Table of Contents

Overview

The objective of the System Security Plan (SSP) document is to have a simple, easy-to-reference document that covers pertinent information about the Controlled Unclassified Information (CUI) environment, in particular for the “GPC Reusable Observable Unified Study Environment (GROUSE)”. This is a “living document” that is meant to be updated as conditions change. The goal of this document is simple - anyone not familiar with such CUI environment as “GROUSE” should be able to read it and gain a fundamental understanding of the systems involved, the risks, and the security controls required to maintain an acceptable level of security.

Essentially, this document provides a centralized repository for knowledge that is specific to the CUI environment and its applicable security controls. The SSP reflects input from those responsible for the systems that make up the CUI environment, including principle investigator, research and technical lead, information owners, system operators, and other stakeholders. According to NIST, the purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system.

Key Stakeholders

Principal Investigator: Dr. Lemuel R. Waitman (DUA Custodian)

Research Lead: Dr. Xing Song (Point of Contact)

Technical Leads: Shaun Ferguson (Lead DevOps)

Security Leads: Ernest Anye

Any key stakeholder changes are required to reported to both MU IRB and CMS for approval before shift of responsibilities.

Roles and Responsibilities

We design three primary roles following the key separation factor of "*accessibility to raw CMS data*":

Role A (Data Provider): Project Staff designated in Role A generates finder file sending to GDIT and EMR datasets sending to MU, who will not be granted with access to CMS data.

Role B (Administrator): Project Staff designated in Role B will function as GROUSE database administrator with full access to raw CMS data and user accounts, upon completion of extensive trainings.

Role C (Analyst): Project Staff designated in Role C will be granted with access to part of CMS data or its limited and de-identified version in accordance with CMS DUA, upon completion of necessary trainings.

Scope and Target Audience

We have has adopted selective principles from 18 control families established in NIST SP 800-53 Rev. 4 guidelines, as the official policy for the GROUSE infrastructure.

CH	ID	FAMILY	SELECTIVE CONTROL NO.
1	AC	Access Control	1,**2**,3,4,5,6,7,8,10,11,12,14,17,18,19,20,21,22
2	AT	Awareness and Training	1,2,3
3	AU	Audit and Accountability	1,**2**,**3**,4,5,6,7,8,9,11,12

4	CA	Security Assessment and Authorization	1,2,**3**,5,6,7
5	CM	Configuration Management	1,**2**,**3**,4,5,6,7,8,9,10,11
6	CP	Contingency Planning	1,9
7	IA	Identification and Authentication	1,**2**,3,4,5,6
8	IR	Incident Response	1,2,4,5,7,8
9	MA	Maintenance	1,3,4,5,6
10	MP	Media Protection	1,2,3,4,5,6
11	PE	Physical and Environmental Protection	1,2,3,4
12	PL	Planning	1,2,4
13	PS	Personnel Security	1,2,3,4,6,7,8
14	RA	Risk Assessment	**1**,2,3,5
15	SA	System and Services Acquisition	1,5,8,9
16	SC	System and Communications Protection	1,2,4,5,8,10,12,13,15,17,18,19,20,21,22,23,28,39
17	SI	System and Information Integrity	**1**,**2**,3,4,5,7,8,10,11,12,16
18	PM	Program Management	2

This SSP applies to all systems, services and users that are part of the GROUSE project. All chapters need to be disseminated to Role-B as required training material. The Overview, Chapter 1 (AC), Chapter 2 (AT), and Chapter 13 (PS) are required to be disseminated to Role-C for onboarding and annual compliance training.

General Architecture Description

Figures 1 provides a non-technical view of the data enclave architecture. Data that flows from multiple sources (including GDIT physical media) will be load into secured S3 bucket via SFTP (or other data extraction mechanism). Staged data will be automated loaded into Snowflake VPC for data transformation (into PCORnet Common Data Model) and de-identification. Approved users (under GPC DSA) will be provisioned with restricted access to analytical applications (e.g. R, Python, SAS) to either limited or de-identified version of the CDM data.

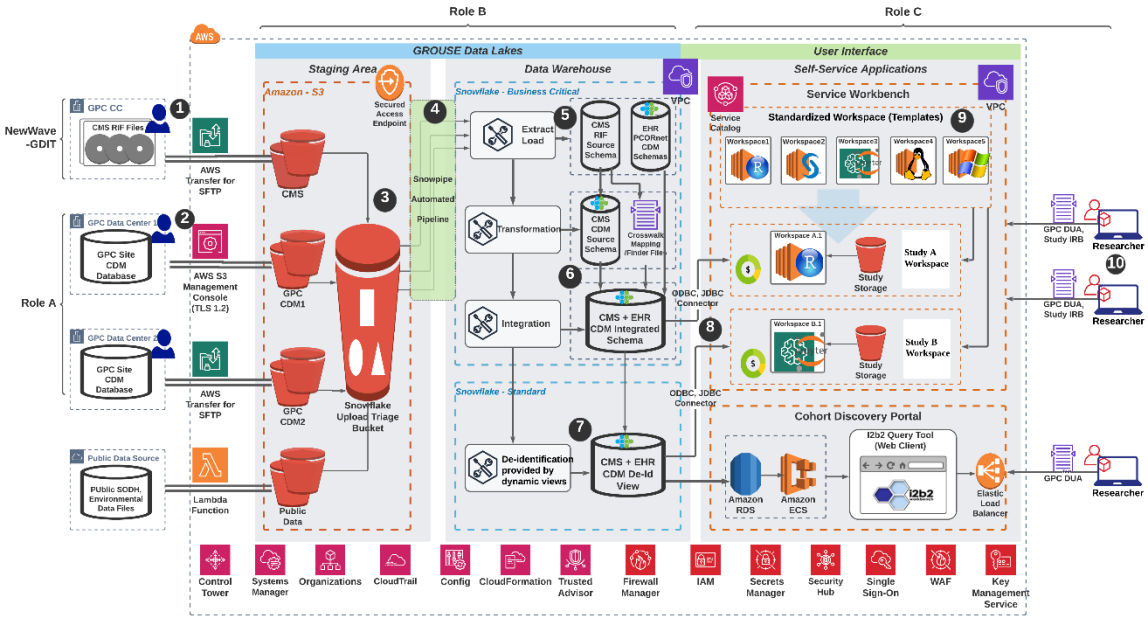

Figure 1 – GROUSE Architecture

Revision History

Version	Owner	Author	Reviewed by	Review Date	Publish Date
1.0	MU-NextGenBMI	Xing Song	Security Leads	05/15/2021	

Family: Access Control

This document establishes the Access Control Policy and Procedure for managing risks within user account management, access enforcement and monitoring, separation of duties, and remote access.

