UTIA IT0123 – Security Awareness, Training, and Education Policy

Effective: October 17, 2016
Last Reviewed: August 23, 2021 **Last Updated:** August 23, 2021

Objective:
This policy has been established to maintain the security skills of the University of Tennessee Institute of Agriculture's (Institute) workforce.

Scope:
This policy applies to members of the Institute workforce who access Institute-owned IT assets, including but not limited to all desktops, laptops, devices, servers, and networks. The workforce, for purposes of this policy, includes all full-time and part-time employees, third-party contractors, volunteers, TSU Extension employees, county-funded employees, and seasonal workers who access Institute-owned IT assets. The workforce, for purposes of this policy only, does not include seasonal workers who never have access to Institute-owned IT assets or any other employee, retired or otherwise, who never access Institute-owned IT assets.

Policy and Procedures:

1. The Institute Chief Information Security Officer (CISO) will plan, implement, and maintain the Institute's security awareness, training, and education program.
2. The Institute workforce will comply with these security awareness, training, and education policy and procedures.
3. As a supplement to the annual security training, employee education is attained through monthly e-newsletters sent by the CISO highlighting relevant IT security topics and current threats.
4. The Institute's CISO will also send emails to the Institute's statewide workforce when major IT security news must be shared, particularly regarding current and new known security threats.
5. The CISO maintains https://UTIAsecurity.tennessee.edu, which includes information about current threats, a knowledge base containing a wide variety of IT Security topics, and an archive of all the monthly e-newsletters.
6. Social media accounts are used by the CISO to notify the Institute's workforce of security tips and announcements.
7. Group IT security training, as well as one-on-one training, is offered upon request.

Security Awareness Training

1. All **new** Institute workforce will complete the assigned training within 30 days after hiring, in order to fulfill their security responsibilities.
2. All **current** Institute workforce will be assigned mandatory refresher training modules annually between September 15 and December 17.
3. Users who have not completed the training will be sent a minimum of two individual reminders from the CISO. On the second reminder, the Dean, Director, and/or Department Head will be copied on the email.
4. Beginning the first week of November, the CISO will send weekly participation updates to each Dean, Director, and Department Head who have users who have not completed the training.
5. As a part of the program, information security training will be used in the evaluation of the personnel performance review. This training should be included in each year's Goals.
6. Institute workforce may receive one (1) CPE credit for security training and professional development upon completion of the total assigned curriculum.
7. Users will have access to security policies, standards, procedures, and rules of behavior for information systems via the UTIA security website (https://UTIAsecurity.tennessee.edu) the UTIA Policies and Procedures site (https://utia.tennessee.edu/utia-policies-and-procedures/), and the UT policy website (http://universitytennessee.policytech.com/).
8. Any user who does not complete the training by the required date will lose access to all Institute-owned or University-owned systems, and the supervisor will be notified. Loss of access will be implemented as follows:
   a. First Missed Deadline
      - NetID account is disabled by 8:00am the following day.
      - The CISO will create individual trouble tickets for tracking purposes.
      - User must call the OIT HelpDesk, Monday-Friday, 8am-5pm. for account reactivation.
      - User has 48 hours after account reactivation to complete the training.
   b. Second Missed Deadline
      - NetID account is disabled by 8:00am the following day, Monday-Friday.
      - Non-compliance with policy will be reported to the Dean, Director, and/or Department Head.
      - Immediate supervisor must request that the account be reactivated.
      - User will receive a written warning that is to be included in the departmental personnel file and will be a part of that year's personnel performance review. (This warning is not a disciplinary action. If the supervisor deems this should have a disciplinary action, the supervisor must go through HR.)
      - User has 24 hours after account reactivation to complete the training.
   c. Third Missed Deadline
      - NetID account is disabled by 8:00am the following day.
      - Network access will be disabled in NetReg for any devices for which that user has access.

- The Institute's Senior Vice President & Senior Vice Chancellor will be notified and will determine if the user's account and access should be reactivated.
- The Institute' Senior Vice President & Senior Vice Chancellor will notify the supervisor of that decision and a copy of the notification will be placed in the personnel file.

9. The Institute's CISO will ensure Institute officials are fully informed of all IT security directives, policies, standards, procedures, etc., with which they must comply in order to carry out the University's mission.

Role-Based Security Training

Institute workforce will be asked to complete training modules that are relevant to their individual job functions and access to data. This role-based training will be divided into the following categories:

- New Employee
- IT Staff
- Business Managers and Budget Directors
- Executive Leadership
- Faculty (most faculty members are responsible to E01 accounts and those users will be assigned the training by UT Knoxville)
- All Others

Security Training Records

Institute CISO information security metrics include:

- Weekly tracking of security training and awareness program participation;
- Feedback to leadership through email notification.

References:

UTIA Glossary of Information Technology Terms
UT Policy IT0123 – Security Awareness, Training, and Education
UTIA IT0115 – Information and Computer System Classification Policy
UT Policy HR0128 – Human Resources Development Policy

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

Approval of Policy

We approve UTIA IT0123 – Security Awareness, Training, and Education Policy as described in this document.

Name	Title	Signature	Date
Tim L. Cross, Ph.D.	Senior Vice President and Senior Vice Chancellor, UTIA	DocuSigned by: Dr. Tim. L. Cross F81A83AFB474435...	8/25/2021 | 12:59:18 PDT
Angela A. Gibson	Chief Information Officer, UTIA	DocuSigned by: 75409DE95BA8458...	8/26/2021 | 11:55:49 PDT
Sandra D. Lindsey	Chief Information Security Officer, UTIA	DocuSigned by: Sandra D Lindsey 213E082B08784A3...	8/27/2021 | 09:05:40 PDT