****

Name of System

Security Plan

**Prepared for:**

Name of System Owner

Date For Security Plan

**Prepared by:**

University of Tennessee, Knoxville

Office Information Technology (OIT)

**Table of Contents**

[1. Information System Name/Title: 3](#_Toc442269174)

[2. Information System Categorization: 3](#_Toc442269175)

[3. Information System Owner: 3](#_Toc442269176)

[4. Authorizing Official: 3](#_Toc442269177)

[5. Other Designated Contacts: 3](#_Toc442269178)

[6. Assignment of Security Responsibility 3](#_Toc442269179)

[7. Information System Operational Status 3](#_Toc442269180)

[8. Information System Type 4](#_Toc442269181)

[9. General System Description/Purpose 4](#_Toc442269182)

[10. System Interconnections/Information Sharing 4](#_Toc442269183)

[11. Related Laws/Regulations/Policies 5](#_Toc442269184)

[12. Minimum Security Controls 5](#_Toc442269185)

[13. Information System Security Plan Completion Date: 9](#_Toc442269186)

[14. Information System Security Plan Approval Date: 9](#_Toc442269187)

[15. Information System Security Controls 9](#_Toc442269188)

[16. Appendix A: System Inventory 58](#_Toc442269189)

# Information System Name/Title:

In this section provide the name and a very short description of the system.

# Information System Categorization:

The Information System Owner has determined the category of risk with the UTK XYZ Information System to be ***MODERATE***. (*see* FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*):

Place an “X” in the appropriate categories below.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Low | Moderate | High |
| Confidentiality | **X** |  |  |
| Integrity | **X** |  |  |
| Availability | **X** |  |  |

# Information System Owner:

Name: Insert name of System Owner

Email: Insert email here: Email@utk.edu

Phone: (865) xxx-xxxx

# Authorizing Official:

Name: Insert name of Authorizing Official

Email: Insert email here: Email@utk.edu

Phone: (865) xxx-xxxx

# Other Designated Contacts:

List any other important system contacts.

# Assignment of Security Responsibility

List security point of contact for the system.

# Information System Operational Status

This system is currently considered: (1) OPERATIONAL, (2) UNDER DEVELOPMENT, OR (3) HAS EXPERIENCED A MAJOR MODIFICATION. (Select one)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| X | Operational |   | Under Development |   | Major Modification |

# Information System Type

This system is considered a: (1) MAJOR APPLICATION or (2) GENERAL SUPPORT SYSTEM. (Select one)

|  |  |  |  |
| --- | --- | --- | --- |
| X | Major Application |   | General Support System |

# General System Description/Purpose

Please describe the system and any sub-system that it contains. This section should be a couple of paragraphs in length and the description should be written so that someone outside of the organization would understand what the overall description and purpose of the System is.

**System Diagrammponents and Interfaces**

Add a diagram or drawing of the system here.



# System Interconnections/Information Sharing

List interconnected systems and provide the system name, agreement type, and purpose of connection.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref.** | **System Name** | **Agreement Type** | **Status** | **Purpose** |
| 1 | Example Destination | Informal Agreement |  Future  | Central Authentication |
| 2 | Example Destination #2 | Business Contract | Active | VPN With State |
| 3 | xxxx | xxxx | xxxx | xxxx |
| 4 | xxxx | xxxx | xxxx | xxxx |

# Related Laws/Regulations/Policies

* University of Tennessee System Policy IT0110, *Acceptable Use of Information Technology Resources.*
* Tennessee Code Annotated § 47-18-2107, 2010 S.B. 2793, *Release of personal consumer information* National Standards and Guidance. NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199).
* The University of Tennessee, Knoxville, *Banner Data Standards Manual*
* NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Systems* (NIST 800-53).
* NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Systems* (NIST 800-53).

# Minimum Security Controls

Please see complete table below for a listing of minimum security controls.

