

Nuclear Regulatory Commission  
 Computer Security Office  
 Computer Security Standard

---

Office Instruction: **CSO-STD-2002**

Office Instruction Title: **System Back-up Standard**

Revision Number: **1.2**

Effective Date: **December 1, 2012**

Primary Contacts: **Kathy Lyons-Burke, SITSO**

Responsible Organization: **CSO/PST**

Summary of Changes: CSO-STD-2002, "System Back-up Standard," provides the standard that must be met for system and data back-ups.

Training: As requested

ADAMS Accession No.: ML100210144

Approvals				
Primary Office Owner	Policies, Standards, and Training		Signature	Date
<b>Standards Working Group Chair</b>	Bill Dabbs		/RA/	9/19/12
<b>Responsible SITSO</b>	Kathy Lyons-Burke		/RA/	9/19/12
<b>CSO Standards DAA</b>	CISO	Tom Rich	/RA/	9/24/12
	Director, OIS	Jim Flanagan	/RA/	9/26/12

**TABLE OF CONTENTS**

**1 PURPOSE ..... 1**

**2 GENERAL REQUIREMENTS ..... 1**

**3 SPECIFIC REQUIREMENTS ..... 1**

    3.1 BACK-UP CREATION AND VALIDATION ..... 2

    3.2 BACK-UP TRANSPORTATION AND ACCESS..... 3

    3.3 BACK-UP STORAGE ..... 3

    3.4 RECOVERY TESTING..... 4

**4 DEFINITIONS..... 5**

**5 ACRONYMS..... 7**

# Computer Security Standard CSO-STD-2002

## System Back-up Standard

---

### **1 PURPOSE**

The purpose of CSO-STD-2002, "System Back-up Standard," is to provide the standard that must be met for system and data back-ups. In addition to supporting good computer security practices, this standard also supports International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27002, "Information technology — Security techniques — Code of practice for information security management" and National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" controls CP-6, CP-9, and CP-10.

### **2 GENERAL REQUIREMENTS**

The purpose of data back-up requirements are to ensure information necessary for operation is available for restoring system and mission supported operations. System back-ups ensure critical information integrity and availability in the event of data corruption, hardware failure, or site-wide disaster. Effective back-up and recovery procedures are critical for continued operations. Unanticipated incidents, such as hard drive and other system failures, can result in devastating consequences if back-up data is not available to restore operation. Back-ups must be protected according to the highest sensitivity of information that is processed, stored, or transmitted by the system and stored on the back-up media. This document applies to all systems.

### **3 SPECIFIC REQUIREMENTS**

Typical back-up methods include full image back-ups, full back-ups, data replication, differential back-ups, and incremental back-ups. Software restored on a computer other than the source of the back-up may require specific configuration attributes to ensure that any software license attributes (e.g. MAC address) are addressed. This may require correspondence with the vendor concerning activation of the software license when restoring the back-up to a different computer.

Back-up media can include magnetic tape, optical disk, or magnetic hard drive. System administrators should purge unnecessary files from systems prior to scheduled back-ups to reduce the time required to perform the back-up and restore the back-up and to reduce the storage space required. System owners shall ensure that back-up processes are performed during off peak hours of system use.

The following sections provide the specific back-up requirements for back-up creation, transportation, storage, and testing.

### 3.1 Back-up Creation and Validation

The system owner must ensure back-up and recovery procedures are developed, documented, approved, maintained, and used for all systems operated by or on behalf of NRC. Back-up and recovery procedures must be managed within the configuration management and change control processes for the system to which the procedures apply, and must be treated as official agency records. The criticality of information systems, data, and allowable outage time for the information system must be assessed to ensure appropriate procedures are developed and resources allocated to the back-up and recovery process. All back-ups must be stored on media separate and distinct from the operational system. At least two copies of each back-up must be maintained. Back-up copies of all records of software licensing must be stored with the appropriate back-up media.

Back-ups must be performed on all information systems to meet or exceed the recovery and restoration requirements specified in NIST Special Publication 800-53; CSO-STD-0020, "Organization Defined Values for System Security Controls;" the System Security Plan (SSP); and Business Impact Analysis (BIA). System owners can identify the system back-up methods (e.g., full, differential, incremental, or full image back-ups) and frequencies (e.g., daily, weekly). System owners must ensure that the chosen back-up methods and frequencies are sufficient to meet or exceed NIST SP 800-53, CSO-STD-0020, and system BIA requirements. The system owner must ensure that all back-up methods, minimum frequencies, and associated information types are documented within the SSP and/or BIA. The system owner must also document the relative point in time the back-ups provide the ability to restore user-level and system-level information in the system. Please refer to the examples below, which provide the relative point in time based on the periodic back-ups and times specified:

- Example 1:

If the following periodic back-ups are used:

- 1) Daily (each system business day) – Incremental back-up of user-level information.
- 2) Weekly – Full back-up of user-level and system-level information.

