Secure Research Environment

Frequently Asked Questions (FAQs)

Version 1.4
June 2016

Prepared by

Information Technology Services

Saint Louis University

SAINT LOUIS UNIVERSITY

TABLE OF CONTENTS

1 Executive Summary

The Secure Research Environment is a computing environment that provides highly-secured computing-servers, database instances and data storage for the university's research community. The Secure Research Environment protects highly-sensitive research data created, used, or stored by the University's research departments.
The Secure Research Environment - Frequently Asked Questions, or *FAQs*, answers some high level questions about the environment and can be used by Saint Louis University users utilizing the Secure Research Environment as an initial training document for this computing environment.

1.1 Review and Update Schedule

This is a living document. The director of Information Security and Compliance has been designated as the representative of the Secure Research Environment Information System Owner and Common Control Provider, and is responsible for reviews and updates following any significant changes to the documented management, operational and technical security controls.

2 Document Revision History

Date	Description of Revision	Document Version	Author
4/5/2016	Initial Working Draft	1.0	K. Berra
4/21/2016	Updated for Team Review (includes input from 4/14 meeting, Peter Juan, and Scott Link)	1.2	A. Timberlake
5/3/2016	Updates to Section 4.8 Governance based on discussion from 5/3 Communications planning meeting	1.3	A. Timberlake
5/25/2016	Finalized for publishing	1.4	A. Szakonyi

3 Background

3.1 What is FISMA?

The Federal Information Security Management Act of 2002 (FISMA) is a law requiring protection of the sensitive data created, stored, or accessed by either the federal government or any entity on behalf of the federal government. The law established a formal Certification and Accreditation (C&A) process that requires a minimum set of security controls and a formal audit prior to obtaining an Authority to Operate (ATO).

3.2 Why is it important now?

In April 2010, the Office of Management and Budget (OMB) issued a memorandum requiring each federal agency to report their FISMA activities to Congress. This memo also reiterated the requirement that agencies include FISMA requirements in all contracts involving sensitive data, as well as grants where sensitive information is created, accessed, or stored on behalf of the federal government.

3.3 Does this apply to contracts and grants?

Compliance with FISMA is mandatory for federal contracts and may be mandatory for grants. The decision is based on two criteria:

(1) if the grant requires the research organization to return the data to the federal project sponsor, and

(2) if the grant has been awarded using a contracting form.

3.4 Why are there different security levels?

The FISMA Certification and Accreditation (C&A) process recognizes that not all sensitive information has the same level of risk and has identified three security categories to identify systems: ***Low***, ***Moderate***, and ***High***. Each level has a mandatory set of security controls, with each level building upon the previous. In addition, FISMA mandates separate evaluations for the ***confidentiality***, ***integrity***, and ***availability*** of the sensitive data. For example, research data containing individually identifiable health information would pose significant consequences to the university if that data was stolen, lost, or inadvertently disclosed, and thus the confidentiality security category would likely be Moderate. This same historical data may not require 24/7 access so the security category for availability may be Low.

It is often depicted in contracts as:

Overall System Security Category	☐ Low	☒ Moderate	☐ High
Overall Impact Levels (High Water Mark)	Confidentiality	Integrity	Availability
	Moderate	Low	Low

Every research project and project sponsor may end up with different security categories, but the basic set of security controls are grouped into Low, Moderate, and High.

3.5 Why is it important to Saint Louis University?

Saint Louis University has a number of research contracts from various sources at any one time, representing a sizeable financial funding source to the research community. As competition for future research funding increases, those universities with an existing FISMA compliance program can leverage that advantage into more contracts. Consequently, a failure to meet existing compliance requirements may result in contract termination and the loss of contract funds.

3.6 We already have a contract so do I have a FISMA requirement?

The 2010 OMB guidance clarifying the federal government's position took several months to disseminate to all federal agencies and contracting officers. Previously awarded contracts must also comply, so the university can expect that during the next contract or grant renewal cycle, every contract and certain grants will have FISMA language added. The university has been advised that if the language is NOT present, we should challenge the project sponsor for clarification. A failure to contractually accept the FISMA requirement will not extend deadlines, but only reduce the time we have to comply.

