UTIA IT0110 - Acceptable Use of Information Technology Resources Security Plan (AUP) – This IT security plan defines the guidelines for the Institute and its IT assets. This plan covers userprivacy; what users will and will not do with regards to using Institute-owned IT assets; Instituteand University rights; copyrights and licenses; personal use; and misuse of IT assets. All faculty, staff, students, and users who access, use, or handle Institute-owned IT assets must read this AUP at least annually, and must understand and comply with its requirements.

UTIA IT0115 – Information and Computer System Classification Plan – This IT security plan explains the classification of data as low, moderate, or high, as well as business critical or normal. This plan applies to all Institute-owned IT assets, as well as all faculty, staff, students, and users who are accessing, using, or handling Institute-owned IT assets. Primary users of an ITasset are required by UTK to classify each year using classify.utk.edu, but the Institute will follow up to ensure that those assets classified as moderate or high are classified correctly.

UTIA IT0115P – Organizational Guidance for the Classification of Information and Systems – These procedures offer guidance for categorizing specific information types at the Institute. These procedures apply to all Institute-owned IT assets, as well as all faculty, staff, students, and users who are accessing, using, or handling Institute-owned IT assets.

UTIA IT0120 – Secure Network Infrastructure Plan – This IT security plan details how the Institute provides a reliable and secure network infrastructure as to protect Institute data. This plan applies to the Institute's IT network infrastructure that is owned and operated by the Institute only. All Institute employees using UT Knoxville's (UTK) network infrastructure mustfollow the appropriate UTK security plans and procedures.

UTIA IT0120P – Secure Network Infrastructure Procedures – These procedures detail how the Institute provides a secure network infrastructure through network wiring, as well as maintenance and monitoring of the network infrastructure. These procedures apply to the Institute's IT network infrastructure that is owned and operated by the Institute only. All Institute employees using UT Knoxville's (UTK) network infrastructure must follow the appropriate UTK security plans and procedures.

UTIA IT0121 – Information Technology Security Program Plan – This IT security plan describes the Institute's overall IT security strategy for protecting users, data, and information systems; outlining information security responsibilities; defining the Authorization Boundary; and documenting current and planned security controls. This plan applies to all Institute-owned IT

University of Tennessee Institute of Agriculture:
UTIA Information Technology Security Plans and Procedures – Brief Summaries

| Version: 3.0 | Effective Date: April 01, 2016 |

assets, as well as all faculty, staff, students, and users who are accessing, using, or handling Institute-owned IT assets.

UTIA IT0122 – Information Security Incident Response Plan – This IT security plan addresses information security incidents that threaten the confidentiality, integrity, and availability (CIA) of the Institute's IT assets, information systems, and the networks that deliver the information. This plan covers what is considered an incident; the event detection and incident confirmation process; the reporting requirements; analysis of the cost of an incident; follow-up activities; and responsibilities of the Incident Response Team.

UTIA IT0122P – Information Security Incident Response and Reporting Procedures – These procedures describe how to report an incident and the responsibilities associated with reporting an incident. It is important that the procedures be followed closely, as certain government and industry regulations can impose heavy fines where incidents are not properly reported.

UTIA IT0123 – Security Awareness, Training, and Education Plan – This IT security Plan details our required annual security awareness training, as well as additional awareness, training, and education efforts. This plan applies to members of the Institute workforce who access Institute-owned IT assets. As such, the Plan defines "workforce" solely for the purposes of the annual security awareness training.

UTIA IT0124 – Information Technology Risk Assessment Plan – This IT security plan provides guidance for the Institute's efforts to assess the levels of risk to disclosure, alteration, and/or destruction of data and assets, and the impact of such risk to the Institute.

UTIA IT0124P1 – Information Technology Risk Assessment Procedures – These procedures define the appropriate steps for completing an IT security risk assessment at the Institute. While it is important for everyone to understand UTIA IT0124 – *Information Technology Risk Assessment Plan*, these procedures are intended to be followed by those directly involved in the risk assessment.

UTIA IT0124P2 – Vulnerability Assessment Procedures – These procedures provide guidance for ensuring compliance with the Vulnerability Management portion of UTIA IT0124 – *Information Technology Risk Assessment Plan*. The procedures apply to Institute-owned IT assets classified as business critical or high, as well as those classified as moderate with specific industry or government requirements, and include specifics about vulnerability scanning and remediation expectations.

