THE UNIVERSITY OF
TENNESSEE
KNOXVILLE

Information Security Program Plan

Prepared for:

Dr. Jimmy Cheek
Chancellor

November 11, 2015

Prepared by:

University of Tennessee, Knoxville
Office of Information Technology (OIT)

Table of Contents

1. Document Control

Version No.	Version Date	Author	Summary of Changes
1.0	2013-08-14	Bob Hillhouse	Initial Document
2.0	2015-11-11	Bob Hillhouse	Updated Security Plan

a. Official Approvals

Jimmy G. Cheek — Date: 11/20/15

Chancellor - Knoxville

Christopher J. Cimino — Date: 11-20-15

Vice-Chancellor, Knoxville, Finance & Administration

Digitally signed by Joel Reeves
DN: cn=Joel Reeves, o=University of Tennessee, ou=Office of Information Technology, email=joel.reeves@utk.edu, c=US
Date: 2015.11.20 13:15:05 -05'00'

Joel E. Reeves, Jr. — Date:

Asst. Vice-Chancellor & Chief Information Officer, Knoxville

Robert A. Hillhouse — Date: 11.20-15

Associate CIO & Chief Information Security Officer

b. Approval Dates

This plan and all updates have been signed and approved on the dates listed below:

Name	Title	Date of Approval	Version No.
Jimmy G. Cheek	Chancellor - Knoxville	August 14, 2013	1.0
Christopher J. Cimino	Vice-Chancellor, Knoxville, Finance & Administration	August 14, 2013	1.0
Joel E. Reeves, Jr.	Asst. Vice-Chancellor & CIO, Knoxville	August 21, 2013	1.0
Robert A. Hillhouse	Associate CIO & Chief Information Security Officer	August 23, 2013 November 11, 2015	1.0 2.0

c. Record of Distribution

This plan and all updates should be distributed to the following:

Office	Date of Distribution
Chancellor	
Vice-Chancellor for Finance & Administration	
Chief Information Officer	
Office of Emergency Management	

2. Executive Summary

This is the University of Tennessee Knoxville (UTK) Information Security Program Plan, created as result of University of Tennessee (UT) System policy IT0121, which details:

> *"Each Campus and institute is responsible for creating, approving, maintaining, and implementing an information security plan based on the National Institute of Standards and Technology (NIST) Risk Management Framework."*

This plan details the information security risks facing the UTK Campus as well as the disposition of mitigating or compensating controls. Pursuant to UT Policy IT0121, this information security plan shall contain the following at a minimum:

1. Identification and assignment of related security responsibilities including who is responsible for accepting risk at each Campus and institute.
2. A description of the baseline controls in place or planned for meeting the security requirements.
3. Interconnecting systems and related Interconnection Security Agreements (ISAs).
4. Campus senior management approval.

3. Purpose

The purpose of the Information Security Program Plan is to provide an overview of the security requirements of the systems on Campus and describe the controls that have been implemented to address those requirements. The Information Security Program Plan also delineates responsibilities and expected behavior of all individuals who access those systems.

Additionally, this plan also lists systems, networks, users and/or data that are *out-of-scope*.

4. Roles and Responsibilities

Pursuant to NIST SP 800-37, the following sections describe the roles and responsibilities of key participants involved in the Campus IT risk management process.

Authorizing Official: The senior Campus official with the authority to accept risk for Campus IT operations. This role authorizes the system for operation based on the system owner's certification that all requirements are met or mitigated.

Information System Owner: The Authorizing Official appoints this person in writing. The information system owner, most often the Campus's Chief Information Officer (CIO), is responsible for the development, maintenance, and administrative approval of the Campus Information Program Security Plan. This role certifies that the Campus is operating with all required or compensatory controls. In areas where controls are not viable for business reasons, the IT risk must be accepted in writing by the Authorizing Official. This role ensures that the Campus is operated in accordance with that plan.

Senior Information Security Officer (SISO): This role is responsible for ensuring that the appropriate operational security posture is maintained for all information systems within scope and as such, works in close collaboration with the system owners. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security awareness training. The SISO may be called upon to assist in the development of security procedures and to ensure compliance with those procedures. In coordination with the information system owner, the SISO plays an active role in the monitoring of central IT systems and the environment of operation that includes developing and updating system security plans, managing and controlling changes to the systems, and assessing the security impact of those changes.

The responsibility for these roles is assigned at UTK as follows.

Role	Name	Title
Authorizing Official	Jimmy G. Cheek	Chancellor - Knoxville
Information System Owner	Joel E. Reeves, Jr.	Asst. Vice-Chancellor & CIO, Knoxville
Senior Information Security Officer	Robert A. Hillhouse	Associate CIO & Chief Information Security Officer

5. Scope

This plan addresses IT resources that are connected to the UTK network. UTK does host systems and also provides information security controls for some systems that are directly managed by other entities on Campus. While those other entities accept responsibility for the risk decisions related to the configuration of their systems, the UTK CIO must be notified of any decisions or significant changes affecting the information security posture or logical position of the UTK Infrastructure.

a. Network

The scope of this plan covers wired and wireless UTK networks. UTK provides Internet services and connectivity to the Campus. UTK manages network connections to various locations across the state. Though the actual hosts and systems at the other sites are out-of-scope, UTK is responsible for maintaining and securing network connectivity with them. See Appendix III for a complete list of interconnections.

b. IT Resources

IT resources at the Knoxville Campus fall into two main categories:

1. **OIT managed resources:** includes all network infrastructure, managed workstations such as lab computers, IT data centers – servers and applications hosted in a physically secure and controlled environment, central IT services such as

messaging, central authentication services – Lightweight Directory Access Protocol (LDAP) and Active Directory (AD), student information systems, and departmental servers managed and hosted by OIT.

2. **Personally or departmentally managed resources:** includes workstations and servers managed by individuals (faculty, staff, or students) or departments. See the section titled *Areas Requiring Supplemental Plans* below for more details.

c. Areas Requiring Supplemental Plans

Some departments, systems, or networks may require additional controls due to information classification or system requirements. Areas that fall under the scope of industry, regulatory, or legal requirements, for example, often require additional controls. The most common of these applicable to the UTK Campus include:

1. The Payment Card Industry Data Security Standard (PCI-DSS) introduces up to 200 information security controls, many of which are likely to be additions to existing controls.
2. The Health Insurance Portability and Accountability Act (HIPAA) requires that specific patient information must be kept private, requiring additional controls in most cases.
3. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Other individuals or departments outside the control of UTK OIT may have additional requirements or reasons for managing their own systems. Although these resources may leverage general support systems such as the network infrastructure or IT data centers, the department or individual is ultimately responsible for the operation and overall information security of these resources. Resources in these categories must either:

1. Generate their own information security plan and seek approval for the plan from the UTK Authorizing Official; or
2. Agree to adopt the Information Security Program Plan, and obtain approval through an Interconnection Security Agreement (ISA) approved by the UTK Authorizing Official.

