

*IT Service Continuity Plan – Scientific Data Storage and Access – CS
DocDB #5032*

GENERAL			
This document is under the Change Management Control Policy.			
Description	This document is the IT Service Continuity Plan for the Scientific Data Storage and Access Service area.		
Purpose	To provide a plan and high level procedures for SDSA service continuity events		
Applicable to	<i>Enstore, dCache and Active Archive service offerings</i>		
Supersedes	N/A		
Document Owner	Service Continuity Manager	Owner Org	Computing
Effective Date	November 2013	Revision Date Review Date	2015-03-19 2016-10-16

VERSION HISTORY			
Version	Date	Author(s)	Change Summary
1.1	7/8/2013	Gene Oleynik	Initial after review
1.2	2015-03-19	Gene Oleynik, Stan Naymola	Yearly review update, post DR exercise update
2.0	2015-10-16	Rolando Ramos	Chg. 10227. Annual Review by Service Continuity Manager

The Computing Sector has created an overall IT Service Continuity Management Plan ([CD-DocDB #4969](#)) that covers the key areas that each individual plan would rely upon in a continuity situation such as command center information, vital records and personnel information. The purpose of this document is to describe the key information needed to recover the Scientific Data Storage and Access service (SDSA) offerings in a business continuity situation once a decision to invoke has been made, and then to manage the business return to normal operation once the service disruption has been resolved.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Scope

Service Area: Scientific Data Storage and Access (SDSA).

Service Offerings: Enstore, dCache, Active Archive Facility

- Enstore is tape based storage that can be accessed directly or through dCache
- dCache is a disk cache file system that can act as a front end file cache for Enstore or can be used as a non-tape backed file cache (volatile dCache)
- Active Archive Facility is a combination of the above two offerings that enables non-Fermilab customers to be able to store and retrieve data from Fermilab.

Service Areas that depend on this service: FermiGrid (volatile dCache dependency)

dCache service instances provided by SDSA and covered in this plan are the Public, D0 and CDF dCache. The CMS dCache is not covered by this plan.

The SDSA Services are provided by the Data Movement and Storage Department (DMS), are operated by the DMS Storage Services Administration (SSA) group, and supported by the DMS Data Movement and Development (DMD) group, which develops Enstore and dCache software.

Recovery Objectives

Recovery Time Objective (RTO)

< 12 hours for critical service.

Recovery Point Objective (RPO)

< 24 hours.

As documented in the SLA (CS-doc-5032), users of the Scientific Data Storage and Access services are expected to be able to buffer 24 hours worth of data and to have the resources to catch up once service is restored.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Recovery Team

In this section describe the other services, roles, and responsibly required for recovering this service.

Service/Role/Function	Responsibility	Dependencies	Expected Response Time
Service Provider	Restore		< 24 hours
Service Provider Support Team	Restore hardware/OS/system software	DMS has an OLA with ECF for dCache hardware and OS	< 4 hours
IT Server Hosting			
Network	Network connectivity, DNS	Cabling, network hardware	< 4 hours (see network SLA)
Facilities	Power and Cooling, equipment moves		< 4 hours?
Application Services	Authentication (Kerberos, Gums)	dCache, Enstore	< 4 hours. (HA failover – see authentication SLA)
External Service Provider	Restore functionality to the tape libraries, move equipment (tape drives)	Enstore tape libraries	< 4 hour
Managed Services	Eject, move and load tapes	DMS has an OLA with Dell Managed Services	< 8 hours
Service Desk	Interface to Users		< 4 hours (see Service Desk SLA)
Backup Services (TIBS)	Weak dependency on code repository backup		?

The recovery team for the SDSA Services are:

1. Gene Oleynik (service owner), Stan Naymola (service manager)
2. CS/SCD/SCF/DMS/SSA operations staff
3. CS/SCD/SCF/DMS/DMD development staff

Other teams that may need to stay in close contact are:

1. Tape library Vendors: Oracle
2. Managed Services
3. Experiment Computing Facilities (ECF) department
4. Network
5. Authentication Services, including GUMs
6. Facilities
7. Service Desk

*IT Service Continuity Plan – Scientific Data Storage and Access – CS
DocDB #5032*

Recovery Strategy

Strategy for initial recovery

If the SDSA staff is the initial incident responder, contact will be made with the Service desk to declare the incident. If the incident is determined to be critical, a Critical Management Team will be formed. The SDSA responder to the incident will inform the Service Owner and work with the Management Team. The Management Team will decide whether this service recovery plan will be executed and will communicate that to the SDSA responder.