3.7 What type of language should I look for to determine if I have a FISMA requirement?

The various federal agencies have different ways of inserting FISMA requirements in contracts and grants. An obvious method is by including a requirement for FISMA compliance in the Statement of Work (SOW). This will usually be accompanied with a requirement to submit a System Security Plan (SSP) and a requirement to obtain an Authority to Operate (ATO) from the project sponsor. Other contracts may have articles titled "Information Security." There may be a reference to comply with OMB A-130, FIPS 199, or other similar language. Finally, language may be inserted anywhere in the contract stating the project "*…will comply with all applicable NIST Standards.*" Don't forget to look at not only the basic contract, but especially at contract modifications or renewals issued in 2010 or later.

3.8 Why must my program comply?

Compliance with applicable federal laws is mandatory. Our federal sponsors must report to Congress annually on their compliance efforts. If they cannot prove to Congress they are addressing the issue, Congress can withhold research funds. This would result in less research dollars for SLU and hurt our national reputation. Individual programs at SLU that do not comply might be threatened with a reduction of research funds if they don't make progress toward compliance. This issue is viewed as a serious challenge.

3.9 What are the consequences if we don't comply?

If we fail to comply with our sponsor's requirements, we should anticipate that our research contracts either will be terminated by default and/or new contracts cannot be awarded. If a project has a contractual obligation to protect data using the FISMA standards and a future audit or breach were to occur, serious repercussions can be anticipated leading to loss of future research grant.

4 Steps to Achieve FISMA Compliance

4.1 What are the steps to achieve FISMA compliance?

The FISMA compliance path on the surface appears to be complicated. In reality, it can be distilled into three distinct phases:

- **Phase I** – Validate the FISMA requirements, define the certification boundary, and determine the appropriate security categories for confidentiality, availability, and integrity[1].
- **Phase II** - Select and implement appropriate security controls from NIST SP 800-53[2] based on the security category, and then conduct an audit of the controls[3], documenting any deficiencies in a Plan of Action and Milestones (POA&M).
- **Phase III** – Remediate all issues identified in the POA&M and then prepare the certification package for the Designated Accreditation Authority (DAA) (typically your project sponsor) who will issue the Authority to Operate (ATO).

There is also an assumption that the security controls will be continually monitored and adjusted based on periodic risk assessments.

4.2 How long does the process take?

The length of the FISMA compliance process is highly variable, depending on several factors such as:

- The security category (Low, Moderate, High)
- The availability of resources with skills and spare time to manage the process
- The current level of security controls
- The total number of users in a project
- The complexity of the computing environment

Additionally, using shared university infrastructures, including Secure Research Environment, that have already been through the process and have an Authority to Operate (ATO), can shorten the process.

4.3 Who determines if we are compliant?

An independent audit is required for all levels of FISMA compliance. At Saint Louis University, that independence may be obtained by having a trained third party either at the University or outsourced, depending upon the complexity. The output of the audit is a Security Test and Evaluation (ST&E) along with the Plan of Action and Milestones (POA&M).

---

[1] As defined in the Federal Information Processing Standard 199 - Standards for Security Categorization of Federal Information and Information Systems and NIST Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories – Volumes 1 & 2

[2] As defined in the NIST Special Publication 800-53 (Revision 3) - Recommended Security Controls for Federal Information Systems and Organizations

[3] As defined in the NIST Special Publication 800-53A (Revision 1) - Guide for Assessing the Security Controls in Federal Information Systems

4.4 How can the university help with the process?

The university's Secure Research Environment team has created a secure computing environment to support the university's research projects. This environment, the Secure Research Environment was completed in January 2016. Secure Research Environment contains a well-defined certification boundary and shared computing resources that will support projects up to the **Moderate** security category.

4.5 What is the Secure Research Environment and can we leverage it for an individual project?

The Secure Research Environment consists of well-defined security perimeters surrounding a variety of computing resources. All access to the Secure Research Environment is tightly controlled through various security systems. All data moving between the Secure Research Environment and the researchers' computers must be encrypted. Data within the Secure Research Environment is stored on encrypted drives.

