**Contents**

[Purpose: 3](#_Toc429123971)

[SOP Scope: 3](#_Toc429123972)

[Definitions 3](#_Toc429123973)

[Procedures: 3](#_Toc429123974)

[Prior to Failure or Disaster 3](#_Toc429123975)

[Failure 4](#_Toc429123976)

[Disaster 4](#_Toc429123977)

# Purpose:

This SOP defines the steps and controls necessary to recover the Information Technology infrastructure in the event of a system failure or system disaster.

# 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.

# Definitions

A system Restart is a start-up of a system after a planned or unplanned stop, that does not require restoring any data or system files.

A system Restore is a Data Recovery or a Rebuild.

A system Data Recovery is a restoration of data from backup tapes necessitated by the loss or corruption of current data on the system.

A system Rebuild is the complete reinstallation of a system, including executable files as well as data from backup tapes.

A Failure is the loss of a single IT system that requires a Restart, a Data Recovery, or a Rebuild.

A Disaster is an event that destroys or disables multiple computer-based systems. Examples include a fire in the IT server room or main building, earthquakes or other natural events, or physical destruction by unauthorized intruders.

# Procedures:

## Prior to Failure or Disaster

Each IT system shall have procedural recovery instructions covering failures and disasters. These instructions should include:

* Names of Individuals and/or positions responsible for restart, rebuild, and data recovery activities.
* Time requirement from the point of failure or disaster to the point of resumed operations.
* The location(s) for rebuilding the system in the event of a disaster
* Detailed procedural instructions for system restart, rebuild, and data recovery. Procedures should include step by step recovery procedures and required configuration settings.
* Detailed procedural instructions on how to verify that the recovery was successful. Procedures can include record counts, file counts, reviews of key reports, etc.
* List of documentation required to record the recovery activities.

## Failure

1. In the event of a system failure, IT personnel should notify the IT Manager.
2. If the failure requires a Restore, the IT Manager will determine whether or not to authorize the Restore after conferring with the Operations Manager.
3. For any failure requiring a Restart and for authorized Restores, the IT personnel performing the operation will follow the procedural instructions for the IT system that needs to be restarted or restored.

## Disaster

1. In the event of a disaster, IT personnel should immediately notify the IT Manager and Operations Manager.
2. The IT Manager will investigate the disaster and determine the initial recovery approach based on the characteristics of the disaster. The general characteristics and corresponding approach for each of 3 scenarios will be:

A - Single site damaged – recovery is possible within the damaged building

B - Single site destroyed – recovery is possible in a different building

C - Multiple sites destroyed – recovery will require a new, off-site building location

1. If the disaster destroys multiple sites (Scenario C), the IT Manager will be responsible for acquiring new hardware and restoring the systems from the off-site repository of systems and system data.
2. If the disaster destroys or damages a single building (Scenarios A and B), the IT systems will be restored in the surviving building. In Scenario A the workers will be able to continue working at their desks in the original building, while in Scenario B they will need to be set up in the surviving building.
3. If the disaster occurs in the Main Building, the IT systems will be restored in the Secondary Building according to the individual procedural instructions for each system Restore, according to the following priority order:
   1. System 1
   2. System 2
   3. System 3
   4. Etc.
4. If the disaster occurs in the Secondary Building, the IT systems will be restored in the Main Building according to the individual procedural instructions for each system Restore, according to the following priority order:
   1. System 1
   2. System 2
   3. System 3
   4. Etc.
5. The IT Manager is responsible for re-acquiring any lost or inoperable equipment for a full restoration of the original hardware environment.

**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

*Computerized Systems Used in Clinical Investigations*, May, 2007, FDA