FRED HUTCH

Data Classification and Handling Policy

Version 4.0

Data Classification and Handling Policy

Responsible Official	Ex: VP, CIT	Date	Version
Reviewed by	VP, CIT; Enterprise Risk Sub-Committee	03/2021	4

Table of Contents

1. Background and Purpose

Fred Hutch relies on its Information Resources and the data contained within those resources to achieve its mission. Fred Hutch has promulgated an Information Security Policy (the "InfoSec Policy"), which is available here: https://centernet.fredhutch.org/cn/p/information-security-policy.html, to protect its Information Resources and to support the confidentiality, integrity, and availability of Information while complying with legislative, academic, research, regulatory and contractual information security requirements. This Information Classification and Handling Policy ("Policy") has been developed in conjunction with the InfoSec Policy and establishes along with the InfoSec Policy. Fred Hutch's organizational information security controls, requirements, and processes. Specifically, this Policy assists Fred Hutch Authorized Users in classifying and handling Fred Hutch information based on its level of sensitivity and value to Fred Hutch by:

- Establishing the classification levels of Fred Hutch information.
- Securely handling Fred Hutch information of varying classifications. These requirements include data protection, access controls and governance around information.
- Specifying how systems, software, applications, and other data handling processes must be implemented to ensure data security and governance are applied commensurate with information classification to protect Fred Hutch information

This Policy applies to all Information Resources and associated systems, processes and procedures used in the conduct of Fred Hutch operations and to all Authorized Users of Fred Hutch Information Resources.

2. Introduction

2.1. Compliance, Enforcement, and Sanctions

Any questions regarding this Policy should be submitted to Center IT Help Desk (helpdesk@fredhutch.org) or the Information Security Office (ISO) (iso@fredhutch.org).

Observance of every element of this Policy may not always be feasible, and the ISO manages and administers an exception process for these situations, which allows the ISO to grant an exception in its discretion:

- A written statement requesting an exception to this Policy may be submitted to the ISO for review and potential approval.
- Those requesting an exception may also collaborate with the ISO to propose an alternative solution.

Authorized Users who are deemed to be Information and/or Information Asset owners by virtue of their roles and responsibilities or by ISO designation, are accountable for monitoring the effectiveness of the information security controls and standards prescribed by this Policy. Teams that design, operate, implement, and/or use the information security controls mandated by this Policy have the responsibility of ensuring that the controls are implemented and remain effective.

Audits of compliance with this Policy shall be performed on a regular basis and may be undertaken at any time. Such audits may be performed by the Chief Ethics and Compliance Officer, the Director of Internal Audit, or by an outside individual or firm at the discretion of management.

Non-compliance with this Policy or any other Fred Hutch policies, standards, and procedures pertinent to the Information Resources may result in disciplinary action, including termination of the right to use Fred Hutch's Information Resources or termination of employment, as well as possible action by law enforcement authorities.

If you become aware of or suspect a violation of Fred Hutch's policies, immediately report the matter Center IT Service Desk (helpdesk@fredhutch.org) or ISO (ISO@fredhutch.org) or Human Resources. Concerns may also be reported to the Chief Ethics and Compliance Officer, the Director of Internal Audit, or the Office of the General Counsel. Finally, Fred Hutch offers confidential, anonymous reporting through the NAVEX Global Web site. NAVEX Global, is an independent third party selected to help Fred Hutch fulfill its commitment to compliance, ethical conduct, and workplace respect in all its programs and activities. The report you provide will be forwarded to the Chief Ethics and Compliance Officer with no identifying information about you, unless you choose to provide such information. If you prefer to speak to a NAVEX Global representative, you may call the hotline at **877-412- 8841.**

2.2. Responsibility

The security of Fred Hutch Information and Fred Hutch Information Resources are the fundamental responsibility of every Authorized User.

Center IT is responsible for the development and administration of this Policy as well as responsible for the Information Security Program in all its governance, assurance, and engineering forms. In fulfilling its responsibilities, the ISO collaborates with key Fred Hutch administrative, scientific and research staff, as well as affiliated organizations including Seattle Cancer Care Alliance, University of Washington, and Seattle Children's Hospital.

The ISO will review this Policy at planned intervals (at minimum, bi-annually) to ensure its continuing alignment with the Information security and organizational strategy, accuracy, relevance, and applicability to legal, regulatory and/or other compliance obligations.

3. Information Classification and Handling Policy

3.1. Scope

Authorized Users are accountable and responsible for complying with this Policy. This Policy applies to every existing or planned implementation of technology or paper-based processes that will handle, process, or store Information.

This Policy covers the following:

- Information Classification Levels
- Information Handling Requirements

This Policy does not specify detailed baselines for implementing recommended security features with applications or infrastructure. See any supporting departmental procedure documentation for instruction.

This Policy does not address Fred Hutch record retention requirements. To see the **Fred Hutch Record Retention and Destruction Policy**, go to:

https://centernet.fredhutch.org/cn/p/record-retention-and-destruction-policy.html

3.2. Accountability

Responsibilities of All Authorized Users

Fred Hutch Authorized Users are accountable and responsible for complying with this Policy. FH Authorized Users must (i) understand FH's data classifications; (ii) consider how these classifications apply to the FH Data under their control; and (iii) implement the security and handling requirements for each classification Teams that design, operate, implement, and/or use these information security controls have the responsibility of ensuring that the controls are implemented and remain effective.

In the event Authorized Users are required or choose to transmit information to third parties, steps must be taken to ensure that the requisite handling requirements apply to such transmission and recipient parties maintain data in commensurate security and handling environments. In some case, data access and use agreements will be necessary to accomplish this objective. The Fred Hutch Office of the General Counsel can be consulted for assistance with establishing any necessary agreements.

Violations of this Policy are referred to HR and may result in discipline, up to and including termination of employment or loss of access privileges.

4. Information Classification Standard Levels and Handling Requirements

Fred Hutch recognizes three levels of information classification. Classification is based on the sensitivity and value of the Information, with Level I being the least confidential and Level III being the most confidential.

- Level I: **Public Domain**- Fred Hutch information appropriate for public view or usage. There is low to no risk from disclosure.
- Level II: **Confidential**- Organizational unit information that is on a need-to-know basis. There is moderate risk from disclosure.
- Level III: **Restricted**- Highly sensitive data that requires strict access and security controls. There is high risk from disclosure.

Information owners and/or their delegates must ensure that all the Information created, input, stored, processed, output by a system or process, or shared between either systems and/or people must be reviewed to identify classification levels.

Information handling requirements are listed under each classification level. All systems and processes shall comply with these requirements prior to implementation.

4.1. Level I: Public Domain – Low to No Risk from Disclosure

4.1.1. Definition of Level I Data

The Public Domain/Low classification applies to Fred Hutch information suitable for public consumption. This level of Information is not considered confidential or restricted in nature and can be released to the public.

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operation, organizational assets, or individuals. No safeguards or protective measures are needed to protect this category of Information from disclosure.

Examples include, but are not limited to, the following:

- Published research results
- Fred Hutch publications and communications [e.g., marketing materials, annual financial statements (after release), press announcements (post publication), public record documents, job postings, etc.]
- Open source software code, configuration, and recipes (e.g., https://github.com/FredHutch/galaxy_ftp)
- Reference genomes
- Released datasets
- Public cryptographic keys

4.1.2. Requirements for Level I Data

Handling Methods

Handling Method	Requirement
Email	Encrypted email preferred
Workstation, Laptop, MCD Storage:	Information may be encrypted in local storage (automatically encrypted local storage is acceptable)

4.2. Level II: Confidential- Moderate Risk from Disclosure

4.2.1. Definition of Level II Data

Confidential data is sensitive, confidential, or private information to Fred Hutch and its operations. It is intended only for internal use on a need-to-know basis between organizational units. If released, organizational units could lose competitive advantages, incur minor to moderate financial or legal consequences, or lose public trust.

The Confidential/Moderate classification applies to Information for which unauthorized disclosure, destruction, or alteration of which reasonably could be expected to cause minor to moderate harm to Fred Hutch, its property, or its personnel, including financial loss, legal liability, or harm to reputation. Data in Level ll are considered Sensitive Data.

