**Contents**

[Purpose: 3](#_Toc429125540)

[SOP Scope: 3](#_Toc429125541)

[Responsibilities 3](#_Toc429125542)

[Definitions 3](#_Toc429125543)

[Procedures: 3](#_Toc429125544)

[Risk Assessment and Control 3](#_Toc429125545)

[Backup Content and Schedule 4](#_Toc429125546)

[Backup Review 4](#_Toc429125547)

[Backup Storage 5](#_Toc429125548)

[Backup Verification Log Review 5](#_Toc429125549)

[Backup Verification Log 6](#_Toc429125550)

[Appendix – Issues Log 8](#_Toc429125551)

# Purpose:

This SOP defines the steps and controls necessary to back up the Information Technology data and systems used in regulated activities, so it is available if necessary for system restoration or recovery.

# SOP Scope:

This SOP applies to all computer-based systems, and any electronic equipment in the infrastructure necessary to keep the computer systems in operation.

# Responsibilities

The IT Manager is responsible for implementing and maintaining the backup processes for computer-based systems and associated records.

# Definitions

The Backup Administrator, or Administrator, in this document, is a role that reports to the IT Manager and is responsible for performing and verifying backup and restore operations.

The Secure Off-Site Location is a local bank vault

A full backup is a backup of all objects and data.

An incremental backup is a backup of all objects and/or data that has been changed since the last backup.

The Backup Verification Log is a monthly tracking document appended to this procedure for recording each system’s backup and backup storage.

# Procedures:

## Risk Assessment and Control

1. For each computerized system, the backup requirements are determined by applying a risk based approach.
	1. The criticality level associated with each system, or major system function, is determined using the process in *SOP System Risk Assessment.*
	2. Systems with criticality level of ‘high’ or ‘medium’ must have an incremental backup each day and full backup each month.
	3. Backup storage location requirements are based on the system’s criticality level.
		1. Backup copies for systems with a criticality level of ‘high’ must be stored at a secure, off-site location.
		2. Backup copies for systems with a criticality level of ‘medium’ must be stored in a secured area in a secondary building which may be on-site or off-site.
		3. Backup copies for systems with a criticality level of ‘low’ can be stored on-site in a designated storage area.

## Backup Content and Schedule

1. The Backup Administrator ensures that nightly incremental backups and monthly full backups are scheduled for the following systems:

|  |  |  |
| --- | --- | --- |
| **System** | **Criticality Level** | **Backup Storage Location** |
| System A | High | Off-site vault X |
| System B | Medium | On-site building Y |
| System C | Medium | On-site building Y |
| System D | Low | Storage cabinet Z |
| Etc. |  |  |

1. The Backup Administrator ensures that copies of all data, software executable code, administrator user-ids and passwords, and installation materials are stored in the backup storage location for all systems referenced in this procedure.

## Backup Review

1. The Backup Administrator reviews the backup log each day to verify that the backups from the previous workday executed correctly.
	1. The Administrator completes the daily row in Section 1 of the Backup Verification Log. The Administrator records the number of objects inspected for each system.
	2. If there are any issues, the Administrator records the description of the issue and the resolution in the Appendix to the Backup Verification Log.
2. The Backup Administrator reviews the backup log the next workday after a monthly backup to verify that the backups from the previous workday executed correctly.
	1. The Administrator completes the monthly row in Section 2 of the Backup Verification Log
	2. If there are any issues, the Administrator records the description of the issue and the resolution in the Appendix to the Backup Verification Log.
3. All systems that are backed up are to have a recovery test at least once each year to ensure that the backups are useable. The test can be a specifically scheduled test, or it can be an actual restoration of the backup for business processes.
	1. The Administrator records the date of the last actual recovery or recovery test for each system in Section 3.
	2. If there are any issues, the Administrator records the description of the issue and the resolution in the Appendix to the Backup Verification Log.

## Backup Storage

1. Each day, the Backup Administrator delivers the previous night’s backups to the backup storage location identified in the table, above.
2. On the first workday after the monthly backups are executed, the Backup Administrator delivers the monthly backups to the backup storage location identified in the table, above.

## Backup Verification Log Review

1. After each monthly backup is executed, the Administrator reviews the Backup Verification Log for the month for accuracy and signs Section 4.
2. The IT Manager reviews the Backup Verification Log for completeness and appropriate resolution of recorded issues, then signs Section 4.
3. The completed and signed Backup Verification Log is retained for the same retention period as the records in the associated systems.

**References:**

 *21 CFR Part 11, Electronic Records; Electronic Signatures,* March 20, 1997

*General Principles of Software Validation: Final Guidance for Industry and FDA Staff*, January 11, 2002, FDA

*Good Practices for Computerised Systems in Regulated “GxP” Environments*, PIC/S, September, 2007

*Guidance for Industry: Computerized Systems Used in Clinical Investigations*, FDA, May, 2007

# Backup Verification Log

**Section 1:** Month: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
|  | Daily Systems – Backup Size |  |  |
| Day | System A | System B | System C | System D | System E | System F | Etc. |  |  | Signature | Date |
| 1 |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |  |  |  |  |
| 27 |  |  |  |  |  |  |  |  |  |  |  |
| 28 |  |  |  |  |  |  |  |  |  |  |  |
| 29 |  |  |  |  |  |  |  |  |  |  |  |
| 30 |  |  |  |  |  |  |  |  |  |  |  |
| 31 |  |  |  |  |  |  |  |  |  |  |  |

**Section 2:** Monthly System Backups Month: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |
| --- | --- | --- | --- |
|  | Monthly Systems – Backup Size |  |  |
| Sys: | System A | System B | System C | System D | System E | System F | Etc. |  |  | Signature | Date |
|  |  |  |  |  |  |  |  |  |  |  |  |

Monthly Backups delivered to designated location: Date delivered: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Section 3:** Date of Last System Recovery or Recovery Test

|  |  |
| --- | --- |
|  | System – Date of Last Recovery or Recovery Test |
| Sys: | System A | System B | System C | System D | System E | System F | Etc. |  |  |  |  |
| Date: |  |  |  |  |  |  |  |  |  |  |  |

**Section 4:** Review and Approval

 Backup Administrator (signature): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 IT Manager (signature): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Appendix – Issues Log

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Issue # | Description | Resolution |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |