Information Security Policies and Procedures for Infinibyte Cloud

Version 1.1

June 17, 2020

Proprietary and Confidential

For Authorized Use Only

THIS PAGE INTENTIONALLY BLANK

REVISION RECORD

Date	Version	Page/Paragraph	Description of Change	Made By:
03/06/2019	0.1	Entire Document	Initial Review Draft	SphereCom
03/12/2019	0.2	Entire Document	SSS Internal Review	Richard Monforti
04/22/2019	1.0	Entire Document	Finalized Document	Richard Monforti
06/17/2020	1.1	Entire Document	Changes to CSP Name and Content	Jeffrey Hsii

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The purpose of this Information Security Policies and Procedures (ISPP) document is to establish policies and procedures to facilitate the timely and effective implementation of required security controls and control enhancements for DLH Infinibyte Cloud (Infinibyte Cloud) systems that will be authorized to process U.S. Government information by the federal government under the Federal Risk and Authorization Management Program (FedRAMP).

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, directed the National Institute of Standards and Technology (NIST) to develop a minimum set of security controls for all federal information systems, and then mandated their use by all federal agencies. In addition, the Office of Management and Budget (OMB) has mandated that all cloud computing services that process Government information will also meet the security requirements specified by the FedRAMP security control overlay.

Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, formalizes these requirements and also directs that the "sensitivity impact" of information processed within each Agency information system be individually evaluated and categorized in accordance with the process specified in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. The resulting sensitivity impact categorization must then be used to select the appropriate set of security controls that are defined in NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST Special Publication (SP) 800-53 further directs federal agencies to conduct an organization-wide information system security assessment and to then develop security plans to meet the stringent privacy and security requirements that are also specified within NIST SP 800-53. Controls for each supporting system may then be "tailored" by the Agency to fit the security plan, assuring that the resulting comprehensive security and privacy strategy complies with all applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance specific to that Agency.

1.2 Scope and Applicability

The Infinibyte Cloud security policies and procedures defined in this document provide baselines that will be utilized for Infinibyte Cloud systems processing U.S. Government information pending the identification of tailored control sets by supported federal organizations. Through a system categorization conducted using FIPS Publication 199, it has been determined that the baseline security categorization for Infinibyte Cloud systems is at the "Moderate" Impact Level. As a result, the security policies in this document address the current NIST SP 800-53 Moderate Impact security controls and enhancements, as defined by FedRAMP.

Security control and organization-defined values, as well as implementation details, shall be documented within the applicable Infinibyte Cloud System Security Plan (SSP). If the Infinibyte Cloud policies and procedures set forth in this document and those subordinate to it are less stringent than the applicable Federal Agency policies, procedures and standards, the Federal Agency requirements shall take precedence and Infinibyte Cloud shall meet the Federal Agency's requirements.

The policies and procedures contained in this document apply to all Infinibyte Cloud personnel to whom access is granted for Infinibyte Cloud systems where U.S. Government information is created, gathered, stored, transmitted or used in any form (i.e., written, verbal, or electronic).

1.3 Roles and Responsibilities

All Infinibyte Cloud personnel to whom access is granted for Infinibyte Cloud systems shall comply with these policies and procedures. Infinibyte Cloud personnel who contract with or supervise work performed by third parties shall be responsible for communicating the requirements of this policy to those third parties, and for overseeing compliance by the third parties.

Violations of these policies and procedures should be reported immediately to the Information System Security Officer (ISSO).

1.3.1 President, Social & Scientific Systems

As the DLH executive in charge of the Social & Scientific Systems (SSS) operating unit, the SSS President shall:

a) Demonstrate corporate-level commitment to the security program by signing and issuing the security policy and procedures document;
b) Ensure that adequate resources are applied to the Infinibyte Cloud security program to make it successful; and
c) Approve any exceptions or waivers to these policies and/or procedures after receiving a recommendation from the ISSO.

1.3.2 Director, Information Technology

The Information Technology (IT) Director shall be ultimately responsible for mission accomplishment, and shall ensure that all necessary resources are effectively applied to develop the security capabilities needed to accomplish the mission. Effective information security policies and procedures that assess and mitigate IT-related mission risks are recognized as an essential element of the Infinibyte Cloud mission support capability.

The IT Director shall:

a) Be responsible for the Infinibyte Cloud IT planning, budgeting, and performance including information security components. Decisions made in these areas shall support

the establishment and maintenance of effective information security policies and procedures;

b) Ensure that the necessary resources and commitment are applied to establish and maintain an Information Security Program for Infinibyte Cloud systems that process U.S. Government information;
c) Ensure that the Infinibyte Cloud systems and services that process Government information meet the requirements stated in the Infinibyte Cloud information security policies and procedures;
d) Annually review and approve the Infinibyte Cloud information security policies and procedures to ensure that they satisfy the purpose, scope, and security compliance requirements for processing U.S. Government information;
e) Ensure that the organization has enough sufficiently trained personnel to protect its IT resources; and
f) Assign Infinibyte Cloud responsibility for information security to an ISSO.

1.3.3 System Owner

The Infinibyte Cloud System Owner shall be responsible for implementing and maintaining those Infinibyte Cloud systems that process U.S. Government information. As a result, the Infinibyte Cloud System Owner shall approve and sign-off on system designs and changes to these information systems (e.g., system enhancement, major changes to software and hardware, etc.). The Infinibyte Cloud System Owner shall clearly understand their role in the context of the information security policies and procedures herein and fully support their processes.

The Infinibyte Cloud System Owner shall:

a) Ensure that proper controls are in place to address integrity, confidentiality, and availability of the information systems and data under their control;
b) Assist the ISSO in developing security documentation specific to the systems under their stewardship;
c) Ensure that approved system changes are implemented in accordance with the approved Plan of Action and Milestones (POA&M); and
d) Ensure that all applicable policies for acquiring systems and services are followed.

1.3.4 Information System Security Officer (ISSO)

The Information System Security Officer (ISSO) shall:

a) Provide overall coordination, direction, and oversight for information security matters for assigned systems;
b) Maintain, interpret, and oversee implementation of these policies and procedures within assigned systems;

c) Establish and formally document the Infinibyte Cloud Information Security Program for assigned systems; and
d) Upon request, provide documentation to U.S. Government Agencies as part of the security Assessment and Authorization (A&A) process.

1.3.5 Authorized Requestors

Authorized requestors are typically DLH project managers who possess essential decision-making authority and responsibility for their individual projects and contracts. Their involvement in every stage of the information security program is crucial to the success of the Infinibyte Cloud security effort and shall help to minimize any unnecessary expenditure of precious resources.

Authorized requestors shall:

a) Take an active role in the implementation of these information security policies and procedures;
b) Ensure that personnel having access to and working with systems that process U.S. Government information have the requisite skills, training and understanding of applicable policies and procedures to effectively fulfill their roles; and
c) Identify issues and recommend changes to the ISSO and/or IT Director.

1.3.6 Privileged Users

Infinibyte Cloud Privileged Users are the ISSO, Architect, System Administrators, Security Administrators and Security Auditors who are responsible for the proper implementation of security controls that are required to meet the security standards identified in these information security policies and procedures.

Infinibyte Cloud Privileged Users shall:

a) Properly implement security controls in their information systems in accordance with Infinibyte Cloud security policy as defined in these information security policies and procedures;
b) Recommend changes to the information security policies and procedures as changes occur to the existing information system environment in order to maintain the effectiveness of established procedures (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational polices, introduction of new technologies, etc.); and
c) Support security assessment and authorization activities conducted on their information systems as requested by the ISSO.

1.3.7 Users

Users are non-privileged employees, contractors, consultants, customers, and others to whom Infinibyte Cloud system access is granted shall:

a) Understand and comply with Infinibyte Cloud security policies;
b) Keep software/applications updated with security patches; and
c) Be aware of actions they can take to better protect information. These actions include, but are not limited to: proper password usage, reporting any suspected incidents or violations of security policy, and following rules to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.

2. APPLICABLE DOCUMENTS

Unless an explicit version/revision is stated, the most recent version/revision of the following documents shall govern this policy:

Federal Laws and Regulations

a) 44 U.S.C. § 3541, Federal Information Security Management Act of 2002
b) Public Law No. 113-283, Federal Information Security Modernization Act of 2014
c) 5 CFR 731.106(a), Designation of Public Trust Positions and Investigative Requirements
d) Office of Management and Budget (OMB) Circular OMB A-130, Managing Federal Information as a Strategic Resource
e) Office of Management and Budget (OMB) Memorandum 04-04, E-Authentication Guidance for Federal Agencies
f) Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules
g) Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard or Federal Employees and Contractors
h) Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
i) Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems
j) Federal Information Processing Standards (FIPS) Publication 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors
k) Federal Continuity Directive 1

National Institute of Standards and Technology (NIST) Special Publications (SP)

l) NIST SP 800-12, Rev 1, An Introduction to Information Security
m) NIST SP 800-16, Information Technology Security Training Requirements: A Role and Performance-Based Model
n) NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Federal Information Systems

o) NIST SP 800-30 Rev 1, Risk Management Guide for Information Technology Systems
p) NIST SP 800-34 Rev 1, Contingency Planning Guide for Federal Information Systems
q) NIST SP 800-35, Guide to Information Technology Security Services
r) NIST SP 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
s) NIST SP 800-40 Rev 3, Creating a Patch and Vulnerability Management Program
t) NIST SP 800-45 Ver. 2, Guidelines on Electronic Mail Security
u) NIST SP 800-46 Rev 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
v) NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems
NIST SP 800-48 Rev 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks
w) NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
x) NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations
y) NIST SP 800-53A Rev 4, Guide for Assessing the Security Controls in Federal Information Systems and Organizations
z) NIST SP 800-60 Rev 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
aa) NIST SP 800-60 Rev 1, Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
bb) NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide
cc) NIST SP 800-63-3, Digital Identity Guidelines
dd) NIST SP 800-64 Rev 2, Security Considerations in the System Development Life Cycle
ee) NIST SP 800-70 Rev 4, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
ff) NIST SP 800-73-4, Interfaces for Personal Identity Verification
gg) NIST SP 800-76-2, Biometric Specifications for Personal Identity Verification
hh) NIST SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV)
ii) NIST SP 800-83 Rev 1, Guide to Malware Incident Prevention and Handling
jj) NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
kk) NIST SP 800-88 Rev 1, Guidelines for Media Sanitization
ll) NIST SP 800-92, Guide to Computer Security Log Management
mm) NIST SP 800-94 Rev 1, Guide to Intrusion Detection and Prevention Systems (IDPS)
nn) NIST SP 800-100, Information Security Handbook: A Guide for Managers
oo) NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
pp) NIST SP 800-144, Guidelines for Security and Privacy in Public Cloud Computing
qq) NIST SP 800-145, The NIST Definition of Cloud Computing
rr) NIST SP 800-160, Vol. 1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
ss) NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

tt) NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Federal Risk and Authorization Management Program

uu) FedRAMP Security Assessment Framework, June 6, 2017
vv) FedRAMP Security Controls Baseline, August 28, 2018
ww) FedRAMP Incident Communications Procedure, December 8, 2017

3. SECURITY CONTROL SELECTION AND ORGANIZATIONALLY-DEFINED PARAMETERS

All Infinibyte Cloud systems within the scope of this ISPP shall implement, at a minimum, the security requirements for Moderate Impact Level information system as defined in NIST SP 800-53. NIST SP 800-53 further directs federal agencies to conduct an organization-wide information system security assessment and then develop security plans to meet the stringent privacy and security requirements that are also specified within NIST SP 800-53. Controls for each supporting system may then be "tailored" using overlays and "organizationally defined parameters" to fit specific mission need, thereby assuring that the resulting comprehensive security and privacy strategy complies with all applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance specific to that Agency.

Therefore, customers are responsible for defining the specific security control set for a system or service within the associated solicitation or Service Level Agreement (SLA). However, if left undefined, this ISPP assumes that the FedRAMP security controls identified as "selected" at the FIPS 199 Moderate Impact Level will meet the customer's requirements to fulfill all "applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance."

Additionally, the policies in this document assume that Federal Agencies will identify all expected operational interfaces, roles, responsibilities, and reporting requirements expected for integration with their Agency policies and procedures at the information system level. These expectations and resulting clarifications shall be documented within the appropriate Infinibyte Cloud System Security Plan. It is also important to note that DLH has no role or authority in federal decisions regarding the use of the provided Infinibyte Cloud systems and services.

4. INTERNAL COORDINATION

These Infinibyte Cloud security policies and procedures shall be coordinated, as required, between the IT Director, Information System Security Officer, Architect, and the DLH Executive Leadership Team.

5. MEASUREMENT AND VERIFICATION

The Infinibyte Cloud information security policies and procedures shall be disseminated to all organizational elements that have a responsibility for the protection of Infinibyte Cloud systems information. The information security policies and associated procedures shall be reviewed and updated annually. The documentation of that input shall clearly demonstrate that each organizational element has determined the appropriate inherited security control elements and obtained approval from the appropriate Authorizing Official(s).

In addition, for any system under the scope of this ISPP, The IT Director and ISSO shall perform the following measurement and verification activities:

a) Confirm that organizational roles and responsibilities for the performance of the review process are identified;
b) Identify who, by name, is assigned responsibility to perform the review/update of relevant policies and procedures;
c) Ensure that review triggers (e.g., specific events scheduled or directed reviews) are identified within relevant policies and procedures;
d) Confirm that updates are applied to the policy and procedures based on outputs or findings generated during the review process;
e) Confirm that configuration tracking of each revision, in each document's revision notes, is applied;
f) Confirm that the revisions are reviewed, approved, and accepted by the responsible parties;
g) Review evidence that policy and procedure reviews occur as required, as scheduled, or as appropriate;
h) Confirm that the updated documents are available for re-dissemination to all individuals accountable and responsible for compliance with this control;
i) Confirm that each individual understands how to ensure that they are using the correct release of the policies and procedures; and
j) Confirm that each individual understands their obligations and responsibilities.

Supplemental procedures may be required for systems that are unique to Infinibyte Cloud or that are subject to local, state or federal laws, Executive Orders, directives, policies, standards, and/or guidance that is unique to that system. Examples include procedures for systems that contain Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), Privacy Act, national security and/or procurement integrity information (e.g., Federal Acquisition Regulation and derivatives thereof).

6. REVIEW AND EXPIRATION

This policy and its associated procedures shall be reviewed at least annually by the IT Director. Unless readopted, the policies and procedures in this document expire three years from the date of approval by the SSS President.

7. ORGANIZATION DISTRIBUTION LIST

The following table contains the official distribution list for the Infinibyte Cloud information security policies and procedures. These members are responsible for ensuring that these information security policies and procedures are available to Infinibyte Cloud personnel. The policies and procedures are located in a restricted location, maintained by the ISSO, and are made available or distributed as needed to all Infinibyte Cloud users. All users have on-line access to the *Information Security Policies & Procedures for Infinibyte Cloud* on the Infinibyte Cloud support site.

Name	Title	Email
Kevin Beverly	President, Social & Scientific Systems	kevin.beverly@dlhcorp.com
Jeffrey Hsii	IT Director and ISSO	jeffrey.hsii@dlhcorp.com
Allen Selwyn	Architect	allen.selwyn@dlhcorp.com
Gale McFall	Security Auditor	gale.mcfall@dlhcorp.com

8. MANAGEMENT COMMITMENT

This plan has been approved by DLH management and is applicable to all operations within its defined scope.

[Signature on File]

_____ _____

Kevin Beverly, Date
President, Social & Scientific Systems

9. INFINIBYTE SYSTEM LEVEL SECURITY POLICIES AND PROCEDURES

The policies in this Section are established to support the implementation of the required security controls and control enhancements for Infinibyte Cloud systems that will be authorized by the U.S. Government under FedRAMP.

The following sections contain the Infinibyte Cloud security policies that address the current Moderate Impact level security controls and enhancements within each NIST SP 800-53 security control family.

9.1 Access Control Policy (AC-1)

9.1.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Access Control security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.1.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Access Control (AC) security control family.

9.1.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Access Control shall be applied:

a) The Architect shall be responsible for ensuring that all technical design functions identified in the policy are incorporated into Infinibyte Cloud systems that process U.S. Government information.

b) The IT Director shall be responsible for ensuring that all system security functions for protecting U.S. Government information are operated in accordance with this policy.

c) Infinibyte Cloud Privileged Users shall have the primary responsibility for implementing proper access control policies for their respective systems.