Confidential/Moderate Information is made available only to individuals with the need and authorization to access it. Because the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, access to other institutions or external individuals is provided with a confidentiality agreement/pledge or information access and/or use agreement. See tables below for handling and security controls applied this type of information.

Examples include, but are not limited to, the following:

- Pre–publication research information and analyses not authorized for release or distribution
- Medical expense information
- Financials
- Legal instruments or agreements
- Transaction documents and reports
- Names and identifiers of servers, drives, and files containing sensitive information.
- Building plans and information about the physical plant
- De-identified research participant information
- Donor information

- Sensitive metadata
- Business strategies – current and future
- Corporate policies, standards, guidelines, and other program documents
- Employee identification numbers
- Server names and IP addresses
- DNS and LDAP info
- Vendor data
- HR data (background checks, salary info, benefits, reviews, personal addresses)

4.2.2. Requirements for Level II Data

Required Handling Methods:

Handling Method	Requirement
On-Premise electronic storage	FH Administrative Control, role-based access control, authentication required
Cloud-Based, Other Off-Premise	Encrypted in transit; authentication; access logging
Electronic Portable Device	Securely stored in controlled area.
Workstation, Laptop, MCD Storage	Encrypted in local storage (automatically encrypted device storage is acceptable)
Electronic Transfer	Encrypted in transit, recipients' systems secure
Transport Media	Secure transport by authorized personnel
Media Re-use Disposal	Sanitized or destroyed before retirement
Access Logging	Date/ time/user/permission change/other activity
Email	FH supported email
Paper (existing grandfathered until modified)	Secure storage, reasonable manual access logging, exposure safeguarding (not left at printer, scanner, or desk)
Mailing/Shipping	"Confidential" label

Required Security Controls:

Security Control	Requirement
Data Encryption	In transit and at rest. (FIPS 140-2, where applicable).

Authentication	Users are to be uniquely authenticated before granted access. Multi-factor Authentication (MFA) should be used when available.
Access Logging	Date/ time/user/permission change/other activity. Reviews should be conducted, at a minimum, on an annual basis.
Access Control	Role-based
Electronic Transfer	Security of sending and receiving systems verified
Storage Management	FH supported local network storage, cloud storage, and email. Encrypted local machine and device storage.
Media Transport	Secure transport by authorized personnel
Media Re-use Disposal	Sanitized or destroyed before retirement
Media Labeling	"Confidential" label for mailing/shipping
Media Protection	Paper documents not exposed or left unattended at printer, scanner, or desk

4.3. Level III: Restricted – High Risk from Disclosure

4.3.1. **Definition of Level III data**

Restricted data is highly sensitive data that requires a need-to-know basis. Restricted data includes data that is protected by governments orders, laws, and regulations. Disclosure of this type of information can result in significant financial or legal consequences.

The Restricted/High classification applies to Information for which unauthorized disclosure, destruction, or alteration reasonably could be expected to cause serious to catastrophic harm to Fred Hutch, its property, or its personnel, including severe financial loss, legal liability, public distrust, or harm to reputation. Access is provided to other institutions or external individuals with a confidentiality agreement/pledge or information access and/or use agreement. See tables below for handling and security controls applied to this type of Information. Data in Level lll are considered Restricted Data.

Examples could include, but are not excluded to, the following:

- Protected Health Information (PHI), Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), and Personally Identifiable Information (PII)
- Controlled Unclassified Information compliant with NIST 800-171
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements.
- U.S. Government Classified Data
- Legally privileged information
- Patentable or data related to current or potential IP

- Information that is the subject of a confidentiality agreement or NDA
- Donor Contact Information and Non-Public Gift Information
- Encumbered - Private Trial Sponsor
- Financial Data Individually Identified
- Human Data Identified Foreign Country (GDPR, Other)
- Passwords and private encryption keys
- Proprietary information, including that belonging to entities other than Fred Hutch
- Electronic communication and documents regarding personal or financial matters or other sensitive subjects
- Hardware or software authentication and/or authorization keys

4.3.2. **Requirements for Classification Level lll**

Required Handling Methods:

Handling Method	Requirement
On-Premise electronic storage	Administrative Control, role-based access control, authentication required, encrypted at rest/transit
Cloud-Based, Other Off-Premise	Encrypted in rest/transit, authentication, security agreement
Electronic Portable Device	Securely stored in controlled area, encrypted
Workstation, Laptop, MCD Storage	Encrypted in local storage (automatically encrypted device storage is acceptable)
Electronic Transfer	Encrypted in Transit, recipients' systems secure
Transport Media	Secure transport by authorized personnel, documented
Media Re-use Disposal	Sanitized or destroyed before retirement
Access Logging	Date/ time/user/permission change/other activity, semi-annual audit
Email	FH supported email, encrypted, Email Delivery Instructions
Paper (existing grandfathered until modified)	Secure storage, manual access logging, exposure safeguarding (not left at printer, scanner, or desk)
Mailing/Shipping	"Restricted" label, instructions

Required Security Controls:

Security Control	Requirement
Data Encryption	In transit and at rest. (FIPS 140-2, where applicable).
Authentication	Users are to be uniquely authenticated before granted access. Multi-factor Authentication (MFA) should be used when available.
Access Logging	Date/ time/user/permission change/other activity. Reviews should be conducted, at a minimum, on a semi-annual basis.
Access Control	Role-based
Electronic Transfer	Security of sending and receiving systems verified
Storage Management	FH supported local network storage, cloud storage, and email. Encrypted local machine and device storage.
Media Transport	Secure transport by authorized personnel, documented
Media Re-use Disposal	Sanitized or destroyed before retirement
Media Labeling	"Restricted" label for mailing/shipping
Media Protection	Paper documents not exposed or left unattended at printer, scanner, or desk

4.3.3. **Controlled Unclassified Information**

Controlled Unclassified Information (CUI) is federal non-classified information the U.S. Government creates or possesses, or that a non-federal entity receives, possesses, or creates for on behalf of the U.S Government. CUI requires information security controls to safeguard or disseminate. These controls must be compliant with the federal regulations specified in 32 CFR Part 2002 (link is external) and NIST SP 800-171 (link is external).

"Information" as defined by the federal CUI Program may include research data and other project information that a research team receives, possesses, or creates in the performance of a sponsored contract. CUI at Fred Hutch is categorized as Level III information. When working with CUI:

Handling Method	
Verify research project will/has received or generate CUI	
Required Documentation Markings	https://www.archives.gov/cui/registry/category-marking-list https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf
Limited Dissemination Controls	https://www.archives.gov/cui/registry/limited-dissemination

Security Control
All systems that use, transmit, or store CUI are required to follow the same handling methods and security controls as **Level III: Restricted Data.**

5. Appendix 1- Definitions

Term	Definition
Authorized User	Fred Hutch employees and Fred Hutch agents, contractors, and other non-employees, including any individual or entity that has authorization from Fred Hutch to access, store, or transmit Fred Hutch Information. Authorized Users include users in possession of, or access to, Fred Hutch Information located at facilities not owned or operated by Fred Hutch, and to circumstances in which non-Fred Hutch devices, processes, or technologies are utilized to obtain access to Fred Hutch systems and/or Fred Hutch Assets or Information.
Confidential Information	The Confidential/Moderate classification applies to Information for which unauthorized disclosure, destruction, or alteration of which reasonably could be expected to cause minor to moderate harm to Fred Hutch, its property, or its personnel, including financial loss, legal liability, or harm to reputation. Data in Level ll are considered Sensitive Data.
De-identified Information	Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. One method, the Safe Harbor method, de-identifies by removing or otherwise obfuscating the 18 HIPAA PHI fields identified in the de-identification guidance from Health and Human Services (HHS) These can be found at www.DHS.com.

Email Delivery Instructions	Template: “This electronic message transmission contains information which may be confidential or privileged. The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender by telephone or by electronic reply, and delete this message.”
Fred Hutch Data	Data created or received by FH Authorized Users while acting on behalf of FH. This does not include intellectual or proprietary data or property owned, licensed, or otherwise legally controlled by a third party.
Individually Identifiable Information (III)	Information that contains elements that either identify an individual or could be used in combination with other easily accessible information to identify an individual in either paper based or electronic format.
Individually Identifiable Health Information (IIHI)	Identifiable health information (in any form or media, whether electronic, paper, or oral including demographic data) that relates to: the individual’s past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).
Information	Any information or processed data, including words, numbers, images, and sounds that Fred Hutch owns, hosts, licenses, stores or manages in any form, for any length of time including employee records, financial reports, and research data.
Information Classification	A designation used to determine the level of safeguards necessary to protect the confidentiality and integrity of various types of information.

