



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

This document contains information that is confidential and is not to be distributed or reproduced without express written permission from the University of Florida.

Document Revision History

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

Table of Contents

<u>DOCUMENT REVISION HISTORY.....</u>	<u>2</u>
<u>EXECUTIVE SUMMARY</u>	<u>11</u>
<u>SECURITY PLAN APPROVAL SIGNATORY AUTHORITY.....</u>	<u>11</u>
<u>SYSTEM ROLES AND RESPONSIBILITIES.....</u>	<u>12</u>
CHIEF INFORMATION OFFICER.....	12
CHIEF INFORMATION SECURITY OFFICER	12
SERVICE OWNER.....	13
APPROVING OFFICIAL	13
<u>UNIVERSITY OF FLORIDA RESEARCH VAULT (UF RESVAULT)</u>	<u>15</u>
CIO (APPROVING OFFICIAL).....	15
CISO.....	15
SERVICE OWNER.....	15
<u>OPERATIONAL STATUS.....</u>	<u>16</u>
<u>CONCEPT OF OPERATIONS.....</u>	<u>16</u>
COMPLIANCE OBJECTIVE	16
SYSTEM DESCRIPTION	16
USE CASE.....	17
INFORMATION SYSTEM CATEGORIZATION AND IMPACT LEVEL	18
DATA CLASSIFICATION	19
INFORMATION SYSTEM PRIVACY IMPACT ASSESSMENT	20
INFORMATION SYSTEM BOUNDARIES.....	20
INFORMATION SYSTEM SOFTWARE LIST	20
INFORMATION SYSTEM HARDWARE LIST	20
OPERATIONAL SECURITY AND BACKUP/RECOVERY STRATEGY	21
COMPLIANCE MONITORING AND REPORTING.....	21
<u>REFERENCES.....</u>	<u>21</u>
<u>ACRONYMS/DEFINITIONS</u>	<u>22</u>
<u>SECURITY AND PRIVACY CONTROLS</u>	<u>23</u>
<u>GENERAL POLICY, STANDARDS AND PROCEDURES</u>	<u>23</u>
<u>ACCESS CONTROL.....</u>	<u>24</u>
SI-4ACCESS CONTROL POLICY AND PROCEDURES (AC-1)	24
ACCOUNT MANAGEMENT (AC-2) [3.1.1] [3.1.2]	24

UF ResVault System Security Plan

AUTOMATED SYSTEM ACCOUNT MANAGEMENT – AC-2 (1).....	24
REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS – AC-2 (2).....	24
DISABLE INACTIVE ACCOUNTS – AC-2 (3).....	25
AUTOMATICALLY AUDIT ACCOUNTS – AC-2 (4).....	25
ACCESS ENFORCEMENT (AC-3) [3.1.1] [3.1.2].....	25
DISCRETIONARY ACCESS CONTROL – AC-3(4).....	25
INFORMATION FLOW ENFORCEMENT (AC-4) [3.1.3].....	25
SEPARATION OF DUTIES (AC-5) [3.1.4].....	25
LEAST PRIVILEGE (AC-6) [3.1.5].....	26
AUTHORIZE ACCESS TO SECURITY FUNCTIONS – AC-6 (1) [3.1.5].....	26
NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS – AC-6 (2) [3.1.6].....	26
PRIVILEGED ACCOUNTS – AC-6 (5).....	26
AUDITING USE OF PRIVILEGED FUNCTIONS – AC-6 (9) [3.1.7].....	26
PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS – AC-6 (10) [3.1.7].....	26
UNSUCCESSFUL LOGIN ATTEMPTS (AC-7) [3.1.8].....	27
SYSTEM USE NOTIFICATION (AC-8) [3.1.9].....	27
SESSION LOCK (AC-11) [3.1.10].....	27
PATTERN-HIDING DISPLAYS – AC-11 (1) [3.1.10].....	27
SESSION TERMINATION (AC-12) [3.1.11].....	27
PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION (AC-14).....	27
REMOTE ACCESS (AC-17) [3.1.1] [3.1.2].....	28
AUTOMATED MONITORING/CONTROL – AC-17 (1) [3.1.12].....	28
PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION – AC-17 (2) [3.1.13].....	28
MANAGED ACCESS CONTROL POINTS – AC-17 (3) [3.1.14].....	28
PRIVILEGED COMMANDS/ACCESS – AC-17 (4) [3.1.15].....	28
WIRELESS ACCESS (AC-18) [3.1.16].....	28
AUTHENTICATION AND ENCRYPTION – AC-18 (1) [3.1.17].....	28
ACCESS CONTROL FOR MOBILE DEVICES (AC-19) [3.1.18].....	28
FULL DEVICE/CONTAINER-BASED ENCRYPTION – AC-19 (5) [3.1.19].....	28
USE OF EXTERNAL INFORMATION SYSTEMS (AC-20) [3.1.20].....	28
LIMITS ON AUTHORIZED USE – AC-20 (1) [3.1.20].....	29
PORTABLE STORAGE DEVICES – AC-20 (2) [3.1.21].....	29
INFORMATION SHARING (AC-21).....	29
PUBLICLY ACCESSIBLE CONTENT (AC-22) [3.1.22].....	29
<u>AWARENESS AND TRAINING.....</u>	<u>30</u>
SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES (AT-1).....	30
SECURITY AWARENESS TRAINING (AT-2) [3.2.1] [3.2.2].....	30
INSIDER THREAT – AT-2 (2) [3.2.3].....	30
ROLE-BASED SECURITY TRAINING (AT-3) [3.2.1] [3.2.2].....	30
SECURITY TRAINING RECORDS (AT-4).....	31
<u>AUDIT AND ACCOUNTABILITY.....</u>	<u>32</u>
AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES (AU-1).....	32
AUDIT EVENTS (AU-2) [3.3.1] [3.3.2].....	32
REVIEWS AND UPDATES – AU-2 (3) [3.3.3].....	32
CONTENT OF AUDIT RECORDS (AU-3) [3.3.1] 3.3.2].....	32
ADDITIONAL AUDIT INFORMATION – AU-3 (1) [3.3.1] [3.3.2].....	33
AUDIT STORAGE CAPACITY (AU-4).....	33

