Standard Operating Procedure
Backup and Recovery

Version History

<table>
<thead>
<tr>
<th>Version #</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Jason Gabriel</td>
<td>11/18/17</td>
</tr>
</tbody>
</table>

Description:
This SOP governs daily operations for backup and restore of data, assignment of responsibility, schedule, testing, monitoring and status reporting for backup and restore operations.

Scope:
This procedure will be followed for all data and server backups and restores. The procedure is intended as both a guide and policy designed to ensure that data critical to operations is backed up and available in the event of a system failure or critical event. This procedure may incorporate elements of the business continuity plan for data backup, schedule, and retention.

Roles:
The IT department manager will assign the role of backup operator and alternate backup operator to members of the IT staff. The backup operator will be responsible for completing backups. The alternate will handle the backups in the event the backup operator is unavailable. Ad-hoc backup and restore requests will be handled by the IT department manager or designated representative. Backup operators will be responsible for reporting success or failure of a backup to the department manager, who in turn will evaluate the need to complete an out of cycle backup. If a restore fails and cannot be recovered, the backup operator will notify the user and department manager for investigation.

Guidelines

1. Backups should be accomplished as much as possible during non-business hours to limit the impact on system performance.
2. Backups that fail to complete will be investigated for cause and reported to IT management.
3. Requirements for full, incremental or differential backups, schedule and restore windows will be determined separately for each system or data store based on operational needs. (See Backup Strategy)
4. Systems and applications deemed critical to operations, i.e. database servers, domain servers, file servers, print servers, etc. will be backed up according to the manufacturer’s recommended processes.
5. The Contingency Plan (CP) should be consulted for restoration times for data stores systems and applications. The backup frequency and types of backups have a direct influence on how rapidly data and systems can be restored. The correct method and schedule should be determined based on the CP as the overriding authority.

6. Data restores will be accomplished during any hour upon request of a data owner.

7. Restores will be tested at least once per quarter per data store. System and application restores will be tested once per year.

8. Backup tapes will be labeled according to the date they were first put in service and what data they contain.

**Backup Strategy**

What must be backed up and the speed in which it must be restored are a matter of company standards, regulatory compliance and an assessment of the impact a loss will have on operations. As a guide to determining what will be backed up and how, the following questions should be answered.

1. **Determine what needs to be backed.**
   - Gather inventories of information systems and data sources.
   - Determine what the system or data source supports; this may require contacting the system owner, database administrator or department heads.
   - Ask the question: Can the business afford to lose this system or data source? If the answer is no, it needs to be backed up.
   - Some systems or data sources may be identified in continuity plans. Consult any such plans when determining what needs to be backed up.

2. **Assess the impact of losing each system or data store for a period of time to determine an RTO (Recovery Time Objective).** RTO is the objective for how many hours the system can be down before it is restored. If the system is not critical but is required, its RTO might be 48 hours, whereas a key database that stops business operations for a department if unavailable might have an RTO of 4 hours or less. Below are some possible questions to consider when determining an RTO.
   - How many employees will be affected by the loss of the system or data store?
   - How many employees will be unable to perform their job?
   - Does the loss of the system cause a life-threatening situation?
   - Does the system affect external customers?
   - Is there a loss of revenue while a system or data store is unavailable?

3. **Using the RTO for each identified system or data store and knowledge about the backup and recovery system; determine the type of backup(s) and schedule that will be necessary to meet the RTO.** The table below lists the different types of backups available.

**Different Types of Backups**

<table>
<thead>
<tr>
<th>Backup Type</th>
<th>Files that are copied over to backup media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>All files, system data, etc.</td>
</tr>
<tr>
<td>Differential</td>
<td>All files added or changed since the last full backup</td>
</tr>
</tbody>
</table>
### Incremental

<table>
<thead>
<tr>
<th>Incremental</th>
<th>All files added or changed since the last full, differential or incremental backup</th>
</tr>
</thead>
</table>

### Daily

| Daily | All files added or changed on the day of the backup |

**Note:** Backup software and systems vary in capability and functionality as well as speed of data transfer. The type of backup and schedule needs to be tailored for each system or data store. As an example, email databases may have an RTO of 2 hours. If the backup strategy for email databases is a full backup every Sunday and incremental backup all other days, a restore on Thursday would require recovering the database from four different data saves: the original full on Sunday and incremental backups done Monday-Wednesday. This may take too much time to complete based on the RTO. A full backup every day would require only one backup to pull from, but storage space or time to constantly create all of the full backups might run over into business hours. A solution to this might be a full backup on Sunday with a nightly differential backup each day only requiring two backups be pulled.

4. **Consult any contingency plans, regulatory compliance requirements and governing directives and make a determination on how many copies of data that should be archived and stored.** Archives are used to go back in time to reconstruct what may have been lost in the present or past. Being able to go back 30, 60 or 90 days to recover a corrupt file may be critical to operations, especially if one does not know exactly when it became corrupt. However, full backup copies of data for every day in the past might be cost prohibitive or not possible. As strategy of full copies for the most recent 30 days and once a month copies at the 60 and 90 day point might be better.

5. **Determine what should be stored offsite.** Once again, consult any governing directives. Most sources of data should be stored offsite for contingencies to ensure they are not destroyed in the event of a disaster. System configurations that can be easily recreated from off the shelf software are not so critical. Also determine the number of copies and the interval in which they should be put into the archive, as well as how often they are rotated out and destroyed.

### Procedures

#### Backup and Recovery Storage Infrastructure

The backup and recovery storage infrastructure consists of the following systems and functional capabilities.

**Synology Drive**

- Primary backup software is Synology Backup.
- Backups are stored offsite on Amazon S3.
- Backup files are encrypted before being sent to the Amazon S3 Service.
- Backups are performed over an encrypted Internet connection.
AWS EC2 Servers

- Primary backup software is Amazon EBS Snapshot. The backup service and console is provided by Amazon Web Services (AWS). All EC2 Servers being backed up have automated snapshot tasks configured using custom cron jobs and python scripts.

- Snapshots are created by AWS by directly cloning the filesystem contents on each configured Elastic Block Storage (EBS) instance. EBS instances can be re-created from the backup copies.

- Storage is provided as part of the Amazon Snapshot Service.

- Offsite backups are performed by custom cron jobs and python scripts. Offsite backups are stored on the Amazon S3 Service in a different region from the EC2 servers.

Data Stores, Systems and Applications:
Document the backup scheduled for each identified system. The following table contains the data stores, systems and applications to be backed up. This table will be updated as systems and data changes.

<table>
<thead>
<tr>
<th>Data or System Name</th>
<th>Description</th>
<th>Backup Frequency</th>
<th>Copies</th>
<th>Offsite Archive</th>
<th>Data Owner</th>
<th>RTO (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Cloud-Based Servers</td>
<td>Every Night</td>
<td>7</td>
<td>Weekly</td>
<td>Jeffrey Allen</td>
<td>4 hrs</td>
</tr>
<tr>
<td>Synology</td>
<td>Internal Network</td>
<td>Every Night</td>
<td>1</td>
<td>Every Night</td>
<td>Jeffrey Allen</td>
<td>24 hrs</td>
</tr>
<tr>
<td></td>
<td>Hard Drive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Procedures:
Specific backup and restore instructions for each identified critical data store, server or application will be created using the following process. This documentation process ensures the procedure

1. Backup Procedures:
   - Automated Backup Tasks (for AWS and Synology)

2. Restoration Procedures:
   - Manual Recovery Process

3. Test Procedures:
   - Automatic Notification of Failed Backups