Backup Policy

Purpose

The purpose of this policy is to institute the necessary controls to mitigate the accidental loss of <Company Name> data. These controls assume that events such as accidental data corruption, deletion, or destruction will occur, and mitigate the impact of such events by maintaining reliable backup copies from which data can be readily restored.

Scope

This policy applies to all <Company Name> systems storing data classified as Customer Confidential, as defined in the Data Classification Policy.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

Customer data stored on <Company Name> infrastructure is backed up in order to mitigate the impact of events such as:

- Accidental deletion by customer or employee
- Corruption of data due to software or human error
- General system failure
- Physical or environmental disaster at a data center site
- External attack resulting in stolen or ransomed data

In order to ensure timely and reliable restoration of data, <Company Name> backup and restore procedures are tested on a periodic basis. Data backups are protected with security equal or greater to that of the original system where said data was stored. Backup copies are retained for a sufficient period of time to ensure that data loss events can be mitigated even

Backup Plan

Customer data is automatically backed up according to a backup configuration scheduled described in the Backup Policy.

Full backups of <Company Name> production databases are performed daily. Where available, database transaction logs are enabled and retained to support point-in-time recovery.

Customer data stored in cloud filestores such as S3 or GCS may be backed up using those systems' built-in versioning capabilities. Versioned systems record version history for each stored object, and offer the ability to restore that object to any previously saved state. Versioning is typically simpler to operate and more cost-efficient than full backup snapshots, especially for file objects that change less frequently.

Restore Testing

Backup restore tests are performed at least quarterly and ensure that the restored system works end-to-end.

On their own, regularly performed backups are not a sufficient mitigator of data loss events. It is possible that, over time, backed-up data and the method used to perform backups drift relative to the rest of the system. As a result of such drift, available backup copies may become unusable, or require extended database recovery times in order to correct the differences.

To safeguard against this possibility, <Company Name> performs quarterly testing of its backup restoration process. Backup copies are restored into a sandbox environment, and end-to-end tests are used to verify correct system operation. Once tests are complete, the full sandbox environment is deleted.

This entire end-to-end process encompassing restoration, testing, and cleanup may be fully automated and executed as part of a test suite.

Backup Storage

Backups are encrypted, stored in geographically independent regions, and have equivalent access control to the original system.

Backup copies of Customer Sensitive data contain all customer information that was present in the original system. Therefore, it is critical that these artifacts have the same or greater level of protection as that of data in the original system.

Access to backup artifacts is limited to individuals or systems involved in restore testing, as well as infrastructure administrators. Backups at rest must be encrypted with the same encryption as the original data store from which they were created.

To ensure the resilience of <Company Name> data, it is critical for backups to be resilient to local data center issues. As such, backup copies are only stored on fault-tolerant systems offering high availability, or are replicated across multiple geographically-disparate cloud regions.

Backup Retention

Backup retention is governed by customer agreements, and business, legal and regulatory requirements.

Full backup copies are retained for a minimum of 30 days, or longer as required by customer agreements or regulatory requirements. The same retention window applies to cloud filestore backups performed using versioning.

Backup copies older than the retention window are promptly deleted by <Company Name> using the cloud provider's default secure deletion method or, when they can be configured to do so, automatically expire and are securely deleted by the cloud provider.

Transaction logs used for point-in-time recovery may be retained for a shorter window than that of full backups, resulting in a potential Recovery Point Objective increase. For more information, see the Business Continuity and Disaster Recovery Policy.