After each question number is the correct response for no risk/corrective action. If (info), the question is merely collecting information (no risk or corrective action). If (decision), the question is meant to determine whether you continue or skip the next section of questions.

Information Technology

Question 1: **Yes**

Are all computers and peripherals (e.g., printers) costing between $1,500 and $4,999.99 listed in the equipment inventory system as sensitive minor equipment and have University equipment tags attached as required by **Policy FI0600**?

Risk:

Policy FI0600 defines computer equipment costing between $1,500 and $4,999.99 as sensitive minor equipment that must be listed in the equipment inventory system and tagged with University equipment tags.

Corrective Action:

Ensure that all computers and peripherals costing between $1,500 and $4,999.99 are listed in the equipment inventory system as sensitive minor equipment and are tagged with University equipment tags. Component parts may be listed under a single tag. The Controller's Office should be contacted to obtain tags.

Question 2: **Yes**

Are the serial numbers and physical locations of all electronic devices (e.g., computers, iPads, printers), even those costing less than $1,500, that are deemed by management assessment to be high risk for loss or theft recorded and kept on file in the department?

Risk:

Information required in the event of theft and to aid in tracking information for warranty, maintenance, and inventory verification records is not accessible. This information is critical if sensitive data is stored on a device that is lost or stolen because the department must report the security incident and follow up as appropriate.

Corrective Action:

Maintain a departmental record of serial numbers and physical locations of all electronic devices, even those costing less than $1,500, that are deemed by management assessment to be high risk for loss or theft.

Question 3: **Yes**
Do you maintain accurate records of who is responsible for computers that are removed from the premises (e.g., permanent assignments or checkout forms)?

Risk:
Computers are more vulnerable to theft or loss if the removal from premises is not documented.

Corrective Action:
Establish a departmental procedure for checking out computers when they are removed from the premises (e.g., permanent assignments or checkout forms). Refer to University **Policy FI0605, #16** for an Equipment Request/Checkout Form.

Question 4: **Yes**
Are antivirus programs loaded on all of your department's computers?

Risk:
The department's computers are vulnerable to virus attacks and loss of valuable data.

Corrective Action:
Select and load an antivirus program on all departmental computers. Contact your campus/institute IT department or computer support group to obtain University-approved antivirus software. **[Policy IT0110, 2(g)]**

Question 5: **Yes**
If your department has computers (including portables) located off campus that are connected to the internet, is the system managed centrally to ensure that the system configuration, and thus data security, is adequate for the classification of data being accessed?

Risk:
Data stored on the computers is vulnerable to being altered or viewed by outside parties.

Corrective Action:
For computers that are located off campus and connected to the internet,

ensure that the system is being centrally managed to ensure data security is adequate for the classification of data being accessed. Contact your campus/institute IT department or computer support group for guidance if necessary.

Question 6: **Yes**
Have all users in your department been instructed to read the campus's or institute's acceptable use policy and University policy on acceptable use of information technology resources **(Policy IT0110)?**

Risk*:*
User practices are an important key to computer security. If not informed on policy, users may inadvertently disclose information or create a vulnerability, which could allow University systems to be compromised.

Corrective Action*:*
Ensure that all departmental users are aware of campus or institute acceptable computer use policies. University policies are detailed in **Policy IT0110**; however, each campus/institute may apply more stringent requirements.

Question 7: **Yes**
Have your departmental staff been informed of how to report a computer security incident?

Risk*:*
If a computer security incident goes unreported or reporting is delayed, data may be lost or unauthorized access will continue.

Corrective Action*:*
Ensure departmental staff are aware of the requirement to report any security-related incidents to the appropriate campus/institute department. **[Policy IT0122]**

Report security incidents as follows:

Chattanooga: Email security@utc.edu
Health Science Center: Email itsecurity@uthsc.edu
System Administration: Email utsaciso@utk.edu
Knoxville: Email security@utk.edu

Institute for Public Service: Email security@utk.edu
Martin: http://www.utm.edu/departments/security/contact.php
Institute of Agriculture: Email utiasecurity@tennessee.edu
Space Institute: http://www.utsi.edu/index.php/security-incident-report/

Question 8: **No**
Are you aware of any passwords or access codes in your department that are known by more than one person?