Overall recovery strategy

The SDSA responder forms a Service Recovery Team for the SDSA services. This team:

- Chooses a Recovery Coordinator to lead the team (nominally the SDSA staff initially responding to the incident).
- Performs a Damage Assessment (if not already done). Damage Assessment is described below.
- Works with the Management Team to send notice of the outage to affected customers.
- Formulates a Recovery Plan from the damage assessment and the scenarios listed below.
 - Determines if alternate hardware or alternate data center is required.
 - Determines whether partial service restoration is required.
 - Takes into consideration priorities in deciding the order of instances to bring up:
 - Public and CMS systems are first priority
 - Run II systems are second priority
 - Notifies the Management Team of the plan.
- Works with Management Team to coordinate the recovery with other services.
- Takes steps and plan securing the environment in the tape library rooms if necessary (see Tape Environment Considerations below).
- Verifies underlying infrastructure is available. This includes facilities (power/cooling), networking (DNS, firewalls, routers, switches), and authentication services for recovery.
- Implements the recovery plan.
- Verifies environment and service readiness (as needed by the type and severity of the outage)
- Enables the service(s).
- Notifies the Management Team when the service(s) are available.
- If partial service was restored and alternate hardware deployed or alternate center used, when the hardware or center is repaired, restores services to normal operations according to the recovery plan.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Damage Assessment Procedure

In the case of a severe loss of service, the service recovery team is to investigate the problem, call in vendors if needed and utilize Computing Sector personnel expertise as required to assess the damage. The team follows this procedure:

1. Determine if there is potential for further disruption or damage to the service and take preventative steps if so.
2. Make a comprehensive list of the damage, damaged equipment, equipment that needs to be replaced, and any damage to tapes or their content, including potential further damage to tape due to degraded environmental conditions.
3. Make an assessment of the time to repair the affected portion of the SDSA service(s) and make it operational.
4. Make an assessment of the free resources in the SDSA services that are still operational and can be used to restore partial or full service to the affected portion.
5. When damage assessment has been completed, the Service Recovery Coordinator is to inform the Service Owner and Management Team of the assessment.

Communications

- If this Continuity Plan is to be activated, the Service Recovery Coordinator is to notify all team members and inform them of the details of the event.
- The Recovery Coordinator is to provide the Management Team with details of the Damage Assessment and resource availability and any immediate steps that need to be taken to prevent further damage.
- The Management Team in consultation with the other recovery teams will decide which resources to utilize for providing limited interim service. This process may engage customer representatives to make decisions about priorities and resources.
- Upon notification from the Service Recovery Coordinator, Team Leaders are to notify their respective teams as needed. Team members are to be informed of all applicable information and prepared to respond.
- The Service Recovery Coordinator is to notify remaining personnel (via notification procedures) on the general status of the incident.

Build From Scratch

Build from scratch considerations are covered in the Appendix

High availability fail-over

The SDSA service offerings do not provide HA fail-over

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Recover at another site or multiple sites

Instances of the SDSA tape based services, Enstore, are located in two Fermilab data centers that are about 1 mile apart: The Feynman Computing Center second floor (FCC2) and the Grid Computing Center Tape Robot Room (GCC TRR). The services span and are active at both sites. If necessary, one of the sites can take on some of the functionality provided at the other. However, any significant recovery of functionality at the alternate site may necessitate the move of a significant amount of resources (servers, movers, disk storage, tapes and tape drives). Restoring service to an alternate location is discussed in the Data Center Loss section below.

SDSA dCache services are all located in FCC2. New acquisitions may be located in the FCC3 data center.

Recovery Scenarios

Building not accessible (Data Center Available)

Completed	Action
	Contact the Critical Incident Command Center. The Computing Sector Continuity plan lists the location of these centers as well as alternate locations.
	Coordinate with the Critical Incident Command Center to execute the overall strategy for recovery.
	When authorized by the Critical Incident Command Center, restore hardware and software that can be accessed remotely.
	When the building becomes accessible and when authorized by the Critical Incident Command Center, restore hardware and software and tape libraries that may require physical intervention.

Server and mover power can be cycled remotely, but some may require on-site presence (for escorting tape library vendor field service staff, for example).

Data Center Failure (Building Accessible)

Completed	Action
	Contact the Critical Incident Command Center. The Computing Sector Continuity plan lists the location of these centers as well as alternate locations.
	Coordinate with the Critical Incident Command Center to execute the overall strategy for recovery.
	When authorized by the Critical Incident Command Center, restore the hardware, software and tape libraries.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Building not accessible and Data Center Failure

Completed	Action
	Contact the Critical Incident Command Center. The Computing Sector Continuity plan lists the location of these centers as well as alternate locations.
	Coordinate with the Critical Incident Command Center to execute the overall strategy for recovery (Data Center Failure Procedure in this document).
	When the Data Center becomes available and when authorized by the Critical Incident Command Center, restore hardware and software that can be accessed remotely.
	When the building becomes accessible and when authorized by the Critical Incident Command Center, restore tape libraries and other hardware that may require physical intervention.

Critical recovery team not available

Completed	Action
	Contact the Critical Incident Command Center or Emergency Services. The Computing Sector Continuity plan lists the location of these centers as well as alternate locations.
	Coordinate with the Critical Incident Command Center to execute the overall strategy, according to the appropriate scenario, for recovery.
	When authorized by the Critical Incident Command Center, restore hardware and software that can be accessed remotely.
	Perform work that can be done remotely. Example - Server power may be cycled remotely, but some actions may require on-site presence (if restoration from Tape requires a physical loading of media, for example).
	When the building becomes accessible and when authorized by the Critical Incident Command Center, restore tape libraries and other hardware that may require physical intervention.

Government Mandated Shutdown of Services

Completed	Action
	Contact the Critical Incident Command Center. The Computing Sector Continuity plan lists the location of these centers as well as alternate locations.
	Coordinate with the Critical Incident Command Center to execute the overall strategy for the shutdown of services.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

	Ensure that all services/servers are in a safe and secure state for recovery at a later time.
	Maintain periodic contact with the Critical Incident Command Center
	Coordinate with the Critical Incident Command Center to execute the overall strategy for recovery.
	When authorized by the Critical Incident Command Center, restore the hardware (VMs) and software.
	When the building becomes accessible and when authorized by the Critical Incident Command Center, restore tape libraries and other hardware that may require physical intervention.

Pandemic (during normal operations)

The SDSA services require specialized knowledge to operate. Most operational tasks can be completed remotely through VPN access. Some operational tasks require the presence of staff on site, in particular tape library operations and tape cartridge I/O operations.

- Vendor field service personnel require an escort into the tape library rooms
- Flipping/un-flipping cartridge write protect tabs requires physical presence
- Entering blank tapes requires physical presence

If necessary, these activities could be managed by unskilled staff under the remote direction of skilled staff.

SDSA Specific Scenarios

Tape Library not operational or damaged

If tape libraries at either FCC or GCC data center are not operational or the data center is inaccessible for a prolonged period of time, partial service may be restored to the other center (or other alternate libraries in the same data center if they are viable).

If a tape library were not operational, it would be a difficult task to remove specific tapes, including blanks. Enstore does not know where tapes are located in the tape library; only the tape library management interface database (e.g. ACSLS or SL8500 console database) knows the mapping between a tape's label and the slot in the tape library where it resides. Once identified, the tapes would need to be manually located and removed by physically entering the library. In addition, physically moving tapes has associated risk (see Tape Environment Considerations in the Appendix). Relocating tapes would not be feasible for a temporary relocation, but could be for a prolonged period such as if the data center or tape library is permanently damaged.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Most data has a single copy at one of these data centers (CMS, Run II). Single copy data is in general either statistical in nature and in large enough quantity that the loss of single tape is not statistically significant, or are backups from another site (for both external and internal customers, e.g. DESDM and local RMAN backups of scientific databases). Other data is duplicated between the data centers. Data that may be duplicated includes:

- Statistical data for which loss of single tape is statistically significant (e.g. MiniBooNe tankdata)
- Small Datasets (e.g. BeamsTools)
- Data that is not statistical and for which file loss is significant

Data that falls into these categories are duplicated (or are being duplicated) to both data centers. This can be done automatically by Enstore, or manually by the experiment (e.g. MINOS makes their own copies). In general, the primary copy that the user accesses is located at FCC and the secondary copy at GCC.

For files that are duplicated by Enstore, in the event of the loss or inaccessibility of primary copies, the secondary copies could be made available. This requires intervention by the administrators.

The high level strategy for this Tape Library not operational scenario is:

1. Pause the affected Enstore Library Managers.
2. If there is any damage to the library (e.g. water damage), consult with the library vendor support on the most suitable action to take to preserve data.
3. Contact the vendor to move any tape drive resources, as decided by the management and recovery teams, to libraries into the alternate libraries.
4. Arrange with Managed Services to move any blanks or tapes to be read from the failed library to the alternate library(s). This step may only be feasible for a more permanent reallocation of tapes (see above). Instead, blank tapes for writes may need to be rush ordered.
5. If primary copies of Enstore duplicated files exist in the affected library and secondary copies exist in an operational library:
 - a. Make a list of these primary copy files and store it in backed up storage (for future restoration of normal operations)
 - b. Administratively swap the primary and secondary roles in the metadata so that users can access the files in the operational library
6. Install additional mover computers for any additional tape drives that have been added to the alternate library.
7. Reconfigure the affected Enstore instances' logical tape library managers to point to the media changers in the alternate tape libraries.
8. Pause the alternate Enstore logical library managers

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

9. Configure the tape drive movers of drives in the alternate tape library so that a portion of the tape drives are dedicated for use by affected logical Enstore libraries. The partitioning of drives is based on the resource allocation agreed upon by the management team.
10. Allocate blank and relocated tapes to these logical libraries
11. If the operating humidity and temperature had changed from their nominal values, wait until the environment has returned to nominal and the acclimation period has passed (see Tape Environment Considerations in the appendix).
12. Resume the affected library managers

Roles of other teams

Managed services team, with the assistance of the Service Owner (in selecting, locating and removing tapes):

- Moves blank tapes from the failed tape libraries to alternate tape libraries for write access recovery as necessary. Load rush ordered blanks.
- Moves selected subsets of written tapes from the failed libraries to the alternative libraries for a read-access recovery as necessary.

Networking Team:

- Replaces and repairs any damaged network elements required for the contingency
- Configures the network for any moved or new computers required to establish the contingency plan as necessary
- Reconfigures the private control LAN topology as necessary.

Tape Library Vendor:

- Moves tape drives from the failed to the alternative library(s) as necessary

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Data Center Loss

The storage services are located in the second floor of FCC2 and in the GCC TRR. These two centers are located about 1 mile apart on the Fermilab site. The SDSA services span and are active at both of these sites. Scientific Data is stored in tape libraries located at both of these sites. Most of the SDSA service's server computers are located on the second floor of FCC, while mover computers that transfer data are collocated with the tape libraries at both locations. The locations of SDSA equipment are:

- FCC2
 - Enstore servers and metadata raid arrays. There are 6 or more servers for each instance of Enstore and there are 3 instances of Enstore. Most of these servers perform critical functions for the service and have critical state data on the RAID arrays.
 - dCache servers. These servers perform critical functions and are single points of failure.
 - dCache pool nodes (disk file servers) and associated RAID
 - 30,000 slots capacity in a cluster of 3 tape libraries (Public and Run II non-RAW data)
 - Movers for tape drives in the FCC tape libraries
 - Infrastructure nodes for managing the service (migration, scanning, etc.)
 - ACSLS (Oracle tape management server) for the tape libraries in FCC
- GCC TRR
 - 40,000 slot capacity in a cluster of 3 tape libraries (CMS) and one stand-alone tape library (Public duplicate copies and backups and Run II RAW data)
 - Movers for the tape drives in the GCC tape libraries
 - Two ACSLS machines – one for CMS, one for everything else (Run II RAW, Public backups, scientific database RMAN backups)
 - A small number of infrastructure nodes, Enstore test system server computers

Moving the services hosted at one of these centers to the other may result in additional load and (potentially severe) service degradation, but some level of service continuity could be maintained. Hardware may need to be moved between the sites in order to provide adequate resources or to establish service(s). In addition, except where noted below, data on tapes at the failed center would not be accessible unless the tapes were moved to the alternative center. The procedure for Tape Library not operational would be followed.

If the GCC data center or the Tape Robot Room located there were inaccessible, Enstore and dCache services can continue to function degraded. Tape storage capacity in GCC would be unavailable and the data on the tapes contained in the libraries at GCC (CMS, Run II RAW, Public backups, and scientific database RMAN backups) would be inaccessible. The procedure for the Tape Library not operational would be followed.