UF ResVault System Security Plan

RESPONSE TO AUDIT PROCESSING FAILURES (AU-5) [3.3.4]	33
AUDIT REVIEW, ANALYSIS AND REPORTING (AU-6) [3.3.1] [3.3.2]	33
PROCESS INTEGRATION – AU6 (1) [3.3.5]	33
CORRELATE AUDIT REPOSITORIES – AU-6 (3) [3.3.5].....	33
AUDIT REDUCTION AND REPORT GENERATION (AU-7) [3.3.6]	34
AUTOMATIC PROCESS – AU-7 (1)	34
TIME STAMPS (AU-8) [3.3.7]	34
SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE – AU-8 (1) [3.3.7].....	34
PROTECTION OF AUDIT INFORMATION (AU-9) [3.3.8]	34
ACCESS BY SUBSET OF PRIVILEGED USERS – AU-9 (4) [3.3.9].....	34
AUDIT RECORD RETENTION (AU-11)	34
AUDIT GENERATION (AU-12) [3.3.1] [3.3.2]	35
<u>SECURITY ASSESSMENT AND AUTHORIZATION</u>	<u>36</u>
SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES (CA-1)	36
SECURITY ASSESSMENTS – (CA-2) [3.12.1] [3.12.2] [3.12.3]	36
INDEPENDENT ASSESSORS – CA-2 (1)	37
SYSTEM INTERCONNECTIONS (CA-3)	37
RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS – CA-3 (5).....	37
PLAN OF ACTION AND MILESTONES (CA-5) [3.12.1] [3.12.2] [3.12.3]	37
SECURITY AUTHORIZATION (CA-6)	37
CONTINUOUS MONITORING (CA-7) [3.12.1] [3.12.2] [3.12.3]	37
INDEPENDENT ASSESSMENT – CA-7 (1).....	38
PENETRATION TESTING – CA-8	38
INTERNAL SYSTEM CONNECTIONS (CA-9)	38
<u>CONFIGURATION MANAGEMENT</u>	<u>39</u>
CONFIGURATION MANAGEMENT POLICY AND PROCEDURES (CM-1)	39
BASELINE CONFIGURATION (CM-2) [3.4.1] [3.4.2]	39
REVIEWS AND UPDATES – CM-2 (1)	39
RETENTION OF PREVIOUS CONFIGURATIONS – CM-2 (3).....	39
CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS – CM-2 (7).....	39
CONFIGURATION CHANGE CONTROL (CM-3) [3.4.3]	40
TEST/VALIDATE/DOCUMENT CHANGES – CM-3 (2).....	40
SECURITY IMPACT ANALYSIS (CM-4) [3.4.4]	40
ACCESS RESTRICTIONS FOR CHANGE (CM-5) [3.4.5]	40
CONFIGURATION SETTINGS (CM-6) [3.4.1] [3.4.2]	40
LEAST FUNCTIONALITY (CM-7) [3.4.6]	40
PERIODIC REVIEW – CM-7 (1) [3.4.7]	40
PREVENT PROGRAM EXECUTION – CM-7 (2) [3.4.7]	41
UNAUTHORIZED SOFTWARE/BLACKLISTING – CM-7 (4) [3.4.8]	41
UNAUTHORIZED SOFTWARE/WHITELISTING – CM-7 (5) [3.4.8].....	41
INFORMATION SYSTEM COMPONENT INVENTORY (CM-8) [3.4.1] [3.4.2]	41
UPDATES DURING INSTALLATIONS/REMOVALS – CM-8 (1) [3.4.1] [3.4.2].....	41
AUTOMATED UNAUTHORIZED COMPONENT DETECTION – CM-8 (3).....	41
NO DUPLICATE ACCOUNTING OF COMPONENTS – CM-8 (5).....	41
CONFIGURATION MANAGEMENT PLAN (CM-9)	42
SOFTWARE USAGE RESTRICTION (CM-10)	42
USER-INSTALLED SOFTWARE (CM-11) [3.4.9]	42