The Secure Research Environment also comes with the appropriate administrative controls, including those policies, procedures, and administrative support required as part of the FISMA certification process.

4.6 When using the Secure Research Environment, which steps must be performed by the individual research projects?

The Secure Research Environment team has completed the initial onboarding process templates. Researchers or project stakeholders requesting the Secure Research Environment resources may utilize these templates to start the onboarding process and discussions.

Common template tasks for the requesting researchers or projecting stakeholders include:

- Establish and document a well-defined certification boundary.
- Identify existing information technology resources (computing servers, databases, applications, etc.) that may need to be migrated into the Secure Research Environment.
- Complete preliminary information documents, including a completed Secure Research Environment questionnaire and System Security Plan (SSP).

4.7 Where do I get started?

The first step for any principal investigator to use the Secure Research Environment is to fill out the Secure Research Environment Tenant Onboarding Questionnaire Form located on our webpage. Someone from the Secure Research Environment team will contact you with next steps.

An initial assessment using the SLU NIST 800-53 Moderate Tenant Scoping Questionnaire will be performed to determine: (1) the operational requirements and (2) the level of security controls required and in place. At this point, your program will be issued a set of action items to accomplish that may include documentation requirements and additional security controls.

4.8 What is the Secure Research Environment governance structure?

The Secure Research Environment governance team is comprised of the following:

- **Associate VP & Deputy Chief Information Officer:** Mark Anderson
- **Chief Information Security Officer (CISO):** Chris Armstrong
- **Director, Research Technology:** Scott Amendola
- **Manager, IT Security Management & Compliance:** Kitty Berra
- **Director, Infrastructure Operations**: Peter Juan
- **Privacy Officer:** Ron Rawson
- **Director of Sponsored Programs:** Joe Sanning

The Secure Research Environment team is comprised of members from the ITS organization along with their specific technology domains:

- Research Technology Group
- IT Security and Compliance
- Infrastructure Operations
- Database Systems
- Identity and Access Management
- Problem and Incident Management
- Change and Configuration Management
- Service Management
- Contracts Management

The SLU FISMA Steering Committee team will meet regularly to review operational metrics for the current projects that are resident in the Secure Research Environment program along with any new requests for admission into Secure Research Environment.
The Secure Research Environment team meets regularly to review specific details and metrics. The SLU ITS Service Management processes such as Incident, Change, Vulnerability and Configuration Management are also dotted-line members of the Secure Research Environment team as those processes are considered foundational to the program.

4.9 What will it cost for my project to achieve FISMA compliance?

There are several different aspects to achieving FISMA compliance that involve cost. The cost to the project will depend on factors such as the information system categorization level (Low, Moderate, or High), the number of project end users, and current security status of the project, among others. The cost will need to be determined on a case-by-case basis.

4.10 What agreements must be in place?

In order to use Secure Research Environment, principal investigators (PIs) must comply with the Secure Research Environment governance structure, adopt and implement all required security controls, and mandate compliance by all authorized users under their authority.
Secure Research Environment has an approved System Security Plan outlining the minimum security controls. Individual projects must submit a System Level Controls Appendix (SLCA) detailing any unique security configurations that are not in place in Secure Research Environment. The SLCAs may add additional security controls, but may not reduce the level of security within Secure Research Environment.

5 Operational Aspects

5.1 What technology and services does the university provide with Secure Research Environment?

Projects with a FISMA compliance requirement must implement not only technical safeguards, but also administrative and physical safeguards. This includes implementing policies and procedures specifically designed to meet the stringent FISMA controls. In addition, in order to remain compliant with FISMA, continuous monitoring and auditing are required to ensure that the safeguards remain effective over time.
As of January 2016, the university is currently implementing the required set of FISMA policies and other safeguards required to remain compliant at a FISMA moderate level. The university also has contracts in place for standard security technologies.

