UT Health San Antonio
Joe R. & Teresa Lozano Long School of Medicine

Department of Population Health Sciences
Clinical Research Informatics Division

STANDARD OPERATING PROCEDURE

SOP Number: CRI.SOP. SDLC-006	**Title: System Backup and Restore**	
Version No.: 1.0	**Effective Date: March 14, 2023**	**Page 1 of 3**
Supersedes Version: N/A **Dated:** N/A	REQUIRED APPROVALS BELOW	
CRI Director:	DocuSigned by: Bill Sanns	**Date:** 3/16/2023
CISIL Approver 1:	DocuSigned by: Elodie Ekoriko	**Date:** 3/16/2023
CISIL Approver 2:	DocuSigned by: Stephen Hargrove 5AEBB2C5776E46A...	**Date:** 3/21/2023

1.0 Purpose

This SOP defines the steps and controls necessary to back up and restore data and systems used in CRI administrative, operational, and research operations.

2.0 Scope

This procedure applies to ROUTINE operations for all server-based software applications and data managed by CRI Technical staff regardless of where they may be hosted. Any DISASTER-related operations are outside the scope of this SOP and are managed through the CRI Business Continuity Plan.

3.0 Responsibility

3.1 Technical Director: role bears responsibility for assuring systems are managed according to federal, state, and local standards.

3.2 System Administrator: role performs all functions related to establishing, managing and maintenance related to Population Health Sciences' managed servers, software, network, and security.

3.3 Application User: role performs all functions related to the access and utilization of the installed software.

4.0 References

4.1 UT System: UTS 165 Information Resources Use and Security

4.2 21 CFR Part 11, Electronic Records; Electronic Signatures, March 20, 1997

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

4.4 Good Practices for Computerised Systems in Regulated "GxP" Environments, PIC/S, September, 2007Guidance for Industry: Computerized Systems Used in Clinical Investigations, FDA, May 2007

5.0 Acronyms and Definitions

Term	Definition
SOP	Standard Operating Procedure
CRI	Clinical Research Informatics

UTHSA	University of Texas Health Science Center San Antonio
VM	Virtual Machine: Used as a generic term to describe a server-based container that will host the software application or service.
IMS	Information Management Services: UTHSA's central IT Operations
Decommission	To remove, retire, or deactivate from active service
COTS	Commercial Off the Shelf Software/System
IDEAS	Informatics Data Exchange and Acquisition System: CRI's primary application development environment
EMR	Electronic Medical Record
Source System	The primary software application that either generates, collects, or manages data

6.0 Procedure

6.1 Backup Categorization

6.1.1 System and data backup categorization is defined by the Technical Director with input from the System or Data Sponsor, System Administrator, and/or project requirements

6.1.1.1 All categorizations are cataloged within the IDEAS CRI Live Environments application

6.1.1.2 Backup Categorizations include:

6.1.1.2.1 **No Backup**: Any software or data readily available from a source system. Examples include COTS software, Source EMR data, etc.

6.1.1.2.2 **Backup**: All CRI-developed source code, data gathered via CRI-managed or developed systems, CRI-manged project files, or information not readily available from a source system.

6.2 Backup Procedure

6.2.1 Backup Systems: All backup files are managed on two CRI-managed servers.

6.2.1.1 Primary Backup Server: The primary backup server is managed within the CRI server environment to allow for the highest data throughput

6.2.1.2 Secondary Backup Server: The secondary server is a mirror of the primary server and is located external to the primary operational environment

6.2.1.3 All backups are full backups. No incremental backup operations are employed.

6.2.2 Backup Software: All CRI backups are either stored as encrypted (data) or on encrypted file systems (code, files, etc.).

6.2.3 Backup Frequency: Any system or environment categorized as "Backup" is backed up nightly

6.2.4 Backup Verification:

6.2.4.1 Human Audit: Weekly, or as needed (determined by the IT Director), the system administrator or named designee reviews the backup logs.

6.3 Restore Procedure: Within the scope of this SOP, a system restore would occur to comply with "normal" business operations that would include any non-urgent or non-mission critical data or systems. Any restore operations outside "normal" operations are managed through disaster recovery operations detailed in the CRI Business Continuity Plan

6.3.1 Restore Tracking: Restore operations are tracked via the CRI Project Tracking and Task Management application.

6.3.2 Restore Operations:

6.3.2.1 Restore operations are dependent on the system or data source

6.3.2.1.1 Source Code: The source is pulled from the CRI version control system and restored in the appropriate location

6.3.2.1.2 Data: Data is retrieved from the primary backup server. NOTE: The secondary system is only used in case of primary backup failure

6.3.2.1.3 COTS, Open Source, Provided Data are retrieved from the source system and installed or copied into the appropriate VM

6.3.2.2 Restore Verification: The restore is complete when verified by either the system administrator or end user (based on need and determination)

7.0 SOP Deviations

Deviations from this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

8.0 Review & Revisions

Review and revisions of this and all SOPs are handled according to CRI.POL.001 *Clinical Research Informatics Quality Management System (QMS)*.

9.0 Attachments

None

10.0 Revision History

Version No.	Revision Date	Description of Revision
0.0		