9.1.4 Applicable Documents

The documents that are applicable to the Access Control policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.1.5 Access Control Policy Requirements

The following table identifies the Infinibyte Cloud access control policies that are contained in this Section.

FAMILY: ACCESS CONTROL (AC-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
AC-2	**Account Management**	**9.1.5.1**
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*	*9.1.5.1*
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*	*9.1.5.1*
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*	*9.1.5.1*
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*	*9.1.5.1*
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT*	*9.1.5.1*
AC-2 (7)	*ACCOUNT MANAGEMENT | ROLE-BASED SCHEME*	*9.1.5.1*
AC-2 (9)	*ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS*	*9.1.5.1*
AC-2 (10)	*ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION*	*9.1.5.1*
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*	*9.1.5.1*
AC-3	**Access Enforcement**	**9.1.5.2**
AC-4	**Information Flow Enforcement**	**9.1.5.3**
AC-4 (21)	*INFORMATION FLOW ENFORCEMENT | PHYSICAL / LOGICAL SEPARATION OF INFORMATION FLOWS*	*9.1.5.3*
AC-5	**Separation of Duties**	**9.1.5.4**
AC-6	**Least Privilege**	**9.1.5.5**
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*	*9.1.5.5*
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*	*9.1.5.5*
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*	*9.1.5.5*
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*	*9.1.5.5*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*	*9.1.5.5*
AC-7	**Unsuccessful Logon Attempts**	**9.1.5.6**
AC-8	**System Use Notification**	**9.1.5.7**
AC-10	**Concurrent Session Control**	**9.1.5.8**
AC-11	**Session Lock**	**9.1.5.9**
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*	*9.1.5.9*
AC-12	**Session Termination**	**9.1.5.10**
AC-14	**Permitted Actions without Identification or Authentication**	**9.1.5.11**
AC-17	**Remote Access**	**9.1.5.12**
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*	*9.1.5.12*
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*	*9.1.5.12*
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*	*9.1.5.12*
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*	*9.1.5.12*
AC-17 (9)	*REMOTE ACCESS | DISCONNECT / DISABLE ACCESS*	*9.1.5.12*
AC-18	**Wireless Access**	**9.1.5.13**
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*	*9.1.5.13*
AC-19	**Access Control for Mobile Devices**	**9.1.5.14**
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*	*9.1.5.14*
AC-20	**Use of External Information Systems**	**9.1.5.15**
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*	*9.1.5.15*
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE DEVICES*	*9.1.5.15*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
AC-21	**Information Sharing**	**9.1.5.16**
AC-22	**Publicly Accessible Content**	**9.1.5.17**

9.1.5.1 Account Management (AC-2)

The IT Director, Architect and ISSO shall ensure that all accounts on Infinibyte Cloud systems are managed by:

a) Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary) to support business functions;
b) Assigning account managers or authorized requestors for information system accounts;
c) Establishing conditions for group membership;
d) Specifying authorized users of the information systems, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
e) Requiring IT Director approval for requests to establish privileged accounts and ISSO approval for requests to establish internal user-level accounts;
f) Creating, enabling, modifying, disabling, and removing Infinibyte Cloud system accounts in accordance with the procedures in Section 9.1.6 (Access Control Procedures) of this document;
g) Monitoring the use of information system accounts;
h) Notifying account managers when accounts are no longer required and when information system users are terminated, transferred, and information system usage or need-to-know changes;
i) Authorizing access to the system based on:
    i) A valid access authorization;
    ii) Intended system usage; and
    iii) Other attributes as required by the organization or associated missions/business functions;
j) Reviewing accounts at least annually; and
k) Establishing a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

The following account management functions shall be implemented by the IT Director and Infinibyte Cloud Privileged Users:

a) [AC-2 (1)] Implementing automated mechanisms to support the management of information system accounts as specified in the system's System Security Plan;
b) [AC-2 (2)] Automatically removing temporary and emergency accounts after a maximum of 30 days;
c) [AC-2 (3)] Disabling inactive user accounts after a maximum of 90 days;
d) [AC-2 (4)] Automatically auditing account creation, modification, disabling, and termination actions and notifying, as required, the appropriate Infinibyte Cloud System Administrator and/or Security Administrator;
e) [AC-2 (5)] Requiring that users log out at the end of a session or be automatically logged out after fifteen (15) minutes of inactivity;
f) [AC-2 (7)] Establishing and administering privileged user accounts with role-based access scheme that organizes allowed information system access and privileges into roles, monitors privileged role assignments, and immediately removes privileged role assignments when no longer appropriate as prescribed in the System Security Plan;
g) [AC-2 (9)] Not permitting the use of shared/group accounts unless they meet the IT Director-defined exception conditions for establishing shared/group accounts;
h) [AC-2 (10)] Regularly validating the on-going need for shared/group account credentials and immediately terminating such credentials when members leave the group or their continued membership is unjustified;
i) [AC-2 (12)(a)] Monitoring information system accounts for atypical use (i.e.; accessing systems at unusual times of day and from locations that are not consistent with normal usage patterns); and
j) [AC-2 (12)(a)] Reporting atypical usage of information system accounts to the proper personnel as defined in the system's System Security Plan.

9.1.5.2 Access Enforcement (AC-3)

The IT Director and ISSO define roles. The Architect shall ensure that Infinibyte Cloud systems enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. This logical access enforcement may be accomplished in any technical manner approved by the system Authorizing Official, including but not limited to: Role Based Access Controls (RBAC), Virtual Private Networks (VPNs), Virtual Local Area Network (VLANs), Secure Sockets Layer (SSL), and/or encryption.

9.1.5.3 Information Flow Enforcement (AC-4)

The Architect and ISSO shall enforce Architect-approved authorizations for controlling the flow of information within the system and between interconnected systems based on information flow control policies that rely on authentication to establish trusted network connections and endpoint certificates.

[AC-4 (21)] In addition, the Architect shall ensure that information flows are logically or physically separated using defined mechanisms that include a zoned architecture (such as VLANs or security groups) and carefully configured firewalls to separate user functionality from system management functionality and to prevent the unauthorized transfer of information.

9.1.5.4 Separation of Duties (AC-5)

The IT Director and ISSO shall:

a) Separate duties of individuals as necessary, to prevent malevolent activity without collusion;
b) Document separation of duties of individuals; and
c) Define information system access authorizations to support separation of duties.

The ISSO shall formally document the separation of duties in a Separation of Duties Matrix, which shall be an attachment to the system's System Security Plan.

9.1.5.5 Least Privilege (AC-6)

The following least privilege techniques shall be implemented and enforced by the ISSO and Architect:

a) Least privilege shall be employed on Infinibyte Cloud information systems, by allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions and explicitly authorizing access to specific information and information systems;
b) [AC-6 (1)] Access to security functions (deployed in hardware, software, and firmware) and security relevant information shall be explicitly authorized by the ISSO;
c) [AC-6 (2)] Users of information system accounts, or roles, with access to security functions shall use non-privileged accounts, or roles, when accessing other system functions. (Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters);
d) [AC-6 (5)] Privileged accounts shall be restricted on the information system to the IT Director, ISSOs, System Administrators, Security Administrators and Security Auditors;
e) [AC-6 (9)] Execution of privileged functions shall be audited as defined in the Audit and Accountability (AU) security controls in Section 9.3 of this policy; and
f) [AC-6 (10)] Non-privileged users shall be prevented from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

9.1.5.6 Unsuccessful Login Attempts (AC-7)

The Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Enforce a limit of no more than three (3) failed access attempts by a user during a 15 minute time period; and
b) Automatically lock the account/node for at least 30 minutes or until released by a System Administrator when the maximum number of unsuccessful attempts is exceeded. The policy applies regardless of whether the login occurs via a local or network connection.

9.1.5.7 System Use Notification (AC-8)

The IT Director and ISSO shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Display an approved system use notification message or banner that provides privacy and security notices before granting access to any system consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. This notification shall state that:
    i) Users are accessing a system that is processing U.S. Government information;
    ii) System usage may be monitored, recorded, and subject to audit;
    iii) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
    iv) Use of the system indicates consent to monitoring and recording.
b) Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and
c) For publicly accessible systems:
    i) Display the system use information when appropriate, before granting further access;
    ii) Display references, if any, to monitoring, recording, or auditing that shall be consistent with privacy accommodations for such systems that generally prohibit those activities; and
    iii) Include in the notice given to public users of the information system, a description of the authorized uses of the system.

9.1.5.8 Concurrent Session Control (AC-10)

The ISSO and Architect shall ensure that Infinibyte Cloud systems limit the number of concurrent privileged user sessions on each system account and/or account type to a maximum of three (3) sessions. Non-privileged user sessions shall be limited to a maximum of two (2) sessions.

9.1.5.9 Session Lock (AC-11)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Prevent further access to the system by initiating a session lock after workstations and mobile devices have been inactive for fifteen (15) minutes or upon receiving a request from a user; and
b) Retain the session lock until the user reestablishes access using established identification and authentication procedures.

[AC-11 (1)] In addition, the IT Director and Architect shall ensure that Infinibyte Cloud systems conceal, via the session lock, information previously visible on the display with a publicly viewable image.

9.1.5.10 Session Termination (AC-12)

The ISSO shall ensure that Infinibyte Cloud systems automatically terminate a privileged user session after thirty (30) minutes of inactivity.

9.1.5.11 Permitted Actions without Identification or Authentication (AC-14)

The System Owner shall:

a) Identify specific user actions that can be performed on the information system without identification or authentication; and
b) Document and provide supporting rationale in the System Security Plan for the information system, those user actions not requiring identification and authentication.

9.1.5.12 Remote Access (AC-17)

The System Owner shall:

a) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
b) Authorize remote access to the information system prior to allowing such connections.

In addition, the IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [AC-17 (1)] Monitor and control remote access methods to the information system;
b) [AC-17 (2)] Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions to the information system;
c) [AC-17 (3)] Route all remote accesses through a defined number of managed network access control points to the information system as documented in the System Security Plan;
d) [AC-17 (4)(a)] Authorize the execution of privileged commands and access to security-relevant information via remote access only for defined needs;
e) [AC-17 (4)(b)] Document the rationale for such access in the System Security Plan for the information system; and
f) [AC-17 (9)] Provide the capability to expeditiously disconnect or disable remote access to the information system within fifteen (15) minutes.

9.1.5.13 Wireless Access (AC-18)

The System Owner shall:

a) Establish usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
b) Authorize wireless access to the information systems prior to allowing such connections.

[AC-18 (1)] The Architect shall ensure that Infinibyte Cloud systems protect wireless access to the system using authentication of users/devices and encryption.

9.1.5.14 Access Control for Mobile Devices (AC-19)

The System Owner shall:

a) Establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
b) Authorize connection of mobile devices to organizational information systems.

[AC-19 (5)] The Architect shall ensure that Infinibyte Cloud systems employ full disk encryption or container encryption to protect the confidentiality and integrity of information on authorized mobile devices.

9.1.5.15 Use of External Information Systems (AC-20)

The System Owner shall, consistent with any trust relationships, establish terms and conditions with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a) Access the information systems from the external information systems; and
b) Process, store, and/or transmit organization-controlled information using the external information systems.

The ISSO shall ensure that Infinibyte Cloud systems implement the following functions:

a) [AC-20 (1)] Permit authorized individuals to use an external information system to access the information systems or to process, store, or transmit Infinibyte Cloud information only when approved by the System Owner. The ISSO shall:
    i) Verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or
    ii) Retain approved information system connection or processing agreements with the organizational entity hosting the external information system.
b) [AC-20 (2)] Restrict the use of Infinibyte Cloud-controlled portable storage media by individuals on external information systems.

9.1.5.16 Information Sharing (AC-21)

The System Owner and Architect shall:

a) Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for defined information sharing circumstances where user discretion is required; and
b) Employ automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. These mechanisms or processes shall be defined in the System Security Plan.

9.1.5.17 Publicly Accessible Content (AC-22)

The System Owner shall:

a) Designate individuals authorized to post information onto a publicly accessible information system;
b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
c) Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
d) Review the content on the publicly accessible information system for nonpublic information at least quarterly and remove such information, if found.

9.1.6 Access Control Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.2 Security Awareness and Training Policy (AT-1)

9.2.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Security Awareness and Training security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.2.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Security Awareness and Training (AT) security control family.

9.2.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Security Awareness and Training shall be applied:

a) The System Owner shall:

   i) Ensure that the security awareness and training program is fully resourced.

b) The ISSO shall:

   i) Establish overall strategy for the security awareness and training program;
   ii) Ensure that the System Owner understands the concepts and strategy of the security awareness and training program, and is informed of the progress of the program's implementation;
   iii) Ensure that the security trainers or security/subject matter professionals understand the Security Assessment and Authorization process so that they can develop appropriate training materials and incorporate Security Assessment and Authorization into training programs to educate the end users;
   iv) Ensure the training organization personnel understand their security training responsibilities;
   v) Ensure that security awareness and training material developed is appropriate and timely for the intended audiences;
   vi) Ensure that security awareness and training material is effectively deployed to reach the intended audience;
   vii) Ensure that users have an effective way to provide feedback on the security awareness and training material and its presentation;
   viii) Ensure that security awareness and training material is reviewed periodically and updated when necessary;

ix) Ensure that all users are sufficiently trained in their security responsibilities; and

x) Ensure that effective security training tracking and reporting mechanisms are in place.

c) Infinibyte Cloud Managers shall:

i) Work with the ISSO to meet shared responsibilities;

ii) Consider developing individual development plans for users in roles with significant security responsibilities;

iii) Promote the professional development and certification of the program staff, full-time or part-time security officers, and others with significant security responsibilities;

iv) Ensure that all users (including contractors) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access;

v) Ensure that users (including contractors) understand specific rules of each system and application they use; and

vi) Work to reduce errors and omissions by users due to lack of awareness and/or training.

d) DLH employees, contractors, consultants and others to whom access is granted shall:

i) Understand and comply with organization security policies and procedures;

ii) Be appropriately trained in the rules of behavior for the systems and applications to which they have access;

iii) Work with management to meet their training needs; and

iv) Be aware of actions they can take to better protect their organization's information. These actions include, but are not limited to: proper password usage, reporting any suspected incidents or violations of security policy, and following rules to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.

9.2.4 Applicable Documents

The documents that are applicable to the Security Awareness and Training policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.2.5 Security Awareness and Training Policy Requirements

The following table identifies the DLH security awareness and training policies that are contained in this Section.

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
AT-2	**Security Awareness Training**	**9.2.5.1**
AT-2 (2)	*SECURITY AWARENESS | INSIDER THREAT*	*9.2.5.1*
AT-3	**Role-Based Security Training**	**9.2.5.2**
AT-4	**Security Training Records**	**9.2.5.3**

9.2.5.1 Security Awareness Training (AT-2)

Basic security awareness training shall be provided to all information system users (including managers, senior executives, and contractors) with a system level account:

a) As part of initial training for new users;
b) When required by system changes; and
c) At least annually thereafter.

Customers are responsible for ensuring that all users of Infinibyte Cloud systems have completed security awareness training in accordance with their organization or Agency's policy.

[AT-2 (2)] DLH basic security awareness training shall also include security awareness training on recognizing and reporting indicators of insider threat.

9.2.5.2 Role-Based Security Training (AT-3)

Role-based security training shall be provided to personnel with assigned security roles and responsibilities:

a) Before authorizing access to the system or performing assigned duties;
b) When required by system changes; and
c) At least annually thereafter.

9.2.5.3 Security Training Records (AT-4)

The DLH Human Resources Department shall:

a) Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and
b) Retain individual training records for a minimum of one (1) year.

9.2.6 Security Awareness and Training Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.3 Audit and Accountability Policy (AU-1)

9.3.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Audit and Accountability security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.3.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Audit and Accountability (AU) security control family.

9.3.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Audit and Accountability shall be applied:

a) The Architect shall be responsible for ensuring that all technical design functions identified in the policy are incorporated into Infinibyte Cloud systems that process U.S. Government information.

b) The IT Director shall be responsible for ensuring that all system security functions for protecting U.S. Government information are operated in accordance with this policy.

c) Privileged Users shall have the primary responsibility for implementing proper audit and accountability policies on their respective systems.