6. Out-of-Scope

As previously mentioned, UTK does host and has established connectivity with systems and networks that are outside the UTK scope of responsibility from an IT risk perspective. In those cases, additional ISAs or information security plans are also required. Two circumstances, in particular, will require additional ISAs or information security plans:

1. An IT resource connected to the UTK network managed by a department that does not report to the UTK Chancellor. These resources currently include:

    a. The University of Tennessee Institute for Public Service (IPS)
    b. Audiology & Speech Pathology, which reports to the University of Tennessee Health Science Center (UTHSC)

c. College of Pharmacy (UTHSC)
d. University of Tennessee Institute of Agriculture (UTIA)
e. The University of Tennessee System Administration (UTSA)

2. An IT resource connected to the UTK network and managed by a department that reports to the UTK Chancellor but whose choice not to be covered by this information security plan has been approved by the UTK Authorizing Official.

The appropriate Authorizing Official must approve both the ISAs and information security plans under the circumstances listed above. These information security plans must, at a minimum, include roles, responsibilities, assets, risks, and include the "Low" controls as defined in the University of Tennessee Statewide Controls Baseline. Additional controls must be added to reduce or mitigate risk to information systems classified as "MODERATE" or "HIGH" as deemed necessary and appropriate.

See Appendix II for list of "Low" baseline controls.

See Appendix III for list of the interconnections UTK has established with areas outside the scope of the Information Security Program Plan, such as campuses, institutes, and service providers.

7. Information Classification

In order to apply the appropriate information security controls to an information system, the system owner must first determine the criticality and sensitivity of information being processed, stored, or transmitted by those systems. This is done through the process of information security categorization, which determines the information security priorities for departmental information systems. *UT Policy IT0115 Information and Computer System Classification* provides additional guidance for the identification of information assets.

Information Technology Impact Assessment

A survey is distributed to Campus departments on a bi-annual basis. The data associated with this completed survey is used to appropriately apply data classification to the application and ultimately help to determine overall IT risks for the distributed systems.

UT Policy IT0115 requires the Campus to classify information systems within the potential impact categories of: low-impact, moderate-impact, or high-impact for the three information security objectives confidentiality, integrity, and availability. The potential impacts and information security objectives are defined below.

1. **Low**: The loss of confidentiality, integrity or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The three information security objectives are low.
2. **Moderate**: The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or

individuals. At least one of the information security objectives is moderate and no information security objective is greater than moderate.

3. **High**: The loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. At least one information security objective is high.

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table Source: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Information Security Objectives:

1. **Confidentiality**: Preserving authorized restrictions of information access, including means for protecting personal privacy and propriety information.
2. **Integrity**: Guarding against improper modification or destruction and includes ensuring information non-repudiation and authenticity.
3. **Availability**: Ensuring timely and reliable access to information.

Information security categorization is a two-step process:

1. Determine the potential impact level as low, moderate or high for the information type processed, stored, or transmitted by the system.
2. Categorize the system using the appropriate values accounting for the potential impact level.

Categorization of the information types that are representative of data input, data stored, data processed, and/or data as an outbound process is the responsibility of the system owner.

All data and information systems managed by OIT will fall into one of the categories for the information security objective types and potential impact levels. Systems meeting the criteria of multiple classification levels must protect the highest level of information on the system. If the system subject to multiple classifications does not protect the highest level, a detailed plan must be provided stating a clear separation of data and the protections for each classification of data on the system.

8. IT Risk Management Methodology

The primary goal of an organization's IT risk management process is to protect the Campus and its ability to *perform its mission*, not just protect IT assets. The IT risk management process should not be treated only as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the Campus.

The UTK Campus uses a formal document called the *UTK IT Risk Management Model*. This tool provides a basis for an effective risk-management methodology that provides the Campus with the practical guidance necessary for both assessing and prioritizing risks identified ***within critical IT systems***. The ultimate goal is to assist the University of Tennessee, Knoxville manage IT-related mission risks.

Campus-level IT threats and associated security risks are listed in Appendix IV.

Appendix I. Inheritable Common Information Security Controls

This appendix lists common information security controls that apply to information systems connected to the UTK infrastructure. Controls are applied based on the different risks presented by each set of systems, and are categorized below accordingly.

1. Network Common Controls

SC-5 Denial of Service (DoS) Protection

This control is fully implemented.

The organization protects against or limits the effects of the following types of denial of service attacks: DOS attacks, un-authorized intrusions, high-bandwidth utilizations, and all unauthorized data connections by employing the protections listed below.

Response:
The UTK network infrastructure is configured in such a way to protect against and limit the effects of DOS attacks, un-authorized intrusions, high-bandwidth utilizations, and all unauthorized data connections by employing the methods listed below:

a. Router and switch access protections including:
    1. Built-in router/switch operating system protections against common attacks like DOS.
    2. Access control lists that reduce incoming Internet traffic to known ports and protocols.
    3. Blacklisting and blocking incoming connections from network addresses which are involved in the sending, hosting, or originating of network based attacks.
    4. Filters that reduce network address spoofing—malicious network traffic disguised as legitimate communication.

b. Intrusion Prevention Systems:
    1. Detect and block a range of network-based attacks based on vendor-provided attack signatures.

c. High bandwidth, redundant connections:
    1. High-capacity Internet connections with additional sources of Internet service.
    2. Backup power for network equipment for core networking devices and other select devices.

d. Additional protections on the UTK wired network include:
    1. Switch port-based access control lists that filter and block unauthorized communication and actions from computers connected to the wired network

2. Protections against network flooding such as broadcast storms and certain denial of service attacks.
3. Measures that prevent unapproved networking equipment, such as switches, from connecting to the network.
4. Safeguards that prevent connected devices from assigning unauthorized network addresses.

SC-7 Boundary Protection

This control is fully implemented.

