UNIT BACKUP & RECOVERY PROCEDURES TEMPLATE

**Table of Contents**

**Backup Configurations 2**

Backup System 2

Backup Jobs 2

*Hourly and Nightly Backup 2*

*Daily 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**

**Backup Configurations**

**Backup System**

All backups are performed using vmWare with Vsphere 6.7, which runs on the server. All backups are written to both the Azure Cloud and to physical tapes.

**Backup Jobs**

**Hourly and Nightly Backup**

Bacch Group suggests that it is unnecessary for Capstone264Hotel to make hourly backups, however their system is capable of creating any kind of backup at any time, and therefore should they choose to begin doing hourly backups, they can implement those actions at any time.

**Daily Backup**

Incremental backups should be performed twice a day, every day, beginning at 12PM and 12AM. These should be stored both on Azure Cloud and on physical Tapes. Tapes should be stored for up to six months on-site. Once the need to save that information has expired, the tapes can be re-used.

**Weekly Backup**

Full backups should be completed every Sunday, beginning at 12AM. These should be stored both on Azure Cloud and on physical Tapes. Tapes should be stored for up to a year in a secure, off-site location. Once the need to save that information has expired, the tapes can be re-used.

**Rationale**

High value data, such as customer 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 a daily backup, our unit should be able to restore this high value data and lose no information.

**Backup Procedures**

**Backup Roles**

The Capstone264Hotel Manager is the primary departmental backup administrator.

The Capstone264Hotel Assistant Manager is the secondary backup administrator.

**Daily Tasks**

Every morning, prior to 9am, the backup administrator reviews the status for the previous day’s backup job (on Mondays, review the entire weekend’s activity) to verify that all jobs were 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 location. 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 is 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**

Capstone264Hotel currently only has one drive that allows for Tape backup, therefor the targets should always be Azure Cloud and the HP StoreEver LTO-5 Ultrium 3280 SAS Backup Tape drive.