<u>CONTINGENCY PLANNING.....</u>	43
CONTINGENCY PLANNING POLICY AND PROCEDURES (CP-1)	43
CONTINGENCY PLAN (CP-2).....	43
COORDINATE WITH RELATED PLANS – CP-2 (1)	43
RESUME ESSENTIAL MISSIONS/BUSINESS FUNCTIONS – CP-2 (3).....	43
IDENTIFY CRITICAL ASSETS – CP-2 (8).....	43
CONTINGENCY TRAINING (CP-3).....	44
CONTINGENCY PLAN TESTING (CP-4).....	44
COORDINATE WITH RELATED PLANS – CP-4 (1)	44
ALTERNATE STORAGE SITE (CP-6)	45
SEPARATION FROM PRIMARY SITE – CP-6 (1).....	45
ACCESSIBILITY – CP-6 (3)	45
ALTERNATE PROCESSING SITE (CP-7)	45
SEPARATION FROM PRIMARY SITE – CP-7 (1).....	45
ACCESSIBILITY – CP-7 (2)	45
PRIORITY OF SERVICE – CP-7 (3).....	45
TELECOMMUNICATIONS SERVICES (CP-8)	45
PRIORITY OF SERVICE PROVISIONS – CP-8 (1).....	45
SINGLE POINTS OF FAILURE – CP-8 (2).....	45
INFORMATION SYSTEM BACKUP (CP-9) [3.8.9].....	46
TESTING FOR RELIABILITY/INTEGRITY – CP-9 (1).....	46
INFORMATION SYSTEM RECOVERY AND RECONSTITUTION (CP-10)	46
TRANSACTION RECOVERY – CP-10 (2).....	46
<u>IDENTIFICATION AND AUTHENTICATION.....</u>	47
IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES (IA-1)	47
IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) (IA-2) [3.5.1] [3.5.2].....	47
NETWORK ACCESS TO PRIVILEGED ACCOUNTS – IA-2 (1) [3.5.3]	47
NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS – IA-2 (2) [3.5.3].....	48
LOCAL ACCESS TO PRIVILEGED ACCOUNTS – IA-2 (3) [3.5.3]	48
NETWORK ACCESS TO PRIVILEGED ACCOUNTS – REPLAY RESISTANT – IA-2 (8) [3.5.4]	48
REMOTE ACCESS-SEPARATE DEVICE – IA-2 (11).....	48
ACCEPTANCE OF PIV CREDENTIALS – IA-2 (12)	48
DEVICE IDENTIFICATION AND AUTHENTICATION (IA-3).....	48
IDENTIFIER MANAGEMENT (IA-4) [3.5.5] [3.5.6]	48
AUTHENTICATOR MANAGEMENT (IA-5) [3.5.1] [3.5.2]	49
PASSWORD-BASED AUTHENTICATION – IA-5 (1) [3.5.7] [3.5.8] [3.5.9] [3.5.10] [3.5.11]	49
PKI-BASED AUTHENTICATION – IA-5 (2).....	49
IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION IA-5 (3)	49
HARDWARE TOKEN-BASED AUTHENTICATION – IA-5 (11)	50
AUTHENTICATOR FEEDBACK (IA-6) [3.5.11]	50
CRYPTOGRAPHIC MODULE AUTHENTICATION (IA-7)	50
IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) (IA-8).....	50
<u>INCIDENT RESPONSE.....</u>	51
INCIDENT RESPONSE POLICY AND PROCEDURES (IR-1)	51
INCIDENT RESPONSE TRAINING (IR-2) [3.6.1] [3.6.2].....	51
INCIDENT RESPONSE TESTING (IR-3) [3.6.3].....	51