UTIA IT0125 – Information Technology Configuration Management Plan – This IT security plan is

necessary for establishing and maintaining the confidentiality, integrity, and availability of the Institute's data and IT assets. The plan defines baseline configurations for all Institute-owned IT assets, and defines asset management and change management with regards to Institute-owned IT assets classified as moderate, high, or business critical.

UTIA IT0125P – Information Technology Change Control Procedures – These procedures have been created as a supplement to UTIA IT0125 – *Information Technology Configuration Management Plan* to consider the changing needs and requirements of the Institute, definingthe change management process and explaining the responsibilities of the Change Advisory Team (CAT).

UTIA IT0127 – Audit and Accountability Plan – This IT security plan necessary for creating a formally documented program for monitoring, managing, and reviewing IT assets, applications,networks, and user activity. While the plan and procedures apply to the Institute's IT assets and anyone who uses them, the brunt of the work will come from the IT community.

UTIA IT0127P – Audit and Accountability Procedures – These procedures define how we are implementing and managing audit controls and records based on UTIA IT0127 – *Audit and Accountability Plan*. While the procedures are fairly technical, they are written more for our IT people to follow. The baseline configurations for Institute-owned IT assets will reflect these procedures and will vary based on systems classified as low, moderate, high, or business critical.

UTIA IT0128 – Contingency Planning Plan – This IT security plan is for Institute-owned IT assets classified as business critical. Once the risk assessment has been performed, we will know who owns these business-critical assets. Those owners will be responsible for developinga contingency plan for their own asset(s), meeting the requirements stated in this plan.

UTIA IT0129 – Physical and Environmental Protection Plan – This IT security plan defines howthe Institute protects Institute-owned IT assets, as well as the facilities housing these assets.
This Plan has ties to several other Institute security policies and most controls affect those ITassets classified as moderate, high, and business critical. This plan requires little more than the use of observation on the part of the users.

UTIA IT0129P – Physical and Environmental Protection Procedures – These procedures define how UTIA IT0129 - *Physical and Environmental Protection Plan* is to be implemented. Many of the responsibilities lie with the UTIA CIO, UTIA CISO, or their designee, while some of the procedures require the IT asset user to be observant.

University of Tennessee Institute of Agriculture:
UTIA Information Technology Security Plans and Procedures – Brief Summaries

| Version: 3.0 | Effective Date: April 01, 2016 |

UTIA IT0130 – Personnel Security Plan for Information Technology – This IT security plan addresses the need to ensure the proper vetting of anyone who works for the Institute or has a legitimate business need to access Institute IT assets or data considered business critical or classified as moderate or high. Just as importantly, the plan ensures that all access will be promptly revoked when a person leaves or no longer needs the access. UT already requires that pre-employment/association vetting will take place. However, upon termination or transfer of the employee, as well as the termination of any association with affiliates or third-party vendors, supervisors are required to notify the local/regional IT representative or UTIA CISO to ensure all access to IT assets and data is revoked as soon as possible.

UTIA IT0131 – Security Assessment and Authorization Plan – This IT security plan establishes security controls required for Institute IT security assessment activities. This plan only applies to those Institute-owned IT assets classified as business critical (those IT assets that a department cannot operate without) and the users who are listed as owner (responsible party) of those assets.

UTIA IT0132 – Identification and Authentication Plan – This IT security plan details the need for all users of Institute-owned IT assets to provide a unique user ID and password/passphrase when using these IT assets. The NetID will be used in most cases, while some IT systems may require the use of a federated account, such as a Google login.

UTIA IT0133 – Security Planning for Systems Plan – This IT security plan defines how the Institute implements security planning for moderate, high, and business critical systems, with "system" meaning the combination of hardware and software used to collect, filter, process, create, and distribute data. The owner of any Institute-owned IT asset classified as moderate, high, or business critical will be required to submit a security plan for that asset, describing the specifics of the asset and the plans for meeting security requirements. The UTIA CISO will provide a template for the IT asset owners.

UTIA IT0134 – System and Communications Protection Plan – This IT security plan addresses the appropriate security controls necessary for protecting the Confidentiality, Integrity, and Availability of Institute-owned IT assets classified as moderate, high, and business critical, as well as the data on those assets. Many of the controls in this plan must be handled by OIT, as UTK owns the network used by the Institute.