Information Resources	Any service, software, technology, procedures, systems, equipment, or devices that are employed, designed, built, operated, maintained, owned , or leased by Fred Hutch and which are used to collect, record, process, store, retrieve, display, transfer, or administer Fred Hutch
Personally Identifiable Information (PII)	An individual's first name or first initial and last name in combination with any one or more data elements which enable identification, such as Social Security number, driver's license number, account number with any required security code, full date of birth, private key unique to an individual to access an electronic record; passport identification number, death insurance policy number or health insurance identification number, medical history or care, or Biometric data.
Protected Health Information (PHI)	Individually Identifiable Health Information (in either paper or electronic format) generated and/or maintained by a Covered Entity as defined by HIPAA. Covered Entities typically include, but are not limited to health care providers, health care facilities, and health insurers. For example: Fred Hutch's self-insured employee health plans are considered to be covered entities and as such their IIHI is PHI and the plans are subject to the requirements of HIPAA Rules. The University of Washington, SCCA, and Seattle Children's Hospital are also covered entities.
Public Information (Level I)	The Public/Low classification applies to Information for which unauthorized disclosure, destruction, or alteration reasonably could be expected to have a limited adverse effect on organizational operation, organizational assets, or individuals. No safeguards or protective measures are needed to protect this category of Information from disclosure.

Restricted Information	The Restricted/High classification applies to Information for which unauthorized disclosure, destruction, or alteration reasonably could be expected to cause serious to catastrophic harm to Fred Hutch, its property, or its personnel, including severe financial loss, legal liability, public distrust, or harm to reputation. Access is provided to other institutions or external individuals with a confidentiality agreement/pledge or information access and/or use agreement. Data in Level Ill are considered Sensitive Data.
Sanitize	A general term referring to the actions taken to render information written on media unrecoverable by both ordinary and extraordinary means.
System	The combination of software (application), information, and platform needed to deliver a service to the end user.

6. Appendix 2- Data Types

This chart identifies common data types and their corresponding Level II or III Classification.

Data Type	Description & Examples	Data Classification
Attorney/Client Privileged Information	Confidential communications between a client and an attorney for the purpose of securing legal advice.	Level III
Attorney Working Documents	Internal investigation information, pre-litigation, and non-public litigation and administrative agency charge, audit, and inquiry information.	Level III
Controlled Unclassified Information (CUI) Requires application of specific regulations **(32 CFR Part 2002 and (NIST SP 800-171)** and marking language. Categories of CUI can be found at here.	Information ***government (Executive Branch) creates or possesses, or a non-government entity creates or possesses on behalf of the government that*** requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies, but is not classified under Executive Order 13526 *or the Atomic Energy Act, as amended.* (https://www.archives.gov/cui/about). These controls must be compliant with the federal regulations specified in 32 CFR Part 2002 and NIST SP 800-171.	Level III
Contractual Non-Disclosure/NDA	Information, materials, data, and records designated confidential by contract, including information obtained by the University from third parties under non-disclosure agreements or any other contract that designates third party information as confidential	Level III
Departmental Administration	Budgetary, departmental, or University planning information. Non-public financial, procurement, health/safety, audit, insurance and claims information.	Level II (Aggregated) Level III (Identified)

Data Type	Description & Examples	Data Classification
Export Controlled Research (ITAR, EAR)	Export Controlled Research includes information that is regulated for reasons of national security, foreign policy, anti-terrorism, or non-proliferation. The International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) govern this data type. Current law requires that this data be stored in the U.S and that only authorized U.S. persons be allowed access to it. • Chemical and biological agents • Scientific satellite information • Certain software or technical data • Military electronics • Nuclear physics information • Documents detailing work on new formulas for explosives	Level lll
FISMA Data	The Federal Information Security Management Act (FISMA) requires federal agencies and those providing services on their behalf to develop, document, and implement security programs for information technology systems and store the data on U.S. soil. This means that, under some federal contracts or grants, information the FH collects or information systems that FH uses to process or store research data need to comply with FISMA.	Level lll
GDPR - Sensitive Information under EU's General Data Protection Regulation	The following personal data is considered 'sensitive' and is subject to specific processing conditions: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership, genetic data, biometric data processed solely to identify a human being, health-related data; data concerning a person's sex life or sexual orientation.	Level lll