UF ResVault System Security Plan

COORDINATION WITH RELATED PLANS – IR-3 (2) [3.6.3].....	51
INCIDENT HANDLING (IR-4) [3.6.1] [3.6.2]	51
AUTOMATED INCIDENT HANDLING PROCESSES – IR-4 (1).....	51
INCIDENT MONITORING (IR-5) [3.6.1] [3.6.2]	52
INCIDENT REPORTING (IR-6) [3.6.1] [3.6.2]	52
AUTOMATED REPORTING – IR-6 (1)	52
INCIDENT RESPONSE ASSISTANCE (IR-7) [3.6.1].....	52
AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION/SUPPORT – IR-7 (1).....	52
INCIDENT RESPONSE PLAN (IR-8).....	52
<u>MAINTENANCE.....</u>	<u>54</u>
SYSTEM MAINTENANCE POLICY AND PROCEDURES (MA-1)	54
CONTROLLED MAINTENANCE (MA-2) [3.7.1] [3.7.2] [3.7.3].....	54
MAINTENANCE TOOLS (MA-3) [3.7.1] [3.7.2].....	54
INSPECT TOOLS – MA-3 (1) [3.7.1] [3.7.2].....	55
INSPECT MEDIA – MA-3 (2) [3.7.1] [3.7.2] [3.7.4]	55
NON-LOCAL MAINTENANCE (MA-4) [3.7.5].....	55
DOCUMENT NON-LOCAL MAINTENANCE – MA-4 (2)	55
MAINTENANCE PERSONNEL (MA-5) [3.7.6].....	55
TIMELY MAINTENANCE (MA-6).....	55
<u>MEDIA PROTECTION.....</u>	<u>56</u>
MEDIA PROTECTION POLICY AND PROCEDURES (MP-1)	56
MEDIA ACCESS (MP-2) [3.8.1] [3.8.2] [3.8.3].....	56
MEDIA MARKING (MP-3) [3.8.4]	56
MEDIA STORAGE (MP-4) [3.8.1] [3.8.2] [3.8.3]	57
MEDIA TRANSPORT (MP-5) [3.8.5].....	57
CRYPTOGRAPHIC PROTECTION – MP-5 (4) [3.8.6].....	57
MEDIA SANITIZATION (MP-6) [3.8.1] [3.8.2] [3.8.3].....	57
MEDIA USE (MP-7) [3.8.7]	57
PROHIBIT USE WITHOUT OWNER – MP-7 (1) [3.8.8]	57
<u>PHYSICAL AND ENVIRONMENTAL PROTECTION.....</u>	<u>58</u>
PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES (PE-1).....	58
PHYSICAL ACCESS AUTHORIZATIONS (PE-2) [3.10.1] [3.10.2].....	58
PHYSICAL ACCESS CONTROL (PE-3) [3.10.3] [3.10.4] [3.10.5].....	58
ACCESS CONTROL FOR TRANSMISSION MEDIUM (PE-4)	58
ACCESS CONTROL FOR OUTPUT DEVICES (PE-5) [3.10.1] [3.10.2]	58
MONITORING PHYSICAL ACCESS (PE-6) [3.10.1] [3.10.2].....	58
INTRUSION ALARMS/SURVEILLANCE EQUIPMENT – PE6 (1)	59
VISITOR ACCESS RECORDS (PE-8).....	59
POWER EQUIPMENT AND CABLING (PE-9)	59
EMERGENCY SHUTOFF (PE-10)	59
EMERGENCY POWER (PE-11)	59
EMERGENCY LIGHTING (PE-12)	59
FIRE PROTECTION (PE-13).....	59
AUTOMATIC FIRE SUPPRESSION – PE-13 (3)	60
TEMPERATURE AND HUMIDITY CONTROLS (PE-14).....	60
WATER DAMAGE PROTECTION (PE-15)	60