Risk:
Sharing passwords or access codes may grant unauthorized individuals access to University assets and confidential records. In addition, if user IDs and passwords are used by multiple persons, the ability to accurately identify unauthorized users during the investigation of security incidents is greatly reduced.

Corrective Action:
Instruct all departmental personnel to maintain confidential passwords and access codes. **[Policy IT0110, 3(a)]**

Question 9: **Yes**
Is unauthorized access to confidential and critical information stored on electronic media, locally or in the cloud, prevented by the use of software or hardware controls such as password protection, file encryption, and locked storage?

Risk:
Unauthorized individuals may gain access to confidential and critical information.

Corrective Action:
Develop and install appropriate software or hardware controls to prevent unauthorized access to confidential and critical data. Ideally, data should be stored using University-owned or -managed hardware and/or software (e.g., OneDrive, Google Drive).

Question 10: **Yes**
Are electronic media (e.g., USB drives, hard drives) containing confidential or sensitive data sanitized before disposal or transfer?

Risk:
Unauthorized individuals may gain access to confidential and critical information if media are not sanitized before disposal or transfer.

Corrective Action:
According to **Policy FI0120, #15 and #16**, electronic media containing confidential or sensitive data should be sanitized before disposal or transfer.

Question 11: **Yes**
Does your department keep a written inventory of software and have proof of license for all copies of software programs in use that are not licensed through the campus or University?

Risk:
A current, written inventory of software discourages the misappropriation of these assets, helps comply with software copyright laws, and enables you to determine the number of licensed copies, any needed upgrades, and older versions that should be retired. Additionally, the department may be using software programs in violation of software copyright laws.

Corrective Action:
Maintain a written inventory of software. Take measures to comply with software copyright requirements: 1) determine the number of licensed copies of each software title in use, 2) determine the number of copies installed on the hard drives of your computers, and 3) remove all unlicensed copies. **[Policy IT0110, 5(f)]**

Question 12: **Yes**
Are essential data files backed up to minimize loss of critical data?

Risk:
Essential data files may be lost or destroyed.

Corrective Action:
Establish a departmental procedure for backing up essential files. The backup schedule should be based on volatility, utilization, and importance of the data. For most departments, daily backups are preferable. Your campus/institute IT department or computer support group can assist in establishing a departmental procedure based on your needs.

Question 13: **Yes**
When an employee terminates or retires from service, does your department submit an IRIS employee termination request as soon as possible so that access to IRIS and other University information systems can be removed promptly?

Risk*:*
Former employees maintain access to University information systems, including private or sensitive data.

Corrective Action*:*
When an employee terminates or retires from service, submit an IRIS employee termination request as soon as possible so that access to IRIS and other University systems can be removed promptly.

Question 14: (decision 15)
Do any of your departmental computers (including departmental servers) store the following types of sensitive data:

- Student grades or any personally identifiable student data other than directory information
- Student/parent financial data
- Health-related information
- Credit card information
- Bank data
- Confidential research data
- Social Security numbers
- Other sensitive data

If you answered "Yes" to Question 14, please go to Question 15 and continue.

If you answered "No" to Question 14, please skip to Question 16 and continue.

Question 15: **Yes**
Have your departmental staff who routinely handle any of the sensitive data itemized below received specialized training on protecting the data to meet the security requirements of the corresponding legislation? (Note: this training would be in addition to the required "Securing the Human" training.)

- Student grades or any personally identifiable student data other than directory information–FERPA
- Student/parent financial data–FERPA, Gramm-Leach-Bliley Act
- Health-related information–HIPAA
- Credit card information–Payment Card Information Data Security Standard
- Bank data–Gramm-Leach-Bliley Act
- Confidential research data–Export Administration Regulations, International Traffic in Arms Regulations, etc.

***Risk**:*
Without training, a user could inadvertently disclose information or create a vulnerability that compromises the system.