AC-1	***Access Control Policy and Procedures***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop, document, and disseminate to all Project Staff:
    a. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
    b. Procedures to facilitate the implementation of the access control policy and associated access controls.
    c. Policies and procedures must be in line with existing ones enforced by parent institutions (e.g., the Data Classification System enforced at University of Missouri System)
2. Review and update the current:
    a. Access control policy on an annual basis or when required by system changes.
    b. Access control procedures on an annual basis or when required by system changes.
    c. Any modifications need to be properly documented using version control.

Procedures: CMS data access control policy will follow the Data Classification Level (DCL) system reinforced at University of Missouri (MU): a) Raw CMS data will be treated as DCL4 (“highly restricted“); b) limited CMS data with only real dates will be treated as DCL3 (“restricted”); c) the fully de-identified data following well-established ”safe harbor” methods will be treated as DCL2 (“sensitive”); d) Only aggregated data with cell counts above 10 that are approved to be used for publication or public dissemination will be treated as DCL 1 (“public”). Regulations, laws and standards that affect data in different DCL tiers include, but are not limited to, the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.), the Export Administration Regulations (15 CFR 730 et seq.), the Health Insurance Portability & Accountability Act (HIPAA) and Payment Card Industry (PCI) standards. These regulations, laws and standards thoroughly address the purpose, scope, responsibility, management commitment, coordination among organizational entities, and DUA compliance associated with different DCL level. In addition, we have developed a full suite of policy and procedures following best practices and NIST-800-53r4 controls from the AC family, which requires an annual review and update (as well as spontaneous review when critical changes is needed).

AC-2	***Account Management***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Work closely with key stakeholders to oversight account provisioning and ongoing monitoring.

2. Ensure access to the system is limited to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
3. Ensure access to the system is limited to the types of transactions and functions that authorized users are permitted to execute.
3. Identify distinct account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
4. Enable a centralized and automated account management with at least one "account manager" appointed and properly trained.
5. Establish conditions and policies for group and role membership.
6. Identify authorized users of the information asset and specifying access privileges for each account.
7. Require appropriate approvals for requests to establish accounts.
8. Grant access to the system based on (1) valid access authorization, (2) intended system usage, and (3) other attributes as required by the organization or associated missions/business functions.
9. Establish, activate, modify, disable, and remove accounts in accordance with defined procedures.
10. Monitors the use of information system accounts (e.g. user accounts).
11. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
12. Not allow the use of guest/anonymous and temporary accounts.
13. Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
14. Deactivate/disable emergency, temporary and expired accounts that are no longer required and accounts of terminated or transferred users.
15. Tracks all types of account changes (e.g. creation, enabling, modifying, disabling, deletion) within audit records without interruptions.
16. Review accounts manually on a periodic basis or at least **annually**.

AC-3	***Access Enforcement***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsibility parties must:

1. Enforce approved authorizations for logical access to the systems and services that are part of the GROUSE project in accordance with DMP-SAQ and associated documents.
2. Ensure the access control model is implemented and public read and write accesses are disabled to all system-related files, objects and directories.

AC-4	***Information Flow Enforcement***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsibility parties must enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with established GROUSE Infrastructure Diagram (Figure 1)	

AC-5	***Separation of Duties***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsibility parties must: 1. Separate duties of individuals as necessary, to prevent malevolent activity without collusion. 2. Implement separation of duties through assigned information asset access authorizations.	

AC-6	***Least Privilege***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsibility parties must: 1. Employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. 2. Ensure that users have the fewest permissions required to perform their job functions. 3. Disable all non-essential functions. 4. Disable the use of removable media boot devices (e.g. thumb drives). 5. Ensure security functions are explicitly authorized. 6. Ensure that users utilize their own account to access system, then escalate privileges to perform administrative functions. 7. Audit all usage of privileged account activities.	

AC-7	***Unsuccessful Login Attempts***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsibility parties must: 1. Enforce a limit of **5 consecutive invalid logon attempts** by a user; and	

2. Automatically lock the account for **at least 30 minutes** when the maximum number of unsuccessful attempts is exceeded; and
3. Automatically alert Role-B administrators so that they can take remediations

AC-8	***System Use Notification***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsibility parties must:

1. Display an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with regulations, standards, and policies.
2. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information asset.

AC-11	***Session Lock***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsibility parties must:

1. Prevent further access to the information asset by initiating a session lock after **15 minutes of inactivity or upon receiving a request from a user**.
2. Retain the session lock until the user reestablishes access using established identification and authentication procedures.
3. Ensure that user sessions are automatically disconnected after **30 minutes of inactivity** or **any potentially malicious activity**.

AC-12	***Session Termination***

Responsible Role: Role-B

Policy: The responsibility parties must:

1. Automatically terminate a user session **after 30 minutes of inactivity**. Some application accounts as pre-defined (e.g., i2b2) can have idle sessions when users are not running queries and scheduled tasks such as ETL scripts running under system level accounts are not considered user sessions.

AC-14	***Permitted Actions without Identification or Authentication***
Responsible Role: Key Stakeholders	
Policy: There are no user actions that can be performed on organizational information systems without identification and authentication and thus, the values for assignment statements can be none.	

AC-17	***Remote Access***
Responsible Role: Key Stakeholders	
Policy: The responsibility parties must ensure that remote connections: 1. Have usage restrictions. 2. Have connection requirements such as cryptography and connected to managed network access control points. 3. Have guidelines for user access. 4. Are monitored through audit records. 5. Explicitly authorizes the usage of privileged commands through the remote connection.	

