**Backup Policy**

# **Purpose:**

To define the Organization’s Backup Strategy by identifying “Data” which is required/important for the Organization to perform operations normally.

The Backup Strategy should address the following:

* Defines Data which needs Backup
* Frequency of Backups, considering:
  + Recovery Time Objective (RTO)\* as per the Management’s directives.
  + Recovery Point Objective (RPO)\* as per the Management’s directives.
* Appropriate Sizing of Backup Repositories, providing enough storage capacity for Backups in the light of defined RTO and RPO.
* Securing Backup Data in Transit (Transmission) and Data at Rest (Repositories)
* Off-Site or Air-Gapped Backups
* Monitoring & Alerting Systems for Backup Operations
* Periodic Testing and Verification of Backup Data
* Periodic review of the Backup Policy

\*RTO - The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes.

The RTO answers the question: “How much time after notification about the business process disruption should it take to resume normal operations?

\*RPO -   The point in time to which data must be recovered after an outage.

# **Scope:**

This Policy addresses Data Backup requirement for the Organization with respect to its desired

RTO - Recovery Time Objective and RPO - Recovery Point Objective.

The Management provides clear instructions to IT as to what Data they deem to be of High Potential Impact, Moderate Potential Impact & of Low Potential Impact.

# **Policy:**

* IT Maintains a detail and precise list of Corporate Data to Backup. For eg.
  + - User Data / Files to back up
    - Physical or Virtual Machines for Machine State Backup
    - Device configurations to Backup
      * + NAS
        + Firewalls
        + Switches and Routers
    - Identify Files and Information that requires extra security when stored as backups
      * + SSH Keys
        + Passwords of Privileged accounts
* Define Recovery Point Objective (RPO) separately for the above mentioned categories
  + - ?
* Define Recovery Time Objective (RTO) separately for the above mentioned categories
  + - ?
* Appropriate Sizing of Backup Repositories, providing enough storage capacity for Backups in the light of defined RTO and RPO.
  + - Organization dedicates enough storage capacity to meet the RPO
* Securing Backup Data in Transit (Transmission) and Data at Rest (Repositories)
  + - Data is moved to Backup Repositories employing a secure channel
    - Backups are Encrypted
* Off-Site or Air-Gapped Backups
  + - Off-Site location is ensure Security and is provisioned with enough Storage capacity to meet the RPO and RTO.
    - Off-Site Syncing should be done in Non-Office hours or when WAN links are least utilized to avoid congestion
* Monitoring & Alerting Systems for Backup Operations
  + - An effective and robust Monitoring System monitors Backup Operations
    - Complimented with an equally effective Alerting System to alert IT and related parties on failures and warnings.
* Periodic Testing and Verification of Backup Data
  + - Backups are restored and tested periodically to ensure backup integrity and their ability to be restored.
      * Critical Backups are tested Every month
      * Data of Non-Critical nature is tested every three months

# **Roles:**

# **Responsibilities:**

The Organization’s IT Dept. ensures that Backup Strategy is inline and compliant with the Backup Policy.

IT Dept. takes responsibility of disclosing any failure to do so which may enable the Management to plan accordingly in case of a Contingency.