9.3.4 Applicable Documents

The documents that are applicable to the Audit and Accountability policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.3.5 Audit and Accountability Policy Requirements

The following table identifies the Infinibyte Cloud audit and accountability policies that are contained in this Section.

FAMILY: AUDIT AND ACCOUNTABILITY (AU-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
AU-2	**Audit Events**	**9.3.5.1**
AU-2 (3)	*AUDIT EVENTS | REVIEWS AND UPDATES*	*9.3.5.1*
AU-3	**Content of Audit Records**	**9.3.5.2**
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*	*9.3.5.2*
AU-4	**Audit Storage Capacity**	**9.3.5.3**
AU-5	**Response to Audit Processing Failures**	**9.3.5.4**
AU-6	**Audit Review, Analysis, and Reporting**	**9.3.5.5**
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*	*9.3.5.5*
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*	*9.3.5.5*
AU-7	**Audit Reduction and Report Generation**	**9.3.5.6**
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*	*9.3.5.6*
AU-8	**Time Stamps**	**9.3.5.7**
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*	*9.3.5.7*
AU-9	**Protection of Audit Information**	**9.3.5.8**
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*	*9.3.5.8*
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*	*9.3.5.8*
AU-11	**Audit Record Retention**	**9.3.5.9**
AU-12	**Audit Generation**	**9.3.5.10**

9.3.5.1 Audit Events (AU-2)

The System Owner, in conjunction with the Architect and ISSO, shall:

a) Determine that the information system is capable of auditing the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege use, process tracking, and system events; For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes;
b) Coordinate the security audit function requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
c) Provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d) Determine continually, that the following events are audited within the information system: successful and unsuccessful account logon events, account management events, object access, privilege functions, permission changes, and system events.

[AU-2 (3)] The System Owner, in conjunction with the Architect and ISSO, shall also review and update the list of auditable events at least annually or whenever there is a change in the threat environment.

9.3.5.2 Content of Audit Records (AU-3)

The ISSO shall ensure that Infinibyte Cloud systems generate audit records containing information that establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

[AU-3 (1)] The Architect and ISSO shall also ensure that Infinibyte Cloud systems generate audit records containing the following additional information:

a) Session, connection, transaction, or activity duration;
b) For client-server transactions, the number of bytes received and bytes sent. This gives bidirectional transfer information that can be helpful during an investigation or inquiry;
c) For client-server transactions, unique metadata or properties about the client initiating the transaction. This could include properties such as an IP address, user name, session identifier or browser characteristics (e.g., a 'User-Agent' string);
d) Details regarding the event 'type': the type of method or action;
e) Characteristics that describe or identify the object or resource being acted upon; and/or
f) Additional informational messages to diagnose or identify the event.

9.3.5.3 Audit Storage Capacity (AU-4)

The Architect and ISSO shall ensure that Infinibyte Cloud systems allocate audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded. The amount of audit storage capacity shall be documented in the System Security Plan.

9.3.5.4 Response to Audit Processing Failures (AU-5)

The IT Director and Architect shall ensure that Infinibyte Cloud systems perform the following actions in the event of an audit processing failure:

a) Alert the ISSO, Security Administrator, Security Auditor, and/or appropriate System Administrators; and
b) Overwrite the oldest audit record or shut down the failed information system component.

9.3.5.5 Audit Review, Analysis, and Reporting (AU-6)

The ISSO and Security Auditor shall:

a) Review and analyze information system audit records at least weekly for indications of inappropriate or unusual activity;
b) Report findings to the System Owner and IT Director.

c) Review available audit storage capacity at least monthly and recommend action to modify available capacity when defined bounds are exceeded; and

[AU-6 (1)] The Architect shall also ensure that Infinibyte Cloud systems employ automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

[AU-6 (3)] The Security Auditor shall analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

9.3.5.6 Audit Reduction and Report Generation (AU-7)

The Architect and ISSO shall ensure that Infinibyte Cloud systems provide an audit reduction and report generation capability that:

a) Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
b) Does not alter the original content or time ordering of audit records.

[AU-7 (1)] The Architect and ISSO shall also ensure that Infinibyte Cloud systems provide the capability to process audit records for events of interest based on specific fields within the audit records defined previously in Section 9.3.5.2 (Content of Audit Records).

9.3.5.7 Time Stamps (AU-8)

The Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Use internal system clocks to generate time stamps for audit records;
b) Record time stamps for audit records in Coordinated Universal Time (UTC); and
c) Meet a one (1) second granularity of time measurement.

[AU-8 (1)] The Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Compare the internal information system clocks at least hourly with an authorized time source that is synchronized to a NIST time source;
b) Re-synchronize the internal system clocks to the authoritative time source when the internal clock differs from the Network Time Protocol (NTP) source by more than one (1) minute;
c) Synchronize to a primary and a secondary time source that are in different geographic regions; and
d) If using Windows Active Directory, all servers shall synchronize time with the time source for the Windows Domain Controller.

9.3.5.8 Protection of Audit Information (AU-9)

The ISSO shall ensure that Infinibyte Cloud systems protect audit information and audit tools from unauthorized access, modification, and deletion.

The ISSO shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [AU-9 (2)] Back up audit records at least weekly onto a physically different system or media than the system being audited; and
b) [AU-9 (4)] Authorize management of audit functionality to only the Security Administrator, Security Auditor and ISSO roles.

9.3.5.9 Audit Record Retention (AU-11)

The ISSO shall ensure that audit records for Infinibyte Cloud systems are retained for a minimum of ninety (90) days online and archived off-line for a period of not less than 180 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

9.3.5.10 Audit Generation (AU-12)

The Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Generate audit records for auditable events on all information system components capable of generating audit records;
b) Only allow the Architect, ISSO, System Owner and Security Auditor to select which auditable events are audited by specific components of the information system; and
c) Generate audit records for the Infinibyte Cloud system's auditable events defined previously in Section 9.3.5.1(d) (Audit Events) with the content defined previously in Section 9.3.5.2 (Content of Audit Records).

9.3.6 Audit and Accountability Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.4 Security Assessment and Authorization (CA-1)

9.4.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Security Assessment and Authorization security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.4.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Security Assessment and Authorization (CA) security control family.

9.4.3 Roles and Responsibilities

Security roles and responsibilities are identified in Section 1.3 (Roles and Responsibilities) of this document.

9.4.4 Applicable Documents

The documents that are applicable to the Security Assessment and Authorization policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.4.5 Security Assessment and Authorization Policy Requirements

The following table identifies the Infinibyte Cloud security assessment and authorization policies that are contained in this Section.

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION (CA-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CA-2	**Security Assessments**	**9.4.5.1**
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*	*9.4.5.1*
CA-2 (2)	*SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS*	*9.4.5.1*
CA-2 (3)	*SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS*	*9.4.5.1*
CA-3	**System Interconnections**	**9.4.5.2**
CA-3 (3)	*SYSTEM INTERCONNECTIONS | UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS*	*9.4.5.2*
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*	*9.4.5.2*
CA-5	**Plan of Action and Milestones**	**9.4.5.3**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CA-6	**Security Authorization**	**9.4.5.4**
CA-7	**Continuous Monitoring**	**9.4.5.5**
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*	*9.4.5.5*
CA-8	**Penetration Testing**	**9.4.5.6**
CA-8 (1)	*PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM*	*9.4.5.6*
CA-9	**Internal System Connections**	**9.4.5.7**

9.4.5.1 Security Assessments (CA-2)

The ISSO shall ensure that assessments are conducted on Infinibyte Cloud systems using the following process:

a) Develop a security assessment plan that describes the scope of the assessment including:
    i) Security controls and control enhancements under assessment;
    ii) Assessment procedures to be used to determine security control effectiveness; and
    iii) Assessment environment, assessment team, and assessment roles and responsibilities.
b) Assess the security controls in the Infinibyte Cloud system at least annually to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements. Annual security control assessments should be planned to ensure that all security controls are fully evaluated every three years;
c) Produce a security assessment report that documents the results of the assessment; and
d) Provide the results of the security assessment, in writing, to the FedRAMP Program Management Office (PMO) and/or Authorizing Official (or the Authorizing Official's designated representative), as applicable.

The ISSO shall also ensure that Infinibyte Cloud systems implement the following functions:

a) [CA-2 (1)] Employ a FedRAMP Third Party Assessment Organization (3PAO) assessor or an independent assessment team to conduct security control assessments;
b) [CA-2 (2)] Include as part of security control assessments, at least annually announced in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; or other System Owner defined forms of security assessment; and
c) [CA-2 (3)] Accept the results of an assessment that was performed by any FedRAMP Accredited 3PAO, an Authorizing Official-approved independent assessor or when the assessment meets the conditions of the FedRAMP Joint Authorization Board (JAB)/Authorizing Official in the FedRAMP Repository.

9.4.5.2 System Interconnections (CA-3)

The System Owner shall:

a) Authorize connections from the information system to other information systems through the use of Interconnection Security Agreements;
b) Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
c) Review and update Interconnection Security Agreements at least annually and on input from the FedRAMP Program Management Office or Authorizing Official.

The System Owner shall also:

a) [CA-3 (3)] Prohibit the direct connection of unclassified, non-national security systems to an external network without the use of Boundary Protections which meet Trusted Internet Connection (TIC) requirements as defined in Appendix H – Cloud Considerations of the TIC 2.0 Reference Architecture document; and

b) [CA-3 (5)] Ensure that a deny-all, permit-by-exception policy is employed for allowing Infinibyte Cloud systems to connect to any external information system.

9.4.5.3 Plan of Action and Milestones (CA-5)

The ISSO shall:

a) Develop a plan of action and milestones for the Infinibyte Cloud 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; and

b) Update the plan of action and milestones at least monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

9.4.5.4 Security Authorization (CA-6)

The System Owner shall:

a) Identify a senior-level Government executive or manager to act as the Authorizing Official for the Infinibyte Cloud system;
b) Ensure that the Authorizing Official authorizes the Infinibyte Cloud system for processing before commencing operations; and
c) Update the security authorization in accordance with OMB A-130 requirements or when a significant change occurs.

9.4.5.5 Continuous Monitoring (CA-7)

The System Owner, in conjunction with the ISSO, shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes:

a) Establishment of defined metrics to be monitored;
b) Establishment of a defined frequency for monitoring and defined frequency for assessments supporting such monitoring;
c) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
d) Ongoing security status monitoring of defined metrics in accordance with the organizational continuous monitoring strategy;
e) Correlation and analysis of security-related information generated by assessments and monitoring;
f) Response actions to address results of the analysis of security-related information; and
g) Reporting the security status of the Infinibyte Cloud system to meet FedRAMP requirements at least monthly.

[CA-7 (1)] In addition, the System Owner shall employ assessors or assessment teams with a defined level of independence to monitor the security controls in their Infinibyte Cloud system(s) on an ongoing basis.

9.4.5.6 Penetration Testing (CA-8)

The System Owner shall ensure that penetration testing is conducted at least annually on their Infinibyte Cloud system(s).

[CA-8 (1)] An independent penetration agent or penetration team shall perform penetration testing on their Infinibyte Cloud system(s) or system components at least annually.

9.4.5.7 Internal System Connections (CA-9)

The System Owner shall:

a) Authorize internal connections for all in-boundary information system components or classes of components to the information system; and
b) Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

9.4.6 Security Assessment and Authorization Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.5 Configuration Management Policy (CM-1)

9.5.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Configuration Management security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.5.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Configuration Management (CM) security control family.

9.5.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Configuration Management shall be applied:

a) The System Owner and ISSO shall implement and follow a configuration and change management program for all assigned information systems;

b) The System Owner shall designate an individual to act as the Configuration Manager for each Infinibyte Cloud system;

c) The Configuration Manager shall be primarily focused on ensuring accurate and timely availability of configuration information for operational and fiscal use; and

d) The Configuration Manager shall act as an interface to other service delivery partners, ensuring effective integration for the Infinibyte Cloud Configuration Management process.

9.5.4 Applicable Documents

The documents that are applicable to the Configuration Management policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.5.5 Configuration Management Policy Requirements

The following table identifies the Infinibyte Cloud configuration management policies that are contained in this Section.

FAMILY: CONFIGURATION MANAGEMENT (CM-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CM-2	**Baseline Configuration**	**9.5.5.1**
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*	*9.5.5.1*
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*	*9.5.5.1*
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*	*9.5.5.1*
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*	*9.5.5.1*
CM-3	**Configuration Change Control**	**9.5.5.2**
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*	*9.5.5.2*
CM-4	**Security Impact Analysis**	**9.5.5.3**
CM-5	**Access Restrictions for Change**	**9.5.5.4**
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*	*9.5.5.4*
CM-5 (3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*	*9.5.5.4*
CM-5 (5)	*ACCESS RESTRICTIONS FOR CHANGE | LIMIT PRODUCTION / OPERATIONAL PRIVILEGES*	*9.5.5.4*
CM-6	**Configuration Settings**	**9.5.5.5**
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*	*9.5.5.5*
CM-7	**Least Functionality**	**9.5.5.6**
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	*9.5.5.6*
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*	*9.5.5.6*
CM-7 (5)	*LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE / WHITELISTING*	*9.5.5.6*
CM-8	**Information System Component Inventory**	**9.5.5.7**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CM-8 (1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*	*9.5.5.7*
CM-8 (3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*	*9.5.5.7*
CM-8 (5)	*INFORMATION SYSTEM COMPONENT INVENTORY | NO DUPLICATE ACCOUNTING OF COMPONENTS*	*9.5.5.7*
CM-9	**Configuration Management Plan**	**9.5.5.8**
CM-10	**Software Usage Restrictions**	**9.5.5.9**
CM-10 (1)	*SOFTWARE USAGE RESTRICTIONS | OPEN SOURCE SOFTWARE*	*9.5.5.9*
CM-11	**User-Installed Software**	**9.5.5.10**

9.5.5.1 Baseline Configuration (CM-2)

The System Owner shall ensure that a current baseline configuration for the information system is developed, documented and maintained under configuration control.

The System Owner shall also:

a) [CM-2 (1)] Review and update the baseline configuration of the information system:
   i) At least annually;
   ii) When required due to significant change as defined in NIST SP 800-37 or when directed by the FedRAMP JAB or Authorizing Official; and
   iii) As an integral part of information system component installations and upgrades.
b) [CM-2 (2)] Ensure that automated mechanisms are employed to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system;
c) [CM-2 (3)] Ensure that at least one (1) older version of baseline configurations is retained as deemed necessary to support rollback;
d) [CM-2 (7)(a)] Issue defined information systems, system components, or devices with defined configurations to individuals traveling to locations that the organization deems to be of significant risk; and
e) [CM-2 (7)(b)] Ensure that defined security safeguards are applied to the devices when the individuals return.

9.5.5.2 Configuration Change Control (CM-3)

The ISSO and Configuration Manager shall:

a) Determine the types of changes to the information systems that are configuration controlled;
b) Review proposed configuration-controlled changes to the information system and approve or disapprove such changes with explicit consideration for security impact analyses;
c) Document configuration change decisions associated with the information system;
d) Implement approved configuration-controlled changes to the information system;
e) Retain records of configuration-controlled changes to the information system for one (1) year or two (2) change cycles of baseline configurations, whichever is greater;
f) Audit and review activities associated with configuration-controlled changes to the information system; and
g) Coordinate and provide oversight for configuration change control activities through the Change Control Board (CCB) that convenes as required.

9.5.5.3 Security Impact Analysis (CM-4)

The System Owner and ISSO, with assistance from the Security Administrators, shall analyze changes to the information system to determine potential security impacts prior to change implementation.

9.5.5.4 Access Restrictions for Change (CM-5)

The System Owner shall ensure that physical and logical access restrictions associated with changes to the information system are defined, documented, approved, and enforced.

The ISSO shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [CM-5 (1)] Enforce access restrictions and supports auditing of the enforcement actions; and
b) [CM-5 (3)] Prevent the installation of any software and firmware components without verification that the component has been digitally signed using a digital certificate or hash verification that is recognized and approved by the System Owner.

The ISSO shall also:

a) [CM-5 (5)(a)] Ensure that privileges to change information system components and system-related information are limited within a production or operational environment to only authorized privileged users who authenticate via a Virtual Private Network (VPN) or other secure connection using two factor authentication; and

b) [CM-5 (5)(b)] Review and reevaluate privileges at least quarterly.