AC-18	***Wireless Access***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsibility parties must ensure that remote connections: 1. Establish usage restrictions and implementation guidance wireless access. 2. Monitor for unauthorized wireless access to the information asset. 3. Authorize wireless access to the information asset prior to connection. 4. Enforce requirements for wireless connections for the information asset. 5. Ensure the system has usage restrictions and encryption for wireless access. Wireless access only includes direct internal wireless connections. 6. Ensure the system has usage restrictions and encryption of data at rest and data in transit for mobile devices which have direct access to the system.	

AC-19	*Access Control for Mobile Devices*
Responsible Role: Key Stakeholders, Role-B	
Policy: Given that certain GROUSE services are web-based, access from mobile devices organization-controlled or otherwise is possible. However, any mobile access to the GROUSE systems is subject to all the controls that are applicable to non-mobile devices. No mobile device specific controls have been developed for access to GROUSE systems.	

AC-20	*Use of External Information Systems*
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information assets, allowing authorized individuals to: a. Access the information asset from the external information systems. b. Process, store, and/or transmit organization-controlled information using the external information systems. 2. Restrict the usage of portable storage devices (e.g., thumb drives, external hard drives) which leave the authorization boundary.	

AC-21	*Information Sharing*
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must only facilitate certain information sharing among pre-defined Project Staff members approved by CMS and central IRB, following a well-established procedure from evaluating and assigning Data Classification Level (DCL) to applying associated policies on data sharing.	

Family: Awareness and Training

This policy establishes the Security Awareness and Training Policy, for managing risks from a lack of security awareness, communication, and training through the establishment of an effective security awareness and education program.

AT-1	***Security Awareness and Training Policy and Procedures***

Responsible Role: Key Stakeholders

Policy: The responsible parties must:

1. Develop, document and disseminate to Project Staff in Role-B and Role-C:
    a. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
2. Review and update the current:
    a. Security awareness and training policy on an annual basis or when required by system changes.
    b. Security awareness and training procedures on an annual basis or when required by system changes.
    c. Any modifications need to be properly documented using version control.

AT-2	***Security Awareness***

Responsible Role: Key Stakeholders

Policy: The responsible parties must:

1. Ensure that the system has a policy for completing security training.
2. Ensure that the system has a security training program/procedure which includes all types of project staff.
3. Ensure that training material is developed strictly following CMS guidelines for training content.
4. Ensure the training includes these policies and procedures from AT family.
5. Ensure the training includes the insider threat information.
6. Training shall be completed before gaining access to the system and every 365 days (annual).

AT-3	***Security Training***

Responsible Role: Key Stakeholders

Policy: The responsible parties must:

1. Ensure the system conducts role-based training (e.g., security, incident response) within 60 days of assuming the role and every 365 days.
2. Ensure the system maintains security and privacy awareness training and role-based system training records for 5 years after employees and contractors complete each training.

Family: Auditing and Accountability

This document establishes the Auditing and Accountability Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

AU-1	***Audit and Accountability Procedures***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop, document, and disseminate to Project Staff in Role-B and Role-C:
    d. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
    e. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
2. Review and update the current:
    a. Audit and Accountability policy on **an annual basis**.
    b. Audit and Accountability procedures **on an annual basis**.
    c. Any modifications need to be properly documented using version control.

AU-2	***Auditable Events***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Determine that the information system is capable of auditing the following events:
    a. Server alerts and error messages;
    b. User log-on and log-off (successful or unsuccessful);
    c. All system administration activities;
    d. Modification of privileges and access;
    e. Start up and shut down;
    f. Application modifications;
    g. Application alerts and error messages;
    h. Configuration changes;
    i. Account creation, modification, or deletion;
    j. File creation and deletion;
    k. Read access to sensitive information;
    l. Modification to sensitive information;

m. Printing sensitive information;

n. Anomalous (e.g., non-attributable) activity;

o. Data as required for monitoring privacy controls;

p. Concurrent log on from different work stations;

q. Override of access control mechanisms;

r. Process creation;

s. Attempts to create, read, write, modify, or delete files containing PHI.

2. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.
3. Provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
4. Audit the following events within the information system **on a monthly basis**:

   a. successful or failed use of administrative privileges

AU-3	***Content of Audit Records***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure that the audit records from the information system contain the following metadata to support the detection, monitoring, investigation, response, and remediation of security and privacy incidents:

   a. Date and time of the event;

   b. Component of the information system (e.g., software component, hardware component) where the event occurred;

   c. Type of event;

   d. User/subject identity;

   e. Outcome (success or failure) of the event;

   f. Program or command that initiated the event;

   g. Execution of privileged functions;

   h. Command line (for process creation events);

   i. Record disclosures of sensitive information, including protected health and financial information.

   j. Log information type, date, time, receiving party, and releasing party;

   k. Verify within every ninety (90) days for each extract that the data is erased or its use is still required. - Filename accessed;

   l. Source and destination IP address or hostname if applicable;

m. Amount of data transmitted during network session;

n. For systems that handle PHI, disclosures of PHI in accordance with HIPAA.

AU-4	***Audit Storage Capacity***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded

AU-5	***Response to Audit Processing Failures***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Alert all Project Staff of Role-B and/or other designated organizational officials in the event of an audit processing failure.
2. Ensure to shut down the relevant GROUSE services until the failure or capacity issue is resolved, in the event of an audit processing failure or instances where audit storage capacity is exceeded without disabling auditing

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

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must ensure that:

1. Audit records are reviewed weekly and manually reviewed at least monthly.
2. Administrator groups logs are inspected at least every 14 days to ensure unauthorized administrator, system, and privileged application accounts have not been created.
3. System logs, network utilization/traffic, security software, and alerts are reviewed automatically on daily basis.
4. Adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations due to credible intelligence.
5. Use automated audit record analysis to review audit records, and correlate automated audit record analysis across the organization.

AU-7	***Audit Reduction and Report Generation***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must provide audit reduction and report generation capability that: 1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and 2. Does not alter the original content or time ordering of audit records. 3. Ensure that all audit records shall be searchable.	

AU-8	***Time Stamps***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Use internal system clocks to generate time stamps for audit records to facilitate logging and monitoring; and 2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets one second granularity of time measurement	

AU-9	***Protection of Audit Information***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Protect audit information and audit tools from unauthorized access, modification, and deletion. 2. Ensure that access to these audit records is limited to the designated Role-B users.	