| **NIST 800-53r4 Control Number:** | **Control Title** | **UT KnoxvilleBaseline Controls** |
| --- | --- | --- |
| LOW | MOD |
| **ACCESS CONTROLS** |
| AC-2 | Account Management | ✓ |   |
| AC-3 | Access Enforcement | ✓ |   |
| AC-5 | Separation of Duties |   | ✓ |
| AC-7 | Unsuccessful Login Attempts | ✓ |   |
| COMMON CONTROL |
| AC-8 | System Use Notification | ✓ |   |
| AC-11 | Session Lock |   | ✓ |
| AC-14 | Permitted Actions without Identification or Authentication | ✓ |   |
| AC-17 | Remote Access | ✓ |   |
| AC-18 | Wireless Access | ✓ |   |
| COMMON CONTROL |
| AC-22 | Publicly Accessible Content |   | ✓ |
| **AWARENESS AND SECURITY TRAINING** |
| AT-2 | Security Awareness | ✓ |   |
| AT-3 | Role Based Security Training | ✓ |   |
| AT-4 | Security Training Records | ✓ |   |
| **AUDIT AND ACCOUNTABILITY** |
| AU-6 | Audit Review, Analysis, and Reporting | ✓ |   |
| AU-8 | Time Stamps |   | ✓ |
| AU-9 | Protection of Audit Information |   | ✓ |
| **SECURITY ASSESSMENT & AUTHORIZATION** |
| CA-2 | Security Assessments | ✓ |   |
| CA-3 | Information System Connections |   | ✓ |
| CA-7 | Continuous Monitoring | ✓ |   |
| **CONFIGURATION MANAGEMENT** |
| CM-2 | Baseline Configuration | ✓ |   |
| CM-6 | Configuration Settings | ✓ |   |
| CM-7 | Least Functionality |   | ✓ |
| CM-8 | Information System Component Inventory | ✓ |   |
| CM-10 | Software Usage Restrictions | ✓ |   |
| **CONTINGENCY PLANNING** |
| CP-2 | Contingency Plan |   | ✓ |
| CP-9 | Information System Backup |   | ✓ |
| CP-10 | Information System Recovery and Reconstitution | ✓ |   |
| **IDENTIFICATION & AUTHENTICATION** |
| IA-2 | Identification and Authentication (Organizational Users) |   | ✓ |
| IA-4 | Identifier Management | ✓ |   |
| COMMON CONTROL |
| IA-5 | Authenticator Management | ✓ |   |
| IA-6 | Authenticator Feedback | ✓ |   |
| IA-8 | Identification and Authentication (Non- Organizational Users) | ✓ |   |
| **INCIDENT RESPONSE** |   |
| IR-2 | Incident Response Training | ✓ |   |
| IR-4 | Incident Handling | ✓ |   |
| COMMON CONTROL |
| IR-5 | Incident Monitoring | ✓ |   |
| COMMON CONTROL |
| IR-6 | Incident Reporting | ✓ |   |
| COMMON CONTROL |
| IR-7 | Incident Response Assistance | ✓ |   |
| COMMON CONTROL |
| IR-8 | Incident Response Plan | ✓ |   |
| COMMON CONTROL |
| **MAINTENANCE** |
| MA-4 | Non-Local Maintenance | ✓ |   |
| MA-5 | Maintenance Personnel | ✓ |   |
| **MEDIA PROTECTION** |
| MP-1 | Media Protection Policy and Procedures | ✓ |   |
| MP-2 | Media Access |   |  ✓ |
| MP-3 | Media Marking |   |  ✓ |
| MP-4 | Media Storage |   |  ✓ |
| MP-5 | Media Transport |   | ✓  |
| MP-6 | Media Sanitization | ✓ |   |
| **PHYSICAL & ENVIRONMENTAL PROTECTION** |
| PE-12 | Emergency Lighting | ✓ |   |
| COMMON CONTROL |
| PE-13 | Fire Protection | ✓ |   |
| COMMON CONTROL |
| **PLANNING** |
| PL-2 | System Security Plan | ✓ |   |
| PL-4 | Rules of Behavior | ✓ |   |
| **PERSONNEL SECURITY**  |
| PS-4 | Personnel Termination | ✓ |   |
| PS-5 | Personnel Transfer | ✓ |   |
| PS-6 | Access Agreements | ✓ |   |
| PS-7 | Third-Party Personnel Security | ✓ |   |
| PS-8 | Personnel Sanctions | ✓ |   |
| **RISK ASSESSMENT** |
| RA-2 | Security Categorization | ✓ |   |
| COMMON CONTROL |
| RA-5 | Vulnerability Scanning | ✓ |   |
| COMMON CONTROL |
| **SYSTEM & SERVICES ACQUISITION** |
| SA-2 | Allocation of Resources | ✓ |   |
| SA-4 | Acquisitions | ✓ |   |
| SA-5 | Information System Documentation | ✓ |   |
| SA-8 | Security Engineering Principles |   | ✓ |
| **SYSTEM & COMMUNICATIONS PROTECTION** |
| SC-2 | Application Partitioning |   | ✓ |
| SC-5 | Denial of Service Protection | ✓ |   |
| COMMON CONTROL |
| SC-7 | Boundary Protection | ✓ |   |
| COMMON CONTROL |
| SC-12 | Cryptographic Key Establishment and Management | ✓ |   |
| SC-13 | Use of Cryptography | ✓ |   |
| SC-15 | Collaborative Computing Devices | ✓ |   |
| SC-17 | Public Key Infrastructure Certificates |   | ✓ |
| SC-20 | Secure Name /Address Resolution Service (Authoritative Source) | ✓ |   |
| **SYSTEM & INFORMATION INTEGRITY** |
| SI-2 | Flaw Remediation | ✓ |   |
| SI-3 | Malicious Code Protection | ✓ |   |
| SI-4 | Information System Monitoring | ✓ |   |
| COMMON CONTROL |
| SI-5 | Security Alerts, Advisories, and Directives | ✓ |   |