9.5.5.5 Configuration Settings (CM-6)

The System Owner shall:

a) Establish and document mandatory configuration settings for IT products employed within the information systems using Center for Internet Security guidelines (where applicable), DoD Security Technical Implementation Guidance, Infinibyte Cloud baseline configuration settings, or industry best practice guidelines in hardening their systems, that reflect the most restrictive mode consistent with operational requirements;
b) Ensure that the configuration settings are implemented;
c) Identify, document, and approve deviations from established configuration settings for all configuration items based on Change Control Board approved changes; and
d) Monitor and control changes to the configuration settings in accordance with the Infinibyte Cloud system's Configuration Management Plan.

[CM-6 (1)] The ISSO shall ensure that Infinibyte Cloud systems also implement automated mechanisms to centrally manage, apply, and verify configuration settings for all configuration items.

9.5.5.6 Least Functionality (CM-7)

The ISSO shall ensure that Infinibyte Cloud systems are configured to:

a) Provide only essential capabilities; and
b) Prohibit or restrict the use of functions, ports, protocols, and/or services prohibited or restricted by the United States Government Configuration Baseline (USGCB), Center for Internet Security, DoD Security Technical Implementation Guidance or Infinibyte Cloud baseline configuration settings.

The ISSO and Configuration Manager shall:

a) [CM-7 (1)(a)] Review the information system at least monthly to identify unnecessary and/or non-secure functions, ports, protocols, and services;
b) [CM-7 (1)(b)] Ensure that defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure are disabled;
c) [CM-7 (5)(a)] Identify all software programs not authorized to execute on the information system; and
d) [CM-7 (5)(c)] Review and update the list of authorized software programs at least annually or when there is a change.

The ISSO shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [CM-7 (2)] Prevent program execution in a technical manner, so as to only allow programs that adhere to policy to run (i.e., white listing); and
b) [CM-7 (5)(b)] Employ a deny-all, permit-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

9.5.5.7 Information System Component Inventory (CM-8)

The ISSO and Configuration Manager shall, for each Infinibyte Cloud system:

a) Develop and document an inventory of information system components that:
    i) Accurately reflects the current information system;
    ii) Includes all components within the authorization boundary of the information system;
    iii) Is at the level of granularity deemed necessary for tracking and reporting; and
    iv) Includes information deemed necessary to ensure property accountability such as hardware inventory specifications (e.g., manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address.
b) Review and update the information system component inventory at least monthly or following any change.

[CM-8 (1)] The Configuration Manager shall also update the inventory of Infinibyte Cloud system components as an integral part of component installations, removals, and information system updates.

Additionally, the ISSO shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [CM-8 (3)(a)] Employ automated mechanisms continuously, using automated mechanisms with a maximum of a five-minute delay in detection to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
b) [CM-8 (3)(b)] Disable network access and/or isolate components when unauthorized components are detected.
c) [CM-8 (3)(b)] Notify the appropriate Infinibyte Cloud System Administrator when a component is disabled or isolated.

[CM-8 (5)] The System Owner shall verify that all components within an Infinibyte Cloud system authorization boundary are not duplicated in other information system inventories.

9.5.5.8 Configuration Management Plan (CM-9)

The ISSO and Configuration Manager shall document and implement a Configuration Management Plan for the information system that:

a) Addresses roles, responsibilities, and configuration management processes and procedures;
b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
c) Defines the configuration items for the information systems and when in the system development life cycle the configuration items are placed under configuration management; and
d) Protects the Configuration Management Plan from unauthorized disclosure and modification.

9.5.5.9 Software Usage Restrictions (CM-10)

The ISSO and Configuration Manager shall:

a) Ensure the use of software and associated documentation in accordance with contract agreements and copyright laws;
b) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

[CM-10 (1)] In addition, the System Owner shall establish and document open source software restrictions.

9.5.5.10 User-Installed Software (CM-11)

The ISSO shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Prohibit the installation of software by users;
b) Enforce software installation policies through user access and privilege restrictions; and
c) Monitor policy compliance continuously.

9.5.6 Configuration Management Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.6 Contingency Planning Policy (CP-1)

9.6.1 Scope

Supporting policy and procedures are provided for each individual security control within the Contingency Planning (CP) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.6.2 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Contingency Planning (CP) security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.6.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Contingency Planning shall be applied:

a) The Contingency Planning Director (CPD) shall be a member of DLH senior management and shall be responsible for all facets of contingency, disaster recovery and incident response planning execution. The CPD shall perform the following Contingency Planning duties:

   i) Make the decision on whether or not to activate the Contingency Plan;
   ii) Provide the initial notification to activate the Contingency Plan;
   iii) Review and approve the Contingency Plan;
   iv) Review and approve the Business Impact Analysis (BIA);
   v) Notify the Contingency Plan Team leads and members as necessary;
   vi) Advise other Contingency Plan Team leads and members as appropriate;
   vii) Issue a recovery declaration statement after the system has returned to normal operations; and
   viii) Designate key contingency planning and recovery personnel.

b) The Contingency Planning Coordinator (CPC) shall lead the day-to-day operation of the Contingency Planning function and shall perform the following Contingency Planning duties:

   i) Develop and document the Contingency Plan under direction of the CPD;
   ii) Create and use the Business Impact Analysis (BIA) to prioritize recovery of components;
   iii) Update the Contingency Plan annually;
   iv) Ensure that annual Contingency Plan training is conducted;
   v) Facilitate periodic Contingency Plan testing exercises;
   vi) Distribute copies of the plan to team members;

vii) Authorize travel and housing arrangements for team members;
viii) Manage and monitor the overall recovery process;
ix) Lead the contingency response effort once the Contingency Plan has been activated;
x) Receive updates and status reports from team members;
xi) Send out communications about the recovery;
xii) Advise the CPD on the recovery status as necessary; and
xiii) Designate key contingency planning personnel.

9.6.4 Applicable Documents

The documents that are applicable to the Contingency Planning policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.6.5 Contingency Planning Policy Requirements

The following table identifies the Infinibyte Cloud contingency planning policies that are contained in this Section.

FAMILY: CONTINGENCY PLANNING (CP-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CP-2	**Contingency Plan**	**9.6.5.1**
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*	*9.6.5.1*
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*	*9.6.5.1*
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*	*9.6.5.1*
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*	*9.6.5.1*
CP-3	**Contingency Training**	**9.6.5.2**
CP-4	**Contingency Plan Testing**	**9.6.5.3**
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*	*9.6.5.3*
CP-6	**Alternate Storage Site**	**9.6.5.4**
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*	*9.6.5.4*
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*	*9.6.5.4*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
CP-7	**Alternate Processing Site**	**9.6.5.5**
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*	*9.6.5.5*
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*	*9.6.5.5*
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*	*9.6.5.5*
CP-8	**Telecommunications Services**	**9.6.5.6**
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*	*9.6.5.6*
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*	*9.6.5.6*
CP-9	**Information System Backup**	**9.6.5.7**
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*	*9.6.5.7*
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*	*9.6.5.7*
CP-10	**Information System Recovery and Reconstitution**	**9.6.5.8**
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*	*9.6.5.8*

9.6.5.1 Contingency Plan (CP-2)

The Contingency Planning Director and Contingency Planning Coordinator shall:

a) Develop a Contingency Plan for the information system that:
   i) Identifies essential missions and business functions and associated contingency requirements;
   ii) Provides recovery objectives, restoration priorities, and metrics;
   iii) Addresses contingency roles, responsibilities and assigned individuals with contact information;
   iv) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

v) Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
vi) Is reviewed and approved by designated officials within the organization;

b) Distribute copies of the Contingency Plan to the Authorizing Official (AO), ISSO (ISSO), Contingency Planning Director (CPD), Contingency Planning Coordinator (CPC) and all applicable personnel identified in the system Contingency Plan;
c) Coordinate contingency planning activities with incident handling activities;
d) Review the Contingency Plan procedures for the information system annually;
e) Update the Contingency Plan to address changes to the organization, information systems, or environment of operation and problems encountered during Contingency Plan implementation, execution, or testing;
f) Communicates Contingency Plan changes to the AO, ISSO, CPD, CPC and all applicable personnel identified in the system Contingency Plan; and
g) Protects the Contingency Plan from unauthorized disclosure and modification.

In addition, the Contingency Planning Coordinator shall:

a) [CP-2 (1)] Coordinate Contingency Plan development with organizational elements responsible for related plans;
b) [CP-2 (2)] Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations;
c) [CP-2 (3)] Plan for the resumption of essential missions and business functions within a time period specified in the system's Contingency Plan and Business Impact Analysis; and
d) [CP-2 (8)] Identify critical information system assets supporting essential missions and business functions.

9.6.5.2 Contingency Training (CP-3)

The Contingency Planning Coordinator shall ensure that contingency training is provided to information system users consistent with their assigned roles and responsibilities:

a) Within ten (10) days of assuming a contingency role or responsibility;
b) When required by information system changes; and
c) At least annually thereafter.

9.6.5.3 Contingency Plan Testing (CP-4)

The Contingency Planning Coordinator shall:

a) Test the Contingency Plan for the information system at least annually using defined tests to determine the effectiveness of the plan and the organizational readiness to execute the plan;
b) Review the Contingency Plan test results; and create a lessons learned document; and
c) Initiate corrective actions, if needed.

[CP-4 (1)] In addition, the Contingency Planning Coordinator shall coordinate Contingency Plan testing with organizational elements responsible for related plans and employ tabletop reviews, operational tests and/or functional exercises (or some combination thereof).

9.6.5.4 Alternate Storage Site (CP-6)

The Contingency Planning Director shall:

a) Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
b) Ensure that the alternate storage site provides information security safeguards equivalent to that of the primary site.

The Contingency Planning Director shall also perform the following actions:

a) [CP-6 (1)] Identify an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats; and
b) [CP-6 (3)] Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline- explicit mitigation actions.

9.6.5.5 Alternate Processing Site (CP-7)

The Contingency Planning Director shall:

a) Establish an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the customer required time period (as described in the Business Impact Analysis), when the primary processing capabilities are unavailable;
b) Ensure that equipment and supplies required to resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
c) Ensure that the alternate processing site provides information security safeguards equivalent to that of the primary site.

The Contingency Planning Director shall also perform the following actions:

a) [CP-7 (1)] Identify an alternate processing site that is separated from the primary processing site to reduce the susceptibility to the same threats;
b) [CP-7 (2)] Identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions; and
c) [CP-7 (3)] Develop alternate processing site agreements that contain priority-of-service provisions in accordance with organization's availability requirements (including recovery time objectives).

9.6.5.6 Telecommunications Services (CP-8)

The Contingency Planning Director shall ensure that the Service Provider that hosts Infinibyte Cloud systems establishes alternate telecommunications services, including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the timelines prescribed in the Business Impact Analysis, when the primary telecommunications capabilities are unavailable.

The Contingency Planning Director Coordinator shall also ensure that the System Hosting Provider:

a) [CP-8 (1)(a)] Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the timelines prescribed in the Business Impact Analysis (including recovery time objectives);
b) [CP-8 (1)(b)] Requests Telecommunications Service Priority for all telecommunications services used for national security/emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier; and
c) [CP-8 (2)] Obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

9.6.5.7 Information System Backup (CP-9)

The Contingency Planning Coordinator shall ensure that personnel operating Infinibyte Cloud systems processing U.S. Government information:

a) Conduct incremental backups daily with full weekly backups of user-level information contained in the information system consistent with recovery time and recovery point objectives;
b) Conduct incremental backups daily with full weekly backups of system-level information contained in the information system consistent with recovery time and recovery point objectives;

c) Conduct incremental backups daily with full weekly backups of information systems documentation including security-related documentation consistent with recovery time and recovery point objectives; and
d) Protect the confidentiality and integrity of backup information at the storage location.

In addition, the Contingency Planning Coordinator shall ensure that personnel operating Infinibyte Cloud systems processing U.S. Government information:

a) [CP-9 (1)] Test backup information at least annually to verify media reliability and information integrity; and
b) [CP-9 (3)] Store backup copies of the operating system and other critical information system software, as well as copies of data and the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.

9.6.5.8 Information System Recovery and Reconstitution (CP-10)

The Contingency Planning Coordinator and ISSO shall ensure that Infinibyte Cloud systems provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

[CP 10 (2)] The Contingency Planning Coordinator and ISSO shall also ensure that Infinibyte Cloud systems implement transaction recovery for information systems that are transaction-based.

9.6.6 Contingency Planning Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.7 Identification and Authentication Policy (IA-1)

9.7.1 Scope

This Section provides supporting policy and procedures for each individual security control within the Identification and Authentication (IA) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.7.2 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Identification and Authentication security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.7.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Identification and Authentication shall be applied:

a) The Architect shall be responsible for ensuring that all technical design functions identified in the policy are incorporated into Infinibyte Cloud systems that process U.S. Government information.

b) The IT Director shall be responsible for ensuring that all system security functions for protecting U.S. Government information are operated in accordance with this policy.

9.7.4 Applicable Documents

The documents that are applicable to the Identification and Authentication policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.7.5 Identification and Authentication Policy Requirements

The following table identifies the Infinibyte Cloud identification and authentication policies that are contained in this Section.

FAMILY: IDENTIFICATION AND AUTHENTICATION (IA-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
IA-2	**Identification and Authentication (Organizational Users)**	**9.7.5.1**
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*	*9.7.5.1*
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*	*9.7.5.1*
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*	*9.7.5.1*
IA-2 (5)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION*	*9.7.5.1*
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*	*9.7.5.1*
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE*	*9.7.5.1*
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PERSONAL IDENTITY VERIFICATION (PIV) CREDENTIALS*	*9.7.5.1*
IA-3	**Device Identification and Authentication**	**9.7.5.2**
IA-4	**Identifier Management**	**9.7.5.3**
IA-4 (4)	*IDENTIFIER MANAGEMENT | IDENTIFY USER STATUS*	*9.7.5.3*
IA-5	**Authenticator Management**	**9.7.5.4**
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	*9.7.5.4*
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PUBLIC KEY INFRASTRUCTURE (PKI)-BASED AUTHENTICATION*	*9.7.5.4*
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION*	*9.7.5.4*
IA-5 (4)	*AUTHENTICATOR MANAGEMENT | AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION*	*9.7.5.4*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
IA-5 (6)	*AUTHENTICATOR MANAGEMENT | PROTECTION OF AUTHENTICATORS*	*9.7.5.4*
IA-5 (7)	*AUTHENTICATOR MANAGEMENT | NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATION*	*9.7.5.4*
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*	*9.7.5.4*
IA-6	**Authenticator Feedback**	**9.7.5.5**
IA-7	**Cryptographic Module Authentication**	**9.7.5.6**
IA-8	**Identification and Authentication (Non-Organizational Users)**	**9.7.5.7**
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*	*9.7.5.7*
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*	*9.7.5.7*
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*	*9.7.5.7*
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*	*9.7.5.7*

9.7.5.1 Identification and Authentication (Organizational Users) (IA-2)

The Architect shall ensure that Infinibyte Cloud systems uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

The Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [IA-2 (1)] Implement multifactor authentication for network access to privileged accounts;
b) [IA-2 (2)] Implement multifactor authentication for network access to non-privileged accounts;

c) [IA-2 (3)] Implement multifactor authentication for local access to privileged accounts;
d) [IA-2 (5)] Require individuals to be authenticated with an individual authenticator when a group authenticator is employed;
e) [IA-2 (8)] Implement replay-resistant authentication mechanisms for network access to privileged accounts;
f) [IA-2 (11)] Implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets defined strength of mechanism requirements as specified in control enhancement IA-2(11) in the System Security Plan; and
g) [IA-2 (12)] Accept and electronically verify Personal Identity Verification (PIV) credentials.

9.7.5.2 Device Identification and Authentication (IA-3)

The Architect shall ensure that Infinibyte Cloud systems uniquely identify and authenticate all access to virtual systems and devices in the security authorization boundary before establishing a remote connection.

9.7.5.3 Identifier Management (IA-4)

The ISSO shall ensure that Infinibyte Cloud system identifiers for users and devices are managed by:

a) Receiving authorization from the System Owner or IT Director to assign a user or device identifier;
b) Selecting an identifier that uniquely identifies an individual or device;
c) Assigning the user identifier to the intended party or the device identifier to the intended device;
d) Preventing reuse of user or device identifiers for at least two (2) years; and
e) Disabling the user identifier after ninety (90) days or inactivity for user level accounts or following a manual review by the ISSO.