AU-11	***Audit Record Retention***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Retain audit records for at least 90 days in “hot” storage and archive storage for at least 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	

AU-12	*Audit Generation*
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Provide audit record generation capability for the list of auditable events defined in "Auditable Events (AU-02)". 2. Allow designated organizational personnel to select which auditable events are to be audited by specific components of the system. 3. Generate audit records for the list of audited events defined in AU-2 with the content as defined in AU-03.	

Family: Security Assessment and Authorization

This policy establishes the Security Assessment and Authorization Policy, for managing risks from inadequate security assessment, authorization, and continuous monitoring of company information assets through the establishment of an effective Security Assessment and Authorization program.

CA-1	***Security Assessment and Authorization Policies and Procedures***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop, document, and disseminate to Project Staff in Role-B:
    a. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
    b. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls.
2. Review and update the current:
    a. Security assessment and authorization policy on an annual basis or when required by system changes.
    b. Security assessment and authorization procedures on an annual basis or when required by system changes.
    c. Any modifications need to be properly documented using version control.

CA-3	***System Interconnections***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Authorize connections from the information system to other information systems through the use of some form of agreement (e.g., Interconnection Security Agreements (ISA)).
2. Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated.
3. Ensure the system uses a deny-all, permit-by-exception policy for any system access to ensure that only those connections which are essential and approved are allowed.
4. Review and update any agreements regarding interconnection security on an annual basis or after a significant change.

CA-5	***Security Authorization***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
2. Update existing plan of action and milestones quarterly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-7	***Continuous Monitoring***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

1. Establishment of metrics to be monitored.
2. Establishment of alert or event-types for monitoring and event thresholds for alerting to support continuous 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.
7. Reporting the security status of organization and the information system to leadership annually.

CA-9	***Internal System Connection***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties will:

1. Authorize internal connections of approved MU information system components (e.g. central logging, security scanning) to the GROUSE system.
2. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.
3. Perform compliance checks on constituent system components prior to the establishment of the internal connection

Family: Configuration Management

This document establishes the Configuration Management Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

CM-1	***Configuration Management Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Configuration Management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Configuration Management policy and associated access controls. 2. Review and update the current: a. Configuration Management policy on an annual basis or when required by system changes. b. Configuration Management procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

CM-2	***Baseline Configuration***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure that: 1. The system has a current baseline configuration image for hosts within the system. 2. The baseline configuration is reviewed and updated **at least annually** or when a critical security patch is necessary. 3. During system upgrades which constitute a significant change, the baseline configuration shall be updated.	

CM-3	***Configuration Change Control***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Define which changes to the system are controlled (i.e., requires approval). 2. Revise proposed changes with explicit attention to impact on security. 3. Document and retains change control decisions for **at least 3 years**.	

4. Audit change control decisions **at least annually**.
5. Test and validate change controls prior to implementation on the production system.

CM-4	***Security Impact Analysis***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Analyze changes to the information systems comprising the GROUSE infrastructure to determine potential security impacts prior to change implementation.	

CM-5	***Access Restrictions for Change***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Define, document, approve, and enforce physical and logical access restrictions for changes to information systems comprising the GROUSE infrastructure.	

CM-6	***Configuration Settings***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Document default configuration settings which follow the most restrictive mode possible for reliable operation. 2. Follow United States Government Configuration Baselines (USGCB) or similar configuration standards (e.g., the Center for Internet Security guidelines (Level 1); National Security Agency (NSA) Configuration Guides) to establish configuration settings or establishes its own configuration settings. 3. Identify, document, and approve any deviations from established configuration settings. 4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.	

CM-7	***Least Functionality***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Configure information systems comprising the GROUSE infrastructure to provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services.
2. Verify through configuration scanning or automated mechanisms **at least monthly** to provide enforcement.

CM-8	***Information System Component Inventory***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must develop, document, and maintain an inventory of the information asset components that exist within information systems comprising the GROUSE infrastructure. Inventory detail must be maintained at a sufficient level for purposes of tracking and reporting. Based on information system specifications, metadata shall include:

1. Each component's unique identifier and/or serial number
2. Information system of which the component is a part
3. Type of information system component (e.g., server, desktop, application)
4. Manufacturer/model information
5. Operating system type and version/service pack level
6. Presence of virtual machines
7. Application software version/license information
8. Physical location (e.g., building/room number)
9. Logical location (e.g., IP address, position with the information system [IS] architecture)
10. Media access control (MAC) address
11. Ownership
12. Operational status
13. Primary and secondary administrators
14. Primary use

CM-11	***Software Usage Restrictions***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system prevents users from installing software through user policies. 2. Monitor the installation of software on the system.	

Family: Contingency Planning

This document establishes the Contingency Planning Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

CP-1	***Contingency Planning Policy and Procedures***
Responsible Role: Key Stakeholders and Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Contingency Planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Contingency Planning policy and associated access controls. 2. Review and update the current: a. Contingency Planning policy on **an annual basis or when required by system changes**. b. Contingency Planning procedures on **an annual basis or when required by system changes**. c. Any modifications need to be properly documented using version control.	

CP-9	***Information System Backup***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system performs full weekly and incremental daily backups of: a. User level data b. System data c. System documentation 2. Backup archives shall include 3 full backups and be stored offsite.	

Family: Identification and Authentication

This document establishes the Identification and Authentication Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

IA-1	***Identification and Authentication Policy and Procedures***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop, document, and disseminate to Project Staff in Role-B:
    a. An Identification and Authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
    b. Procedures to facilitate the implementation of the Identification and Authentication policy and associated access controls.
2. Review and update the current:
    a. Identification and Authentication policy on an annual basis or when required by system changes.
    b. Identification and Authentication procedures on an annual basis or when required by system changes.
    c. Any modifications need to be properly documented using version control.

IA-2	***Identification and Authentication (Organizational User)***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Require that organizational users uniquely identify and authenticate into company information assets.
2. Ensure that the information system implements multifactor authentication (MFA) for network access to privileged accounts.
3. Ensure that the information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

IA-3	***Device Identification and Authentication***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. uniquely identify the IP Addresses of the devices that can establish a connection to GROUSE systems

IA-4	***Identifier Management***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Receive authorization from a designated organizational official to assign a user or device identifier.
2. Select an identifier that uniquely identifies an individual or device.
3. Assign the user identifier to the intended party or the device identifier to the intended device.
4. Prevent reuse of user or device identifiers for 3 years to which it is assigned to an active user or device.
5. Disable inactive identifiers after 60 days of inactivity.