Data Type	Description & Examples	Data Classification
Identifiable Human Subject Research	Individually identifiable research data containing sensitive information about human subjects, included coded-data with a key.	Level lll
Payment Card Industry (PCI) Information	Information related to credit, debit, or other payment card, such as credit/debit card account number or expiration date.	Level lll
Personal Identifiable Information (PII)	See definition in Appendix 1: Definitions. Examples: • Name • Address • Social Security Number • Driver's License Number • Passport Number	Level lll
Proprietary	Proprietary intellectual property in which FH asserts ownership that is created by FH employees in connection with their work (Trade Secrets). Proprietary information or data may also pertain to content, data or materials provided to FH Authorized Users by a third party or developed by FH Authorized Users for a third party, such as industry sponsor, under contractual agreement. Parts of a FH NIH Award application may be designated as proprietary to shield release under FOIA.	Level lll
Protected Health Information	See definition in Appendix 1: Definitions. Examples: • Medical History • Prescription History • Health Insurance Details • Family Medical Records • Disabilities, Special Requirements	Level lll

Data Type	Description & Examples	Data Classification
Student Education Records (FERPA)	Records that contain information directly related to a student and that are maintained by FH or by a person acting for FH. Governs release of, and access to, student education records.	Level lll
Security Access Information about systems or applications which hold sensitive Level ll or Level lll data.	Authentication keys, passwords, server name, (other)	Level lll
Unpublished Research	Unpublished grant proposals, research data, manuscripts, and associated correspondence.	Level lll

7. Contacts

Information Security Office (ISO@fredhutch.org)

8. References

FIPS 199

NIST 800-53/800-171

As with nearly all industry segments, FH adopts federally developed security standards and controls. NIST Federal Information Processing Standard (FIPS) 199 (Standards for Security Categorization of Federal Information and Information Systems) is used by FH as the authoritative reference used for categorizing its information and Information Systems. FIPS bases categorization on the risk associated with compromising confidentiality, integrity, or availability. NIST Special Publication (SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, is the authoritative reference used in defining the specific administrative, physical, and technical controls that are required for compliance with the Fred Hutch Information and Classification Standard. NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems, is derived from FIPS 199 and SP 800-53, and focuses on the application of security and privacy controls on the protection of federal data created or held in nonfederal systems. Due to the length of the control descriptions, this table provides links to related controls in SP 800-53. Contact the ISO for clarification if needed.

Control	Description
Technical Access Control AC-3 Access Enforcement	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=50
Technical Access Control AC-4 Information Flow Enforcement	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=55
Technical Access Control IA-2 Identification and Authentication	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=159

Operational Media Protection MP-4 Media Storage	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=199
Operational Media Protection MP-6 Media Sanitization	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=201
Operational Personnel Security PS-3 Personnel Screening	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf#page=250

9. Revision History

These entries describe the general revision history of the document.

Rev. #	Rev. Date	Authors	Change Description
1.0	October 13, 2017	Lisa Coleman Gerianne Sands Mary Gardner Ric Testagrossa Glenn Kaleta Chris Briggs	Initial version
2.0	March 23, 2018	Chris Briggs	Contacts section added. Workstation et al local storage encryption requirement added
3.0	October 12, 2018	Lisa Coleman David Krogh Mike Nescot Mary Stoll Eric Valentine	Annual review
4.0	March 9, 2021	Mike Nescot Susan Glick	Simplified language, replaced title “Strictly Confidential” with “Restricted” to align with industry standard, added handling requirements for Controlled Unclassified Information (CUI), refined some of the definitions, added references to Data Governance, added section “Data Types” for clarification and reference, clarified NIST frameworks.