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

If the FCC second floor data center were unavailable, the Enstore and dCache services would also be unavailable since they are all located in FCC2. These services are provided by many computers (3 instances x 6+ servers + RAID arrays for Enstore and at least a dozen for dCache). For these reasons, if the FCC2 data center were unavailable, the SDSA services would be unavailable until the data center was restored. If FCC2 were lost permanently or for a very long period, building the SDSA services from scratch may make sense and the Build from Scratch procedure in the Appendix would be followed. In this case, in addition to following the Build from scratch and Tape library not operational procedures, limited resources would need to be prioritized:

1. Form a team to assess the impact and work with customers to form a disaster recovery plan to return partial essential service and to eventually return full service
2. Document the impact to the customers and the resources that are available to restore partial service
3. Meet with the customers to come up with a mutually satisfactory plan to share resources and bring up partial essential service
4. Acquire additional resources if necessary (e.g. blank tapes)
5. Formulate a plan to restore full service and meet with customers to get agreement on the plan

Roles of other teams

Managed services team, with the assistance of the Service Owner (in selecting, locating and removing tapes):

- Moves blank tapes from the failed tape libraries to alternate tape libraries for write access recovery as necessary. Load rush ordered blanks.
- Moves selected subsets of written tapes from the failed libraries to the alternative libraries for a read-access recovery as necessary.
- Move any servers and disk arrays as needed

Networking Team:

- Replaces and repairs any damaged network elements required for the contingency
- Configures the network for any moved or new computers required to establish the contingency plan as necessary
- Reconfigures the private control LAN topology as necessary.

Tape Library Vendor:

- Moves tape drives from the failed to the alternative library(s) as necessary

Roles of other teams

Managed services team, with the assistance of the Service Owner (in selecting, locating and removing tapes):

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

- Moves blank tapes from the failed tape libraries to alternate tape libraries for write access recovery as necessary. Load rush ordered blanks.
- Moves selected subsets of written tapes from the failed libraries to the alternative libraries for a read-access recovery as necessary.

ECF Department:

- Help move any dCache nodes to new locations., configure and install OS as needed, host level operations

Return to Operations

Return to operations procedure:

1. If this recovery is from a partial degraded interim recovery to a full recovery, the following additional steps must be made to restore full service
 - a. Restore any relocated service components and server computers back to their original location and configuration
 - b. Replace any mover computers, tape drives for the repaired libraries if any were moved during the recovery
 - c. Restore any modified duplicated file's secondary and primary roles for files that had this change made for partial recovery
 - d. Restore the affected Enstore instances mover configurations as necessary.
 - e. Schedule moving any relocated tapes back to the recovered libraries with the Managed Services team or on an emergency basis.
2. Establish all dependent services are operational and running (LAN, Private LAN, authentication and facilities)
3. Rebuilt file systems must fsck OK.
4. Monitoring must indicate that service components are fully functional or that there is acceptable partial functionality (e.g. some monitoring) in some components. In general enstore servers and dCache admin nodes should be fully operational.
5. > 50% of Enstore mover computers for a given library are available.
6. Tape libraries are all up and inventoried (exceptions may be made for partial restoration)
7. Test transfers of files (Enstore and/or dCache) complete successfully.
8. Environment temperature and humidity are nominal and the tape acclimation time has transpired (see Tape Environment Considerations in the Appendix)
9. Resume the repaired instance

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

Roles of other teams:

Tape library vendor

- Return tape drives from the alternate library to the recovered library if necessary

Managed Services Team

- Move the blanks, written tapes, and any other tapes that were originally moved in the recovery from the alternate library to the recovered libraries as directed by request from the Service Recovery Team.

ECF Department

- Bring up dCache servers and disk arrays

Appendix

Build From Scratch

Most components of Enstore and dCache can be relocated or collocated on servers with other service components. In general, DMS/SSA attempts to bring the service back up on replacement hardware, which may be from on-site spares or a warranty replacement. In lieu of timely replacement hardware, the affected service component may be collocated to a server with other service components. This may degrade the service but will maintain continuity until replacement hardware can be deployed. In the case a system may need to be built from scratch, the steps are, for each affected system:

- Identify facilities resources where the equipment will go: rack, network and power
- Move and installation of all hardware if necessary
- Establish network connectivity for data LAN and private Control LANs
- Installation of the OS and system software (dCache:ECF, Enstore:DMS/SSA, ACSLS:Oracle)
- Establishing network connectivity for the service(s)
- Reconfiguration of cfengine/puppet and services if necessary.
- Reconfiguration of puppet for dCache OS and system software (by ECF) if necessary.
- Installation of the application(s) software from rpm server and FTP server
- Configuration of the system(s) through cfengine or puppet (ECF for dCache)
- Configuration of application(s) through cfengine or puppet/application configuration infrastructure
- Restoration of SDSA databases from backup (Enstore, Chimera, dCache – See Metadata Loss Considerations section below)

This typically can be done within a several hours for a single server once hardware is available, powered and connected to the network. Building and testing a full service from scratch will, in general, take several to many days.