IA-5	***Authenticator Management***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must ensure the systems:

1. Verify that the correct identifier is being issued to a person or device during authenticator distribution.
2. Have a standard for authenticator schema (e.g., first initial, last name, number if duplicate).
3. Meet or exceed enforcement of the following minimum password requirements:
4. Password length must be at least 15 characters.
5. Password must be rotated at most every 60 days.
6. Only encrypted representations of passwords can be stored and transmitted.
7. Allow the use of a temporary password for system logons with an immediate change to a permanent password.
8. Enforce a minimum of number of changed characters when new passwords are created (i.e., "Password history size") at twelve (12) at minimum.
9. Prohibit the use of dictionary names or words.

IA-6	***Authenticator Feedback***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Family: Incident Response

This document establishes the Incident Response Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

IR-1	***Incident Response Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. An Incident Response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Incident Response policy and associated access controls. 2. Review and update the current: a. Incident Response policy on an annual basis or when required by system changes. b. Incident Response procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

IR-2	***Incident Response Training***
Responsible Role: Key Stakeholders	
Policy: The responsible parties must provide Project Staff in Role-B incident response training: 1. within a month of assuming an incident response role 2. at least annually on practices associated with incident response 3. when required by information system changes.	

IR-4	***Incident Handling***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system can investigate security incidents, to include preparation, detection, analysis, containment, eradication, and recovery. Ensure the system tracks security incidents (e.g., physical, technical, and privacy).	

2. Ensure that the system requires personnel to report potential incidents and investigate the potential incident.
3. Develop, adhere to or adopt within their incident response plans, incident handling capabilities for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The incident handling activities will be coordinated with contingency planning activities and lessons learnt from ongoing incident handling activities will be incorporated into incident response procedures, training and testing.

IR-5	***Incident Monitoring***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must track and document information system security incidents on an ongoing basis.	

IR-7	***Incident Response Assistance***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	

IR-8	***Incident Response Assistance***
Responsible Role: Key Stakeholders, Role-B	

Policy: The responsible parties must ensure the system has 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
8. Is reviewed and approved by the applicable Incident Response Team Leader

9. Distributes copies of the incident response plan to:
    a. CMS Chief Information Security Officer
    b. CMS Chief Information Officer
    c. Information System Security Officer
    d. CMS Office of the Inspector General/Computer Crimes Unit
    e. All personnel within the organization Incident Response Team
    f. All personnel within the PII Breach Response Team
    g. All personnel within the organization Operations Centers
10. Reviews the incident response plan on an annual basis
11. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing
12. Communicates incident response plan changes to the organizational elements listed above
13. Protects the incident response plan from unauthorized disclosure and modification

Family: System Maintenance

This document establishes the System Maintenance Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

MA-1	***System Maintenance Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A System Maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the System Maintenance policy and associated access controls. 2. Review and update the current: a. System Maintenance policy on an annual basis or when required by system changes. b. System Maintenance procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

MA-3	***Maintenance Tools***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure that the system: 1. Utilizes diagnostic hardware, software, or firmware maintenance tools that have not been improperly modified. 2. Checks media containing diagnostic and test programs being introduced into the system for malicious code.	

MA-4	***Non-Local Maintenance***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Authorize, monitor, and control non-local maintenance and diagnostic activities. 2. Allow the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information asset. 3. Employ strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions.	

4. Maintain records for non-local maintenance and diagnostic activities.
5. Terminate all sessions and network connections when non-local maintenance is completed.

MA-5	***Maintenance Personnel***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel.
2. Ensure that personnel performing maintenance on the information asset have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information asset maintenance when maintenance personnel do not possess the required access authorizations.

MA-6	***Timely Maintenance***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Obtain maintenance support and/or spare parts for information systems/assets within defined service level agreements

Family: Media Protection

This document establishes the Media Protection Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

MP-1	***Media Protection Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Media Protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Media Protection policy and associated access controls. 2. Review and update the current: a. Media Protection policy on an annual basis or when required by system changes. b. Media Protection procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

MP-3	***Media Marking***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Mark information system media indicating the distribution limitations, handling caveats, and applicable security markings of the information and exempts media not containing any line item RESDAC data or counts with cell size less than 10.	

MP-4	***Media Storage***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Physically control and securely store any media either in secure data center environment or in an institution managed safe. The information system media are also protected until the media are destroyed or sanitized using approved equipment, techniques and procedures.	

MP-5	***Media Transport***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must ensure the system protects media while being transported. This includes:

1. If hand carried, using a securable container (e.g., locked briefcase) via authorized personnel
2. If shipped, trackable with receipt by commercial carrier
3. Maintaining accountability for information system media during transport outside of controlled areas.
4. Documenting activities associated with the transport of information system media; and
5. Restricting the activities associated with the transport of information system media to authorized personnel.

MP-6	***Media Sanitization***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure the system securely stores digital media and is overwritten once with a "00000000x" pattern or degaussed with a NIST approved magnet.
2. Sanitize all digital media prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies as well as policy and procedures set forth in hereafter.
3. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

MP-7	***Media Use***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure the system sanitizes media prior to disposal or reuse and tracks such activities.
2. Ensure the system prohibits the use of personally owned media.
3. Ensure any portable media devices have an identified owner.

MP-CMS-01	***Media Disposal***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: Not maintain records of disposed media which contain sensitive information.	

Family: Physical and Environmental Protection

This document establishes the Physical and Environmental Protection Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

PE-1	***Physical and Environmental Protection Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Physical and Environmental Protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Physical and Environmental Protection policy and associated access controls. 2. Review and update the current: a. Physical and Environmental Protection policy on an annual basis or when required by system changes. b. Physical and Environmental Protection procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

PE-2	***Physical Access Authorizations***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides. 2. Issue authorization credentials for facility access 3. Review the access list detailing authorized facility access by individuals on an annual basis. 4. Remove individuals from the facility access list when access is no longer required.	