***Corrective Action**:*
The department should ensure that all employees are trained on how to protect confidential data and comply with legislation requirements.

***Question 16:* Yes**
Has your department classified all University systems and information under your department's control as defined in University **Policy IT0115**, Information and Computer System Classification, including assigning information owners and system owners?

***Risk**:*
Lack of accountability occurs when information does not have an assigned owner. Failure to appropriately classify information sets/systems can lead to inappropriate or ineffective application of security controls.

***Corrective Action**:*
Classify all departmentally controlled systems and information by following your campus/institute's classification procedure. Contact your campus/institute IT department or computer support group for guidance.

***Question 17:* Yes**
Does your department follow your campus/institute's defined vulnerability management program? Vulnerability management includes patch management for systems in your department through a central resource that automatically installs operating system and third-party software (e.g.,

Adobe, Java, Firefox) security updates and/or implementing procedures to ensure that updates are installed in a timely manner.

***Risk**:*
Failure to patch vulnerabilities can lead to compromised systems including information loss, corruption, or unauthorized data access.

***Corrective Action**:*
Ensure computer operating systems are set to automatically install security updates or implement procedures to ensure that the updates are installed in a timely manner. Contact your campus/institute IT department or computer support group for guidance on the vulnerability management program. **[Policy IT0110, 2(h)]**

***Question 18:* Yes**
Does your department provide access to systems and information only to employees who need those resources to perform their job duties?

***Risk**:*
Improper privileges can inappropriately provide access to sensitive or confidential information, increase the risk of infection from malicious software, and lead to unauthorized activity.

***Corrective Action**:*
Ensure access to systems and information is limited to employees who need those resources to perform their job duties. Contact your campus/institute IT department or computer support group for guidance if necessary.

Question 19: (decision 20-21)
Does your department conduct **any** business through e-commerce (e.g., accepting credit cards over the internet either through a departmental server or a third-party vendor, Point of Sale System)?

If you answered "Yes" to Question 19, please go to Question 20 and continue.

If you answered "No" to Question 19, please skip to Question 22 and continue.

After each question number is the correct response for no risk/corrective action. If (info), the question is merely collecting information (no risk or corrective action). If (decision), the question is meant to determine whether you continue or skip the next section of questions.

Question 20: **Yes**
Do you have written internet sales policies and procedures that have been reviewed by the Office of Audit and Compliance?

Risk:
The department may not have the appropriate controls in place to prevent fraud or loss of data.

Corrective Action:
Contact the finance office and request a review of your internet sales policies and procedures. See **Policy FI0310, #29** and **Policy FI0311**.

Question 21: **Yes**
Do you annually complete a Payment Card Industry (PCI) Data Security Standards Self-Assessment Questionnaire and submit it to the campus/institute chief business officer as required by **Policy FI0311, #3(k)**?

Risk:
The department may not be complying with the credit card company's compliance programs and may lose the ability to process credit card transactions.

Corrective Action:
Contact your campus/institute business office and/or the finance office to request the latest version of the questionnaire or visit the PCI Security Council's site at https://www.pcisecuritystandards.org/saq/index.shtml.

Question 22: **(Info)**
Has an IT risk assessment been completed for your department's IT assets and electronic business processes, including all cloud-based applications?
Note: this question is for informational purposes only. No risk will be displayed and no corrective action necessary.

MONEY HANDLING

Question 23: **No**
Do members of your teaching faculty ever collect money from students

(e.g., foreign trips, supplies)? If your department has no teaching faculty, please answer N/A.

***Risk**:*
Policy FI0310, #10 prohibits teaching faculty from collecting money from students. This policy serves to protect faculty from any liability associated with handling the money and to avoid potential conflicts of interest with students.

***Corrective Action**:*
Money from students should be collected by departmental staff and not by teaching faculty. Arrangements should be made to transfer this responsibility.

Question 24: (decision 25-26)
Does your department handle any funds for organizations outside the University (e.g. student organizations such as fraternities)?

If you answered "Yes" to Question 24, please go to Question 25 and continue.