# Information System Security Plan Completion Date:

Insert completion date here.

# Information System Security Plan Approval Date:

Insert approval date here.

# Information System Security Controls

**Section Instructions**

* Provide a response in each of the control areas that pertains to your specific system.
* After you provide a response, each of your controls should have one of the check-boxes at the top of the control marked to announce implementation status.
* As system owner, you want to have as many fully-implemented controls as possible.
* There may be scenarios where you only have a partial response as an answer. This is fine, but take some time to provide an answer in your response that elaborates why this control is only partially implemented.
* There may be scenarios where you have not implemented a control for your system. This is fine, but take some time to provide an answer in your response that elaborates why this control is not / could not be implemented for your system.
* Some of the controls may be inheritable from the Campus Security Plan, these controls are clearly marked as inheritable.
* Please provide as many supporting documents as you can.
* Replace or remove all red text in the document.

AC-2 **Account Management**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Identifies and selects the following types of information system accounts to support system mission’s/business functions: SYSTEM Account Administrators;
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by departmental approvers for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with documented security guidelines;
7. Monitors the use of information system accounts;
8. Notifies account managers:
	1. When accounts are no longer required;
	2. When users are terminated or transferred; and
	3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
	1. A valid access authorization;
	2. Intended system usage; and
	3. Other attributes as required by the system or associated mission’s/business functions;
10. Reviews accounts for compliance with account management requirements quarterly; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-3 **Access Enforcement**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**AC-5 Separation of Duties**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization:**

1. Separates critical duties;
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-7 **Unsuccessful Login Attempts – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

The system:

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

Response:

The system representative will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate response.

* Intrusion Prevention Systems detect and block specific types of “brute force” password attacks that use automated methods to guess passwords.
* 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.
* LDAP systems lock accounts if they experience 10 unsuccessful login attempts in a 5-minute period, locking the account for 5 minutes.
* AD systems lock accounts if they experience 5 unsuccessful login attempts in a 5-minute period, locking the account for 5 minutes.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-8 **System Use Notification**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Displays to users a notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
2. Users are accessing a protected information system;
3. Information system usage may be monitored, recorded, and subject to audit;
4. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
5. Use of the information system indicates consent to monitoring and recording;
6. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
7. For publicly accessible systems:
8. Displays system use information before granting further access;
9. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
10. Includes a description of the authorized uses of the system.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**AC-11 Session Lock**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system:**

1. Prevents further access to the system by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-14 **Permitted Actions Without Identification or Authentication**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Identifies any actions that can be performed on the information system without identification or authentication consistent with organizational/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-17 **Remote Access**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AC-18 **Wireless Access – Inheritable Control**
[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the organization prior to allowing such connections.

Response:
The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate response.

1. 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.
2. Authorizes wireless access to the organization prior to allowing such connections. Additional protections are listed in the bulleted list below.
	* 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.
	* Access control lists blocking certain types of undesirable or malicious network communication on specific network ports and services
	* Safeguards preventing computers from assigning unauthorized network addresses.

Technical precautions prevent hosts from impersonating important networking devices or services.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**AC-22 Publicly Accessible Content**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [Assignment: organization-defined frequency] and removes such information, if discovered.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AT-2 **Security Awareness Training**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):**

1. As part of initial training for new users;
2. When required by information system changes; and
3. Bi-annually thereafter.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**AT-3 Role Based Security Training**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization provides role-based training to personnel with assigned security roles and responsibilities:**

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. Bi-annually thereafter.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AT-4 **Security Training Records**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for 12 months.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AU-6 **Audit Review, Analysis, and Reporting**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Reviews and analyzes information system audit records as needed for indications of inappropriate or unusual activity; and
2. Reports findings to appropriate individuals.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AU-8 **Time Stamps**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets a five minute synchronization variance.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

