Backup Policy

1.1 Purpose of backup policy

The purpose of a backup policy is to establish guidelines and procedures for creating, managing, and maintaining backups of important data and systems. A backup policy outlines the frequency of backups, the types of backups that will be performed, where backups will be stored, who is responsible for performing backups, and how long backups will be retained.

The main goal of a backup policy is to ensure that in the event of a disaster, data and systems can be recovered and restored quickly and efficiently, minimizing downtime and data loss. A backup policy also helps to ensure compliance with legal and regulatory requirements for data retention and privacy. Additionally, it helps to establish a consistent approach to data backup and recovery across an organization, ensuring that everyone is following the same procedures and protocols.

1.2 Policy/Procedures

Active Directory:

- Daily system state backups of all domain controllers.
- Retention period of 30 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.

DHCP:

- Regular backups of the DHCP server database.
- Retention period of 7 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.

DNS:

- Regular backups of the DNS server database.
- Retention period of 7 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.

File and Print Servers:

- Regular backups of all important file shares.
- Retention period of 30 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.

Web Application:

- Regular backups of the web application and its associated databases.
- Retention period of 30 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.
- Ensure backups capture any custom configuration files or scripts.

Database:

- Regular backups of the database.
- Retention period of 30 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.
- Ensure backups capture any custom configuration files or scripts.

Virtualization Environment:

- Regular backups of all virtual machines and their associated configurations.
- Retention period of 30 days.
- Test restores of backups to ensure they are valid.
- Ensure backups are stored offsite or in a secure location.
- Ensure backups capture any custom configuration files or scripts.

Overall:

- Ensure all backups are automated and run regularly.
- Monitor backup logs to ensure they complete successfully.
- Document the backup policy and review it regularly.
- Ensure backups are encrypted and protected during transfer and storage.
- Implement a disaster recovery plan that includes restoring from backups.