UNIT BACKUP & RECOVERY PROCEDURES TEMPLATE

This template is provided as a guide for University of Florida units when developing documentation to support the UF Backup and Recovery Policy. Examples provided in this template are just that, and not intended to establish university requirements.

The goal of this document is to describe the backup environment, decisions that led to it, and procedures for using the environment in a sufficient level of detail that an IT person with no knowledge of the unit will be able to perform essential backup or recovery functions.

Table of Contents

Backup Configurations 2

Backup System 2

Backup Jobs 2

Hourly Backup 2

Nightly Backup 2

Weekly Backup 2

Backup Procedures 2

Backup Roles 2

Daily Tasks 2

Offsite Tape Rotation 3

Tape Disposal 3

Recovery Testing 3

Individual File Recovery Testing 3

Full System Recovery Testing 3

Testing After System Changes 4

Appendix A: Backup Targets 4

Appendix B: Recovery Test Log 4

Appendix C: Tape Inventory Log 4

Appendix D: Adding New Backup Targets 4

Appendix E: Restoration of Individual Files 4

Appendix F: Restoration of a Complete System 5

# Backup Configurations

## Backup System

All backups are performed using BackupWiz 4.7, which runs on the server Dept-Backup01. All backups are written to either disk or LTO tape.

## Backup Jobs

The following backup jobs are configured based upon RTO[[1]](#footnote-1)/RPO[[2]](#footnote-2) of the target. Targets are then added to the matching job to enable backups.

### Hourly Backup

Incremental backups are performed hourly and written to disk attached to Dept-Backup01. Backups are stored for a minimum of 7 days. This job is intended for targets with an RPO less than two hours. It must be combined with a weekly full backup to enable complete recovery.

### Nightly Backup

Incremental backups are performed each weekday, between 1am and 6am to LTO tape. Tapes are recycled after 14 days. This job is intended for targets with an RPO of one business day. It must be combined with a weekly full backup to enable complete recovery.

### Weekly Backup

Full backups are performed weekly, between 1am Saturday and 6am Monday to LTO tape. The tapes for the first backup of each month are preserved for 12 months, all other backups are preserved for at least 6 weeks. This is a complete backup used for complete system recovery, and all targets must be configured for this backup job. Additionally, it can be used as the sole backup for targets with a RPO greater than 7 days.

### Rationale

High value data, such as patient records, is backed up on an hourly basis in order to minimize disruption in the event of a major incident. Utilizing both a weekly full back-up and an hourly backup, our unit should be able to restore this high value data and lose no more than two hours of transactions. Because of the frequency of these backups, there is a greater consumption of tapes for our hourly back-ups and so we limit the scope to high value data.

It has been determined by the division head that the remaining data, such as inter-office memos, can sustain up to a loss of one business day of productivity to reproduce. That data is backed up nightly.

Data that is infrequently changed, such as that which is downloaded from a public catalog, can be managed as part of the weekly full backup and does not need to be considered in the nightly or hourly backup schedules.

# Backup Procedures

## Backup Roles

Joe Blow is the primary departmental backup administrator

Jane Know is the secondary backup administrator

## Daily Tasks

Every morning, prior to 9am, the backup administrator reviews the status for the previous day’s backup jobs (on Mondays, review the entire weekend’s activity) to verify that all jobs completed successfully. Any errors or unsuccessful jobs must be investigated to determine the cause and action taken immediately to complete unsuccessful jobs. The IT Director is notified immediately of any unsuccessful backup jobs.

# Offsite Tape Rotation

Every Monday, the tapes from the weekend’s full backups are removed from the tape library, and stored in the offsite storage safe located in room XXX at the UF East Campus Office Building. Tapes stored off-site that are due to return to service are taken back to the data center for re-use.

Because the tapes may contain sensitive or restricted data, during transit to and from the offsite location, the courier may not make any stops or leave the tapes unattended at any time. The Tape Inventory Log is updated to reflect the new location of tapes.

# Tape Disposal

Tapes that generate errors on more than 2 occasions are removed from service. If the tape contents are still within the retention period, contents are copied to a serviceable tape prior to disposal.

Tapes past their service life are marked ‘To Be Disposed” removed from the active tape inventory, logged in the Media Disposal Log, and taken to the UF Secure Media Disposal service. Tapes are secured in the locked media cabinet while awaiting disposal.

# Recovery Testing

Once per quarter, the Primary and Secondary Backup Administrators conduct recovery tests to verify the recovery procedures and validate the proper functioning of the backup system. Performance of Recovery Tests is logged in the Recovery Test Log. Recovery Testing failures are reported to the IT Director.

The Recovery procedures in this document are used to conduct the recovery test, and the procedures are updated at this time, if needed.

Recovery testing is timed, and the results used to verify if the RTO for backup targets is achievable.

## Individual File Recovery Testing

Each quarterly test includes a recovery of individual files. For this test, the backup administrators select several files at random (files that have not been modified since the most recent backup) to restore from the most recent backup. The checksum of the restored files are compared to the original, inability to restore all of the files or any difference in the checksum is noted as a failure.

## Full System Recovery Testing

At least once per year, the backup administrators conduct a full system (bare metal) recovery of a backup target. A new Virtual Machine is created, restored fully from the most recent backup of the target, and then tested for completeness of the restore and functionality of the system after restoration.

## Testing After Backup System Changes

After any change, upgrade or update to any component of the backup system, including hardware, software or operating system of the backup server, a recovery test is performed. This test includes restoring from backups made prior to the change, as well as conducting a test backup and restore using the new configuration.

# Appendix A: Backup Targets

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Server Name** | **Operating System** | **Backed up to** | **Backup Jobs** | **RTO** | **RPO** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Appendix B: Recovery Test Log

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Test Target** | **Objects Recovered** | **Result** | **Elapsed Time** | **Test Performed By** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Appendix C: Tape Inventory Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tape ID** | **Date placed in Service** | **Location** | **Backup Jobs** | **Date Removed from Service** |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix D: Adding New Backup Targets

Create directions for adding a new target to be backed up

# Appendix E: Restoration of Individual Files

Create directions for restoring individual files or folders

# Appendix F: Restoration of a Complete System

Create directions for complete system restoration of a target (‘bare-metal’)

1. Recovery Time Objective – The maximum time limit that a service can be down after a disaster. [↑](#footnote-ref-1)
2. Recovery Point Objective – The maximum age of data that can be lost due to a major incident. [↑](#footnote-ref-2)