UF | UNIVERSITY of FLORIDA
Information Technology

UF Research Vault (ResVault)

System Security Plan (SSP)

Version 1.0
February 2018

Prepared for:

UFIT Research Computing
University of Florida
2001 Museum Road
PO Box 118440
Gainesville, FL 32611

Document Revision History

Date	Description of Revision	Document Version	Author
08 February 2018	Release	1.0	Erik Deumens David Stricklin

Table of Contents

Executive Summary

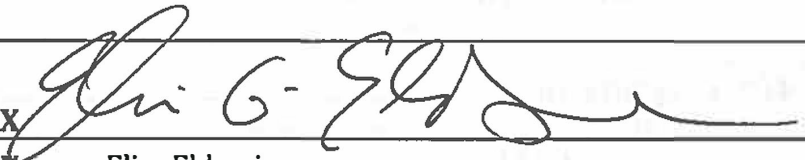
The System Security Plan (SSP) details the implementation of the security controls for the University of Florida Research Vault (UF ResVault). This SSP is written in accordance with the governance in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision 1, Guide for Developing Security Plans for Information Technology Systems.*

The security controls selected for the UF ResVault are determined in accordance with the governance of *NIST SP 800-53, Revision 4,* and *Recommended Security Controls for Federal Information Systems and Organizations.*

The UF ResVault system also meets the requirements of *NIST 800-171.* The security controls selected were based on a Moderate Impact system and the UF ResVault system is classified accordingly. The system is designed as a "general support system" as defined in NIST 800-18 for storing and processing data according to FIPS-200 that is classified according to FIPS-199 as moderate or according to NARA as CUI.

The UF ResVault system is designed further to provide a base for compliance with other security compliance requirements based upon such as the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS 3.1).

Security Plan Approval Signatory Authority

X 
Name: Elias Eldayrie **Title/Office**: Vice President and Chief Information Officer and Approving Official
X 
Name: Rob Adams **Title/Office:** Chief Information Security Officer
X 
Name: Erik Deumens **Title/Office:** Director, Research Computing

System Roles and Responsibilities

Chief Information Officer

- Designates a chief information security officer (CISO),
- Develops and maintains an organization-wide information security program,
- Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements,
- Ensures compliance with applicable information security requirements, and
- Reports annually, in coordination with the other senior organization officials, to the organization head on the effectiveness of the organization information security program, including progress of remedial actions.

Chief Information Security Officer

- Performs information security duties as the primary duty,
- Heads an office with the mission and resources to assist in ensuring organization compliance with information security requirements,
- Periodically assesses risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization,
- Develops and maintains risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each organization information system to ensure compliance with applicable requirements,
- Facilitating development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems,
- Ensuring that organization personnel, including contractors, receive appropriate information security awareness training,
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities,
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices,
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the organization,
- Developing and implementing procedures for detecting, reporting, and responding to security incidents,
- Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the organization, and
- Supporting the CIO in annual reporting to university leadership on the effectiveness of the information security program, including progress of remedial actions.

Service Owner

The service owner is responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

- Work closely with developers and testers to ensure functional designs and also assigns duties, responsibilities, and scope of authority to project personnel,
- May drive and participate in design, development, and implementation,
- Develops and maintains plans, policies, and procedures for all project phases,
- Develops the system security plan in coordination with information owners, the system administrator, the Chief Information Security Officer and functional end users,
- Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,
- Updates the system security plan whenever a significant change occurs and,
- Assists in the identification, implementation, and assessment of the common security controls,
- Ensures information sent within the system is stored safely and can be transmitted securely,
- May plan (and sometimes implement) security systems for the organization, including encryption systems, networks, and antivirus systems. The system must be monitored constantly to make sure sensitive information cannot be leaked. When problems arise, the officer should be able to troubleshoot and make corrections immediately. He/she may also carry out "what-if" scenarios and security audits to make sure the system is effective, and the results of these audits are reviewed in order to implement changes,
- Elevate security issues to management and file accurate reports regarding any and all issues,
- Facilitate the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes,
- Conduct risk and vulnerability assessments of information systems to identify security risks, and
- Develop policies and procedures to ensure information systems are defended against unauthorized access.

Approving Official

The approving official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally accept the risk of operating the information system.

