Data Backup Policy

1.0 Overview

A backup policy is similar to an insurance policy - it provides the last line of defence against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document.

2.0 Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

3.0 Scope

This policy applies to all data stored on corporate systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

4.0 Policy

4.1 Identification of Critical Data

The company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.

4.2 Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

• All data determined to be critical to company operation and/or employee job function.

• All information stored on the corporate file server(s) and email server(s), as well as these servers operating systems and logs. It is the user's responsibility to ensure any data of importance is moved to the file server.

• All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

• Logs and configuration of network devices such as switches, routers, etc.

• Information stored on employee desktops if the backup administrator deems such information necessary and backup facilities exist for such an endeavour. The backup administrator may instead choose to back up a standard desktop configuration and restore data from the file server at his or her discretion.

4.3 Backup Frequency

Backup frequency is critical to successful data recovery. The company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Mirroring from Primary to Secondary Bucket

Frequency: Every day

Mirroring to Archives Bucket

Frequency: Every Friday night

Mirroring to Local Drive

Frequency: Every 05th of each month

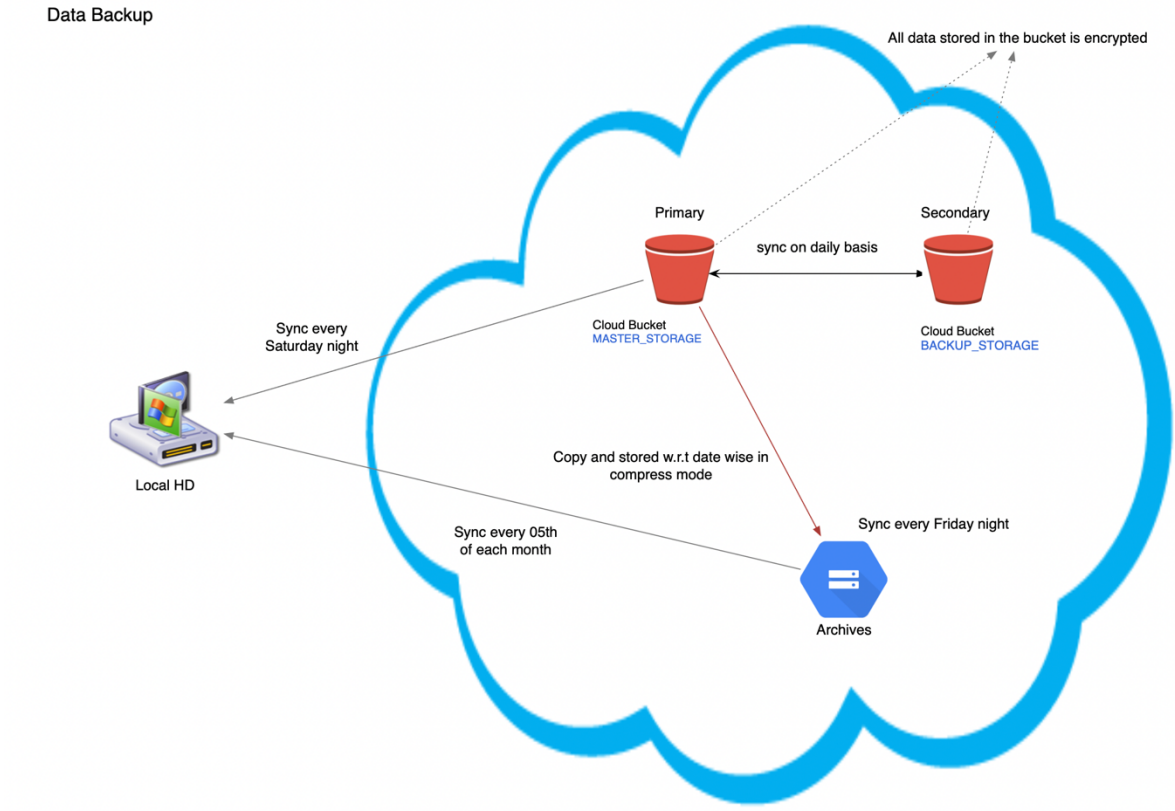
4.4 Off-Site Rotation

Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the company's uptime requirements. All the cloud storage bucket are backup to local drives and archives drives to maintain geographic separation.

4.5 Backup Storage

Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often confidential, company data, precautions must be taken that are commensurate to the type of data being stored. The company has set the following guidelines for backup storage.

All data will be stored in approved cloud storage buckets. Cloud Storage enables organizations to store, access, and maintain data so that they do not need to own and operate their own data centres, moving expenses from a capital expenditure model to operational. Cloud Storage is scalable, allowing organizations to expand or reduce their data footprint depending on need.



4.6 Backup Retention

When determining the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements (note that the backup retention policy must confirm to the company's data retention policy and any industry regulations, if applicable):

All Backups in primary / secondary bucket must be saved for 14 days.

All Backups in Archives must be saved for 8 weeks.

4.7 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.

4.8 Restoration Testing

Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems. Backup restores must be tested when any change is made that may affect the backup system, as well as twice per year.

5.0 Enforcement

This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Revision History

Revision 1.0, 08/09/2024