The organization:

a. Monitors and controls communications at the external boundary of the information system and at key internal boundaries within the information system;
b. Implements sub-networks for publicly accessible system components that are logically separated from internal organizational networks; and
c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Response:
The Campus:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system.
    1. This is done by using access control lists at the border to block certain services, such as NetBIOS, select Microsoft Windows networking services, Remote Desktop Protocol (RDP), and printer services like LPR and LPD.

b. Implements sub-networks for publicly accessible system components that are logically separated from internal organizational networks.
    1. Filters to prohibit communication with unallocated network address spaces that are traditionally used by attackers.
    2. "Null routes" that prevent network communication from a compromised or offending host and do not forward it to the intended recipient.
    3. "Do-not-access" lists of blocked network address ranges.

c. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
    1. The detailed connections can be seen in Appendix III of this document.

SI-4 Information System Monitoring

This control is partially implemented.

The organization:

a. Monitors the network to detect:
    1. Attacks and indicators of potential attacks in accordance with NIST, CERT, MIS-ISAC, and Manufacturer Notifications; and
    2. Unauthorized local, network, and remote connections;
b. Identifies unauthorized use of IT resources through various network service tools;
c. Deploys monitoring devices:
    1. Strategically within the organization infrastructure to collect organization-determined essential information; and
    2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to the Campus's operations and assets, individuals, other organizations based on law enforcement information, intelligence information, or other credible sources of information;
f. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, directives, policies, or regulations; and
g. Provides log data associated with critical systems to system owners of regulatory or standards related systems on an as-needed basis.

Response:
Intrusion Prevention Systems monitor information systems for network-based attacks and anomalous traffic. Applications (such as "IP Audit"), that collect baselines and samples of network communication patterns for select, high-risk networks, are used to proactively mitigate attacks.

Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, SIEM analysis of critical systems, audit record monitoring software, network monitoring software).

This control is partially implemented based on requirements in section g. Additional work will need to be done to properly monitor system associated with FERPA, HIPAA, and PCI data.

AC-6 Least Privilege

This control is partially implemented.

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Response:
Network Segmentation Protections include:

a. Separating general Campus networks from untrusted networks such as the Internet, the Student Residential Network (ResNET), and the wireless visitor network.
b. Information systems that have registered with the Network Registration system (NetReg) are permitted network access.

Each campus entity shall also apply least privilege to the development, implementation, and operation of organizational information systems.

AC-7 Unsuccessful Login Attempts

This control is fully implemented.

The organization:

a. Enforces a limit of 5 consecutive invalid logon attempts by a user during a 5-minute period; and
b. Automatically locks the account/node for a 5-minute period when the maximum number of unsuccessful attempts is exceeded.

Response:

a. Intrusion Prevention Systems detect and block specific types of “brute force” password attacks that use automated methods to guess passwords.
b. There are protections in place that prevent login attacks; for example, off-Campus networks and the "UT-OPEN" wireless networks are prohibited from accessing critical services such as UTK's Active Directory.
c. LDAP systems lock accounts if they experience 5 unsuccessful login attempts in a 5-minute period, locking the account for 5 minutes.
d. AD systems lock accounts if they experience 5 unsuccessful login attempts in a 5-minute period, locking the account for 5 minutes.

AC-18 Wireless Access

This control is fully implemented.

The organization:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b. Authorizes wireless access prior to allowing such connections.

Response:

a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access as connectivity is only granted after completing the network registration process. An exception to this would be the UT-Visitor and the EDUROAM networks. Network registration is not required on the UT-Visitor or the EDUROAM networks.
b. Authorizes wireless access to the organization prior to allowing such connections. Additional protections are listed in the list below.
    1. Private network addressing for computers on the "UT-Visitor" and "UT-Open" wireless networks. This addressing limits direct communication to "UT-Visitor" and "UT-Open" network computers from other computers off-Campus.
    2. Access control lists blocking certain types of undesirable or malicious network communication on specific network ports and services
    3. Safeguards preventing computers from assigning unauthorized network addresses.
    4. Technical precautions prevent hosts from impersonating important networking devices or services.

AC-19 Access Control for Mobile Devices

This control is fully implemented.

The organization:
a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b. Authorizes the connection of mobile devices to organizational information systems.

Response:
Mobile devices are only connected to organizational systems after completing the network registration process. Device identification and authorization is accomplished and enforced through this registration process. Additional usage restrictions are detailed in UT policy titled *IT0110-Acceptable use of Information Technology Resources*.

RA-2 Security Categorization

This control is fully implemented.

The organization:
a. Categorizes information and the organization in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance;
b. Documents the security categorization results (including supporting rationale) in the security plan for the organization; and
c. Ensures that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Response:
Information is categorized as mandated in UT Policy titled *IT0115-Information and Computer System Classification*. This process provides a guide to identify university-owned IT assets and to determine the level of IT risk to disclosure, alteration, and/or destruction of the information and the impact to UTK. This policy applies to all students, faculty, staff, and others, referred to as users throughout the policy, while accessing, using, or handling the UTK's information technology resources. In the policy, "users" includes but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access. All "users" are required to be familiar with and comply with this policy.

RA-5 Vulnerability Scanning

This control is partially implemented.

The organization:

a. Scans for vulnerabilities in the organization and hosted applications on a quarterly basis and when new vulnerabilities potentially affecting the system/applications are identified and reported;
b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    1. Enumerating platforms, software flaws, and improper configurations;
    2. Formatting checklists and test procedures; and
    3. Measuring vulnerability impact;
c. Analyzes vulnerability scan reports and results from security control assessments;
d. Remediates legitimate vulnerabilities quarterly in accordance with an organizational assessment of risk; and
e. Shares information obtained from the vulnerability scanning process and security control assessments with system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Response:
Pertaining to all critical systems, scheduled network-based vulnerability scans are carried out quarterly, on an as-needed basis, and when investigating possible information system compromises. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Vulnerability scans are performed on systems any time significant changes are made to the technical configuration. This type of vulnerability scanning should also be integrated into the individual system development life cycle so that all machines are scanned prior to being placed into a production-level role.

2. Systems Common Controls

IA-3 Device Identification and Authentication

This control is fully implemented.

The organization uniquely identifies and authenticates critical equipment before establishing a network connection.

Response:
Information systems and devices are uniquely identified through the Network Registration system (NetReg.) Devices must be registered before a network address is assigned. Mobile devices are only connected to organizational systems after completing the network registration process. Device identification and authorization is accomplished and enforced through this registration process. Additional usage restrictions are detailed in information technology policy titled "IT0110-Acceptable use of Information Technology Resources."