AU-9 **Protection of Audit Information**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system protects audit information and audit tools from unauthorized access, modification, and deletion.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CA-2 **Security Assessments**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Develops a security assessment plan that describes the scope of the assessment including:
	1. Security controls and control enhancements under assessment;
	2. Assessment procedures to be used to determine security control effectiveness; and
	3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation bi-annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to OIT leadership.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**CA-3 System Interconnections**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements annually.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CA-7 **Continuous Monitoring**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:**

1. Establishment of continuous metrics reports to be monitored;
2. Establishment of summary reports for monitoring and quarterly validations for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to management quarterly.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CM-2 **Baseline Configuration**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CM-6 **Configuration Settings**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes and documents configuration settings for information technology products employed within the information system using documented standard that reflect the most restrictive mode consistent with operational requirements;
2. Implements the configuration settings;
3. Identifies, documents, and approves any deviations from established configuration settings for system hosts/servers/applications based on documented standards; and
4. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**CM-7 Least Functionality**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: (These functions will differ between systems. System-level thought and due-diligence should be given in order to address this control.)

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**CM-8 Information System Component Inventory**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Develops and documents an inventory of information system components that:
	1. Accurately reflects the current information system;
	2. Includes all components within the authorization boundary of the information system;
	3. Is at the level of granularity deemed necessary for tracking and reporting; and
	4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
2. Reviews and updates the information system component inventory [Assignment: organization-defined frequency].

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CM-10 **Software Usage Restrictions**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**CP-2 Contingency Planning**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Develops a contingency plan for the information system that:
	1. Identifies essential missions and business functions and associated contingency requirements;
	2. Provides recovery objectives, restoration priorities, and metrics;
	3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
	4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
	5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
	6. Is reviewed and approved by department managers;
2. Distributes copies of the contingency plan to departmental directors.
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system annually;
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to the OIT offices; and
7. Protects the contingency plan from unauthorized disclosure and modification.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CP-9 **Information System Backup**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Conducts backups of user-level information contained in the information system weekly
2. Conducts backups of system-level information contained in the information weekly;
3. Conducts backups of information system documentation including security-related documentation weekly; and
4. Protects the confidentiality, integrity, and availability of backup information at storage locations.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

CP-10 **Information System Recovery and Reconstitution**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IA-2 Identification and Authentication**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IA-4 Identifier Management**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system manages information system identifiers by:**

1. Receiving authorization from management to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for one year; and
5. Disabling the identifier after one year of inactivity.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IA-5 Authenticator Management**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization manages information system authenticators by:**

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type];
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IA-6 Authenticator Feedback**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IA-8 Identification and Authentication (Non-Organizational Users)**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-2 Incident Response Training**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:

1. Within 90 days of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. annually thereafter.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-4 Incident Handling – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization:**

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

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

1. 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.
2. Each Campus must periodically review, test, and approve their security incident response plans and procedures and document the results.
3. Each Campus 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.
4. 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-5 Incident Monitoring – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The** organization **tracks and documents information system security incidents.**

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-6 Incident Reporting – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization:**

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

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-7 Incident Response Assistance – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

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

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**IR-8 Incident Response Plan – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system**:

1. 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;
2. Distributes copies of the incident response plan to Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements;
3. Reviews the incident response plan Annually;
4. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
5. Communicates incident response plan changes to both the CIO and the UTK stakeholders; and
6. Protects the incident response plan from unauthorized disclosure and modification.

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MA-4 Nonlocal Maintenance**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MA-5 Maintenance Personnel**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MP-2 Media Access**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization restricts access to copies of system data, backup data, hard drives, USB keys and assorted related media to appropriate personnel or roles.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MP-3 Media Marking**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts data and systems classified as LOW categorization from marking as long as the media remain within departmental control.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MP-4 Media Storage**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

Physically controls and securely stores **copies of system data, backup data, hard drives, USB keys and assorted related media** and protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MP-5 Media Access**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Protects and **copies of system data, backup data, hard drives, USB keys and assorted related media** during transport outside of controlled areas using documented methods;
2. Maintains accountability for information system media during transport outside of controlled areas;
3. Documents activities associated with the transport of information system media; and
4. Restricts the activities associated with the transport of information system media to authorized personnel.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**MP-6 Media Sanitization**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PE-12 Emergency Lighting – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  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:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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).

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PE-13 Fire Protection – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

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

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate response.