UTIA IT0135 – System and Information Integrity Plan – This IT security plan addresses the appropriate security controls necessary for the regular and timely maintenance of Institute- owned IT assets classified as moderate, high, or business critical. This maintenance is necessary for protecting the

University of Tennessee Institute of Agriculture:
UTIA Information Technology Security Plans and Procedures – Brief Summaries

| Version: 3.0 | Effective Date: April 01, 2016 |

integrity of the assets and data on those assets.

UTIA IT01xx – Information Technology Access Control Plan – This IT security plan has been created to ensure that authenticated users access only those IT assets and data for which the user has been authorized to access, and is closely associated with several other Institute security plans. If individuals are compliant with each of the referenced plans, this plan will not require additional effort.

UTIA IT01xx – Media Protection Plan – This IT security plan defines media to include paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, mobile computing devices, networking devices, and all-in-one printers. Following this plan is critical for securing the confidentiality of the Institute's data by guarding data from unauthorized access and disclosure throughout the lifetime of the media. This plan discusses destruction of media once the appropriate retention period has expired, including special instructions for media with sensitive data.

UTIA IT01xx – System and Services Acquisition Plan – This IT security plan defines the Institute's system and services acquisition program, and how this program is used to evaluate IT assets purchased by the Institute. This plan addresses allocation of resources, as well as the life cycle and acquisition process for IT assets. This plan applies to all Institute-owned IT assets.

UTIA IT0301P – Google Drive Procedures – These procedures allow for a consistent and secure method of sharing files with Institute employees, as well who those who work with the Institute but are not employed by the Institute. The sharing of such data is permitted only through the UTK Google Apps for Education (UT Google Drive), and NOT through personal Google accounts. UT Google Drive is certified for storing most sensitive data, including HIPAA data.

UTIA IT0302 – Information Technology Formal Exception Plan – Institute employees are expected to maintain full compliance with all IT security plans and procedures. Sometimes it may not be possible for a specific IT asset to meet all parts of every plan or procedure. This IT security plan provides a formal, written process for requesting temporary exemption from a plan or procedure. The plan discusses the exception process.

UTIA IT0302F – Information Technology Plan Exception Request Form – This form is to be completed if a portion of an Institute IT security plan or procedure cannot be fully complied with, based UTIA IT0302 – *Information Technology Formal Exception Plan*. The form will be reviewed by the appropriate leadership and a final decision will be made by the UTIA CISO.

University of Tennessee Institute of Agriculture:
UTIA Information Technology Security Plans and Procedures – Brief Summaries

| Version: 3.0 | Effective Date: April 01, 2016 |

UTIA IT0303P – Security Camera Procedures – These procedures have been created to provide guidelines for the installation of and use of any and all video surveillance equipment (security cameras) on property owned and or operated by the Institute. The use of such camera will be for the purpose of monitoring premises for vandalism, theft, or other safety measures. These procedures apply only to security cameras installed and utilized and any non-Knoxville campus location.

UTIA IT0303F – Security Camera Information Form – This form was created to be used in conjunction with UTIA IT0303P – Security Camera Procedures and applies to non-Knoxville campus locations owned, operated, or provided by the Institute and where the UT Police Department does **not** have jurisdiction.

UTIA IT0304P – Network Registration Procedures – These procedures were created to maintain a consistent manner of registering all IT assets used by the Institute within IT Knoxville's network registration system. The procedures include information on choosing the correct domain and the correct group, as well as information on what to do when an Institute-owned ITasset is repurposed.

UTIA IT0305F – Information Technology Asset Checkout Form – This editable PDF form is for any department, center, or unit who provides Institute-owned IT assets on a checkout-type basis. Not all departments, centers, and units offer this service, but this form should be used by those who do.

UTIA IT0311 – Payment Card Industry (PCI) Security Plan – This IT security plan addresses PCI requirements for accepting and processing credit cards by all Institute merchants. These requirements are based on PCI Data Security Standards (DSS), as well as UT Policy FI0311 – *Credit Card Processing.*

UTIA IT0312 – Payment Card Industry (PCI) Security Awareness Program – This program meets the PCI DSS requirement for a formal security awareness program to make personnel aware of cardholder data security. This program applies to all Institute employees who process and/or transmit credit card, debit card, or eCommerce transactions on behalf of an Institute merchant.

UTIA Glossary of Information Technology Terms – The glossary contains definitions of information technology terms found in the Institute's IT security policies and procedures.

For more information, contact Sandy Lindsey, UTIA Chief Information Security Officer, at (865) 974-7292, or email sandy@tennessee.edu.