Supporting Documentation:
IT0110-Acceptable Use of Information Technology Resources

3. Support Common Controls

IR-4 Incident Handling

This control is fully implemented.

The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b. Coordinates incident handling activities with contingency planning activities; and
c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Response:
As further detailed in UT policy *IT0122-Security Incident Reporting and Response*, the Campus implements a process for detecting, containing, and recovering from security events and incidents. UTK considers incident response a part of the definition, design, and development of mission/business processes and information systems.

a. IT0122 mandates that each Campus must develop and maintain:
    1. An information security incident response plan (IRP) identifying security incident response (IR) objectives and prioritization.
    2. Procedures for technical staff and users that detail detecting, communicating, responding to, and reporting information security incidents.

3. A data breach notification procedure which complies with applicable state and federal laws and regulations such as HIPAA, as well as industry security standards such as Payment Card Industry Data Security Standard (PCI-DSS) and similar privacy standards.

b. Each Campus must periodically review, test, and approve their security incident response plans and procedures and document the results.
c. Each Campuses must report, on a periodic basis, all Security Incidents to the UTSA CISO. The CISO will provide instructions for reporting and make the accumulated information available to appropriate parties.
d. Incident Response plans and procedures must require:
    1. Collection, distribution, and response to relevant information system alerts and advisories on a regular basis.
    2. A responsibilities document detailing the employee position and role responsible for specific activities.
    3. Monitoring and tracking of Security Incidents through resolution.
    4. Protecting potential forensic evidence from corruption.
    5. Perform capture of security event reports and review suspected Security Incidents.
    6. Response to suspected Security Incidents including analysis, containment, Eradication, recovery, and follow-up reporting.
    7. Providing assistance to users during recovery from Security Incidents.
    8. Appropriate response by administration to reported security violations and incidents.
    9. Sharing information on Security Incidents and common vulnerabilities or threats with owners of connected information systems.
    10. Compliance with related Campus policies.
    11. Process for communicating with other UTK officials and outside parties when appropriate (e.g. UTK legal, public relations, law enforcement, ISP's, external expertise, etc.)
    12. Prioritization or severity ratings of Security Incidents.
    13. Senior management approval.

IR-5 Incident Monitoring

This control is fully implemented.

The organization tracks and documents information system security incidents.

Response:
UTK tracks and documents each security incident reported. Records about each incident, status, and other pertinent information are to be stored in a central repository. As stated in UT Policy *IT0122-Security Incident Reporting and Response*, the Campus mandates a process for detecting, containing, and recovering from security events and incidents.

IR-6 Incident Reporting

This control is fully implemented.

The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within 48 hours; and
b. Reports security incident information to the office of the UTK CISO.

Response:
As required by UT policy *IT0122-Security Incident Reporting and Response Policy* and detailed in the *UTK Incident Response Plan*, UTK cooperates with General Counsel, Media Relations, and involved parties to report security incidents to designated authorities when required by law or regulatory compliance. The types of security incidents reported, the content, and timeliness of the reports, and the designated reporting authorities reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance.

IR-7 Incident Response Assistance

This control is fully implemented.

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the organization for the handling and reporting of security incidents.

Response:
As required by UT policy *IT0122-Security Incident Reporting and Response Policy*, incident response assistance is provided through the UTK OIT HelpDesk and Support department. Additional helpful resources that may be used to identify and recover from security incidents are available on the UTK ISO website.

IR-8 Incident Response Plan

This control is fully implemented.

The organization:

a. Develops an incident response plan that:
    1. Provides the organization with a roadmap for implementing its incident response capability;
    2. Describes the structure and organization of the incident response capability;
    3. Provides a high-level approach for how the incident response capability fits into the overall organization;
    4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by Assignment: organization-defined personnel or roles;

b. Distributes copies of the incident response plan to Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements;
c. Reviews the incident response plan Annually;
d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e. Communicates incident response plan changes to both the CIO and the UTK stakeholders; and
f. Protects the incident response plan from unauthorized disclosure and modification.

Response:
Formal incident response procedures are in place to coordinate an official incident response. These procedures define security incidents, how to deal with different classes of incidents, the appropriate recovery steps, and how to report incidents, if needed. The Campus has developed and implemented a coordinated approach to incident response that is detailed in the *UTK Incident Response Plan*. Organizational missions, business functions, strategies, goals, and objectives for incident response are considered when determining the structure of incident response capabilities. The UTK Incident Response Plan also applies to external organizations and external service providers.

4. 4. Data Center Common Controls

PE-2 Physical Access Authorizations

This control is partially implemented.

The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the organization resides;
b. Issues authorization credentials for facility access;
c. Reviews the access list detailing authorized facility access by individuals Bi-Annually; and
d. Removes individuals from the facility access list when access is no longer required.

Response:
As this control only applies to areas within facilities that have not been designated as publicly accessible, the following controls exist in the following data centers: Stokely Management Center (SMC), Kingston Pike Building (KPB), and Humanities & Social Sciences (HSS);

a. A list of individuals with authorized access to the data center is maintained by Central Alarm;
b. Unescorted access to the facility is restricted to personnel with required security clearances, formal access authorizations, and validated need for access;
c. Only the Operations Manager or the UTK Chief Information Officer can issue authorization credentials;
d. Central Alarm has been instructed not to grant any individual access to a data center unless an access request has been issued directly from the Data Center Operations Manager or the UTK Chief Information Officer. No other entity has the authority to issue such requests;
e. The Data Center Operations Manager reviews and approves the access list and authorization credentials every six months;
f. When an individual no longer requires access to the data centers, the Data Center Operations Manager sends a request to Central Alarm to remove them from the authorized access list.

PE-3 Physical Access Control

This control is fully implemented.

The organization:

a. Enforces physical access authorizations at entry/exit points to the facility where the organization resides by;
    1. Verifying individual access authorizations before granting access to the facility; and
    2. Controlling ingress/egress to the facility using access badge or key;
b. Maintains physical access audit logs for the organization data center locations;

c. Provides cages, cameras, or locking cabinet racks to control access to areas within the facility officially designated as publicly accessible;
d. Escorts visitors and monitors visitor activity always;
e. Secures keys, combinations, and other physical access devices;
f. Inventories all critical devices every year and
g. Changes combinations and keys as needed and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Response:
These security controls exist in the following data centers: SMC and HSS.

a. If a data center is accessed during holidays, after hours (HSS), or during administrative closing, a security system must also be disarmed upon entry using a PIN number;
b. Keycard readers are used to enforce physical access authorizations at designated entry/exit points to the facility;
c. Central Alarm verifies authorization requests from the Data Center Operations Manager prior to granting individual access to the facility;
d. Visitors are allowed to enter the facility **only** if they are escorted by an authorized OIT staff member at all times. Visitors must also sign the Visitor's Log;
e. Lockable physical casings do **not** exist to protect data center equipment from illegal tampering. This is impractical with regards to maintenance. Other security controls in-place sufficiently deter unapproved access or tampering.