[IA-4 (4)] The Architect and ISSO shall also ensure that Infinibyte Cloud system individual identifiers uniquely identify each individual in accordance with their appropriate affiliation (i.e., contractor or foreign national).

9.7.5.4 Authenticator Management (IA-5)

The Architect and ISSO shall ensure that Infinibyte Cloud system authenticators are properly managed by:

a) Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;
b) Establishing initial authenticator content for authenticators defined by the organization;
c) Ensuring that authenticators have sufficient strength of mechanism for their intended use;
d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
e) Changing default content of authenticators upon information systems installation;
f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);
g) Changing/refreshing authenticators at least every sixty (60) days for password-based authenticators;
h) Protecting authenticator content from unauthorized disclosure and modification;
i) Requiring individuals to take, and having devices implement, security safeguards to protect authenticators; and
j) Change authenticators for group/role accounts when membership to those accounts changes.

The Architect and ISSO shall also ensure that, for password-based authentication, Infinibyte Cloud systems meet the following requirements:

a) [IA-5 (1)(a)] Enforce a minimum password complexity of twelve (12) characters and must contain at least one (1) each of upper-case letters, lower-case letters, numbers, and special characters*;*
b) [IA-5 (1)(b)] Enforce a minimum of one (1) character change or as many as required by the system, when new passwords are created;
c) [IA-5 (1)(c)] Encrypt passwords in storage and in transmission;
d) [IA-5 (1)(d)] Enforce password minimum and maximum lifetime restrictions of one (1) day minimum, sixty (60) days maximum;
e) [IA-5 (1)(e)] Prohibit password reuse for twenty-four (24) passwords remembered; and
f) [IA-5 (1)(f)] Allow the use of a temporary password for system logons with an immediate change to a permanent password.

The Architect and ISSO shall ensure that, for PKI-based authentication, Infinibyte Cloud systems meet the following requirements:

a) [IA-5 (2)(a)] Validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
b) [IA-5 (2)(b)] Enforce authorized access to the corresponding private key;
c) [IA-5 (2)(c)] Map the authenticated identity to the account of the individual or group; and

d) [IA-5 (2)(d)] Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

Additionally, the Architect and ISSO shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [IA-5 (3)] Require that the registration process to receive all hardware/biometric multifactor authenticators be conducted in person before a designated registration authority with authorization by the System Owner;
b) [IA-5 (4)] Employ automated tools to determine if password authenticators are sufficiently strong to satisfy requirements set by the System Owner. If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms are used to audit the strength of created password authenticators;
c) [IA-5 (6)] Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access;
d) [IA-5 (7)] Ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys; and
e) [IA-5 (11)] Employ mechanisms for hardware token-based authentication that satisfy token quality requirements defined by the System Owner.

9.7.5.5 Authenticator Feedback (IA-6)

The Architect and ISSO shall ensure that Infinibyte Cloud systems obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

9.7.5.6 Cryptographic Module Authentication (IA-7)

The Architect shall ensure that Infinibyte Cloud systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

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

The Architect and ISSO shall ensure that Infinibyte Cloud systems uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).

[IA-8 (1), IA-8 (2), IA-8 (3), IA-8 (4)] The Architect shall also ensure that Infinibyte Cloud systems accept and verify a client Agency's Personal Identity Verification (PIV) credentials based on Federal Identity, Credential, and Access Management (FICAM) profile requirements.

9.7.6 Identification and Authentication Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.8 Incident Response Policy (IR-1)

9.8.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Incident Response security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.8.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Incident Response (IR) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.8.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Incident Response shall be applied:

a) The Contingency Planning Director (CPD) is a member of DLH senior management and shall be responsible for all facets of contingency, disaster recovery and incident response planning execution. The CPD shall perform the following incident response duties:

   i) Maintain the incident response policy;
   ii) Review and approve the Incident Response Plan;
   iii) Review and approve other incident response related procedures;
   iv) Notify the Contingency/Incident Response Team leads and members as necessary;
   v) Advise other Contingency/Incident Response Team leads and members as appropriate;
   vi) Issue a recovery declaration statement after the incident has been resolved and the system has returned to normal operations; and
   vii) Designate the Contingency Planning Coordinator and other key personnel.

b) The Contingency Planning Coordinator (CPC) shall lead the day-to-day operation of the Incident Response function and shall perform the following incident response duties:

   i) Develop and document the Incident Response Plan under direction of the CPD;
   ii) Update the Incident Response Plan annually;
   iii) Ensure that annual incident response training is conducted;
   iv) Facilitate periodic incident response testing exercises;

v) Distribute copies of the Incident Response Plan to incident response team members;
vi) Coordinate incident response activities with the applicable System Hosting Provider(s);
vii) Authorize travel and housing arrangements for team members, if required;
viii) Manage and monitor the overall incident response process;
ix) Receive updates and status reports from team members;
x) Send out communications about the response and recovery;
xi) Report updates, status, and recommendations to the CPC; and
xii) Designate key incident response personnel.

c) The ISSO shall be responsible for working with the CPD and CPC to prepare and implement computer security incident response policies and procedures. The ISSO shall also be responsible for the regular audits and vulnerability scans required in accordance with the requirements documented in the System Security Plan. When requested by the Contingency Planning Director or Contingency Planning Coordinator, the ISSO shall perform the following incident response duties:

i) Provide technical advice, assistance, and aid in incident investigation and recovery;
ii) Make notifications to Agency Points of Contact (POC) as required;
iii) Work with the Contingency Planning Coordinator, Infinibyte Cloud System Administrators and users to formulate an initial response;
iv) Provide updates and incident follow-up as needed to the POCs and the DLH management team; and
v) Ensure adequate documentation of all reported computer security incidents and events.

9.8.4 Applicable Documents

The documents that are applicable to the Incident Response policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.8.5 Incident Response Policy Requirements

The following table identifies the Infinibyte Cloud incident response policies that are contained in this Section.

FAMILY: INCIDENT RESPONSE (IR-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
IR-2	**Incident Response Training**	**9.8.5.1**
IR-3	**Incident Response Testing**	**9.8.5.2**
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*	*9.8.5.2*
IR-4	**Incident Handling**	**9.8.5.3**
IR-5	**Incident Monitoring**	**9.8.5.4**
IR-6	**Incident Reporting**	**9.8.5.5**
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*	*9.8.5.5*
IR-7	**Incident Response Assistance**	**9.8.5.6**
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*	*9.8.5.6*
IR-7 (2)	*INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*	*9.8.5.6*
IR-8	**Incident Response Plan**	**9.8.5.7**
IR-9	**Information Spillage Response**	**9.8.5.8**
IR-9 (1)	*INFORMATION SPILLAGE RESPONSE | RESPONSIBLE PERSONNEL*	*9.8.5.8*
IR-9 (2)	*INFORMATION SPILLAGE RESPONSE | TRAINING*	*9.8.5.8*
IR-9 (3)	*INFORMATION SPILLAGE RESPONSE | POST-SPILL OPERATIONS*	*9.8.5.8*
IR-9 (4)	*INFORMATION SPILLAGE RESPONSE | EXPOSURE TO UNAUTHORIZED PERSONNEL*	*9.8.5.8*

9.8.5.1 Incident Response Training (IR-2)

The Contingency Planning Coordinator shall provide incident response training to information system users consistent with assigned roles and responsibilities:

a) Within ten (10) days of assuming an incident response role or responsibility;
b) When required by information system changes; and
c) At least annually thereafter.

9.8.5.2 Incident Response Testing (IR-3)

The Contingency Planning Coordinator shall test and/or exercise the incident response capability for the information system annually using a combination of tabletop reviews, operational tests, and/or functional exercises to determine the incident response effectiveness and document the results.

[IR-3 (2)] The Contingency Planning Coordinator shall coordinate incident response testing with organizational elements responsible for related plans to include the Authorizing Official, the System Hosting Provider and the IT Director.

9.8.5.3 Incident Handling (IR-4)

The Contingency Planning Coordinator, System Owner, and ISSO shall:

a) Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
b) Coordinate incident handling activities with contingency planning activities; and
c) Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

[IR-4 (1)] The ISSO shall ensure that Infinibyte Cloud systems employ automated mechanisms to support the incident handling process.

9.8.5.4 Incident Monitoring (IR-5)

The ISSO shall ensure that Infinibyte Cloud systems track and document information system security incidents on an ongoing basis.

9.8.5.5 Incident Reporting (IR-6)

The ISSO and Contingency Planning Director shall:

a) Require personnel to report suspected security incidents to the ISSO and Contingency Planning Director immediately; and
b) Report security incident information to according to US-CERT Federal Incident Notification Guidelines, the FedRAMP Incident Communications Procedure or other contractual requirements, as specified in the Infinibyte Cloud Incident Response Plan.

[IR-6 (1)] The ISSO shall ensure that Infinibyte Cloud systems employ automated mechanisms to support the reporting of security incidents.

9.8.5.6 Incident Response Assistance (IR-7)

The Contingency Planning Coordinator and ISSO shall serve as an incident response support resource, integral to the Infinibyte Cloud incident response capability and offer advice and assistance to users of the information systems for the handling and reporting of security incidents.

[IR-7 (1)] The ISSO shall also ensure that Infinibyte Cloud systems employ automated mechanisms to increase the availability of incident response-related information and support.

The Contingency Planning Coordinator shall also:

a) [IR-7 (2)(a)] Establish a direct, cooperative relationship between its response capability and external providers of information system protection capability; and
b) [IR-7 (2)(b)] Identify organizational incident response team members to the external providers.

9.8.5.7 Incident Response Plan (IR-8)

The Contingency Planning Director, Contingency Planning Coordinator and ISSO shall:

a) Develop an Incident Response Plan that:
    i) Provides the organization with a roadmap for implementing its incident response capability;
    ii) Describes the structure and organization of the incident response capability;
    iii) Provides a high-level approach for how the incident response capability fits into the overall organization;
    iv) Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
    v) Defines reportable incidents;
    vi) Provides metrics for measuring the incident response capability within the organization;
    vii) Defines the resources and management support needed to effectively maintain and mature an incident response capability; and

viii) Is reviewed and approved by designated officials within the organization;

b) Distribute copies of the Incident Response Plan to managers and employees supporting the Infinibyte Cloud system, the 3PAO (or other independent assessor) and the Authorizing Official;
c) Review the Incident Response Plan at least annually;
d) Update the Incident Response Plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
e) Communicate Incident Response Plan changes to managers and employees supporting the Infinibyte Cloud system, the 3PAO (or other independent assessor) and the Authorizing Official; and
f) Protect the Incident Response Plan from unauthorized disclosure and modification.

9.8.5.8 Information Spillage Response (IR-9)

The Contingency Planning Coordinator and ISSO shall:

a) Identify the specific information involved in the information system contamination;
b) Ensure that the Contingency Planning Director, Authorizing Official and Customer Agency ISSO are alerted following any information spillage using a method of communication not associated with the spill;
c) Isolate the contaminated information system or system component;
d) Eradicate the information from the contaminated information system or component;
e) Identify other information systems or system components that may have been subsequently contaminated; and
f) Perform other actions as specified by the Authorizing Official or Customer Agency ISSO.

The Contingency Planning Coordinator and ISSO shall also:

a) [IR-9 (1)] Assume primary responsibility for responding to information spills;
b) [IR-9 (2)] Provide information spillage response training annually;
c) [IR-9 (3)] Implement incident response procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions; and
d) [IR-9 (4)] Employ security safeguards for personnel exposed to information not within assigned access authorizations.

9.8.6 Incident Response Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.9 Maintenance Policy (MA-1)

9.9.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Maintenance security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.9.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Maintenance (MA) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.9.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Maintenance shall be applied:

a) The ISSO shall assign maintenance activities to the Infinibyte Cloud System Administrators and System Hosting Provider in accordance with approved contractual agreements and the NIST SP 800-53 security requirements.

b) The Infinibyte Cloud System Administrators shall perform maintenance duties assigned to them in accordance with the direction received from the ISSO.

c) The System Hosting Provider shall be responsible for all maintenance activities associated with their facilities in accordance with approved contractual agreements.

9.9.4 Applicable Documents

The documents that are applicable to the Maintenance policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.9.5 Maintenance Policy Requirements

The following table identifies the Infinibyte Cloud maintenance policies that are contained in this Section.

FAMILY: MAINTENANCE (MA-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
MA-2	**Controlled Maintenance**	**9.9.5.1**
MA-3	**Maintenance Tools**	**9.9.5.2**
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*	*9.9.5.2*
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*	*9.9.5.2*
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*	*9.9.5.2*
MA-4	**Nonlocal Maintenance**	**9.9.5.3**
MA-4 (2)	*NONLOCAL MAINTENANCE | DOCUMENT NONLOCAL MAINTENANCE*	*9.9.5.3*
MA-5	**Maintenance Personnel**	**9.9.5.4**
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*	*9.9.5.4*
MA-6	**Timely Maintenance**	**9.9.5.5**

9.9.5.1 Controlled Maintenance (MA-2)

The ISSO shall:

a) Ensure that Infinibyte Cloud System Administrators schedule, perform, document, and review records of maintenance and repairs on Infinibyte Cloud system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c) Explicitly approve the removal of the Infinibyte Cloud system or system components from the System Hosting Provider facilities for off-site maintenance or repairs;

d) Ensure that Infinibyte Cloud System Administrators sanitize equipment to remove all information from associated media prior to removal from System Hosting Provider facilities for off-site maintenance or repairs;

e) Ensure that Infinibyte Cloud System Administrators and Security Administrators check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and

f) Ensure that maintenance records include, at a minimum: date and time of maintenance; name of individual performing the maintenance, a description of the maintenance performed and a list of the equipment removed or replaced (including identification numbers if applicable) in Infinibyte Cloud system maintenance records.

9.9.5.2 Maintenance Tools (MA-3)

The ISSO shall approve, control, and monitor information system maintenance tools.

[MA-3 (1)] The System Hosting Provider and/or the Infinibyte Cloud System Administrator shall inspect the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

[MA-3 (2)] The Infinibyte Cloud System Administrator shall check media containing diagnostic and test programs for malicious code before the media are used in the Infinibyte Cloud information system.

[MA-3 (3)] The Infinibyte Cloud System Administrator shall prevent the unauthorized removal of maintenance equipment containing Infinibyte Cloud system or customer information by:

a) Verifying that there is no Infinibyte Cloud system or customer information contained on the equipment;

b) Sanitizing or destroying the equipment;

c) Retaining the equipment within the System Hosting Provider facility; or

d) Obtaining an exemption from the System Owner and/or customer explicitly authorizing removal of the equipment from the System Hosting Provider facility.

9.9.5.3 Nonlocal Maintenance (MA-4)

The ISSO shall:

a) Approve and monitor nonlocal maintenance and diagnostic activities;

b) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with the security policy documented in the Infinibyte Cloud system's System Security Plan;

c) Ensure that strong authenticators are employed in the establishment of nonlocal maintenance and diagnostic sessions;

d) Maintain records for nonlocal maintenance and diagnostic activities; and

e) Ensure that session and network connections are terminated when nonlocal maintenance is completed.

[MA-4 (2)] The ISSO shall document the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections in the Infinibyte Cloud system's System Security Plan.

9.9.5.4 Maintenance Personnel (MA-5)

The ISSO shall:

a) Establish a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;

b) Ensure that non-escorted personnel performing maintenance on the Infinibyte Cloud information system have required access authorizations; and

c) Designate DLH and/or System Hosting Provider personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

[MA-5 (1)] The ISSO shall:

a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

   i) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved DLH and/or System Hosting Provider personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

   ii) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, the Infinibyte Cloud System Administrator shall ensure that all volatile information storage components within the Infinibyte Cloud system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b) Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

9.9.5.5 Timely Maintenance (MA-6)

The ISSO shall ensure that maintenance support and/or spare parts for Infinibyte Cloud system components are obtained within sufficient time of a failure to meet the Recovery Time Objectives (RTO) in the system's Business Impact Analysis.

9.9.6 Maintenance Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.10 Media Protection Policy (MP-1)

9.10.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Media Protection security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.10.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Media Protection (MP) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.10.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Media Protection shall be applied:

a) The ISSO shall assign media protection activities to the Infinibyte Cloud System Administrators and System Hosting Provider in accordance with approved contractual agreements and U.S. Government security requirements.

b) The Infinibyte Cloud System Administrators shall perform media protection duties assigned to them in accordance with the direction received from the ISSO.

c) The System Hosting Provider shall be responsible for all other media protection activities in accordance with approved contractual agreements.