SDSA service software is distributed in the form of rpms. If rpms are not available, they can be built from the GIT software code repository (Enstore), which is a service provided by the Scientific Computing Division and the DESY code distribution (dCache). It is important to note that the software repository and their backups are maintained in the FCC2 data center - there are no alternate sites. The distribution repositories for Enstore and dCache are kept at FCC but are also replicated to GCC.

Recovery of RAID arrays may involve hardware replacement (controller/failed disks) or replacement of the entire array and restoration of the data from the failing hardware or from backups. In the latter case, due to the size and complexity of the databases, this may take a significant time for which service

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

may be unavailable or degraded. Database restoration may also require involvement from the DMS Data Movement Development group (see Metadata Loss Considerations below).

Document sets CS-doc-5090 (Enstore) and CS-doc-5091 (dCache) contain further information on restoring these systems from scratch and metadata databases from backups.

Oracle maintains 3 ACSLS Sun/Oracle servers that are responsible for managing the tape libraries and with which Enstore communicates to direct tape mounts and dismounts and provide for other tape cartridge I/O operations. Each of these is a single point of failure for specific instances of Enstore. These servers contain databases of tapes, drives and slots. These databases are backed up to a second local disk, and can also be recovered fairly quickly from the tape libraries, which maintain databases themselves (DMS rebuilds the ACSLS database from the tape library database in this manner when they update ACSLS software). These servers are under 24x7 maintenance for hardware, the ACSLS software, and operating system (Solaris). The process for building these from scratch is to contact Oracle, via SNOW or directly off-hours, to service the hardware.

Metadata Loss Considerations

Backups of the metadata (Chimera/pnfs namespace and Enstore databases) for each instance of the SDSA services are made daily. Recent backups are available on disk on the instance of the SDSA service and are copied to tape daily to both GCC and FCC tape libraries. Restores from backup are exercised frequently as part of managing the service. The restoration process is to

1. Restore the hardware if needed and perform tests to make sure it is sound.
2. Restore the OS and system software.
3. Restore the service application software.
4. Follow the procedure to restore the database from backup.
5. Validate the restored database is functional.
6. Plan and perform post-restoration work, if needed, to backfill entries in the database.

Tape Environment Considerations

Data are written to tape on tracks that are less than 5 microns in width and pitch. The readability of a track is sensitive to the dimensional stability of the media. Tape media dimensions will vary with changes in humidity and temperature. A tape drive may have difficulty reading a tape at a humidity and temperature significantly different than what it was written at. This can result in poor read performance or read failure.

Recommendations from the tape and tape library manufacturers are:

1. Operating Ideal 72°F, 45% RH. Recommended Range: 68-77°F, 40-50%RH
2. Maximum ranges: 60-90°F, 20-80% RH

IT Service Continuity Plan – Scientific Data Storage and Access – CS DocDB #5032

3. Recommended acclimation period: 72 hours

In the case of a loss of climate control, steps should be taken to keep the climate in the tape library rooms within the maximum ranges listed above, and as close as possible to the recommended ranges. Depending on the ambient outside temperature and humidity and the length of the outage, the tapes may need to be acclimated to the environment for up to 72 hours before they can be used. Tapes should not be written to until they are acclimated. Exceptions may be necessary if writing is urgent and the risk is deemed acceptable.

The high-density tapes used in these libraries are delicate. T10000T2 tapes, for example, are 5.2 microns thick and the track pitch is 3.5 micron. Subjecting a tape to shock by dropping it more than a few feet can damage the edge of the tape and make the data on it unreadable or unusable for writes. Bulk moves of tapes should be avoided where possible, but if necessary, the tapes should be handled with care and transported in cases designed specifically for the transport of data tapes

Future Considerations

Propose action items to cover known vulnerabilities.

1. Currently, recent disk backups of the metadata databases are only available at FCC. Tape backups are available at both sites. We plan to replicate at least the Enstore database to a server in GCC and are considering doing the same for the Chimera namespace database. We could make these (lower performance) copies for failover purposes.
2. The source code and rpm and their TIBs backup are all located at FCC. We should make copies at GCC for DR purposes. Repos are being duplicated to GCC.