PE-6 Monitoring Physical Access

This control is fully implemented.

The organization:
a. Monitors physical access to the facility where the organization resides to detect and respond to physical security incidents;
b. Reviews physical access logs as needed and upon occurrence of a related and critical incident; and
c. Coordinates results of reviews and investigations with the Organizational incident response capability.

Response:
The following controls exist in the following data centers: Stokely Management Center (SMC), Kingston Pike Building (KPB), and Humanities & Social Sciences (HSS);
a. Central Alarm monitors physical access to secured campus buildings to detect and respond to physical security incidents;
b. Physical access logs are reviewed only when needed;
c. Video camera surveillance systems have been installed in all of the OIT data centers; Monitoring: cameras begin recording when their motion sensor is activated and recording storage capacity remains dependent on disk space (estimated storage span is 2-3 weeks)

PE-8 Visitor Access Records

This control is fully implemented.

The organization:

a. Maintains visitor access records to the facility where the organization resides for a year; and
b. Reviews visitor access records as necessary to support any incidents.

Response:
Central Alarm maintains an access log for each entry point where there is a keycard reader and also whenever PIN access is made. The following controls exist in the following data centers: Stokely Management Center (SMC), Kingston Pike Building (KPB), and Humanities & Social Sciences (HSS).

PE-9 Power Equipment and Cabling

This control is fully implemented.

The organization protects power equipment and power cabling for the organization from damage and destruction.

Response:
All UPS and post-UPS power distribution systems at all data center locations are located inside the data center with the IT equipment protected from power fluctuations and, therefore, has the same physical controls in place as the IT equipment itself. Generators at all locations are outside behind locked fences or cages. Power cabling to the UPS is via switchgear in secure areas and travels through rigid metal or plastic conduit in public areas.

PE-11 Emergency Power

This control is fully implemented.

The organization provides a short-term uninterruptible power supply to facilitate both an orderly shutdown of the organization and/or a transition of the organization to long-term alternate power in the event of a primary power source loss.

Response:
Uninterrupted Power System (UPS) systems provide 15 to 20 minutes on battery in the event of short-term power interruptions. To address long-term power interruptions, a diesel generator is configured to activate within 20 seconds following an outage. These controls exist in the following data centers: Stokely Management Center (SMC), Kingston Pike Building (KPB), and Humanities & Social Sciences (HSS).

PE-12 Emergency Lighting

This control is fully implemented.

The organization employs and maintains automatic emergency lighting for the organization that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Response:
Automatic emergency lighting is activated in the event of power interruptions or outages. As this control applies primarily to facilities containing concentrations of information system resources, the following controls exist in the following data centers: Stokely Management Center (SMC), Kingston Pike Building (KPB), and Humanities & Social Sciences (HSS).

PE-13 Fire Protection

This control is partially implemented.

The organization employs and maintains fire suppression and detection devices/systems for the organization that are supported by an independent energy source.

Response:

a. Fire detection and suppression systems (FM200 or Halon) are in place within the SMC and KPB data centers*;
b. Fire protection systems utilize the same power grid as the computer hardware;
c. Hand-held fire extinguishers are available within each data center.

Each of the two equipment rooms in the Stokely Management Center (SMC) is equipped with its own FM200 system. KPB's interior uplink room is equipped with an independent Halon fire suppression system.

*The HSS data center does not have a fire suppression system.

PE-14 Temperature and Humidity Controls

This control is fully implemented.

The organization:

a. Maintains temperature and humidity levels within the facility where the organization resides at in order to provide a healthy environment for the critical information systems;
b. Monitors temperature and humidity levels in real-time.

Response:
These security controls exist in the following data centers: SMC, KPB, and HSS.

a. Liebert Computer Room Air Conditioning (CRAC) units provide environmental temperature and humidity controls;
b. Environmental conditions are monitored via AVTech RoomAlert monitoring units through AVTech DeviceManager software.

PE-15 Water Damage Protection

This control is fully implemented.

The organization protects information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Response:
These security controls exist in the following data centers: SMC, KPB, and HSS.

a. Master shut-off or isolation valves protect information systems from water damage. Access to these valves is held by Facility Services;
b. AVTech RoomAlert units also detect the presence of water.

Appendix II. Low Baseline Controls

This section contains a list of "LOW" information security controls that are to be implemented on UT-Owned IT Resources classified as "LOW" using the guidance available in policy IT0115. Justification for controls that are not implemented must be approved by the department head and reviewed and accepted by the UTK SISO.

NIST 800-53r4 Control Number:	**Control Title**	**UT 800-53r4 BASELINE CONTROLS**	
		Priority	LOW
ACCESS CONTROLS			
AC-1	Access Control Policy and Procedures	P1	✓
AC-2	Account Management	P1	✓
AC-3	Access Enforcement	P1	✓
AC-4	Information Flow Enforcement	P1	
AC-5	Separation of Duties	P1	
AC-6	Least Privilege	P1	
AC-7	Unsuccessful Login Attempts	P2	✓
AC-8	System Use Notification	P1	✓
AC-9	Previous Logon (Access) Notification	P0	
AC-10	Concurrent Session Control	P2	
AC-11	Session Lock	P3	
AC-12	Withdrawn ---		
AC-13	Withdrawn ---		
AC-14	Permitted Actions without Identification or Authentication	P1	✓
AC-15	Withdrawn ---		
AC-16	Security Attributes	P0	
AC-17	Remote Access	P1	✓
AC-18	Wireless Access	P1	✓
AC-19	Access Control for Mobile Devices	P1	
AC-20	Use of External Information Systems	P1	
AC-21	User-Based Collaboration and Information Sharing	P0	
AC-22	Publicly Accessible Content	P2	
AC-23	Data Mining Protection	P0	
AC-24	Access Control Decisions	P0	
AC-25	Publicly Accessible Content	P0	
AWARENESS AND SECURITY TRAINING			
AT-1	Security Awareness and Training Policy and Procedures	P1	✓
AT-2	Security Awareness	P1	✓
AT-3	Security Training	P1	
AT-4	Security Training Records	P3	✓
AT-5	Contacts with Security Groups and Associations	P3	
AUDIT AND ACCOUNTABILITY			
AU-1	Audit and Accountability Policy and Procedures	P1	✓
AU-2	Auditable Events	P1	
AU-3	Content of Audit Records	P1	
AU-4	Audit Storage Capacity	P1	