9.10.4 Applicable Documents

The documents that are applicable to the Media Protection policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.10.5 Media Protection Policy Requirements

The following table identifies the Infinibyte Cloud media protection policies that are contained in this Section.

FAMILY: MEDIA PROTECTION (MP-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
MP-2	**Media Access**	**9.10.5.1**
MP-3	**Media Marking**	**9.10.5.2**
MP-4	**Media Storage**	**9.10.5.3**
MP-5	**Media Transport**	**9.10.5.4**
MP-5 (4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*	*9.10.5.4*
MP-6	**Media Sanitization**	**9.10.5.5**
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*	*9.10.5.5*
MP-7	**Media Use**	**9.10.5.6**
MP-7 (1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*	*9.10.5.6*

9.10.5.1 Media Access (MP-2)

The ISSO shall restrict access to all Infinibyte Cloud system and customer digital and/or non-digital media to authorized system support personnel who have signed a Rules of Behavior for the Infinibyte Cloud system.

9.10.5.2 Media Marking (MP-3)

The ISSO shall:

a) Ensure that Infinibyte Cloud System Administrators mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b) Exempt non-removable media types from marking as long as the media remain within the cage or other controlled area within the System Hosting Provider's facility where the Infinibyte Cloud system resides.

9.10.5.3 Media Storage (MP-4)

Infinibyte Cloud System Administrators shall:

a) Physically control and securely store Infinibyte Cloud system digital media containing sensitive information within the cage or other controlled area within the System Hosting Provider's facility where the Infinibyte Cloud system resides, while non-digital media with sensitive information shall be stored in a locked office or storage container; and

b) Protect Infinibyte Cloud system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

9.10.5.4 Media Transport (MP-5)

The ISSO shall ensure that media is not be transported outside of the cage or other controlled area within the System Hosting Provider's facility without the customer's clear and explicit permission and direction. Should Infinibyte Cloud system media require transportation, the ISSO shall ensure that:

a) All media with sensitive information is protected and controlled during transport outside of controlled areas using encryption for digital media using a FIPS 140-2 validated encryption module or a locked container for non-digital media;
b) Accountability for Infinibyte Cloud system media is maintained during transport outside of controlled areas;
c) Activities associated with the transport of Infinibyte Cloud system media are documented; and
d) Activities associated with transport of Infinibyte Cloud system media are restricted to authorized DLH personnel. Media containing customer information shall be hand-carried by authorized DLH or customer personnel, or may be securely transported using a secure delivery method authorized by the customer (e.g., United States Postal Service Registered Mail).

[MP-5 (4)] The Infinibyte Cloud System Administrators shall employ FIPS 140-2 validated cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

9.10.5.5 Media Sanitization (MP-6)

The ISSO shall ensure that all information and media are disposed of properly in accordance with the Infinibyte Cloud system's System Security Plan.

If an Infinibyte Cloud storage device or computer system is sold, transferred, or otherwise disposed of, all sensitive and/or confidential program or data files on any storage media shall be completely erased or otherwise made unreadable as specified in NIST Special Publication 800-88, Guidelines for Media Sanitization. The physical media that the data is stored on shall be overwritten using a DoD/NSA approved process or physically destroyed. Any media that is destroyed shall be documented in a Certificate of Destruction, which shall be made available to the customer upon request.

[MP-6 (2)] If DLH is performing media sanitization, the Infinibyte Cloud System Administrator shall test sanitization equipment and procedures at least annually to verify that the intended sanitization is being achieved.

9.10.5.6 Media Use (MP-7)

The ISSO shall restrict access to all Infinibyte Cloud system and customer digital and/or non-digital media to authorized system support personnel who have signed an Access Agreement or Rules of Behavior for the Infinibyte Cloud system. The ISSO and Infinibyte Cloud System Administrators shall restrict the use of portable/removable digital storage, such as Compact Discs (CDs) or Universal Serial Bus (USB) drives, on Infinibyte Cloud systems. Portable/removable digital storage shall only be used to import or export customer data, as specifically requested by the customer. No customer data shall be copied, used, or otherwise transferred onto media outside the Infinibyte Cloud system security boundary without the customer's clear and explicit permission and direction.

[MP-7 (1)] The use of portable storage devices in Infinibyte Cloud systems is prohibited when such devices have no identifiable owner.

9.10.6 Media Protection Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.11 Physical and Environmental Protection Policy (PE-1)

9.11.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Physical and Environmental Protection security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.11.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Physical and Environmental Protection (PE) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.11.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Physical and Environmental Protection shall be applied:

a) The ISSO shall assign physical and environmental protection activities to the System Hosting Provider in accordance with approved contractual agreements and U.S. Government security requirements.

b) The System Hosting Provider shall be responsible for all physical and environmental protection activities within their facilities in accordance with approved contractual agreements.

9.11.4 Applicable Documents

The documents that are applicable to the Physical and Environmental policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.11.5 Physical and Environmental Protection Policy Requirements

The following table identifies the Infinibyte Cloud physical and environment protection policies that are contained in this Section.

FAMILY: PHYSICAL AND ENVIRONMENT PROTECTION (PE-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
PE-2	**Physical Access Authorizations**	**9.11.5.1**
PE-3	**Physical Access Control**	**9.11.5.2**
PE-4	**Access Control for Transmission Medium**	**9.11.5.3**
PE-5	**Access Control for Output Devices**	**9.11.5.4**
PE-6	**Monitoring Physical Access**	**9.11.5.5**
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*	*9.11.5.5*
PE-8	**Visitors Access Records**	**9.11.5.6**
PE-9	**Power Equipment and Cabling**	**9.11.5.7**
PE-10	**Emergency Shutoff**	**9.11.5.8**
PE-11	**Emergency Power**	**9.11.5.9**
PE-12	**Emergency Lighting**	**9.11.5.10**
PE-13	**Fire Protection**	**9.11.5.11**
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*	*9.11.5.11*
PE-13 (3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*	*9.11.5.11*
PE-14	**Temperature and Humidity Controls**	**9.11.5.12**
PE-14 (2)	*TEMPERATURE AND HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS*	*9.11.5.12*
PE-15	**Water Damage Protection**	**9.11.5.13**
PE-16	**Delivery and Removal**	**9.11.5.14**
PE-17	**Alternate Work Site**	**9.11.5.15**

9.11.5.1 Physical Access Authorizations (PE-2)

At the facility level, the ISSO shall ensure that the System Hosting Provider:

a) Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b) Issues authorization credentials for facility access;

c) Reviews the access list detailing authorized facility access by individuals at least annually; and

d) Removes individuals from the facility access list when access is no longer required.

At the information system level, the ISSO shall also:

a) Develop, approve, and maintain a list of individuals with authorized physical access to the cage or other area within the facility where the information system resides;

b) Reserved;

c) Review the access list detailing authorized information system physical access by individuals at least annually; and

d) Remove individuals from the information system physical access list when access is no longer required.

9.11.5.2 Physical Access Control (PE-3)

At the facility level, the ISSO shall ensure that the System Hosting Provider:

a) Enforces physical access authorizations at entry/exit points to the facility by;

   1) Verifying individual access authorizations before granting access to the facility; and

   2) Controlling ingress/egress to the facility using guards, identification cards, badges, or entry devices such as key card readers or biometrics;

b) Maintains physical access audit logs for facility and data center entry/exit points;

c) Provides safeguards to control access to areas within the facility officially designated as publicly accessible;

d) Escorts visitors and monitors visitor activity continuously;

e) Secures keys, combinations, and other physical access devices;

f) Inventories physical access devices annually; and

g) Changes combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

At the information system level, the ISSO shall also:

a) Reserved;

b) Maintain physical access audit logs for cage or other area within the facility where the information system resides;

c) Reserved;

d) Escort visitors and monitor visitor activity continuously in all circumstances within restricted access area where the Infinibyte Cloud information system resides;

e) Secure keys, combinations, and other physical access devices for the cage or other area within the facility where the information system resides;

f) Inventory physical access devices annually; and

g) Change combinations and keys at least annually and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

9.11.5.3 Access Control for Transmission Medium (PE-4)

The ISSO shall ensure that the System Hosting Provider controls physical access to distribution and transmission lines within the Hosting Provider's facilities using guards, identification cards, badges, and/or entry devices such as key card readers or biometrics.

9.11.5.4 Access Control for Output Devices (PE-5)

The ISSO shall ensure that Infinibyte Cloud System Administrators control physical access to Infinibyte Cloud information system output devices to prevent unauthorized individuals from obtaining the output.

9.11.5.5 Monitoring Physical Access (PE-6)

The ISSO shall ensure that the System Hosting Provider:

a) Monitors physical access to the facility where the Infinibyte Cloud information system resides to detect and respond to physical security incidents;

b) Reviews physical access logs at least monthly and upon occurrence of potential indications of incident events; and

c) Coordinates results of reviews and investigations with the Infinibyte Cloud incident response capability.

[PE-6 (1)] The ISSO shall ensure that the System Hosting Provider monitors physical intrusion alarms and surveillance equipment.

9.11.5.6 Visitors Access Records (PE-8)

At the facility level, the ISSO shall ensure that the System Hosting Provider:

a) Maintains visitor access records to the facility where the information system resides for a minimum of one year; and

b) Reviews facility visitor access records at least monthly.

At the information system level, the ISSO shall also:

a) Maintain visitor access records to the cage or other area within the facility where the information system resides for a minimum of one year; and

b) Review visitor access records for the cage or other area within the facility where the information system at least monthly.

9.11.5.7 Power Equipment and Cabling (PE-9)

The ISSO shall ensure that the System Hosting Provider protects power equipment and power cabling within the facility hosting the Infinibyte Cloud information system from damage and destruction.

9.11.5.8 Emergency Shutoff (PE-10)

The ISSO shall ensure that the System Hosting Provider:

a) Provides the capability of shutting off power to the Infinibyte Cloud information system or system components in emergency situations;

b) Places emergency shutoff switches or devices on power distribution systems to facilitate safe and easy access for personnel; and

c) Protects emergency power shutoff capability from unauthorized activation.

9.11.5.9 Emergency Power (PE-11)

The ISSO shall ensure that the System Hosting Provider provides a short-term uninterruptible power supply to transition the Infinibyte Cloud information system to long-term alternate power in the event of a primary power source loss.

9.11.5.10 Emergency Lighting (PE-12)

The ISSO shall ensure that the System Hosting Provider employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

9.11.5.11 Fire Protection (PE-13)

The ISSO shall ensure that the System Hosting Provider employs and maintains fire suppression and detection devices/systems that are supported by an independent energy source.

[PE-13 (2)] The ISSO shall ensure that the System Hosting Provider employs fire suppression devices/systems for the information system that provide automatic notification of any

activation to the System Hosting Provider's Facility Management Team and emergency responders.

[PE-13 (3)] The ISSO shall ensure that the System Hosting Provider employs an automatic fire suppression capability when the facility is not staffed on a continuous basis.

9.11.5.12 Temperature and Humidity Controls (PE-14)

The ISSO shall ensure that the System Hosting Provider:

a) Maintains temperature and humidity levels within the facility where the information system resides within the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) standards; and

b) Monitors temperature and humidity levels continuously.

[PE-14 (2)] The ISSO shall ensure that the System Hosting Provider employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

9.11.5.13 Water Damage Protection (PE-15)

The ISSO shall ensure that the System Hosting Provider protects the Infinibyte Cloud system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key System Hosting Provider personnel.

9.11.5.14 Delivery and Removal (PE-16)

The ISSO shall authorize, monitor, and control system components entering and exiting the cage or other area within the facility where the information system resides and maintains records of those items.

9.11.5.15 Alternate Work Site (PE-17)

The ISSO shall:

a) Employ applicable NIST SP 800-53 security controls at alternate work sites;

b) Assess as feasible, the effectiveness of security controls at alternate work sites; and

c) Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

9.11.6 Physical and Environmental Protection Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.12 Security Planning Policy (PL-1)

9.12.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Security Planning security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.12.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Security Planning (PL) security control family.

In the context of this policy, the term "System Hosting Provider" refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.12.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Security Planning shall be applied:

a) The ISSO shall be the primary individual responsible for system-level Security Planning activities.

9.12.4 Applicable Documents

The documents that are applicable to the Security Planning policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.12.5 Security Planning Policy Requirements

The following table identifies the Infinibyte Cloud security planning policies that are contained in this Section.

FAMILY: PLANNING (PL-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
PL-2	**System Security Plan**	**9.12.5.1**
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	*9.12.5.1*
PL-4	**Rules of Behavior**	**9.12.5.2**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*	*9.12.5.2*
PL-8	**Information Security Architecture**	**9.12.5.3**

9.12.5.1 System Security Plan (PL-2)

The ISSO shall:

a) Develop a System Security Plan for information systems that:
   i) Is consistent with the Infinibyte Cloud enterprise architecture;
   ii) Explicitly defines the authorization boundary for the system;
   iii) Describes the operational context of the information systems in terms of mission and business processes;
   iv) Provides the security categorization of the information system including supporting rationale;
   v) Describes the operational environment for the information system and relationships with or connections to other information systems;
   vi) Provides an overview of the security requirements for the system;
   vii) Identifies any relevant overlays, if applicable;
   viii) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
   ix) Is reviewed and approved by the Authorizing Official or designated representative prior to plan implementation.

b) Distribute copies of the System Security Plan and communicate subsequent changes to the plan to personnel managing and operating the Infinibyte Cloud system, Authorizing Official representatives, and/or the 3PAO (or other independent security assessor) representatives;

c) Review the System Security Plan for the Infinibyte Cloud information system at least annually;

d) Update the System Security Plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and

e) Protect the System Security Plan from unauthorized disclosure and modification.

[PL-2 (3)] The ISSO shall also plan and coordinate security-related activities affecting the information system with the System Hosting Provider before conducting such activities in order to reduce the impact on other organizational entities.

9.12.5.2 Rules of Behavior (PL-4)

The ISSO shall:

a) 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;
b) 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 systems;
c) Review and update the rules of behavior at least every three (3) years; and
d) Require individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised or updated.

[PL-4 (1)] The ISSO shall also ensure that the rules of behavior include explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

9.12.5.3 Information Security Architecture (PL-8)

The ISSO shall:

a) Ensure that an information security architecture is developed for the information system that:
    i) Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
    ii) Describes how the information security architecture is integrated into and supports the enterprise architecture; and
    iii) Describes any information security assumptions about, and dependencies on, external services;
b) Review and update the information security architecture annually to reflect updates in the enterprise architecture; and
c) Ensure that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

9.12.6 Security Planning Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.13 Personnel Security Policy (PS-1)

9.13.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Personnel Security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.13.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Personnel Security (PS) security control family.

9.13.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Personnel Security shall be applied:

a) The DLH Human Resources department shall oversee and administer the DLH personnel security program.

b) The ISSO shall ensure that the Infinibyte Cloud personnel security policies are implemented for systems under their purview.

9.13.4 Applicable Documents

The documents that are applicable to the Personnel Security policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.13.5 Personnel Security Policy Requirements

The following table identifies the Infinibyte Cloud personnel security policies that are contained in this Section.

FAMILY: PERSONNEL SECURITY (PS-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
PS-2	**Position Risk Designation**	**9.13.5.1**
PS-3	**Personnel Screening**	**9.13.5.2**
PS-3(3)	*PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES*	*9.13.5.2*
PS-4	**Personnel Termination**	**9.13.5.3**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
PS-5	Personnel Transfer	9.13.5.4
PS-6	Access Agreements	9.13.5.5
PS-7	Third-Party Personnel Security	9.13.5.6
PS-8	Personnel Sanctions	9.13.5.7

9.13.5.1 Position Risk Designation (PS-2)

The IT Director shall:

a) Assign a risk designation to all organizational positions;
b) Establish screening criteria for individuals filling those positions; and
c) Review and revise position risk designations at least every three (3) years.

9.13.5.2 Personnel Screening (PS-3)

The DLH Human Resources department shall:

a) Screen individuals prior to authorizing access to the information systems; and
b) If required in subsequent iterations, rescreen individuals to include: reinvestigation during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation required for other moderate risk positions or any low risk positions.

