned IT asset become compromised, the user who is logged in at the time of the compromise will be contacted for information regarding any investigation. Unauthorized or improper access to any Institute-owned IT asset is subject to disciplinary action.

Users who are authorized to access IT assets classified as moderate, high, or business critical are also required to use two-factor authentication to access those assets. The Institute is

working with The University of Tennessee Knoxville (UTK) to develop a multi-factor authentication solution.

Identifier Management

UTK's Office of Information Technology (OIT) assigns a unique NetID, or user ID, to all Institute employees as appropriately authorized upon hiring. OIT is responsible for managing the NetID system. NetIDs are unique to each person and the reuse of NetIDs is not allowed.

The Institute uses the NetID that has been assigned as the user's unique identifier throughout employment or association with the Institute. There are instances when an associate of the Institute (i.e., volunteer, friend, third-party vendor, etc.) requires use of an Institute-owned IT asset. Such NetIDs can be requested through the OIT HelpDesk and may need to be sponsored by the appropriate unit, department, county, or center.

The NetID absolutely must be used for accessing Institute-owned IT assets classified as moderate, high, or business critical. The NetID, or federated account where appropriate, must be used for accessing certain systems like SUPER, IRIS, Volmail, Office 365, etc., and the VPN, or access will not be granted. Supervisors are responsible for determining the level of access necessary and must convey this information to the party(s) responsible for assigning the access. Should a person's job duties change, the supervisor shall notify the appropriate party(s) to adjust the level of access given. After a period of 180 consecutive days in which a user has not accessed a device or system, access to the NetID will be disabled. Systems not able to use the NetID or LDAP authentication must provide the CISO with a plan for meeting this 180-day limit. Access will be disabled immediately upon termination of employment.

Guest or anonymous accounts are prohibited. If a shared account is required in certain situations, a formal exception request must be submitted and approved (UTIA IT0302 – *Information Technology Formal Exception Plan*).

Authenticator Management

Once the NetID is assigned, the employee is required to log in and create his/her password and security questions. The password must meet certain complexity requirements:

- Minimum of 8 and maximum of 16 characters
- At least three of the following:
  - Uppercase letters
  - Lowercase letters
  - Numbers
  - Special characters (accepted: `~!@#$^&*()_-={}|[]:;'<>?,)
- May not contain a significant portion of the username or displayname
- May not reuse the last 10 passwords

NetID passwords must be changed periodically. The timeframe for changing a password depends on the classification of data being accessed. In addition to the NetID password, some users must use two-factor authentication based on the type of data being accessed.

Passwords must never be shared with anyone (see UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan*).

Authenticator Feedback

Business critical, moderate, and high information systems must obscure feedback of authentication information during the authentication process in order to protect the information from potential unauthorized use. Obscuring the feedback of authentication information means masking the information as it is entered to prevent others from seeing in on the screen. This can be done, for example, by using asterisks as a user types in a password. University and Institute systems are doing this where the NetID is being used.

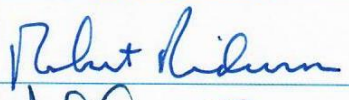
References:

UTIA Glossary of Information Technology Terms
UT Policy IT0132 – *Identification and Authentication*
UTIA IT0110 – *Acceptable Use of Information Technology Resources Security Plan (AUP)*
UTIA IT0115 – *Information and Computer System Classification Plan*
UTIA IT01xx – *Media Protection Plan*
UTIA UT01xx – *Information Technology Access Control Plan*
UTIA IT0302 – *Information Technology Formal Exception Plan*
UTIA IT0302P – *Information Technology Formal Exception Request Form*
NIST SP 800-53 – *Security and Privacy Controls for Federal Information Systems and Organizations*

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

Approval of Plan

We approve UTIA IT0129 – *Physical and Environmental Protection Plan* as described in this document.

Name	Title	Signature	Date
Tim Cross, Ph.D.	Chancellor, UTIA		4/17/18
Robert L. Ridenour, Jr.	Chief Information Officer, UTIA		4/17/2018
Sandra D. Lindsey	Chief Information Security Officer, UTIA		04/16/2018