AU-5	Response to Audit Processing Failures	P1	
AU-6	Audit Review, Analysis, and Reporting	P1	✓
AU-7	Audit Reduction and Report Generation	P2	
AU-8	Time Stamps	P1	
AU-9	Protection of Audit Information	P1	
AU-10	Non-repudiation	P1	
AU-11	Audit Record Retention	P3	
AU-12	Audit Generation	P1	
AU-13	Monitoring for Information Disclosure	P0	
AU-14	Session Audit	P0	
AU-15	Alternate Audit Capability	P0	
AU-16	Cross-Organizational Auditing	P0	
SECURITY ASSESSMENT & AUTHORIZATION			
CA-1	Security Assessment and Authorization Policies and Procedures	P1	✓
CA-2	Security Assessments	P2	✓
CA-3	Information System Connections	P1	
CA-4	Withdrawn ---		
CA-5	Plan of Action and Milestones	P3	✓
CA-6	Security Authorization	P3	
CA-7	Continuous Monitoring	P3	✓
CONFIGURATION MANAGEMENT			
CM-1	Configuration Management Policy and Procedures	P1	✓
CM-2	Baseline Configuration	P1	✓
CM-3	Configuration Change Control	P1	
CM-4	Security Impact Analysis	P2	
CM-5	Access Restrictions for Change	P1	
CM-6	Configuration Settings	P1	✓
CM-7	Least Functionality	P1	
CM-8	Information System Component Inventory	P1	
CM-9	Configuration Management Plan	P1	
CM-10	Software Usage Restrictions	P1	✓
CM-11	User Installed Software	P1	
CONTINGENCY PLANNING			
CP-1	Contingency Planning Policy and Procedures	P1	✓
CP-2	Contingency Plan	P1	
CP-3	Contingency Training	P2	
CP-4	Contingency Plan Testing and Exercises	P2	
CP-5	Withdrawn ---		
CP-6	Alternate Storage Site	P1	
CP-7	Alternate Processing Site	P1	
CP-8	Telecommunications Services	P1	
CP-9	Information System Backup	P1	
CP-10	Information System Recovery and Reconstitution	P1	✓
CP-11	Predictable Failure Prevention	P1	
CP-12	Alternate Communications Protocol	P0	
CP-13	Safe Mode	P0	
IDENTIFICATION & AUTHENTICATION			

IA-1	Identification and Authentication Policy and Procedures	P1	✓
IA-2	Identification and Authentication (Organizational Users)	P1	
IA-3	Device-to-Device Identification and Authentication	P1	
IA-4	Identifier Management	P1	✓
IA-5	Authenticator Management	P1	✓
IA-6	Authenticator Feedback	P1	✓
IA-7	Cryptographic Module Authentication	P1	
IA-8	Identification and Authentication (Non- Organizational Users)	P1	✓
IA-9	Service Identification & Authorization	P0	
IA-10	Alternative Authentication	P0	
IA-11	Adaptive Identification & Authentication	P0	
IA-12	Re-authentication	P0	
INCIDENT RESPONSE			
IR-1	Incident Response Policy and Procedures	P1	✓
IR-2	Incident Response Training	P2	✓
IR-3	Incident Response Testing and Exercising	P2	
IR-4	Incident Handling	P1	✓
IR-5	Incident Monitoring	P1	✓
IR-6	Incident Reporting	P1	✓
IR-7	Incident Response Assistance	P3	✓
IR-8	Incident Response Plan	P1	✓
IR-9	Information Spillage Response	P0	
MAINTENANCE			
MA-1	System Maintenance Policy and Procedures	P1	✓
MA-2	Controlled Maintenance	P2	
MA-3	Maintenance Tools	P2	
MA-4	Non-Local Maintenance	P1	✓
MA-5	Maintenance Personnel	P1	✓
MA-6	Timely Maintenance	P1	
MEDIA PROTECTION			
MP-1	Media Protection Policy and Procedures	P1	✓
MP-2	Media Access	P1	
MP-3	Media Marking	P1	
MP-4	Media Storage	P1	
MP-5	Media Transport	P1	
MP-6	Media Sanitization	P1	✓
MP-7	Media Use	P1	
MP-8	Media Downgrading		
PHYSICAL & ENVIRONMENTAL PROTECTION			
PE-1	Physical and Environmental Protection Policy and Procedures	P1	✓
PE-2	Physical Access Authorizations	P1	
PE-3	Physical Access Control	P1	
PE-4	Access Control for Transmission Medium	P1	
PE-5	Access Control for Output Devices	P1	
PE-6	Monitoring Physical Access	P1	
PE-7	Withdrawn ---		
PE-8	Access Records	P3	

PE-9	Power Equipment and Power Cabling	P1	
PE-10	Emergency Shutoff	P1	
PE-11	Emergency Power	P1	
PE-12	Emergency Lighting	P1	✓
PE-13	Fire Protection	P1	✓
PE-14	Temperature and Humidity Controls	P1	
PE-15	Water Damage Protection	P1	
PE-16	Delivery and Removal	P1	
PE-17	Alternate Work Site	P1	
PE-18	Location of Information System Components	P2	
PE-19	Information Leakage	P0	
PE-20	Port & I/O Device Access	P0	
PLANNING			
PL-1	Security Planning Policy and Procedures	P1	✓
PL-2	System Security Plan	P1	✓
PL-3	Withdrawn ---		
PL-4	Rules of Behavior	P1	✓
PL-5	Withdrawn ---		
PL-6	Withdrawn ---		
PL-7	Security Concept of Operations	P0	
PL-8	Security Architecture	P0	
PERSONNEL SECURITY			
PS-1	Personnel Security Policy and Procedures	P1	✓
PS-2	Position Categorization	P1	
PS-3	Personnel Screening	P1	
PS-4	Personnel Termination	P2	✓
PS-5	Personnel Transfer	P2	✓
PS-6	Access Agreements	P3	✓
PS-7	Third-Party Personnel Security	P1	✓
PS-8	Personnel Sanctions	P3	✓
RISK ASSESSMENT			
RA-1	Risk Assessment Policy and Procedures	P1	✓
RA-2	Security Categorization	P1	✓
RA-3	Risk Assessment	P1	
RA-4	Withdrawn ---		
RA-5	Vulnerability Scanning	P1	✓
SYSTEM & SERVICES ACQUISITION			
SA-1	System and Services Acquisition Policy and Procedures	P1	✓
SA-2	Allocation of Resources	P1	✓
SA-3	Life Cycle Support	P1	
SA-4	Acquisitions	P1	✓
SA-5	Information System Documentation	P2	✓
SA-6	Withdrawn ---		
SA-7	Withdrawn ---		
SA-8	Security Engineering Principles	P1	
SA-9	External Information System Services	P1	
SA-10	Developer Configuration Management	P1	
SA-11	Developer Security Testing	P2	

SA-12	Supply Chain Protections	P1	
SA-13	Withdrawn ---		
SA-14	Critical Information System Components	P2	
SA-15	Development Process, Standards, and Tools	P2	
SA-16	Developer-Provided Training	P1	
SA-17	Developer Security Architecture and Design	P1	
SA-18	Tamper Resistance and Detection	P0	
SA-19	Anti-Counterfeit	P0	
SYSTEM & COMMUNICATIONS PROTECTION			
SC-1	System and Communications Protection Policy and Procedures	P1	✓
SC-2	Application Partitioning	P1	
SC-3	Security Function Isolation	P1	
SC-4	Information In Shared Resources	P1	
SC-5	Denial of Service Protection	P1	✓
SC-6	Resource Priority	P0	
SC-7	Boundary Protection	P1	✓
SC-8	Transmission Integrity	P1	
SC-9	Transmission Confidentiality	P1	
SC-10	Network Disconnect	P2	
SC-11	Trusted Path	P0	
SC-12	Cryptographic Key Establishment and Management	P1	✓
SC-13	Use of Cryptography	P1	✓
SC-14	Public Access Protections	P1	✓
SC-15	Collaborative Computing Devices	P1	✓
SC-16	Transmission of Security Attributes	P0	
SC-17	Public Key Infrastructure Certificates	P1	
SC-18	Mobile Code	P1	
SC-19	Voice Over Internet Protocol	P1	
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	✓
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	✓
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	✓
SC-23	Session Authenticity	P1	
SC-24	Fail in Known State	P1	
SC-25	Thin Nodes	P0	
SC-26	Honeypots None	P0	
SC-27	Operating System-Independent Applications	P0	
SC-28	Protection of Information at Rest	P1	
SC-29	Heterogeneity	P0	
SC-30	Virtualization Techniques	P0	
SC-31	Covert Channel Analysis	P0	
SC-32	Information System Partitioning	P1	
SC-33	Withdrawn ---		
SC-34	Non-Modifiable Executable Programs	P0	
SC-35	Technical Surveillance Countermeasures Survey	P0	
SC-36	Honey clients	P0	
SC-37	Distributed Processing and Storage	P0	

SC-38	Malware Analysis	P0	
SC-39	Out-of-Band Channels	P0	
SC-40	Operations Security	P0	
SC-41	Process Isolation	P1	✓
SC-42	Wireless Link Protection	P0	
SYSTEM & INFORMATION INTEGRITY			
SI-1	System &Information Integrity Policy & Procedures	P1	✓
SI-2	Flaw Remediation	P1	✓
SI-3	Malicious Code Protection	P1	✓
SI-4	Information System Monitoring	P1	✓
SI-5	Security Alerts, Advisories, and Directives	P1	✓
SI-6	Security Functionality Verification	P1	
SI-7	Software and Information Integrity	P1	
SI-8	Spam Protection	P1	✓
SI-9	Information Input Restrictions	P2	
SI-10	Information Input Validation	P1	
SI-11	Error Handling	P2	
SI-12	Information Output Handling and Retention	P2	✓
SI-13	Withdrawn ---		
SI-14	Non-persistence	P0	
PROGRAM MANAGEMENT			
PM-1	Information Security Program Plan	P1	✓
PM-2	Senior Information Security Officer	P1	✓
PM-3	Information Security Resources	P1	✓
PM-4	Plan of Action and Milestones Process	P1	✓
PM-5	Information System Inventory	P1	✓
PM-6	Information Security Measures of Performance	P1	✓
PM-7	Enterprise Architecture	P1	
PM-8	Critical Infrastructure Plan	P1	
PM-9	Risk Management Strategy	P1	✓
PM-10	Security Authorization Process	P1	✓
PM-11	Mission/Business Process Definition	P1	✓

Appendix III. UTK Network Interconnections

The table below lists the interconnections UTK has established with areas outside the scope of the Information Security Program Plan, such as other campuses, learning institutes, and Internet service providers.

	Destination	Agreement Type	Status	Purpose
1	NetTN	Contract with AT&T	In place	Internet connectivity and InterCampus communication
2	TransitRail	Informal Agreement	Planned: Formal ISA	Commodity Internet
3	Level 3	Informal Agreement	Planned: Formal ISA	Secondary Internet service provider
4	SoX	Informal Agreement	Planned: Formal ISA	Internet 2 provider
5	UT Chattanooga	Informal Agreement	Planned: Formal ISA	Information exchange
6	UT Martin (with remote locations)	Informal Agreement	Planned: Formal ISA	Information exchange
7	UT Health Science Center	Informal Agreement	Planned: Formal ISA	Information exchange
8	UT Institute of Agriculture	Informal Agreement	Planned: Formal Security Plan	Information exchange
9	Teragrid	Informal Agreement	Planned: Formal ISA	Research
10	Oak Ridge National Lab	Informal Agreement	Planned: Formal ISA	Information exchange
11	UT Medical Center	Informal Agreement	Planned: Formal ISA	Information exchange
12	Knoxville Radiology Group	Business Associate Agreement	In Place	Information exchange
13	Tremont Research Facility	Informal Agreement	Planned: Formal ISA	Information exchange
14	Paciolan	Informal Agreement	Planned: Formal ISA	Connection to Athletics' Ticket Office vendor
15	Education Networks of America	Informal Agreement	Planned: Formal ISA	Information exchange
16	MEDICAT	Business Associate Agreement	In Place	Information exchange

Appendix IV. – Enterprise IT Risks

The threats listed below represent a dynamic listing of risk scenarios that are being constantly evaluated at the UTK Campus.