- Accepts system security plans,
- Accepts the risk of operation of the information system,
- Issues an interim authorization approval to operate the information system under specific terms and conditions, or

- Denies approval to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

University of Florida Research Vault (UF ResVault)

CIO (Approving Official)

Name	Elias Eldayrie
Title	Vice President and Chief Information Officer
Company / Organization	University of Florida
Address	1 Tigert Hall, Gainesville, FL 32611
Phone Number	352-273-1788
Email Address	eldayrie@ufl.edu

CISO

Name	Rob Adams
Title	Chief Information Security Officer
Company / Organization	University of Florida
Address	1 Tigert Hall, Gainesville, FL 32611
Phone Number	352-392-6980
Email Address	rob@ufl.edu

Service Owner

Name	Erik Deumens
Title	Director, Research Computing
Company / Organization	University of Florida
Address	PO Box 118435, 2001 Museum Road, Gainesville, FL 32611
Phone Number	352-392-6980
Email Address	deumens@ufl.edu

Operational Status

The UF ResVault system is currently in operation.

Concept of Operations

Compliance objective

UF ResVault is managed using the process and procedures that closely follow what is mandated by the FISMA acts of 2002 and 2014 for systems owned by and operated for the federal government.

- Data processed by projects set up in ResVault is classified following FIPS-199.
- ResVault is classified according to FIPS-200 to meet data requirements classified at the "moderate" impact level for Confidentiality, Integrity, and/or Availability.
- Controls are implemented and maintained for ResVault as specified in 800-53 Moderate and 800-171.
- A system security plan (SSP) with Plan of Actions and Milestones (POAM) is maintained for ResVault according to NIST 800-18.
- Approval to operate is obtained by the system owner and operator from the appropriate university official.
- The implementation of the controls is assessed by an organization independent of the system owner, UF Information Technology, with annual assessments thereafter.

DISCLAIMER

The NIST documentation can be applied as best practice and standard for operating any information system owned by and operated for any organization. Because of the possible narrow interpretation that FISMA compliance implies that the system is owned by and operated for the federal government:

- We do not claim that ResVault is "FISMA complaint".
- We do not claim that any cloud service that is used as a connected system to ResVault is FedRAMP certified.
- We do not claim that ResVault is a "cloud service provider (CSP)" that is FedRAMP certified.

System Description

UF ResVault is a general support system located at the University of Florida, Gainesville, FL. Users are located on the campus and throughout the United States, and are allowed to use

the system via remote access. UF ResVault functions completely within systems at this location.
UF ResVault provides High Performance Computing (HPC), High Throughput Computing (HTC), High-Performance Data Analytics (HPDA), and High-Performance Artificial Intelligence (HPIA) capabilities to UF researchers for research that involves restricted data. The computing environment is self-contained with a minimum of connections to other systems. All connections are rigorously controlled. Data is encrypted at rest and in flight and is processed inside highly secured and isolated Secure Virtual Machines (SVM). Date cannot be moved out of the environment, except by users with special authorization to ensure compliant data management. The end-user device that is used to connect to the ResVault system is completely isolated from the ResVault data environment. Fully encrypted data is backed up locally with a copy on a site out of the State of Florida. The keys to decrypt the data is not kept on these backups so that data recovery cannot be performed.

UF ResVault is designed to enable research for a multitude of isolated projects by teams of people with specific research needs, constraints and missions. The UF ResVault is designed to serve the needs of each project while keeping the confidentiality, integrity, and availability of information protected at the appropriate level. Configuration security also segregates project information to prevent unauthorized disclosure or sharing of information. UF ResVault provides the necessary infrastructure to enable research partnerships with federal agencies and other organizations for which research projects, data and technical processes must adhere to specific security guidelines per applicable regulations or contract. All research projects are completely segregated from other projects as documented in Appendix A.

The environment involves the use of an encrypted (FIPS 140-2 compliant) storage, network, and processing infrastructure for all of the physical servers, virtual servers running on the physical servers, client virtual desktop infrastructure, as well as all of the databases for the information system.

Use Case

UF ResVault users access ResVault services by connecting to the environment with a custom encrypted connection based on the Transport Layer Protocol (TLS) and Secure Shell (SSH), and then employing immutable VMs to create desktops hosted within UF ResVault to perform project specified functions. User authentication to the UF ResVault environment is performed using their UF GatorLink username and password and the DUO Security Multi-Factor Authentication service. Access is managed by UFIT Research Computing in coordination with the project principal. The projects within UF ResVault specify the data, applications, and additional security requirements needed to perform business functions. See Appendix A for details on setting up projects in UF ResVault.