Then, the system can restore information to the following relative point in time:

- 1) User-level information: Restore information as of the prior system business day.
- 2) System-level information: Restore information as of the prior week.

- Example 2:

If the following periodic back-ups are used:

- 1) Daily - Incremental back-up of user-level information
- 2) Monthly – Full back-up of user-level and system-level information.

Then, the system can restore information to the following relative point in time:

- 1) User-level information: Restore information as of the prior system business day.
- 2) System-level information: Restore information as of the prior month.

- Example 3:

If the following periodic back-ups are used:

- 1) Weekly – Incremental back-up of user-level and system-level information.
- 2) Monthly – Full back-up of user-level information.
- 3) Quarterly - Full back-up of system-level information.

Then, the system can restore information to the following relative point in time:

- 1) User-level and system-level information: Restore information as of the prior week.

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

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

All back-ups must be performed in such a way that the data can be recovered as needed. Accurate logs of back-up contents, the date and time of the back-up, and the back-up storage location(s) must be maintained.

Encryption methods shall be employed to protect the confidentiality and integrity of system back-ups. Encryption shall be performed in accordance with CSO-STD-2009, "Cryptographic Control Standard."

All back-ups must be labeled using human readable labels containing at least the following information in accordance with CSO-STD-2004, "Electronic Media and Device Handling."

- Date of back-up
- Unique system identifier
- Back-up method (e.g., full image, incremental, replication)
- Type of information backed-up (e.g., user-level information, system information)

### **3.2 Back-up Transportation and Access**

Back-up data shall be physically protected during media transport to or from offsite storage in addition to the cryptographic protection. Only authorized individuals shall handle and transport back-up media and their access must be periodically reviewed for appropriateness.

### **3.3 Back-up Storage**

One of the back-up copies shall be transferred and stored at an approved and secured offsite storage facility immediately after its creation. This allows for recovery from situations in which the primary facility is damaged or inaccessible. The second copy shall remain at the location

where the system is operating for a rapid recovery from a single system or hardware failure. Back-ups shall be protected from water, fire, and electrical damage. Retention periods for back-ups 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 Business Impact Analysis for any system or system component.

An alternate storage site shall be established and maintained for back-ups of moderate and high systems. The alternate storage site must be separated from the primary storage site so as not to be susceptible to the same hazards, should be supplied by a power source different from the primary data center, and should be provisioned by an alternate or duplicate Internet service provider in order not to be susceptible to the same hazards. Accessibility problems for the site shall be identified along with any mitigating actions required in the event of an area-wide disruption or disaster. For high impact systems, this site shall be configured in accordance with recovery time and recovery point objectives as required for business continuity management.

Alternate storage locations must comply with NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems."

### **3.4 Recovery Testing**

The system owner shall test their ability to restore information from their back-ups 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 (NSSs)

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 shall be provided for high sensitivity and classified systems. Classified system owners shall ensure a near-real-time failover capability is provided for the information system as mission needs require.

## 4 DEFINITIONS

Differential back-up	A differential back-up contains the changes made since the last full back-up was performed.
Full back-up	A full back-up includes all computer and system data.
Full image back-up	A full image back-up is an exact electronic image of the operating system and data storage media.
Incremental back-up	An incremental back-up contains the changes made since the last back-up was executed.
Program data	The data supporting computer programs, such as database data files, web application files, and web server files.
Replication	Replication automatically distributes changes to a master computer or data source on other computers or data sources, which are referred to as slaves.
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 Business Impact Analysis (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

This page intentionally left blank.

## 5 ACRONYMS

BIA	Business Impact Analysis
CP	Contingency Plan
CSO	Computer Security Office
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
MAC	Media Access Control
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
SP	Special Publication
SSP	System Security Plan

## 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 CSO web page	Upon request
14-Dec-10	1.1	Added system back-up information extracted from the MD 12.5 draft	Distribution at ISSO forum and posting on CSO web page	Upon request
19-Sept-12	1.2	Modified test of back-up 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 CSO web page.	Upon request