Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-2002**
Office Instruction Title:	**System Backup Standard**
Revision Number:	**2.0**
Effective Date:	**September 17, 2018**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-2002, “System Backup Standard,” provides the minimum security requirements that must be met for system and data backups.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	8/23/18
CIO	David Nelson	/RA/	8/28/18
CISO	Jonathan Feibus	/RA/	8/23/18

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-2002

System Backup Standard

---

1 PURPOSE

CSO-STD-2002, “System Backup Standard,” provides the minimum security requirements that must be applied to all Nuclear Regulatory Commission (NRC) system and data backups.

This standard is intended to be used by system administrators and Information System Security Officers (ISSOs), to ensure that system backups are performed in accordance with this standard.

2 GENERAL REQUIREMENTS

This section addresses the general requirements that all system administrators, and ISSOs, who are authorized to administer system backups must comply with as the minimum set of controls. System backups ensure critical information integrity and availability in the event of data corruption, hardware failure, or site-wide disaster. Effective backup and recovery procedures are critical for continued operations.

System backups must be protected according to the highest sensitivity of information that is processed, stored, or transmitted by the system and stored on the backup media. All system backups must conform to the set of requirements specified in this standard and Contingency Planning (CP) controls specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (as amended), “Security and Privacy Controls for Federal Information Systems and Organizations.”

3 SPECIFIC REQUIREMENTS

This section provides specific security requirements that apply to all system backups. Typical backup methods include full image backups, full backups, data replication, differential backups, and incremental backups.

Backup media can include optical disk, solid state drive (SSD) or magnetic hard drive. System administrators should purge unnecessary files from systems prior to scheduled backups to reduce the time required to perform the backup, restore the backup, and to reduce the storage space required. System owners should ensure that backup processes are performed during off peak hours of system use.

The following sections provide the specific backup requirements for backup creation, transportation, storage, and testing.

3.1 Backup Creation and Validation

The following requirements for backup creation, recovery, and validation apply:

- The system owner must ensure backup and recovery procedures are developed, documented, approved, maintained, and used for all systems operated by or on behalf of NRC. The procedures must be approved by the system ISSO.
- Backup and recovery procedures must be managed within the configuration management and change control processes for the system to which the procedures apply, and treated as official agency records by posting the procedures in the Agencywide Documents and Access Management System (ADAMS).
- The criticality of information systems, data, and allowable outage time for the information system must be assessed and documented within the system Business Impact Analysis (BIA) to ensure appropriate procedures are developed and resources allocated to the backup and recovery process.
- All backups must be stored on media separate and distinct from the operational system.
- Backup copies of all records of software licensing must be stored with the appropriate backup media.
- The system owner must ensure that the chosen backup and recovery methods and frequencies are sufficient to meet or exceed CSO-STD-0020, “Organization Defined Values for System Security Controls,” and system BIA and System Security Plan (SSP) requirements.
- The system owner must ensure that all backup methods, minimum frequencies, and associated information types are documented within the SSP and/or BIA.
- The system owner must document the relative point-in-time (e.g., the maximum number of hours, days, or months) the backups provide the ability to restore user-level and system-level information in the system.
- Encryption methods will be employed to protect the confidentiality and integrity of system backups. Encryption will be performed in accordance with CSO-STD-2009, “Cryptographic Control Standard.”
- Accurate logs of backup contents, the date and time of the backup, and the backup storage location(s) must be maintained.
- All backups must be labeled using labels containing at least the following information in accordance with CSO-STD-2004, “Electronic Media and Device Handling:”
    - Date of backup
    - Unique system identifier
    - Backup method (e.g., full image, incremental, replication)
    - Type of information backed-up (e.g., user-level information, system information)

The following list provides a recommended set of periodic backups to assist in meeting system recovery and restoration requirements. The list includes the suggested frequency, specific data types to include in the backup, and possible backup methods:

1. Daily – Each system business day a backup of the user-level information that is found in the system must be performed. This is a full, differential, or incremental backup that includes the changes made to the system since the last backup was performed.
2. Weekly – Each week a full backup of all user-level and system-level information contained in the system must be performed.
3. Quarterly or as needed – Full image backups of the system images must be performed at least quarterly and within two weeks of any system image change.

