Reg #: 3562

KHAGARAH Development Organization (KDO)

KDO
Data Backup Policy

KHAGARAH DEVELOPMENT ORGANIZATION
(KDO)

Nazish
Nazish Mohsin
Dy. General Secty
BOD
KDO
23.08.23

Farah Shahid
ED. KDO
23. Aug. 23

Contents

Nazish

1. Purpose of the Policy.

The purpose of this policy is to outline the procedures for securing KDO's critical data, ensuring the integrity, availability, and accessibility of information through regular and reliable backups. This policy aims to prevent data loss due to hardware failures, disasters, or human error and ensures that the organization can recover important data efficiently in case of a system failure or emergency.

2. Scope of the Policy.

This policy applies to all digital data created, processed, and stored by KDO, including but not limited to operational records, financial data, project documents, emails, and databases. It encompasses all electronic data stored on KDO's systems, such as servers, desktops, laptops, and other digital platforms.

3. Backup Procedures Frequency.

Daily Backups: Critical data, such as financial transactions, staff records, project-related documents, and other essential operational data, will be backed up on a daily basis. These backups will occur outside of working hours to minimize disruption to daily operations.

Weekly Full Backups: A complete backup of all organizational data, including both current and archival records, will be performed once a week. This backup ensures that a recent full copy of all data is available for recovery purposes.

4. Backup Storage.

External Hard Drives: All backup data will be stored on external hard drives. These drives are specifically chosen for their portability, reliability, and large storage capacities, making them ideal for managing substantial volumes of organizational data.

Off-Site Storage: To mitigate the risk of losing both operational and backup data in case of a localized disaster (e.g., fire, theft, or flood), the backup external hard drives will be stored in a secure off-site location each day. The off-site storage will be maintained in a locked, fireproof cabinet to ensure the protection of backup drives.

5. Backup Rotation.

Rotation of Backup Devices: A rotation system will be in place to maintain a balance between current and historical backup data. Backup external hard drives will be replaced periodically with a new drive (usually weekly) to ensure that the most recent data is stored securely while still preserving older backup copies.

Data Retention: Backup copies will be retained for a minimum of one year to ensure that sufficient historical records are available for reference, auditing, or data recovery needs. Older backups that are no longer required will be securely wiped or physically destroyed.

6. Data Security.

Encryption and Password Protection: All backup data stored on external hard drives will be encrypted to protect sensitive organizational and financial information. Access to the drives will be password-protected, ensuring that only authorized personnel can retrieve or access the data.

Nazish

7. Access Control.

Only specific individuals within the organization, namely the IT Manager and Executive Director, will have physical and electronic access to the external backup devices. These individuals will be responsible for ensuring the integrity and security of backup data.
Backup Verification and Testing:

8. Monthly Verification.

A full verification of the backup system will be conducted monthly to ensure the integrity of the data stored on external hard drives. This process includes checking whether the backup files are accessible, complete, and free of errors.

9. Testing Restores.

The IT Department will conduct quarterly tests of data restoration processes by randomly selecting backup data and restoring it to a test system. This testing ensures that the backup files are functional and can be relied upon in the event of a data recovery situation.

10.Backup Reports.

The IT Department will document all backup activities, including the success or failure of backup operations, and submit monthly reports to the Executive Director for review.

11.Retention and Disposal.

Retention Period: Backup data will be retained for one year, unless extended retention is required by legal, project-specific, or regulatory requirements. During this period, data will be readily available for restore or auditing purposes.

12.Secure Disposal.

When backup data is no longer needed, or when the retention period has expired, the external hard drives will undergo secure disposal. Data will be wiped using certified software to ensure that no recoverable data remains on the device. If disposal of the hard drive is necessary, it will be physically destroyed to prevent unauthorized recovery.

13.Responsibility and Oversight.

The IT Department is responsible for carrying out the backup operations, ensuring that backups are completed on time, and that data is securely stored and protected.
The Executive Director will oversee the backup process and ensure compliance with this policy. They will also receive regular updates on the status of backups, verification tests, and any issues that arise during backup operations.
Any issues identified during the verification or testing process will be immediately addressed by the IT Department, with corrective actions documented and reviewed by the Executive Director.

Nazish

14.Disaster Recovery and Restoration.

Emergency Recovery: In the event of data loss due to a system failure, disaster, or human error, the IT Department will initiate the data recovery process by restoring the most recent backup from the off-site location.

15.Restoration Time.

The IT Department is responsible for ensuring that restored data is available within a reasonable timeframe, depending on the size and complexity of the data loss situation.
Recovery Procedures: A Disaster Recovery Plan (DRP) will be maintained to guide the restoration process, specifying roles, responsibilities, and recovery steps.

This Data Backup Policy ensures that KDO's critical data is securely backed up, stored off-site, and readily available for restoration in case of emergencies. The policy aims to safeguard the organization from data loss, maintain business continuity, and support compliance with relevant data protection and retention requirements. Regular audits, testing, and reviews ensure that the policy is followed and that backup procedures are continually improved. KDO Data Backup Policies are continually improved.

Nazish

Nazish Mohsin
Dy. General Secratery
BOD
KDO
23.08.23.

FARAH SHAHID
Executive DIRECTOR
23. Aug. 2023.