[PS-3 (3)] The ISSO shall ensure that individuals accessing an Infinibyte Cloud system that processes, stores, or transmits information requiring special protection:

a) Have valid access authorizations that are demonstrated by assigned official government duties; and
b) Satisfy personnel screening criteria, as required by specific information.

9.13.5.3 Personnel Termination (PS-4)

The ISSO and DLH Human Resources department shall ensure that the following personnel security actions occur upon termination of individual employment:

a) Disable information system access on the same day as notification of the termination;
b) Terminate/revoke any authenticators/credentials associated with the individual;
c) Conduct exit interviews that include a discussion of the individual's responsibilities for continuing to protect and not to disclose sensitive or classified information to which they may have previously been given access;
d) Retrieve all security-related organizational information system-related property;
e) Retain access to organizational information and information systems formerly controlled by the terminated individual; and
f) Notify the IT Director and Architect within the same day of termination.

9.13.5.4 Personnel Transfer (PS-5)

The ISSO and DLH Human Resources department shall:

a) Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
b) Initiate Human Resource actions within five (5) days following the formal transfer action;
c) Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
d) Notify the IT Director and Architect within five days of formal transfer action.

9.13.5.5 Access Agreements (PS-6)

The ISSO and DLH Human Resources department shall:

a) Develop and document access agreements for organizational information systems;
b) Review and update the access agreements at least annually; and
c) Ensure that individuals requiring access to organizational information and information systems:
    i) Sign appropriate access agreements prior to being granted access; and
    ii) Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at least annually.

9.13.5.6 Third-Party Personnel Security (PS-7)

The IT Director shall:

a) Establish personnel security requirements including security roles and responsibilities for third-party providers;

b) Require third-party providers to comply with personnel security policies and procedures established by the organization;
c) Document personnel security requirements;
d) Require third-party providers to notify the ISSO of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges on the same day that the action occurred; and
e) Monitor third-party provider compliance.

9.13.5.7 Personnel Sanctions (PS-8)

The DLH Human Resources department shall:

a) Employ a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
b) Notify the IT Director and Architect on the same day that the action occurred when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

9.13.6 Personnel Security Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.14 Risk Assessment Policy (RA-1)

9.14.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the Risk Assessment security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.14.2 Scope

This Section provides supporting policy and procedures for each individual security control within the Risk Assessment (RA) security control family.

9.14.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to Risk Assessment shall be applied:

a) The ISSO shall manage and oversee the Risk Assessment activities for the systems under their purview.

9.14.4 Applicable Documents

The documents that are applicable to the Risk Assessment policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.14.5 Risk Assessment Policy Requirements

Risk Assessments shall be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

The following table identifies the Infinibyte Cloud risk assessment policies that are contained in this Section.

FAMILY: RISK ASSESSMENT (RA-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
RA-2	**Security Categorization**	**9.14.5.1**
RA-3	**Risk Assessment**	**9.14.5.2**
RA-5	**Vulnerability Scanning**	**9.14.5.3**
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*	*9.14.5.3*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*	*9.14.5.3*
RA-5 (3)	*VULNERABILITY SCANNING | BREADTH / DEPTH OF COVERAGE*	*9.14.5.3*
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*	*9.14.5.3*
RA-5 (6)	*VULNERABILITY SCANNING | AUTOMATED TREND ANALYSES*	*9.14.5.3*
RA-5 (8)	*VULNERABILITY SCANNING | REVIEW HISTORIC AUDIT LOGS*	*9.14.5.3*

9.14.5.1 Security Categorization (RA-2)

The ISSO shall ensure that:

a) Information and the information systems are categorized in accordance with FIPS Publication 199;
b) Security categorization results (including supporting rationale) are documented in the System Security Plan for the information system; and
c) The security categorization decision is reviewed and approved by the Authorizing Official or designated representative.

9.14.5.2 Risk Assessment (RA-3)

The ISSO, in cooperation with an accredited FedRAMP 3PAO or other independent assessor, shall ensure that:

a) An assessment of risk is conducted that includes 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) Risk assessment results are documented in a Security Assessment Report;
c) Risk assessment results are reviewed in accordance with OMB A-130 requirements or when a significant change occurs;
d) Risk assessment results are disseminated to managers supporting the Infinibyte Cloud system and the Authorizing Official; and
e) Risk assessments are updated in accordance with OMB A-130 requirements or whenever there are 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.

9.14.5.3 Vulnerability Scanning (RA-5)

The ISSO shall ensure that:

a) Scans are conducted for vulnerabilities in the information system and hosted applications at least monthly (for operating systems, web applications and databases) and when new vulnerabilities that could potentially affect the system/applications are identified and reported;
b) Vulnerability scanning tools and techniques are employed that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
    i) Enumerating platforms, software flaws, and improper configurations;
    ii) Formatting and making transparent, checklists and test procedures; and
    iii) Measuring vulnerability impact;
c) Vulnerability scan reports and results from security control assessments are analyzed by Security Operations personnel;
d) Legitimate vulnerabilities are remediated in accordance with an organizational assessment of risk; high-risk vulnerabilities shall be mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities shall be mitigated within ninety (90) days from date of discovery; low risk vulnerabilities shall be mitigated within 180 days from date of discovery and
e) Information obtained from the vulnerability scanning process and security control assessments is shared with Infinibyte Cloud system developers and management personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

The ISSO shall also ensure that:

a) [RA-5 (1)] Vulnerability scanning tools are employed that include the capability to readily update the list of information system vulnerabilities scanned;
b) [RA-5 (2)] The list of information system vulnerabilities scanned are updated prior to the commencement of any new scans, or when new vulnerabilities are identified and reported;
c) [RA-5 (3)] Vulnerability scanning procedures demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked);
d) [RA-5 (5)] Privileged access authorization to operating systems, web services and databases are included for all scans;

e) [RA-5 (6)] Mechanisms are employed that compare the results of vulnerability scans over time to determine trends in information system vulnerabilities; and
f) [RA-5 (8)] Reviews of historic audit logs are conducted to determine if a vulnerability identified in the information system has been previously exploited.

9.14.6 Risk Assessment Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.15 System and Services Acquisition Policy (SA-1)

9.15.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the System and Services Acquisition security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.15.2 Scope

This Section provides supporting policy and procedures for each individual security control within the System and Services Acquisition (SA) security control family.

9.15.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to System and Services Acquisition shall be applied:

a) The System Owner shall ensure that systems and services are acquired in accordance with the applicable requirements in this policy.

9.15.4 Applicable Documents

The documents that are applicable to the System and Services Acquisition policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.15.5 System and Services Acquisition Policy Requirements

The following table identifies the Infinibyte Cloud system and services acquisition policies that are contained in this Section.

FAMILY: SYSTEM AND SERVICES ACQUISITION (SA-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SA-2	**Allocation of Resources**	**9.15.5.1**
SA-3	**System Development Life Cycle**	**9.15.5.2**
SA-4	**Acquisition Process**	**9.15.5.3**
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*	*9.15.5.3*
SA-4 (2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*	*9.15.5.3*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SA-4 (8)	*ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN*	*9.15.5.3*
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*	*9.15.5.3*
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*	*9.15.5.3*
SA-5	**Information System Documentation**	**9.15.5.4**
SA-8	**Security Engineering Principles**	**9.15.5.5**
SA-9	**External Information System Services**	**9.15.5.6**
SA-9 (1)	*EXTERNAL INFORMATION SYSTEMS | RISK ASSESSMENTS / ORGANIZATIONAL APPROVALS*	*9.15.5.6*
SA-9 (2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*	*9.15.5.6*
SA-9 (4)	*EXTERNAL INFORMATION SYSTEMS | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*	*9.15.5.6*
SA-9 (5)	*EXTERNAL INFORMATION SYSTEMS | PROCESSING, STORAGE, AND SERVICE LOCATION*	*9.15.5.6*
SA-10	**Developer Configuration Management**	**9.15.5.7**
SA-10 (1)	*DEVELOPER CONFIGURATION MANAGEMENT | SOFTWARE / FIRMWARE INTEGRITY VERIFICATION*	*9.15.5.7*
SA-11	**Developer Security Testing and Evaluation**	**9.15.5.8**
SA-11 (1)	*DEVELOPER SECURITY TESTING AND EVALUATION | STATIC CODE ANALYSIS*	*9.15.5.8*
SA-11 (2)	*DEVELOPER SECURITY TESTING AND EVALUATION | THREAT AND VULNERABILITY ANALYSES*	*9.15.5.8*
SA-11 (8)	*DEVELOPER SECURITY TESTING AND EVALUATION | DYNAMIC CODE ANALYSIS*	*9.15.5.8*

9.15.5.1 Allocation of Resources (SA-2)

The System Owner shall ensure that:

a) A determination of information security requirements for the Infinibyte Cloud information system is included in mission/business process planning;
b) The resources required to protect the information system or information system service is determined, documented, and allocated as part of its capital planning and investment control process; and
c) A discrete line item for information security is established in programming and budgeting documentation.

9.15.5.2 System Development Life Cycle (SA-3)

The System Owner and ISSO shall:

a) Manage the information systems using System Development Life Cycle (SDLC) procedures for the system development life cycle methodology that includes information security considerations;
b) Define and document information system security roles and responsibilities throughout the system development life cycle;
c) Identify individuals having information system security roles and responsibilities; and
d) Integrate the organizational information security risk management process into system development life cycle activities.

9.15.5.3 Acquisition Process (SA-4)

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

a) Security functional requirements;
b) Security strength requirements;
c) Security assurance requirements;
d) Security-related documentation requirements;
e) Requirements for protecting security-related documentation;
f) Description of the information system development environment and environment in which the system is intended to operate; and
g) Acceptance criteria.

The System Owner shall take the following actions:

a) [SA-4 (1)] Require the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed;

b) [SA-4 (2)] Require the developer of the information system to provide design and implementation information for the security controls to be employed to include: security-relevant external system interfaces; high-level design; low-level design; source code and/or hardware schematics;
c) [SA-4 (8)] Require the developer of the information system to produce a plan for the continuous monitoring of security control effectiveness that contains at least the minimum requirement as defined in Section 9.4.5.5 (Continuous Monitoring) of this ISPP;
d) [SA-4 (9] Require the developer of the information system to identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use by the customer; and
e) [SA-4 (10)] Ensure that only information technology products on the FIPS 201-approved products list are employed for Personal Identity Verification (PIV) capability implemented within Infinibyte Cloud systems containing U.S. Government information.

9.15.5.4 Information System Documentation (SA-5)

The ISSO shall:

a) Obtain administrator documentation for the information system, system component, or information system service that describes:
    i) Secure configuration, installation, and operation of the information system; component, or service;
    ii) Effective use and maintenance of security features/functions; and
    iii) Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
b) Obtain user documentation for the information system, system component, or information system service that describes:
    i) User-accessible security features/functions and how to effectively use those security features/functions;
    ii) Methods for user interaction, which enables individuals to use the system in a more secure manner; and
    iii) User responsibilities in maintaining the security of the system, component, or service;
c) Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and prepares supplemental documentation in response;
d) Protect documentation as required, in accordance with the risk management strategy; and

e) Distribute documentation to all personnel supporting the Infinibyte Cloud system and, as appropriate, the independent security control assessor (e.g., 3PAO).

9.15.5.5 Security Engineering Principles (SA-8)

The ISSO and System Owner shall ensure that information system security engineering principles are applied in the specification, design, development, implementation, and modification of the information system based upon the guidelines identified in NIST SP 800-160.

9.15.5.6 External Information System Services (SA-9)

The System Owner shall:

a) Require that providers of external information system services comply with organizational information security requirements and employ NIST SP 800-53 Security Controls Baseline(s) if Federal information is processed or stored within the external system;
b) Define and document oversight and user roles and responsibilities with regard to external information system services; and
c) Ensure that FISMA/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored to monitor security control compliance by external service providers on an ongoing basis.

The System Owner shall require that information system developers/integrators:

a) [SA-9 (1)(a)] Conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services;
b) [SA-9 (1)(b)] Ensure that the acquisition or outsourcing of dedicated information security services is approved by the IT Director;
c) [SA-9 (2)] Require providers of all external systems where Federal information is processed or stored to identify the functions, ports, protocols, and other services required for the use of such services;
d) [SA-9 (4)] Employ security safeguards defined by the IT Director to ensure that the interests of all external systems where Federal information is processed or stored is consistent with and reflect organizational interests; and
e) [SA-9 (5)] Restrict the location of information processing, information data, and information services supporting U.S. Government customers to the Continental United States (CONUS), Alaska, and Hawaii locations, based on potential government customer requirements or conditions.

9.15.5.7 Developer Configuration Management (SA-10)

The System Owner and ISSO shall require that information system, system component, or information system service developers/integrators:

a) Perform configuration management during information system design, development, implementation, and operation;
b) Document, manage and control the integrity changes to the information system, system component, or information system service;
c) Implement only organization-approved changes to the system, component, or service;
d) Document approved changes to the system, component, or service and the potential security impacts of such changes; and
e) Track security flaws and flaw resolution within the system, component, or service and report findings to the IT Director. For JAB authorizations, security flaws and flaw resolution within the system, component, or service shall also be reported to the FedRAMP ISSO(s).

[SA-10 (1)] The System Owner and ISSO shall also require the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

9.15.5.8 Developer Security Testing and Evaluation (SA-11)

The System Owner and ISSO shall require that information system, system component or information system services developers:

a) Create and implement a security test and evaluation plan;
b) Perform system integration, system and regression testing/evaluation at the release level;
c) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
d) Implement a verifiable flaw remediation; and
e) Correct flaws identified during security testing/evaluation.

For Infinibyte Cloud FedRAMP-authorized systems, the System Owner and ISSO shall require that information system, system component or information system services developers:

a) [SA-11 (1)] Employ static code analysis tools to identify common flaws and document the results of the analysis;
b) [SA-11 (2)] Perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service; and
c) [SA-11 (8)] Employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

9.15.6 System and Services Acquisition Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.16 System and Communication Protection Policy (SC-1)

9.16.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the System and Communications Protection security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.16.2 Scope

This Section provides supporting policy and procedures for each individual security control within the System and Communications Protection (SC) security control family.

In the context of this policy, the term “System Hosting Provider” refers to the commercial Infrastructure as a Service (IaaS) Cloud Service Provider (for cloud-based systems) or the colocation data center (for Infinibyte Cloud-hosted systems).

9.16.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to System and Communications Protection shall be applied:

a) The Architect shall be responsible for ensuring that all technical design functions identified in the policy are incorporated into Infinibyte Cloud systems that process U.S. Government information.

b) The IT Director shall be responsible for ensuring that all system security functions for protecting U.S. Government information are operated in accordance with this policy.

9.16.4 Applicable Documents

The documents that are applicable to the System and Communication Protection policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.16.5 System and Communications Protection Policy Requirements

The following table identifies the Infinibyte Cloud system and communications protection policies that are contained in this Section.

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION (SC-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SC-2	**Application Partitioning**	**9.16.5.1**
SC-4	**Information in Shared Resources**	**9.16.5.2**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SC-5	**Denial of Service Protection**	**9.16.5.3**
SC-6	**Resource Availability**	**9.16.5.4**
SC-7	**Boundary Protection**	**9.16.5.5**
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*	*9.16.5.5*
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*	*9.16.5.5*
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*	*9.16.5.5*
SC-7 (7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*	*9.16.5.5*
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*	*9.16.5.5*
SC-7 (12)	*BOUNDARY PROTECTION | HOST-BASED PROTECTION*	*9.16.5.5*
SC-7 (13)	*BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS / MECHANISMS / SUPPORT COMPONENTS*	*9.16.5.5*
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*	*9.16.5.5*
SC-8	**Transmission Confidentiality and Integrity**	**9.16.5.6**
SC-8 (1)	*TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*	*9.16.5.6*
SC-10	**Network Disconnect**	**9.16.5.7**
SC-12	**Cryptographic Key Establishment and Management**	**9.16.5.8**
SC-12 (2)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | SYMMETRIC KEYS*	*9.16.5.8*
SC-12 (3)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | ASYMMETRIC KEYS*	*9.16.5.8*
SC-13	**Cryptographic Protection**	**9.16.5.9**
SC-15	**Collaborative Computing Devices**	**9.16.5.10**
SC-17	**Public Key Infrastructure Certificates**	**9.16.5.11**
SC-18	**Mobile Code**	**9.16.5.12**
SC-19	**Voice Over Internet Protocol**	**9.16.5.13**

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SC-20	**Secure Name / Address Resolution Service (Authoritative Source)**	**9.16.5.14**
SC-21	**Secure Name / Address Resolution Service (Recursive or Caching Resolver)**	**9.16.5.15**
SC-22	**Architecture and Provisioning for Name / Address Resolution Service**	**9.16.5.16**
SC-23	**Session Authenticity**	**9.16.5.17**
SC-28	**Protection of Information at Rest**	**9.16.5.18**
SC-28 (1)	*PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION*	*9.16.5.18*
SC-39	**Process Isolation**	**9.16.5.19**

9.16.5.1 Application Partitioning (SC-2)

The Architect shall ensure that Infinibyte Cloud systems separate user functionality (including user interface services) from information system management functionality.