1. Fire detection and suppression systems (FM200 or Halon) are in place within the SMC and KPB data centers\*;
2. Fire protection systems utilize the same power grid as the computer hardware;
3. 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PL-2 System Security Plan**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Develops a security plan for the information system that:
	1. Is consistent with the organizations enterprise architecture;
	2. Explicitly defines the authorization boundary for the system;
	3. Describes the operational context of the information system in terms of missions and business processes;
	4. Provides the security categorization of the information system including supporting rationale;
	5. Describes the operational environment for the information system and relationships with or connections to other information systems;
	6. Provides an overview of the security requirements for the system;
	7. Identifies any relevant overlays, if applicable;
	8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
	9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to the OIT CIO;
3. Reviews the security plan for the information system bi-annually;
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PL-4 Rules of Behavior**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [Assignment: organization-defined frequency]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PS-4 Personnel Termination**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization, upon termination of individual employment:**

1. Disables information system access within one day;
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of system access and data transfer;
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies management within one day.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PS-5 Personnel Transfer**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates all actions within one day of notification of transfer.
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies management within one day of notification of transfer.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PS-6 Access Agreements**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements annually; and
3. Ensures that individuals requiring access to organizational information and information systems:
	1. Sign appropriate access agreements prior to being granted access; and
	2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PS-7 Third-Party Personnel Security**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify management of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within one day and
5. Monitors provider compliance.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**PS-8 Personnel Sanctions**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
2. Notifies management within one day when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**RA-2 Security Categorization – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization:**

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

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**RA-5 Vulnerability Scanning – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization:**

1. 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;
2. 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;
3. Analyzes vulnerability scan reports and results from security control assessments;
4. Remediates legitimate vulnerabilities quarterly in accordance with an organizational assessment of risk; and
5. 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:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SA-2 Allocation of Resources**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SA-4 Acquisition Process**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SA-5 Information System Documentation**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
	1. Secure configuration, installation, and operation of the system, component, or service;
	2. Effective use and maintenance of security functions/mechanisms; and
	3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
	1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
	2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
	3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and takes appropriate due diligence in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to department management.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SA-8 Security Engineering Principles**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-2 Application Partitioning**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system separates user functionality (including user interface services) from information system management functionality.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-5 Denial of Service (DoS) Protection – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  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 system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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:

1. 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.
2. Intrusion Prevention Systems:
	1. Detect and block a range of network-based attacks based on vendor-provided attack signatures.
3. 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.
4. 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-7 Boundary Protection – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

The organization:

1. Monitors and controls communications at the external boundary of the information system and at key internal boundaries within the information system;
2. Implements sub-networks for publicly accessible system components that are logically separated from internal organizational networks; and
3. 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 system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate response.

**The Campus:**

1. 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.
2. 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.
3. 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-12 Cryptographic Key Establishment and Management**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-13 Cryptographic Protection**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-15 Collaborative Computing Devices**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
2. Provides an explicit indication of use to users physically present at the devices.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-17 Public Key Infrastructure Certificates**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.**

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SC-20 Secure Name / Address Resolution Service (Authoritative Source)**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SI-2 Flaw Remediation**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within 30 days of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SI-3 Malicious Code Protection**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
	1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
	2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SI-4 Information System Monitoring – Inheritable Control**

[ ]  This control is inherited from the UTK Information Security Program Plan.

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

The organization:

1. 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;
2. Identifies unauthorized use of IT resources through various network service tools;
3. 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;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. 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;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, directives, policies, or regulations; and
7. Provides log data associated with critical systems to system owners of regulatory or standards related systems on an as-needed basis.

Response:

The system owner will need to determine if this control response IS/IS NOT inherited from the Knoxville Campus Information Security Program Plan. If the control response IS inherited, please validate the verbiage below. If the control response is not accurate for your system, please remove verbiage below and create an accurate 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.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

**SI-5 Security Alerts, Advisories, and Directives**

[ ]  This control is not implemented.

[ ]  This control is partially implemented.

[ ]  This control is fully implemented.

**The system:**

Receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;

Generates internal security alerts, advisories, and directives as deemed necessary;

Disseminates security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and

Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Response:

Please provide an answer for the control listed directly above.

Supporting Documentation:

Please list any supporting documentation such as policies, procedures, guidelines or references.

# Appendix A: System Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address** | **IP Name** | **Environment** | **Function** |
| 1 | 160.36.xxx.xxx | testing.utk.tennessees.edu | Production | Web Server |
| 2 | 160.36.xxx.xxx | Testing2.oit.utk.edu | Development | Database Server |
| 3 | 160.36.xxx.xxx | Testing3.utk.tennessee.edu | Production | Web Server |