Threat Scenario	Likelihood	Impact	Risk Index	Relative Risk	Notes
Data Loss	4	5	20	HIGH RISK	Data exposure or loss prevention controls are based on policy, and include classifying sensitive data, discovering that data across and enterprise, enforcing controls, and reporting and auditing to ensure policy compliance. [Data leaving the campus]
Malware	5	4	20	HIGH RISK	Malware is a general term for any software that gets installed on your machine and performs unwanted tasks, often for some third party's benefit. Spyware and adware can be included here and can range from being simple annoyances to being a serious security problem. This includes Zero-Day exploits.
Phishing	5	4	20	HIGH RISK	Phishing is the name given to the practice of sending emails purporting to come from a genuine company operating on the Internet. The emails are an attempt to trick consumers into disclosing personal information at false websites which may later be used to commit fraud and/or identity theft.
Viruses	5	4	20	HIGH RISK	Trojans and Worms replicate by being copied into a computer boot sector or document. Viruses can be transmitted as attachments and be distributed via different forms of media.
BYOD and Mobile Device Management	5	4	20	HIGH RISK	BYOD threats to the campus posed by an employee or student-owned mobile device can be as complex as a sophisticated malware attack designed to snoop on an employee's browsing activity or as simple as email on a lost phone.

Patch Management	4	4	16	HIGH RISK	When patching information systems, we expect to reduce vulnerabilities, improve performance, improve usability, and assist in achieving compliance.
Intellectual Property Theft	4	4	16	HIGH RISK	Copyright infringement and patent infringement is about robbing people of their ideas, inventions, trade secrets, proprietary property, and creative expressions. Intellectual property theft costs U.S. businesses billions of dollars each year.
Logical Access Control	4	4	16	HIGH RISK	Access control in this case includes the mechanisms used to ensure that resources and services are granted to only those users who are entitled to them. Examples include passwords, permissions, firewalls, rule sets, keys, or tokens.
System Penetration	4	4	16	HIGH RISK	Layered security as a best-practice. This includes the use of perimeter controls, segmented networks, and host-based firewall controls.
Social Engineering	4	4	16	HIGH RISK	Social engineering is the art of manipulating people so they give up confidential information. The typos of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or access your computer.
DNS Poisoning	3	5	15	HIGH RISK	DNS cache poisoning occurs when and Internet server has its domain name table compromised by malicious code.
Local Admin Account Usage	5	3	15	HIGH RISK	Running as "administrator" on workstations. This situation could allow the unintentional execution of applications or the installation of unwanted software.
Rogue Wireless Devices	5	3	15	HIGH RISK	A rogue wireless device is a system that has been installed on a secure network without explicit authorization from an administrator/decision-maker.

SPAM	5	3	15	HIGH RISK	Deceitful emails can put your personal and professional information at risk as well as acting as a entry point for other, more serious viruses.
Advanced Persistent Threat	4	3	12	MODERATE RISK	An APT can remain undetected for long periods of time with the purpose of stealing data versus causing damage to systems.
Website Defacement	3	4	12	MODERATE RISK	This type of vandalism can be a large problem for the systems of the campus environment.
System Administration Practices	3	4	12	MODERATE RISK	System administration practices vary, but general practice include: periodic security audits, adequate backups, security configurations, management procedures, documented and tested security settings, and training.
Brute Force Password Cracking	3	4	12	MODERATE RISK	A brute force attack is one of the most common attacks conducted against information systems. The aim of this attack is to gain access to user accounts by repeatedly trying to guess the password of a user or a group of users.
COOP / DR Plans	3	4	12	MODERATE RISK	A COOP is a departmental plan for the restoration of critical resources identified in a Business Impact Analysis. All units, departments, and divisions of the campus that serve a critical role or maintain an essential function are required to participate in COOP and disaster planning.
Key Person Dependency	4	3	12	MODERATE RISK	Relying on one person to maintain critical services can severely compromise day-to-day operations if problems occur.
Network Sniffing	3	4	12	MODERATE RISK	A packet sniffer is used to capture usernames and passwords, which can be used for further network exploits. Other bits of sensitive information may be captured as well.
Perimeter Security	4	3	12	MODERATE RISK	Every company has a network perimeter - where the "trusted"

					network ends and the "untrusted" Internet begins.
Separation of Duties	3	4	12	MODERATE RISK	SoD is the concept of having more than one person required to complete a task that has been deemed as critical. Addressing this should also address collusion.
Device Theft	3	4	12	MODERATE RISK	Laptop computers, Network Attached Storage (NAS), external storage, tablets, cellular phones, and other personal electronics have become a target of choice for thieves all over the country. Why? Because they are small, valuable, can be removed quickly, are easily hidden, and there is a market for them.
Physical Infrastructure Attacks	2	5	10	MODERATE RISK	The two major objectives of physical infrastructure are personnel safety and access control. Are the appropriate physical entry controls in place to allow only authorized personnel access to critical assets?
TCP/IP Hijacking	3	3	9	MODERATE RISK	Sometimes known as cookie hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
Distributed Denial of Service (DDOS)	3	3	9	MODERATE RISK	A Denial of Service attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system consuming most or all of its resources.
External Connectivity for Partner Networks	3	3	9	MODERATE RISK	Interconnectivity with other organizations, networks, and tools.
IP Spoofing/Masquerading	3	3	9	MODERATE RISK	Spoofing is an attempt by unauthorized users to gain access to a system by posing as an authorized user. Spoofing involves passing fraudulent information for some malicious goal and can be implemented in many different ways.

Use and Enforcement of Strong Passwords	2	4	8	MODERATE RISK	Passwords are the first line of defense against interactive attacks. Protecting information systems and data often comes down to using strong passwords.
Back Door / Trap Door	2	3	6	MODERATE RISK	A back door is a means of access to a computer program or website that bypasses normal security mechanisms. Whether installed as an administrative tool or a means of attack, a back door is a security risk, because there are always individuals out there looking for any vulnerability to exploit.
Security Integration with SDLC	2	3	6	MODERATE RISK	Enterprise-security best practices and engineering principles need to be integrated into all aspects of the SDLC for the campus.
Eavesdropping	2	2	4	LOW RISK	In the world of computer networks and in some cases, universities, the default position is often that "anything can access anything", which is weak from a security perspective. Formal network segmentation, encryption, and network access control are mitigations for this issue.
System Tampering	2	2	4	LOW RISK	Electronic or technical vandalism.