If you answered "No" to Question 24, please skip to Question 27 and continue.

Question 25: **Yes**
Was written approval obtained from the campus/institute chief business officer to handle funds for each outside organization?

***Risk**:*
Policy FI0312 requires departments to submit a written request including procedures for using and managing the funds to the campus/institute chief business officer for approval to handle funds for organizations outside the University. Failure to ensure that proper safeguards are in place could expose the University to unnecessary liability if the funds are lost or stolen.

***Corrective Action**:*
A written request should be forwarded to the chief business officer specifying the scope of the University employee's duties in handling funds for outside organizations, the amount of money involved, and the reason(s) it is in the

University's best interests. A separate fund may need to be established in the University's accounting system (IRIS).

Question 26: **No**
Does your department receive electronic payments (e.g., credit cards, debit cards, electronic checks) over the internet using University resources on behalf of an outside organization?

Risk*:*
Receiving electronic payments requires compliance with the PCI Data Security Standards, and the University cannot guarantee compliance for an outside organization for which it has no control. The University could also incur credit card fees not reimbursed by third parties.

Corrective Action*:*
Discontinue using University internet resources for handling e-commerce transactions for outside organizations.

Question 27: (decision 28-end)
Does your department receive money? (Note: answer yes if your department receives any funds in any form from any source)

If you answered "Yes" to Question 27, please go to Question 28 and continue.

If you answered "No" to Question 27, you have completed the questionnaire.

Question 28: **Yes**
Are all funds received by the department immediately recorded by cash register, in an official University receipt book, in the University's online receipting system (UTK/UTIA), or by a procedure approved by the Office of Audit and Compliance?

Risk*:*
Policy FI0310, #6 requires all money received by the department to be recorded by cash register, in an official University receipt book, or by another authorized procedure. Not doing so may allow a theft of unrecorded funds to go undetected.

Corrective Action:
Record all money received by cash register, in an official University receipt book, in the University online receipting system, or by another authorized procedure.

Question 29: **Yes**
Are all checks received by your department made payable to the University, not to departments or any University official or employee?

Risk:
Checks not made payable to the University could be fraudulently cashed or deposited to non-University accounts.

Corrective Action:
Ensure that customers are instructed to make checks payable to the University. **[Policy FI0310, 7]**

Question 30: **Yes**
Do your employees restrictively endorse all checks (including checks received by mail) with the University's official endorsement stamp immediately upon receipt?

Risk:
Checks not restrictively endorsed could be fraudulently cashed or deposited to non-University accounts.

Corrective Action:
Restrictively endorse all checks with the University's official endorsement stamp immediately upon receipt. **[Policy FI0310, 7]**

Question 31: **Yes**
Are the receipt numbers (or a suitable deposit identifier) recorded in IRIS (ZK document)?

Risk:
Reconciling specific receipts to specific deposits may be difficult if the receipt numbers are not recorded.

Corrective Action:
Record the receipt numbers or suitable deposit identifier in IRIS as required by **Policy FI0310, #17**.

***Question 32:* Yes**
Is money received transmitted to the campus central cashier or deposited within three business days?

Risk:
Undeposited money is significantly more vulnerable to theft or loss. Large amounts of undeposited funds also may represent a significant loss of investment revenue for the University.

Corrective Action:
Ensure that money received is transmitted or deposited within three business days. **[Policy FI0310, 15]**

***Question 33:* No**
Is any money received by your department ever withheld from a deposit?

Risk:
University fiscal policy requires that money received be deposited intact and inclusive of all receipts on hand. Failure to do so might prevent proper accountability of funds and make it difficult to reconcile receipts to the departmental ledger. **[Policy FI0310, 2]**

Corrective Action:
Ensure that deposits include all money on hand received by the department.

***Question 34:* No**
Do employees ever use cash received by the department to make departmental purchases?

Risk:
Using cash received to make departmental purchases makes it difficult to track funds received and could lead to inaccurate departmental revenue and expense records. Additionally, such purchases bypass controls established to ensure that University purchases comply with applicable state and federal requirements.