PE-3	***Physical Access Control***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure the system:	

1. Verifies individual access authorizations before granting access to the facility.
2. Controls ingress/egress to the facility using guards and/or defined physical access control systems/devices (defined in the applicable security plan)
3. Maintains physical access audit logs for defined entry/exit points (defined in the applicable security plan)
4. Provides defined security safeguards (defined in the applicable security plan) to control access to areas within the facility officially designated as publicly accessible.
5. Escorts visitors and monitors visitor activity in defined circumstances requiring visitor escorts and monitoring (defined in the applicable security plan).
6. Secures keys, combinations, and other physical access devices.
7. Inventories defined physical access devices (defined in the applicable security plan) no less often than every 90 days.
8. Changes combinations and keys for defined high-risk entry/exit points (defined in the applicable security plan) within every 365 days, and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

PE-4	***Physical Access Control***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure that: 1. Telephone and network hardware and transmission lines are protected. 2. Unused physical ports (e.g., wiring closets, patch panels, etc.) are physically or logically disabled, locked, or barred	

Family: Security Planning

This document establishes the Security Planning Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

PL-1	***Security Planning Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Security Planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Security Planning policy and associated access controls. 2. Review and update the current: a. Security Planning policy on an annual basis or when required by system changes. b. Security Planning procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

PL-2	***System Security Plan***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties will: 1. Develop a security plan for the information system that: a. Is consistent with the organization's enterprise architecture. b. Explicitly defines the authorization boundary for the system. c. Describes the operational context of the information system in terms of missions and business processes. d. Provides the security categorization of the information system including supporting rationale. e. Describes the operational environment for the information system and relationships with or connections to other information systems. f. Provides an overview of the security requirements for the system. g. Identifies any relevant overlays, if applicable. h. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions. i. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.	

2. Distribute copies of the security plan and communicates subsequent changes to the plan to Director, KUMC-MI.
3. Review the security plan for the information system annually.
4. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.
5. Protects the security plan from unauthorized.

PL-4	***Rules of Behavior***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties will:

1. Establish and make 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. Receive 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. Review and update the rules of behavior on an annual basis.
4. Require 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

Family: Risk Assessment

This document establishes the Risk Assessment Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

RA-1	***Risk Assessment Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Risk Assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Risk Assessment policy and associated access controls. 2. Review and update the current: a. Risk Assessment policy on an annual basis or when required by system changes. b. Risk Assessment procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

RA-2	***Security Categorization***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Categorize information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance 2. Categorize information and the information system in accordance with Data Classification System and accompanied regulations enforced at University of Missouri. 3. Documents the security categorization results (including supporting rationale) in the security plan for the information system.	

RA-5	***Vulnerability Scanning***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system utilizes an automated vulnerability scanner which complies with organizational policies.	

2. Ensure that scans for vulnerabilities in the information system and hosted applications should be ran once at least **every 72 hours** or when a new threat has been discovered.
3. Ensure that scans for vulnerabilities in the information system and hosted applications must be authenticated to the target system as a privileged user with a dedicated account.
4. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
    a. Enumerating platforms, software flaws, and improper configurations
    b. Formatting checklists and test procedures
    c. Measuring vulnerability impact
5. Remediate “CRITICAL” and “HIGH” vulnerabilities immediately, and “MODERATE” and “LOW” vulnerabilities on a quarterly basis, in accordance with assessment results. Remediations will be handled manually based on built-in recommendations from AWS after consulting with Security Team, which will be converted to automated workflow when feasible.

Family: System and Services Acquisition

This document establishes the System and Services Acquisition Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

SA-1	***System and Services Acquisition Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A System and Services Acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the System and Services Acquisition policy and associated access controls. 2. Review and update the current: a. System and Services Acquisition policy on an annual basis or when required by system changes. b. System and Services Acquisition procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

SA-5	***Information System Documentation***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure the system is well documented by Role-B Administrators, to include: 1. Configuration of the individual hosts within the system 2. How to perform maintenance of security functions 3. Known vulnerabilities (can be tracked through a Plan of Action and Milestones, or POA&M) 4. Other documentation as needed for use and operation of the system.	

SA-8	***Security Engineering Principles***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Apply information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	

SA-9	*External Information System Services*

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure that any external services (third-party tools for ticketing, messaging, auditing, monitoring, etc.) outside of the accreditation/authorization boundary comply with organizational information security requirements.
2. Require that providers of external information system services comply with organizational information security requirements and employ Policies and Procedures specified in this SSP in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
3. Define and document government oversight and user roles and responsibilities with regard to external information system services.
4. Monitor the security control compliance by external service providers on an ongoing basis according to multiple policies specified in this SSP (e.g., AC-5, PS-7).

Procedures: Current AWS Guardrail Accelerator (GA) engagement is governed by a fully executed Enterprise Customer Agreement (ECA) and BAA between DLT (https://www.dlt.com/) and University of Missouri system. It is mutually agreed in writing that:

1. DLT will not have access to your data.
2. DLT only has access to the costs, so we can bill you for your usage every month.

In terms of the compliance requirement, it is specifically described in Section 3 of the DLT ECA:

Security. DLT will implement reasonable and appropriate measures for the Network designed to help Customer secure Customer Content and Customer Data against accidental or unlawful loss, access or disclosure (the "Security Objectives") in accordance with the Security Standards incorporated herein as Attachment "A". Notwithstanding anything in this Agreement to the contrary, DLT may modify the Security Standards from time to time, but will continue to provide at least the same level of security as is described in the Security Standards on the Effective Date. DLT represents that as of the Effective Date, DLT Contractor/Agent, AWS, is certified as compliant with ISO 27001. DLT shall promptly notify Customer if at any time DLT becomes aware that AWS is no longer certified as compliant with ISO 27001. Without limiting the foregoing, for the AWS Services identified as FISMA compliant, DLT in conjunction with third party independent auditors will conduct annual reviews of the security of the Network and adequacy of DLT's information security program as measured against the NIST SP 800-53 security controls. The AWS GovCloud (US) is the only AWS region that has physical and logical access controls that limit access to the Network by DLT (which, for the avoidance of doubt, includes AWS) personnel to U.S. Persons. Access to these machines is limited to U.S. Persons. DLT shall not permit foreign nationals, as defined by 22 CFR part 120.16, including employees, contractors, and visitors, in controlled areas unless properly escorted at all times.