UF ResVault System Security Plan

DELIVERY AND REMOVAL (PE-16)	61
ALTERNATE WORK SITE (PE-17) [3.10.6]	61
<u>PLANNING</u>	62
SECURITY PLANNING POLICY AND PROCEDURES (PL-1)	62
SYSTEM SECURITY PLAN (PL-2)	62
COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES – PL-2 (3).....	62
RULES OF BEHAVIOR (PL-4)	63
SOCIAL MEDIA AND NETWORKING RESTRICTION – PL-4 (1).....	63
INFORMATION SECURITY ARCHITECTURE (PL-8)	63
<u>PERSONNEL SECURITY</u>	64
PERSONNEL SECURITY POLICY AND PROCEDURES (PS-1)	64
POSITION RISK DESIGNATION (PS-2)	64
PERSONNEL SCREENING (PS-3) [3.9.1] [3.9.2]	64
PERSONNEL TERMINATION (PS-4) [3.9.1] [3.9.2]	64
PERSONNEL TRANSFER (PS-5) [3.9.1] [3.9.2]	65
ACCESS AGREEMENTS (PS-6)	65
THIRD-PARTY PERSONNEL SECURITY (PS-7)	65
PERSONNEL SANCTIONS (PS-8)	65
<u>RISK ASSESSMENT</u>	66
RISK ASSESSMENT POLICY AND PROCEDURES (RA-1)	66
SECURITY CATEGORIZATION (RA-2)	66
RISK ASSESSMENT (RA-3) [3.11.1]	67
VULNERABILITY SCANNING (RA-5) [3.11.2]	67
UPDATE TOOL CAPABILITY – RA-5 (1).....	67
UPDATE BY FREQUENCY/PRIOR TO NEW SCAN/WHEN IDENTIFIED – RA-5 (2) [3.11.3].....	67
PRIVILEGED ACCESS – RA-5 (5) [3.11.2].....	67
<u>SYSTEM AND SERVICES ACQUISITION</u>	68
SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES (SA-1)	68
ALLOCATION OF RESOURCES (SA-2)	68
SYSTEM DEVELOPMENT LIFE CYCLE (SA-3)	68
ACQUISITION PROCESS (SA-4)	69
FUNCTIONAL PROPERTIES OF SECURITY CONTROLS – SA-4 (1).....	69
IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS – SA-4 (2).....	69
FUNCTIONS/PORTS/PROTOCOLS/SERVICES IN USE – SA-4 (9).....	69
INFORMATION SYSTEM DOCUMENTATION (SA-5)	69
SECURITY ENGINEERING PRINCIPLES (SA-8) [3.13.1] [3.13.2] [3.13.5]	70
EXTERNAL INFORMATION SYSTEMS SERVICES (SA-9)	70
IDENTIFICATION OF FUNCTIONS/PORTS/PROTOCOLS/SERVICES – SA-9 (2).....	71
DEVELOPER CONFIGURATION MANAGEMENT (SA-10)	71
DEVELOPER SECURITY TESTING AND EVALUATION (SA-11)	71
<u>SYSTEM AND COMMUNICATIONS PROTECTION</u>	72
SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES (SC-1)	72
APPLICATION PARTITIONING (SC-2) [3.13.3]	72

