UTIA IT0302 – Information Technology Formal Exception Plan

Effective: April 17, 2016
Last Reviewed: March 28, 2024 **Last Updated:** June 02, 2020

Objective:
To protect the confidentiality, integrity, and availability of the University of Tennessee Institute of Agriculture's (Institute) information technology (IT) assets, full compliance with all IT plans and procedures is expected. However, some circumstances may exist when a plan or procedure cannot be fully implemented regarding an IT asset(s) in a given area. This plan is to provide a formal, written process for requesting exemption from an Institute IT plan or procedure.

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 IT assets.

Plan:
It is important to understand that choosing not to comply with an Institute IT plan or procedure is quite different from not being able to comply with a portion of the plan or procedure. Anyone who accesses, uses, or handles any Institute IT asset is required to do everything possible to comply with these plans and procedures. Unfortunately, there may be instances when it is not possible to be fully compliant, so a written request for an exemption is required. These instances must be submitted to the Institute's Chief Information Security Officer (CISO).

In order to be considered for an exception, the UTIA IT0302F – Information Technology Plan Exception Request Form must be completed. This form will include as many details as possible about these topics:

1. Description of the business process related to the exception and who it impacts
2. Description of non-compliance
3. Business justification for non-compliance
4. Hardware (MAC) address for each network interface card in the computer being used
5. Description of data potentially affected by non-compliance
6. Potential risk associated with non-compliance
7. Maintenance plan, including mitigating controls for managing risk associated with non-compliance
8. Anticipated period of non-compliance
9. Proposed date to review progress toward compliance
10. Any additional information to support need for exception

The requester will discuss with the Director/Department Head and, if in agreement, both parties will sign and submit the form to the Institute's CISO. Upon submission, the CISO will conduct an initial review of the exception request based on risk to the Institute. The CISO will then send to the appropriate Budget Director and Institute leadership (e.g., unit Dean) for additional review. Once the Budget Director and Institute leadership have approved the request, it will be forwarded back to the Institute's CISO for final approval. The decision will be provided in writing, along with the review date or expiration date, if approved.

Exceptions will be cataloged on a private security site with limited access. In the event of an audit, contact the CISO for access.

If an exception is approved, a review date or expiration date will be assigned. If still non-compliant, a new UTIA IT0302F – Information Technology Plan Exception Request Form must be submitted. Please note that if an exception is approved once, it is not guaranteed to be approved again, as this process is not meant to last in perpetuity.

In the event of any significant change (i.e., business process, who is impacted, change in the person responsible for managing the risk associated with the exception request), a new UTIA IT0302F – Information Technology Plan Exception Request Form must be submitted at once.

References:
UTIA Glossary of Information Technology Terms
UTIA IT0302F – Information Technology Plan Exception Request Form
UTIA IT0124 – Information Technology Risk Assessment Plan
UTIA IT0124P1 – Information Technology Risk Assessment Procedures
UTIA IT0115 – Information and Computer System Classification Plan

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