Data Privacy. (a) DLT represents and warrants to Customer that: (i) as of the Effective Date AWS has self-certified that AWS complies with the Privacy Shield principles and meets the

requirements of the U.S.-EU Privacy Shield framework; (ii) that AWS will maintain (and that DLT will ensure that AWS maintains) such self-certification to the Privacy Shield framework throughout the Term of this Agreement; and (iii) all Customer Data and Customer Content transferred from the EU to the U.S. will be processed in accordance with those requirements.

(b) Customer may specify the regions in which Customer Content and Customer Data will be stored and accessible by End Users, but if Customer is receiving AWS GovCloud (US), all Customer Content and Customer Data in connection with the AWS GovCloud (US) will be stored in the United States because all AWS GovCloud (US) region servers are located in the United States (i.e., with respect to Customer Content and Customer Data in connection with the AWS GovCloud (US), Customer will not have the option to have such stored by DLT outside of the United States). Notwithstanding anything in this Agreement to the contrary, DLT will not move Customer Content or Customer Data from the selected regions to any other locations ("Unselected Locations") unless required to comply with Applicable Law or a binding order of an Authority. DLT will give Customer as much advance notice as is reasonably practicable of any such order or request of an Authority to allow Customer to seek a protective order or other appropriate remedy (except to the extent DLTs compliance with the foregoing would cause it to violate a binding order of a court, governmental body or regulatory body or Applicable Law). Subject to Sections 3.2(b) and (c), Customer consents to DLT's collection, use and disclosure of information associated with the Service Offerings in accordance with the Privacy Policy, and to the processing of Customer Content and Customer Data in, and transfer of Customer Content into, the regions Customer selects.

(c) Disclosure of Customer Content. DLT acknowledges that Customer is obligated to comply with FERPA and the Gramm–Leach–Bliley Act (the "Act"). Notwithstanding anything in this Agreement to the contrary, DLT shall not use or disclose Customer Content or Customer Data, including education records as defined by FERPA and data regulated by the Act, except as necessary (i) to provide the Service Offerings to Customer and any End Users in accordance with the Documentation (and any such disclosures by DLT in connection with this clause (i) shall only be to DLT Contactor/Agents who satisfy the definitions of "School Officials" with a "legitimate education interest" as those terms are defined in FERPA); or (ii) to comply with Applicable Law (including subpoenas) or a binding order of an Authority. DLT will give Customer reasonable notice of any such request of a governmental or regulatory body (including any subpoena) to allow Customer to seek a protective order or other appropriate remedy (except to the extent DLT's compliance with the foregoing would cause it to violate a binding order of an Authority or Applicable Law).

(d) FERPA Obligations. DLT agrees that DLT is a "School Official" (as that term is used in FERPA) with a "legitimate educational interest" in any Customer Data or Customer Content that is protected by FERPA and, therefore, DLT agrees that with respect to all Customer Data and Customer Content that is protected by FERPA that DLT accesses, receives, stores or controls, DLT will comply with all obligations that FERPA imposes on a "School Official". DLT will use Customer Data and Customer Content only for the purpose of fulfilling its duties under this Agreement. By way of illustration and not of limitation, DLT shall not use such data for its own benefit and, in particular, will not engage in "data mining" of Customer Data or Customer Content or the sale of Personal Data, including, without limitation, the sale of End User e-mail

addresses. Notwithstanding anything in this Agreement to the contrary, DLT will not decrypt Customer Data or Customer Content or access or read unencrypted Customer Data or Customer Content. Notwithstanding anything in this Agreement to the contrary, nothing in this Agreement, including Section 4.2, is intended to limit DLT's obligations under Sections 3.2 (b) and (c).

(e) Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Obligations. Within a commercially reasonable period of time after DLT's receipt of a written request from Customer, DLT shall execute a business associate agreement with Customer in the form attached hereto as Exhibit F (the "Business Associate Agreement"); provided however separate Customer Account(s) will be designated for HIPAA compliant workloads ("HIPAA Compliant Customer Accounts"). DLT's HIPAA obligation under this Agreement shall arise only in connection with HIPAA Compliant Customer Accounts, which, for the avoidance of doubt, are referred to as "HIPAA Accounts" in the form of Business Associate Agreement attached hereto as Exhibit F. If Customer does not at any time during the Term make the request referenced in the first sentence of this Section 3.2(d), DLT shall not be required to execute a Business Associate Agreement with Customer and there shall not be any HIPAA Compliant Customer Accounts. The form of Business Associate Agreement attached as Exhibit F is hereby incorporated into this Agreement by reference, and once the Business Associate Agreement is executed by the parties, the Business Associate Agreement shall automatically be incorporated into this Agreement by reference.

Family: Systems and Communications Protection

This document establishes the Systems and Communications Protection Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

SC-1	***Systems and Communications Protection Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Systems and Communications Protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Systems and Communications Protection policy and associated access controls. 2. Review and update the current: a. Systems and Communications Protection policy on an annual basis or when required by system changes. b. Systems and Communications Protection procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

SC-2	***Application Partitioning***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Separate user functionality, including user interface services, from information asset management functionality, between administrative/privileged users and regular/non-privileged users	

SC-7	***Boundary Protection***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure the system has boundary protection (e.g., firewall, IDS/IPS): 1. Must operate on a deny-all, permit-by-exception principle. 2. Must utilize stateful inspection mechanisms. 3. Must utilize 2 different vendors for boundary protection.	

4. If the system has a public component, web traffic coming into the system must have malware detection and monitoring of traffic which is stored in a secured centralized logging database administered by Role-B.
5. Logs from devices must be sent to a secured centralized logging database without interruption.

SC-8	***Transmission Confidentiality and Integrity***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Separate user functionality, including user interface services, from information asset management functionality, between administrative/privileged users and regular/non-privileged users	

SC-10	***Network Disconnect***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure that the system can terminate a network connection at the end of session or automatically disconnects after 30 minutes of inactivity.	