Corrective Action:
Ensure that cash received by the department is not retained and used to make departmental purchases. **[Policy FI0310, 2]**

Question 35: **Yes**
Does an employee who does not handle money reconcile records of money received, such as receipts or cash register tapes, to bank deposit records and the departmental ledger?

Risk:
A theft of money may be concealed or may not be detected in a timely fashion.

Corrective Action:
Assign duties so that an employee who does not handle money reconciles money received to the bank deposit records and the departmental ledger. **[Policy FI0310, 8]**

Question 36: **Yes**
Have all employees who handle money been assigned specific duties such as receiving and recording payments, preparing deposits, or reconciling money received to the bank deposit and departmental ledger (as opposed to having various employees perform the duties on an "as available" basis)?

Risk:
The absence of specific assignments may result in some duties not being performed and may cause difficulty in identifying responsible individuals in the case of fraudulent activity.

Corrective Action:
Employees should be assigned to specific money-handling duties, and these duties should be reviewed routinely to ensure compliance.

Question 37: **Yes**
When an employee who handles money is absent, does another employee perform his or her duties?

Risk:
An employee who always performs the money-handling duties may be able to hide fraudulent activities from supervisors and other employees.

Corrective Action:
Consider assigning specific money-handling duties to other employees periodically (e.g., when the primary employee is on leave).

Question 38: **No**
If your department has accounts receivable (e.g., prepares invoices), do employees who receive money also maintain accounts receivable records?

Risk:
Employees may be able to fraudulently manipulate accounts receivable records to cover a theft, e.g., by falsifying receivables records or by "lapping" customer payments (credit one account by extracting money from another).

Corrective Action:
Employees who handle money should not maintain accounts receivable records. **[Policy FI0310, 8]**

Question 39: **No**
Are employees who have access to checks written to the University also responsible for University petty cash bank accounts (e.g., writing checks, reconciling accounts)?

Risk:
Employees could potentially steal money by cashing checks written to the University through the petty cash bank account.

Corrective Action:
Assign duties to ensure that employees who have access to checks written to the University are not responsible for University petty cash bank accounts.

Question 40: **Yes**
If your department uses cash registers to record cash receipts, are the registers cleared at the end of each day by someone other than the cashier?

Risk:
Cashiers could report less than the actual amount of sales.

Corrective Action:
If possible, assign someone who has no monetary responsibilities and does not operate the cash register to clear cash registers at the end of the day. **[Policy FI0310, 13]**

Question 41: **Yes**
If your department issues refunds, are the refunds approved by the department head or his/her designee and supported by documentation that includes the following:

- Name of the person, institution, or company receiving the refund (original payer)
- Mailing address
- Reason for the refund
- Proof of purchase (e.g., University receipt number or deposit information of when the money was originally received)
- Dollar amount of the refund
- Cost center, fund, WBSE, general ledger account where the refund is to be charged (usually the same cost center, fund, WBSE, general ledger account of the original receipt)
- The department head's approval

Risk:
Employees may be able to issue and/or patrons may be able to obtain fraudulent refunds. Additionally, if no merchandise is returned due to a fraudulent refund, inventory could be overstated.

Corrective Action:
Ensure that all refunds are supported with proof of purchase and approved by the department head or his/her designee. **[Policy FI0310, 21]**

Question 42: **No**
Does your department ever send money through campus mail?

Risk:
Money transferred through campus mail is not secured from theft or loss.

Corrective Action:
Ensure that money is not sent through campus mail. **[Policy FI0310, 9]**

***Question 43:* Yes**
Have all employees who handle money taken leave within the past 12 months?

Risk:
Employees who do not take time off may be able to hide fraudulent activities from supervisors and other employees.

Corrective Action:
Consider requiring or requesting employees to take some annual leave each year or periodically reassign duties to other employees.

***Question 44:* Yes**
Is it current practice to perform a criminal background check and to check character references and previous employment histories before hiring employees who handle money?

Risk:
Employees who handle money who have committed fraudulent or questionable actions in the past are more likely to commit fraudulent or questionable acts again.