UF ResVault System Security Plan

INFORMATION IN SHARED RESOURCES (SC-4) [3.13.4]	72
DENIAL OF SERVICE PROTECTION (SC-5)	72
BOUNDARY PROTECTION (SC-7) [3.13.1] [3.13.2] [3.13.5]	72
ACCESS POINTS – SC-7 (3)	73
EXTERNAL TELECOMMUNICATIONS SERVICES – SC-7 (4)	73
DENY BY DEFAULT/ALLOW BY EXCEPTION – SC-7 (5) [3.13.6]	73
PREVENT SPLIT TUNNELING FOR REMOTE DEVICES – SC-7 (7) [3.13.7]	73
TRANSMISSION CONFIDENTIALITY AND INTEGRITY (SC-8) [3.13.8]	73
CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION – SC-8 (1)	73
NETWORK DISCONNECT (SC-10) [3.13.9]	73
CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT (SC-12) [3.13.10]	73
CRYPTOGRAPHIC PROTECTION (SC-13) [3.13.11]	74
COLLABORATIVE COMPUTING DEVICES (SC-15) [3.13.12]	74
PUBLIC KEY INFRASTRUCTURE CERTIFICATES (SC-17)	74
MOBILE CODE (SC-18) [3.13.13]	74
VOICE OVER INTERNET PROTOCOL (SC-19) [3.13.14]	74
SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) (SC-20)	74
SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) (SC-21)	74
ARCHITECTURE AND PROVISIONING (FOR NAME/ADDRESS RESOLUTION SERVICE) (SC-22)	74
SESSION AUTHENTICITY (SC-23) [3.13.15]	75
PROTECTION OF INFORMATION AT REST (SC-28) [3.13.16]	75
PROCESS ISOLATION (SC-39)	75
<u>SYSTEM AND INFORMATION INTEGRITY</u>	76
SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES (SI-1)	76
FLAW REMEDIATION (SI-2) [3.14.1]	76
AUTOMATED FLAW REMEDIATION STATUS – SI-2 (2) [3.14.3].....	76
MALICIOUS CODE PROTECTION (SI-3) [3.14.1] [3.14.2] [3.14.3] [3.14.5]	76
CENTRAL MANAGEMENT – SI-3 (1).....	77
AUTOMATIC UPDATES – SI-3 (2) [3.14.4].....	77
INFORMATION SYSTEM MONITORING (SI-4) [3.14.6] [3.14.7]	77
AUTOMATED TOOLS FOR REAL-TIME ANALYSIS – SI-4 (2)	78
INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC – SI-4 (4) [3.14.6].....	78
SYSTEM GENERATED ALERTS – SI-4 (5).....	78
SECURITY ALERTS, ADVISORIES, AND DIRECTIVES (SI-5) [3.14.1] [3.14.2] [3.14.3]	78
SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY (SI-7)	78
INTEGRITY CHECKS – SI-7 (1).....	78
INTEGRATION OF DETECTION AND RESPONSE – SI-7 (7)	78
SPAM PROTECTION (SI-8)	78
CENTRAL MANAGEMENT – SI-8 (1).....	78
AUTOMATIC UPDATES – SI-8 (2)	78
INFORMATION INPUT VALIDATION (SI-10)	79
ERROR HANDLING (SI-11)	79
INFORMATION HANDLING AND RETENTION (SI-12)	79
MEMORY PROTECTION (SI-16)	79
<u>APPENDICES</u>	80
APPENDIX A UF RESVAULT PROJECT HANDBOOK	81
APPENDIX B UF RESVAULT GENERAL USER RULES OF BEHAVIOR (ROB)	85

UF ResVault System Security Plan

APPENDIX C UF RESVAULT SYSTEM ADMINISTRATOR HANDBOOK.....	87
APPENDIX D UF RESVAULT PRIVILEGED USER RULES OF BEHAVIOR (ROB).....	92
APPENDIX E UF RESVAULT REPORTING SPECIFICATIONS.....	95
APPENDIX F UF RESVAULT ARCHITECTURAL OVERVIEW	100
APPENDIX G UF RESVAULT PLAN OF ACTION AND MILESTONES (POAM) (CONFIDENTIAL).....	108
APPENDIX H UF RESVAULT NETWORK HOSTS AND SERVER MAP (CONFIDENTIAL)	112

Executive Summary

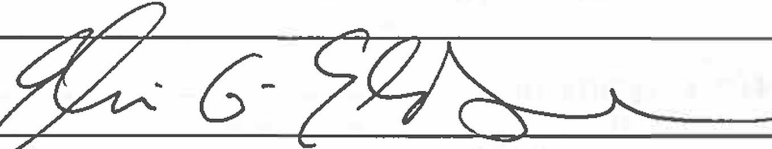
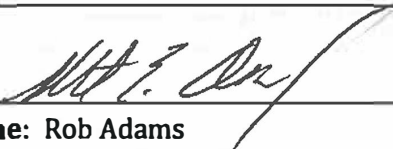

The System Security Plan (SSP) details the implementation of the security controls for the University of Florida Research Vault (UF ResVault). This SSP is written in accordance with the governance in the *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Revision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

UF ResVault System Security Plan

- 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

UF ResVault System Security Plan

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). Data 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.