5.2 How is the sensitive information protected?

Secure Research Environment consists of well-defined security perimeters surrounding a variety of computing resources. All access to Secure Research Environment is tightly controlled through various security systems. All data moving between Secure Research Environment and the researchers' computers must be encrypted. Data within Secure Research Environment is stored on encrypted drives. The outer perimeter meets the security requirements in NIST 800-53 controls framework. The facility is secured with cleared staff. Emergency generators and uninterruptable power provide contingency operational systems in the event of power disruptions. Data backups are encrypted and stored securely on redundant systems.

5.3 What operational steps are necessary to leverage Secure Research Environment?

Adding a research project to Secure Research Environment first requires all users to be on the Secure Research Environment Security Domain. All connections into the environment are managed through the use of security technology such that end user devices are not allowed to remove and store sensitive data.

5.4 What type of training is required?

All users are advised to complete the SLU FISMA 101 Training, which includes reading and comprehending the information in this document. This document is designed to supplement, not replace, all other mandatory user training directed from SLU's Research and ITS divisions.
Users are reminded that external project sponsors will often have other mandatory training requirements that are unique to the sponsor.

5.5 How will it change the way we currently conduct research?

Regardless if the project uses Secure Research Environment or not, all project workstations that have access to sensitive data must be encrypted with a pre-boot encryption package, have a minimum set of security controls enabled, and have password resets that align with current SLU standards.

5.6 How will I access the data in Secure Research Environment?

All access to Secure Research Environment is tightly controlled through various security systems. From within the university network, typical users can access Secure Research Environment resources by browsing to a secured online web portal and by supplying the necessary security credentials. From outside the university network, users must first establish a VPN connection. After the VPN connection is established, the user can then browse to a secured online web portal and supply the necessary security credentials. For other access methods specific to a project or to a research need, please contact IT Security and Compliance.

5.7 How can I access SLU-net services when I'm connected to Secure Research Environment?

The connection to Secure Research Environment is exclusive. The connection, when active, disables all other network functions to prevent an accidental release of sensitive data to non-trusted devices. While connected to Secure Research Environment, you will not be able to print, send, or receive e-mail, or connect to other shared drives or services that are not within the Secure Research Environment environment. Access to the rest of the campus network, including the print servers, will be temporarily suspended while the workstation is connected to the Secure Research Environment. Printers and print servers will be automatically connected again when the Secure Research Environment connection is terminated.

5.8 Can I print when connected to Secure Research Environment?

Printing of data and reports subject to FISMA is not permitted by policy, unless the printer is included within the individual project's certification boundary. Your PI determines if printers are needed at the beginning of the project. The reason that printing is not normally allowed is that FISMA requires an auditable physical perimeter and SLU printers are not normally located in secure areas. Printing of non-FISMA-controlled documents is allowed by policy, but cannot be accomplished when connected to Secure Research Environment.

5.9 What type of user groups will be established?

Each research project's PI will be required to identify "project leads" and "users." The project lead may be one in the same as the system or application owner. The project leads are those designated individuals within a research project who are authorized to submit change requests to the Secure Research Environment team to add, modify, and remove users from the project. Project leads will also periodically review audit logs to ensure all access to the data was authorized. Users are all other individuals working on the project that have been granted access to the project resources.

5.10 How does the university meet the "continuous monitoring" requirements?

All FISMA projects have a requirement for continuous monitoring. The Secure Research Environment team has deployed several tools to monitor for intrusions and unauthorized activities. The Service Desk staff is available for high-priority emergencies. The Secure Research Environment team is responsible for daily review of continuous monitoring metrics and a subset of the team reviews overall operational health of the environment. It is the responsibility of any and all research project team members to report any suspicious activity or if there appears to be a security issue.

5.11 What happens if there is a security incident?

FISMA requires a robust security incident response process. Continuous monitoring tools will alert the Service Desk and the Secure Research Environment team if an event reaches pre-defined thresholds. All project staff will be expected to immediately report security incidents to the Service Desk or IT Security Compliance. If an event is traced to one of the project's computers, the principal investigator and the user will be expected to fully cooperate with the investigation. The system may be temporarily removed from the network to protect the integrity of the environment.

5.12 Where can I get help?

The first place to obtain general information is with the Research Technology Group at RGT@slu.edu.