



National Park Service
U.S. Department of the Interior

Natural Resource Stewardship and Science

GRSM Standard Operating Procedure: Backup, Storage & Recovery

Suggested Citation: National Park Service. 2016. GRSM Standard Operating Procedure: Backup, Storage & Recovery. Version 2016-07-20. National Park Service, Great Smoky Mountains National Park. Gatlinburg, Tennessee.

Contents

Purpose.....	3
Scope	3
Introduction	3
Data Backup	3
Methods.....	3
Media.....	3
Off-Site Data Storage	3
Data Recovery	4
System Recovery	4
Recovery Procedure.....	4
Microsoft SQL Server Backup, Storage & Recovery	4
Recommended Enterprise Database Disaster Recovery Strategy	4
Properly Removing Orphaned Databases from Legacy Systems.....	5
Identifying Staff Roles Whose Function is to Implement Database Maintenance Plan.....	5
SQL Server Backup Strategy for GRSM Databases	5
Roles and Responsibilities.....	5
Contact Information	5
Attachments	6
References.....	6

Version History		
Version	Update Date	Changes
20160719	20160719	Revised draft to appropriate format

Purpose

This document provides information on the steps being taken by Great Smoky Mountains National Park (GRSM) to secure its data against loss.

Scope

The procedures in this document will apply to Great Smoky Mountains National Park elements, including Headquarters, North District, Twin Creeks, Sugarlands Visitor Center, and South District Area. More areas will be added as necessary equipment is put in place.

Introduction

Data security is one of the fundamental responsibilities held by GRSM. To ensure that the data maintained and managed by the Park are secure, a strategy that creates regular back-up copies of data has been developed. GRSM stores data and information in various formats. Microsoft Access and Microsoft SQL Server are the two means by which databases are managed. SQL Server is a Microsoft product used to manage and store information; it is a relational database management system.

Data Backup

GRSM IT creates backups of all servers on nightly, weekly and quarterly bases in accordance with the "NPS IT Contingency Plan Statement" (June, 2005). Non-critical systems workstations (e.g., the "C" Drive on each individual machine) are not defined by policy, and backups will be the responsibility of the end user.

Methods

- **Full backup** captures all files selected for backup. Depending on the volume of data and frequency, full backups can require a large storage capacity and a significant amount of time to record the information. In cases where much of the data does not change from backup to backup, other options may be considered. An initial full backup was performed to encompass all park data and information.
- **Differential backup** stores files that were created or modified since the last full backup. This method takes less time to complete than a full backup and may require fewer storage units than an incremental approach because only the full backup tape and the last incremental tape would be needed for restoration. One disadvantage is that the differential backups take longer because the amount of data since the last full backup increases daily until the next full backup is run. All daily and weekly backups are differential.

Media

Decisions regarding what backup media to use need to consider the amount of data to be backed up, the backup frequency and the required retention, recovery and transport requirements, destruction and restoration procedures, availability, media security and cost. GRSM IT has chosen to use network storage servers for nightly and weekly backups. External hard drives are used to store quarterly backups. Physical access controls are put into place for all backup media (locked doors and safes can accomplish this objectives). Environmental protection is also addressed through controlling temperature, water, dust and magnetism. Media is also marked with a label that addresses any special instructions or media log information (day of the week, type of backup, serial number). All system backups are tested to ensure data integrity and media reliability.

Off-Site Data Storage

Offsite data storage is to ensure that the system level information used to run GRSM are not only stored, protected and cycled continually, but that they have the ability to provide a link between the media stored and the alternate processing site.

All critical data are backed up and stored at an offsite location that is geographically separated from our primary storage sites. Information on data content and structure is stored with the data as well. Contingency Plan, licensing and any vendor information is included as part of the backup materials.

Offsite storage facilities and practices include the following:

- o Limitations against unauthorized access facility and media
- o Adequate fire prevention (smoke detectors, fire detectors and appropriate fire suppression) systems are in place
- o Fire rated safes/vaults
- o Auxiliary power systems
- o Proper environmental (temperature, water, magnetism, humidity, etc.) controls
- o Adequate communication capabilities
- o Adequate transportation and handling capabilities
- o Use of high impact-resistant transportation and storage containers
- o A IT disaster recovery plan that addresses priorities based on Park needs

Data Recovery

System Recovery

Great Smoky Mountains National Park system recovery includes but is not limited to patches; registry information, configuration settings, application and system software and information from the most recent backups. Nearly all hardware, software, and peripherals are standardized throughout the organization.

Recovery Procedure

These set of procedures provide an outline of equipment and damage assessment in the case of an incident. The recovery procedures will work in concert with the contingency plan.