Corrective Action:
Ensure that a background check is performed and other references are checked before hiring employees who will handle money.

***Question 45:* Yes**
Does your department keep funds in a safe or under lock and key if they must be kept overnight until they can be deposited?

Risk:
Funds could be lost or stolen.

Corrective Action:
Funds kept overnight should be kept in a safe or under lock and key **[Policy FI0310, 9].**

Question 46: **Yes**
If your department's money is kept in a safe or under lock and key, is the combination or number of keys restricted to three or fewer employees?

Risk*:*
Too many employees may have access to money. Generally, the risk of loss from theft or error increases with the number of employees who have access to money. If too many people have the safe combination or keys to access money, identifying those persons responsible for any shortages would be difficult.

Corrective Action*:*
Limit the number of employees who know the safe combination or limit keys to three or fewer. **[Policy FI0310, 9]**

Question 47: **No**
Do former employees or any other unauthorized persons know your safe combination or have a key?

Risk*:*
Unauthorized persons who know the department's safe combination or have a key may secretly gain access to money.

Corrective Action*:*
When employees leave the department, the safe combination or key should be changed to reduce the chance of theft. **[Policy FI0310, 9]** In addition, consider periodically changing the combination or key to reduce the chance of theft.

Question 48: **No**
Has your department had a cash shortage greater than $250 within the past year which was not reported to the Office of Audit and Compliance and the campus business office?

Risk*:*
The shortage may not have been investigated properly, and control weaknesses conducive to loss or theft may still exist.

Corrective Action:
Ensure that all shortages greater than $250 are reported to the Office of Audit and Compliance and the campus business office. **[Policy FI0131, 3]**

Question 49: **No**
Has your department had a shortage (of any amount) in the past year where employee theft was suspected which was not reported to the Office of Audit and Compliance?

Risk:
The shortage or theft of money may not have been investigated properly and control weaknesses conducive to loss or theft may still exist.

Corrective Action:
Ensure that all shortages where employee theft is suspected are reported to the Office of Audit and Compliance. **[Policy FI0130]**

Question 50: **No**
Is any of your department's money ever commingled with personal funds or other non-business-related funds (such as for flowers, postage, or coffee)?

Risk:
Commingling of funds could result in abuse of University funds. In addition, a lack of distinction between University and personal funds may cause confusion in reconciling overages or shortages in either fund.

Corrective Action:
Ensure that departmental money is not commingled with personal funds or other non-business-related funds.

Question 51: **No**

Does your department maintain a "reserve" fund to collect overages and/or cover shortages?

Risk:
Overages and shortages are not being identified and accounted for properly.

***Corrective Action**:*
Discontinue using a "reserve" fund to collect overages and/or cover shortages.

***Question 52:* Yes**
Do employees who handle money have up-to-date written departmental instructions and procedures (other than University fiscal policy or campus business policy) to guide them in their money-handling duties?

***Risk**:*
University policies and procedures important for protecting University funds may not be followed if employees do not have access to written procedures to guide them through unusual or infrequent occurrences.

***Corrective Action**:*
Develop written instructions and procedures to guide employees in their money-handling duties. Review the written procedures annually to ensure they are up-to-date. **[Policy FI0310, 4]**

Question 53: (decision 54)
Does your department accept credit or debit card payments?

If you answered "Yes" to Question 53, please go to Question 54 and continue.

If you answered "No" to Question 53, you have completed the questionnaire.

***Question 54:* Yes**
Did you apply for your merchant number to accept credit or debit card payments through the CBO and CIO as required by **Policy FI0311, #9**?

***Risk**:*
If you did not go through the campus business office and finance office, an appropriate account may not have been established for accepting credit or debit card payments.

After each question number is the correct response for no risk/corrective action. If (info), the question is merely collecting information (no risk or corrective action). If (decision), the question is meant to determine whether you continue or skip the next section of questions.

Corrective Action:

The department should contact the finance office to apply for an appropriate account to accept credit or debit card payments. **[Policy FI0311, 9]**