9.16.5.2 Information in Shared Resources (SC-4)

The Architect shall ensure that Infinibyte Cloud systems prevent unauthorized and unintended information transfer via shared system resources.

9.16.5.3 Denial of Service Protection (SC-5)

The IT Director shall ensure the Infinibyte Cloud System Administrators configure the Infinibyte Cloud firewalls to monitor network traffic and to protect against or limit the effects of denial of service attacks such as Distributed Denial of Service (DDoS), Man In The Middle (MITM), IP Spoofing, Port Scanning, Packet and Flooding attacks. Additionally, the IT Director shall ensure coordination with the hosting System Hosting Provider service provider to further strengthen defenses against DDoS attacks.

9.16.5.4 Resource Availability (SC-6)

The IT Director shall ensure that the Infinibyte Cloud System Administrators protect the availability of resources by allocating Infinibyte Cloud system resources by priority and redundancy.

9.16.5.5 Boundary Protection (SC-7)

The IT Director and Infinibyte Cloud System Administrators shall:

a) Monitor and control communications at the external boundary of the system and at key internal boundaries within the system;
b) Implement sub-networks for publicly accessible system components that are logically separated from internal organizational networks; and
c) Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

Additionally, the IT Director and Infinibyte Cloud System Administrators shall:

a) [SC-7 (3)] Limit the number of external network connections to the system;
b) [SC-7 (4)(a)] Implement a managed interface for each external telecommunication service;
c) [SC-7 (4)(b)] Establish a traffic flow policy for each managed interface;
d) [SC-7 (4)(c)] Protect the confidentiality and integrity of the information being transmitted across each interface;
e) [SC-7 (4)(d)] Document each exception to the traffic flow policy with a supporting mission/business need and duration of that need;
f) [SC-7 (4)(e)] Review exceptions to the traffic flow policy at least annually and remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need;
g) [SC-7 (5)] Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception) at managed interfaces on the information system;
h) [SC-7 (7)] Prevent devices from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks;
i) [SC-7 (8)] Route internal communications traffic to external networks through authenticated proxy servers within the managed interfaces of boundary protection devices;
j) [SC-7 (12)] Implement defined host-based boundary protection mechanisms at defined information system components;
k) [SC-7 (13)] Isolate security tools, mechanisms, and support components associated with system and security administration from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system; and

l) [SC-7 (18)] Fail securely in the event of an operational failure of a boundary protection device.

9.16.5.6 Transmission Confidentiality and Integrity (SC-8)

The IT Director and Architect shall ensure that Infinibyte Cloud systems protect the integrity of transmitted information.

[SC-8 (1)] The IT Director and Architect shall also ensure that Infinibyte Cloud systems implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission unless otherwise protected by alternative physical measures, such as a hardened or alarmed carrier Protective Distribution System (PDS).

9.16.5.7 Network Disconnect (SC-10)

The IT Director shall ensure that Infinibyte Cloud systems terminate the network connection associated with a communications session at the end of the session or no longer than thirty (30) minutes of inactivity. Long running batch jobs and other required long running operations shall not be subject to this time limit of inactivity, unless otherwise specified by the customer.

9.16.5.8 Cryptographic Key Establishment and Management (SC-12)

The IT Director and Architect shall ensure that Infinibyte Cloud systems establish and manage cryptographic keys for required cryptography modules employed within the information systems in accordance with U.S. Government approved and validated cryptography mechanisms.

The IT Director and Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SC-12 (2)] Produce, control, and distribute symmetric cryptographic keys using NIST FIPS-compliant key management technology and processes; and
b) [SC-12 (3)] Produce, control, and distribute asymmetric cryptographic keys using pre-positioned keying material that protect the user's private key.

9.16.5.9 Cryptographic Protection (SC-13)

For Infinibyte Cloud systems processing U.S. Government information, the Architect shall ensure that Infinibyte Cloud systems implement FIPS-approved cryptographic algorithms in accordance with applicable federal laws, Executive Orders, directives policies, regulations and standards.

9.16.5.10 Collaborative Computing Devices (SC-15)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Prohibit remote activation of collaborative computing devices; and
b) Provide an explicit indication of use to users physically present at the devices.

9.16.5.11 Public Key Infrastructure Certificates (SC-17)

If required, Infinibyte Cloud public key certificates shall be:

a) Issued under a certificate policy approved by the System Owner; or
b) Obtained from a service provider approved by the System Owner.

9.16.5.12 Mobile Code (SC-18)

The Architect and System Owner shall:

a) Define acceptable and unacceptable mobile code and mobile code technologies;
b) Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
c) Authorize, monitor, and control the use of mobile code within the information systems.

9.16.5.13 Voice Over Internet Protocol (SC-19)

Infinibyte Cloud systems shall not utilize Voice over Internet Protocol (VoIP) technologies.

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

Infinibyte Cloud systems shall not provide external name/address resolution services.

9.16.5.15 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (SC-21)

Infinibyte Cloud systems shall not provide external name/address resolution services.

9.16.5.16 Architecture and Provisioning For Name / Address Resolution Service (SC-22)

Infinibyte Cloud systems shall not provide external name/address resolution services.

9.16.5.17 Session Authenticity (SC-23)

The Architect shall ensure that Infinibyte Cloud systems provide mechanisms to protect the authenticity of communications sessions.

9.16.5.18 Protection of Information at Rest (SC-28)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information protect the confidentiality and integrity of information at rest.

[SC-28 (1)] The ISSO shall also ensure that Infinibyte Cloud systems implement cryptographic mechanisms to prevent unauthorized disclosure and modification of defined information system components.

9.16.5.19 Process Isolation (SC-39)

The Architect shall ensure that Infinibyte Cloud systems maintain a separate execution domain for each executing process.

9.16.6 System and Communications Protection Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

9.17 System and Information Integrity Policy (SI-1)

9.17.1 Purpose

This Infinibyte Cloud security policy provides requirements for implementing the System and Information Integrity security control family as specified in NIST SP 800-53 for Infinibyte Cloud systems processing U.S. Government information.

9.17.2 Scope

This Section provides supporting policy and procedures for each individual security control within the System and Information Integrity (SI) security control family.

9.17.3 Roles and Responsibilities

In addition to the security roles and responsibilities identified in Section 1.3 (Roles and Responsibilities) of this document, the following additional roles and responsibilities specific to System and Information Integrity shall be applied:

a) The Architect shall be responsible for ensuring that all technical design functions identified in the policy are incorporated into Infinibyte Cloud systems that process U.S. Government information.

b) The IT Director shall be responsible for ensuring that all system security functions for protecting U.S. Government information are operated in accordance with this policy.

9.17.4 Applicable Documents

The documents that are applicable to the System and Information Integrity policies contained in this section are identified in Section 2 (Applicable Documents) of this document.

9.17.5 System and Information Integrity Policy Requirements

The following table identifies the Infinibyte Cloud system and information integrity policies that are contained in this Section.

FAMILY: SYSTEM AND INFORMATION INTEGRITY (SI-1)

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SI-2	**Flaw Remediation**	**9.17.5.1**
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*	*9.17.5.1*
SI-2 (3)	*FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS*	*9.17.5.1*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SI-3	**Malicious Code Protection**	**9.17.5.2**
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*	*9.17.5.2*
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*	*9.17.5.2*
SI-3 (7)	*MALICIOUS CODE PROTECTION | NO SIGNATURE-BASED DETECTION*	*9.17.5.2*
SI-4	**Information System Monitoring**	**9.17.5.3**
SI-4 (1)	*INFORMATION SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM*	*9.17.5.3*
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*	*9.17.5.3*
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*	*9.17.5.3*
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*	*9.17.5.3*
SI-4 (14)	*INFORMATION SYSTEM MONITORING | WIRELESS INTRUSION DETECTION*	*9.17.5.3*
SI-4 (16)	*INFORMATION SYSTEM MONITORING | CORRELATE MONITORING INFORMATION*	*9.17.5.3*
SI-4 (23)	*INFORMATION SYSTEM MONITORING | HOST-BASED DEVICES*	*9.17.5.3*
SI-5	**Security Alerts, Advisories, and Directives**	**9.17.5.4**
SI-6	**Security Function Verification**	**9.17.5.5**
SI-7	**Software, Firmware, and Information Integrity**	**9.17.5.6**
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*	*9.17.5.6*
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*	*9.17.5.6*
SI-8	**Spam Protection**	**9.17.5.7**
SI-8 (1)	*SPAM PROTECTION | CENTRAL MANAGEMENT*	*9.17.5.7*
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*	*9.17.5.7*

NIST SP 800-53 Security Control or Enhancement	Title	Security Policy Paragraph Number
SI-10	**Information Input Validation**	**9.17.5.8**
SI-11	**Error Handling**	**9.17.5.9**
SI-12	**Information Handling and Retention**	**9.17.5.10**
SI-16	**Memory Protection**	**9.17.5.11**

9.17.5.1 Flaw Remediation (SI-2)

The IT Director and ISSO shall ensure that the following actions are performed:

a) Identify, report, and correct information system flaws;
b) Test software updates related to flaw remediation for effectiveness and potential side effects on Infinibyte Cloud information systems before installation;
c) Install security-relevant software and firmware updates within thirty (30) days from date of release of updates; and
d) Incorporate flaw remediation into the organizational configuration management process.

The IT Director and ISSO also shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SI-2 (2)] Employ automated mechanisms at least monthly to determine the state of information system components with regard to flaw remediation;
b) [SI-2 (3)(a)] Measure the time between flaw identification and flaw remediation; and
c) [SI-2 (3)(b)] Establish benchmarks for taking corrective actions within thirty (30) days from date of release of updates.

9.17.5.2 Malicious Code Protection (SI-3)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
b) Update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
c) Configure malicious code protection mechanisms to:

i) Perform periodic scans of the information systems to include end-points at least weekly and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
ii) Block malicious code, quarantine malicious code, and/or send alerts to the administrator in response to malicious code detection; and

d) Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information systems.

The IT Director and Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SI-3 (1)] Centrally manage malicious code protection mechanisms;
b) [SI-3 (2)] Ensure that the information system automatically updates malicious code protection mechanisms; and
c) [SI-3 (7)] Implement non-signature-based malicious code detection mechanisms.

9.17.5.3 Information System Monitoring (SI-4)

The Architect, IT Director, System Owner and Security Administrators shall:

a) Monitor the information system to detect:
    i) Attacks and indicators of potential attacks in accordance with monitoring objectives defined by the System Owner; and
    ii) Unauthorized local, network, and remote connections;
b) Identify unauthorized use of the information system through techniques and methods defined by the System Owner;
c) Deploy monitoring devices:
    i) Strategically within the information system to collect organization-determined essential information; and
    ii) At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d) Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
e) 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;
f) Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and

g) Provide information system monitoring information defined by the System Owner to the IT Director as needed.

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SI-4 (1)] Connect and configure individual intrusion detection tools into an information system-wide intrusion detection system;
b) [SI-4 (2)] Employ automated tools to support near real-time analysis of events;
c) [SI-4 (4)] Monitor inbound and outbound communications traffic continuously for unusual or unauthorized activities or conditions;
d) [SI-4 (5)] Alert Infinibyte Cloud System Administrators, Security Administrators and incident response personnel when the indications of compromise or potential compromise occur in accordance with the system's Incident Response Plan;
e) [SI-4 (14)] Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system;
f) [SI-4 (16)] Correlate information from monitoring tools employed throughout the information system; and
g) [SI-4 (23)] Implement host-based monitoring mechanisms on information system components as defined by the System Owner.

9.17.5.4 Security Alerts, Advisories, and Directives (SI-5)

The ISSO shall:

a) Receive information system security alerts, advisories, and directives from US-CERT on an ongoing basis;
b) Generate internal security alerts, advisories, and directives as deemed necessary;
c) Disseminate security alerts, advisories, and directives to system security personnel and administrators with configuration/patch-management responsibilities including but not limited to the System Owner, System Program Managers, Privileged Users and other personnel with security-related responsibilities; and
d) Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

9.17.5.5 Security Function Verification (SI-6)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Verify the correct operation of security functions when anomalies are discovered;

b) Perform this verification upon system startup and restart or at least monthly upon command by users with appropriate privilege;
c) Notify Infinibyte Cloud System Administrators and Security Administrators of failed security verification tests; and
d) Restart or shut the information system down and notify Infinibyte Cloud System Administrators and Security Administrators when anomalies are discovered.

9.17.5.6 Software, Firmware, and Information Integrity (SI-7)

The IT Director and Architect shall ensure that Infinibyte Cloud systems use integrity verification tools to detect unauthorized changes to system software, firmware, and information.

The IT Director and Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SI-7 (1)] Perform an integrity check of System Owner-defined software, firmware, and information at startup, when a security-relevant event is identified, and at least monthly; and
b) [SI-7 (7)] Incorporate detection of unauthorized changes to the information system into the organizational incident response capability.

9.17.5.7 Spam Protection (SI-8)

If services are running that are subject to spamming, the IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
b) Update spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

If services are running that are subject to spamming, the IT Director and Architect shall also ensure that Infinibyte Cloud systems processing U.S. Government information:

a) [SI-8 (1)] Centrally manage spam protection mechanisms; and
b) [SI-8 (2)] Automatically update spam protection mechanisms.

9.17.5.8 Information Input Validation (SI-10)

The IT Director and Architect shall ensure that Infinibyte Cloud systems check the validity of information inputs, as defined by the System Owner.

9.17.5.9 Error Handling (SI-11)

The IT Director and Architect shall ensure that Infinibyte Cloud systems processing U.S. Government information:

a) Generate error messages that provide information necessary for corrective actions without revealing sensitive information that could be exploited by adversaries; and

b) Reveal error messages only to personnel authorized by the System Owner, such as the ISSO, Infinibyte Cloud System Administrators and Security Administrators.

9.17.5.10 Information Handling and Retention (SI-12)

The ISSO shall ensure that Infinibyte Cloud systems handle and retain both information within the information systems and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements as defined by the System Owner.

9.17.5.11 Memory Protection (SI-16)

The Architect shall ensure that Infinibyte Cloud systems implement System Owner-defined technologies to protect memory from unauthorized code execution.

9.17.6 System and Information Integrity Procedures

The IT Director shall ensure that procedures are written and in-place to support the implementation of this policy. These procedures shall be maintained and controlled by the ISSO in a restricted location and made available or distributed as needed.

APPENDICES

APPENDIX A: Acronyms

Acronym	Definition
3PAO	Third Party Assessment Organization
A&A	Assessment and Authorization
AO	Authorizing Official
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BIA	Business Impact Analysis
CCB	Change Control Board
CIS	Center for Internet Security
CONUS	Continental United States
CPC	Contingency Planning Coordinator
CPD	Contingency Planning Director
DoD	Department of Defense
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
IaaS	Infrastructure as a Service
IDPS	Intrusion Detection and Prevention Systems
ISPP	Information Security Policies and Procedures
ISSO	ISSO
IT	Information Technology
ITS	Information Technology Services
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
JAB	Joint Authorization Board
NIST	National Institute of Standards and Technology Information Processing Standards
NTP	Network Time Protocol
OMB	Office of Management and Budget
PDS	Protective Distribution System

Acronym	Definition
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PMO	Program Management Office
POA&M	Plan of Action and Milestone
POC	Point of Contact
RBAC	Role Based Access Control
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SP	Special Publication
SSL	Secure Sockets Layer
SSP	System Security Plan
SSS	Social & Scientific Systems
TIC	Trusted Internet Connection
U.S.	United States
US-CERT	United States Computer Emergency Readiness Team
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
VPN	Virtual Private Network