- Replace or repair damaged equipment
- Upgrade damaged equipment
- Reconfigure replaced/damaged/upgraded equipment
- Set up for processing at alternate site
- Retrieve backup media, software, licenses, and plans from offsite storage
- Contact vendors for repairs or replacement of hardware and software
- Re-evaluate IT priorities based on business needs
- Verify location of relocated personnel to ensure proper delivery of IT resources
- Schedule testing of equipment and software prior to resuming normal processing
- Properly document all recovery actions taken
- Verify proper operations of the following services:
 - o Voice and Data telecommunications
 - o LAN access
 - o Server operations
 - o Workstation operation and LAN access
 - o Remote Access service
 - o Help desk
 - o Internet/Web access

For all critical incidents GRSM IT staff will work to restore data and functionality to park data and systems. Additional resources will be acquired if necessary.

Microsoft SQL Server Backup, Storage & Recovery

Recommended Enterprise Database Disaster Recovery Strategy

SQL database backups of up to 5 days are stored on the existing database server if implementing nightly backups. Backups are implemented automatically using scripts after normal business hours so as not to affect performance during business hours. Server disk image backups occur generally around 12 a.m.,

backups are scheduled so as not to interfere with other nightly processes being run through the Data Center. Please note that server disk images DO NOT properly backup SQL databases OR truncate SQL transaction logs.

Backups of up to 30 days are stored locally on an encrypted external hard drive. It is important to remember that off-site backups are taken only of our production database server, so any development databases (if requiring backup) should be stored externally as well as on the database server.

Properly Removing Orphaned Databases from Legacy Systems

Development and production databases should be properly removed after the database is no longer in use. This can occur when databases have moved to another environment, the systems used to access the database have been taken offline, or the protocol is no longer active.

Identifying Staff Roles Whose Function is to Implement Database Maintenance Plan

The GIS/DM Specialist is considered the Database Administrator (DBA) and is in charge of executing the Recommended Enterprise Database Disaster Recovery Strategy. A DBA should, at a minimum, possess Role Based Security Training (RBST) requirements mandated by DOI IT which include many SQL management skills including disaster recovery.

SQL Server Backup Strategy for GRSM Databases

GRSM uses the Simple recovery model for backing up SQL databases. This recovery model allows the DBA to take a full database backup at any time without worrying about maintaining the transaction logs. In simple mode, a full backup “truncates” the transaction logs. Any recovery simply allows the DBA to restore from the last full backup. It is very important to note, however, that with simple mode, a backup is only as good as the time it was backed up. i.e. if a backup was taken at 0200, and a database failure occurred at 1400, a restore operation will only restore the database to the 0200 timestamp.

In full recovery mode, if the DBA had taken hourly log backups up to 1400, a full and transaction log recovery would restore the database to any point in time up to 1400. Few, if any, enterprise databases within the park that would benefit from a full recovery model given the complexity in managing it. A full backup (in simple mode) should be created before any bulk operation that could result in significant change to the database or schema.

Finally, no database recovery model is valid until the DBA is confident that it works. A recovery plan is considered valid when the DBA, with confidence, has practiced and is comfortable with performing a restore on a database in their control. Testing any recovery procedures on a test database before implementing the practice on a production database is essential.

Please note that during a full OS recovery or moving a SQL database to another instance, additional recovery steps are required that in most cases cannot be automated. These recovery steps include: implementing security assignments, roles, and the database owner as well as service account configuration.

Roles and Responsibilities

Role	Responsibility
Data Manager	Periodically check daily IT backups
	Informing data stewards of the GRSM backup and recovery procedures including its limitations
	Undergoing RBST
	Checking SQL backups
GIS Specialist	Develops automated backup routines for all SQL databases and monitors their daily completion
	Performs SQL database recovery operations
	Performs weekly and monthly off-site copies of the “X Drive”
IT	Maintains SQL backup media

	Maintains legacy software and licenses for which old data may need to be restored to
--	--

Acronyms and Definitions

DBA- Database administrator
DOI IT- Department of the Interior Information Technology
OS- Operation system
RBST- Role-based security training

Contact Information

Great Smoky Mountains National Park
National Park Service
Gatlinburg, TN

Kendra Straub
Data manager
(865)436-1703
Kendra_Straub@nps.gov

Thomas Colson
GIS Specialist
(865)436-1701
Thomas_Colson@nps.gov

Matthew Poe
IT Specialist
(865)436-1215
Matthew_Poe@nps.gov

Attachments

None

References

National Park Service, 2006. Standard Procedures for Backup, Storage & Recovery. Sequoia and Kings Canyon National Parks Information Technology Branch.

National Park Service, 2006. National Park Service General Support System: Backup Activity Plan. Sequoia and Kings Canyon National Parks Information Technology Branch.

NPS-NETN (2008). Data Management Standard Operating Procedure: Data Back-up and Security, Version 2.1, Northeast Temperate Network-National Park Service, Woodstock, Vermont.

NPS-ROMN (2007). Backing Up the Network's Digital Information, Version 1.0, Rocky Mountain Network-National Park Service, [<http://www1.nrintra.nps.gov/im/units/romn/>], Fort Collins, Colorado.