SC-12	***Network Disconnect***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system has a cryptographic key management system which complies with HHS standards	

SC-13	***Cryptographic Protection***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure the system uses FIPS 140-2 validated cryptographic modules for transmission of data. 2. Ensure the system uses FIPS 140-2 validated cryptographic modules for protecting data at rest	

SC-15	***Collaborative Computing Devices***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure that the system prohibits remote activation of devices and provides an indication of use to those users present at the device	

SC-28	***Collaborative Computing Devices***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Protect the confidentiality and integrity of information at rest	

Family: System and Information Integrity

This document establishes the System and Information Integrity Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

SI-1	***System and Information Integrity Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A System and Information Integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the System and Information Integrity policy and associated access controls. 2. Review and update the current: a. System and Information Integrity policy on an annual basis or when required by system changes. b. System and Information Integrity procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

SI-2	***Flaw Remediation***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure the system: 1. Identifies system flaws. 2. Tests updates prior to installation on production systems 3. Corrects security-related system flaws within 10 business days on production servers, 30 days on non-production servers. 4. Centrally manages flaw remediation. 5. Tracks and approves any security-related patches which are not installed.	

SI-3	***Malicious Code Protection***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must ensure the system: 1. Ensures the system uses malicious code protection which:	

2. Has up to date virus definitions
3. Scans important file systems every 12 hours and full system every 72 hours

SI-4	***Information System Monitoring***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure the system uses intrusion detection systems or intrusion protection systems (IDS/IPS) to monitor network communication. Both must be capable of decrypting network traffic.
2. Ensure inbound and outbound communication is monitored.
3. Monitor GROUSE systems to detect:
    a. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives
    b. Unauthorized local, network, and remote connections
    c. Unauthorized use of the information system through regular review of logs and activity.
4. Deploy monitoring devices:
    a. Strategically within the information system to collect organization-determined essential information;
    b. At ad hoc locations within the system to track specific types of transactions of interest to the organization
    c. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion
5. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provide organization-defined information system monitoring information to organization-defined personnel or roles as needed.

SI-7	***Software and Information Integrity***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Deploy tools and capabilities to monitor changes to critical resources such as operating system software components, system firmware, and vital applications

SI-8	***Spam Protection***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Employ spam protection mechanisms at information asset entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.
2. In addition, spam protection mechanisms (including signature definitions) must be updated when new releases are available in accordance with organizational configuration management policy and procedures.

SI-10	***Information Input Validation***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure the system validates user input before accepting it into the system (e.g., sanitize user input within username and password fields).

SI-11	***Error Handling***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
2. Reveal error messages only to organization-defined personnel or roles.

SI-12	*Information Input Validation*
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Ensure that the system retains information in accordance with federal law, CMS policy, and HIPAA requirements. 2. Handle and retain both information within and output from the information system in accordance with applicable federal laws, directives, policies, regulations, standards, and operational requirements	

Family: Personnel Security

This document establishes the Personnel Security Policy and Procedure for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access.

PS-1	***Personnel Security Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Develop, document, and disseminate to Project Staff in Role-B: a. A Personnel Security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. b. Procedures to facilitate the implementation of the Personnel Security policy and associated access controls. 2. Review and update the current: a. Personnel Security policy on an annual basis or when required by system changes. b. Personnel Security procedures on an annual basis or when required by system changes. c. Any modifications need to be properly documented using version control.	

PS-2	***Position Risk Designation***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties will: 1. Assign a risk designation to all Project Staff Roles. 2. Establish screening criteria for individuals filling those positions. 3. Review and update position risk designations biennially or when required by system changes. screens individuals prior to authorizing access to information system 4. Not re-screen individuals on a regular basis who are designated as low risk, based on PS-2 above.	

PS-3	***Personnel Security Policy and Procedures***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties will: 1. Screen individuals prior to authorizing access to information system 2. Not re-screen individuals on a regular basis who are designated as low risk, based on PS-2 above.	

PS-4	***Personnel Termination***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must ensure that employee termination follows the following steps:

1. Disables information system access before or during termination.
2. Terminates/revokes any authenticators/credentials associated with the individual.
3. Conducts exit interviews that include a discussion of non-disclosure of information security and privacy information.
4. Retrieves all security-related organizational information system-related property.
5. Retains access to organizational information and information systems formerly controlled by the terminated individual.
6. Notifies responsible parties within one (1) calendar day.

PS-6	***Access Agreements***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Develop and document access agreements for organizational information systems.
2. Review and update the access agreements when required by CMS or by GROUSE system changes.
3. Ensure that individuals requiring access to organizational information and information systems:
   a. Sign appropriate access agreements prior to being granted access
   b. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or annually.

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

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Ensure that 3rd party service providers (contractors, CSPs, vendor maintenance) follow the same personnel requirements as full-time employees.
2. Ensure that 3rd party service providers (contractors, CSPs, vendor maintenance) will only have restricted access to the GROUSE systems.
3. Ensure that all of the activities of any 3rd party personnel will be monitored closely with automated alerts sent to responsible parties when necessary.

4. In case of a contingency that involves physical access to CMS data, the third-party personnel will be accompanied by the responsible parties.

PS-8	***Personnel Sanctions***
Responsible Role: Key Stakeholders, Role-B	
Policy: The responsible parties must: 1. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures. 2. Notify CMS within a week when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction	

Family: Program Management

PM-2	***Senior Information Security Officer***

Responsible Role: Key Stakeholders, Role-B

Policy: The responsible parties must:

1. Identify senior information security officer (SISO) with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
2. Engage the senior information security officer (SISO) throughout the policy and procedures development phase as well as post-deployment phase to continuously monitor security control requirements

Procedures: The identified SISO will need to:

1. Be trained on HIPAA, Access Control policies and procedures (AC), Audit and Accountability policies and procedures (AU), as well as Incidence Response policies and procedures (IR);
2. Continuously monitor and review system vulnerabilities with proper tools;
3. Identify and classify system risks and work with Role-B to device remediation strategies;
4. Identify security monitoring gaps and work with Role-B to set up additional alerts to enhance timely reporting of system risks;
5. Participate quarterly or annually review with the responsible parties to:
    a. Conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
    b. Document risk assessment results and disseminates them to Key Stakeholders and Organizational Chief Information Security Officer.
    c. Update and/or modify system security policies and procedures to reflect any significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.