3.2 Backup Transportation and Access

Backup data will be physically protected during media transport by authorized means to or from offsite storage in addition to the cryptographic protection.

3.3 Backup Storage

The following requirements for system backup storage apply:

- One backup copy must be transferred and stored at an approved and secured offsite storage facility immediately after its creation.
- The second copy must remain at the location where the system is operating for a rapid recovery from a system failure. The backup copies will be protected from water, fire, and electrical damage.
- Retention periods for backups must be sufficient to meet system restoration requirements and NRC and National Archives and Records Administration (NARA) document retention requirements. Longer retention requirements can be specified in the BIA for any system or system component.
- An alternate storage site will be established and maintained for backups of moderate and high systems in accordance with Contingency Planning requirements specified in NIST SP 800-53 (as amended).
- Alternate storage locations must comply with NIST SP 800-34 (as amended), “Contingency Planning Guide for Federal Information Systems.”

3.4 Cloud-Based Backup

The system owner can specify use of cloud-based backup service for sensitive but unclassified information by utilizing only Federal Risk and Authorization Management Program (FedRAMP) compliant cloud service providers.

The FedRAMP cloud service provider must have a Federal Information Processing Standard (FIPS) 199 (as amended), “Standards for Security Categorization of Federal Information and Information Systems,” security categorization that meets or exceeds the level of the NRC information that will be backed up on the service and must be approved for use by the NRC Authorizing Official (AO) for this purpose.

3.5 Recovery Testing

The system owner will test their ability to restore information from their backups to verify media reliability and information integrity according to the following timeframes:

- *Annually* for moderate availability sensitivity systems
- *Semi-annually* for high availability sensitivity systems
- *Monthly* for National Security Systems (NSS)

The capability to reimage information system components within 24 hours from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components will be provided for high sensitivity and classified systems. Classified system owners will ensure a near-real-time failover capability is provided for the information system as mission needs require.

APPENDIX A. ACRONYMS

ADAMS	Agencywide Documents and Access Management System
AO	Authorizing Official
BIA	Business Impact Analysis
CP	Contingency Planning
CSO	Computer Security Organization
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
ISSO	Information System Security Officer
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSS	National Security Systems
OCIO	Office of the Chief Information Officer
SP	Special Publication
SSD	Solid State Drive
SSP	System Security Plan
STD	Standard

APPENDIX B. GLOSSARY

Differential backup	Contains the changes made since the last full backup was performed.
Full backup	Includes all computer and system data.
Full image backup	An exact electronic image of the operating system and data storage media.
Incremental backup	Contains the changes made since the last backup was executed.
Replication	Automatically distributes changes to a primary computer or data source on other computers or data sources, which are referred to as secondary.
System business day	A day in which normal operations for an information system are conducted. This is generally Monday, Tuesday, Wednesday, Thursday, or Friday, and typically excludes weekends and holidays; other systems may only operate during specific timeframes within the year, (e.g., if a system supports a specific event or activity). System business days are defined in the information system's BIA.
System-level information	Information that pertains to the operating system, programs, configuration files, and information system documentation.
Unnecessary files	Files that are not important to the NRC mission, the user, or needed to reconstitute the system.
User data	Files that are important to the users and are needed to continue their job functions after a recovery from an incident or a catastrophic event. Examples include user email archives and documents.
User-level information	Program and user data.

CSO-STD-2002 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
21-Jan-10	1.0	Initial issuance	Distribution at ISSO forum and posting on ISD Web page	Upon request
14-Dec-10	1.1	Added system backup information extracted from the MD 12.5 draft.	Distribution at ISSO forum and posting on ISD Web page	Upon request
19-Sep-12	1.2	Modified test of backup for NSSs to match CNSSI 1253 minimum value of monthly. Modified in response to Standards Working Group feedback.	Distribution at standards working group, ISSO forum, and posting on the ISD Web page	Upon request
21-Aug-18	2.0	Updated with latest requirements.	Post to OCIO/CSO Web page	Upon request
7-Jan-19	2.0	Errata changes for document identifier and organizational changes.	Post to OCIO/CSO Web page	N/A
8-Sep-20	2.0	Errata changes to replace master and slaves to primary and secondary terms in Appendix B, Glossary.	Post to OCIO/CSO website	N/A