digio

BACKUP MANAGEMENT POLICY

Document name	Backup Management Policy
Version	v1.1.3
Document author	IT Steering Committee
Last updated/reviewed on	15th March, 2023
Review frequency	Annual
Approved by	Sanket Nayak Co-Founder & Director

Digiotech Solutions Private Limited
Corporate office: 1st Floor, Tower-B, 2Gethr, Mantri Commercio, Bellandur, Off Outer Ring Road, Bangalore, 560 103
Regd office: C-1603, Oak Block, Salarpuria Greenage Apartments, Bomannahalli, Hosur Main Road, Bangalore 560 068

W: www.digio.in
E: support@digio.in
M: +919535536823

digio

Purpose: This document defines DIGIO's backup policy and is intended to ensure that, in the event of an emergency or when otherwise required, essential data (including, but not limited to data, logs, records, code, technical documentation etc) and emails of employees will be backed up and restored.
Scope: This policy is applicable to the protection of critical data of end user of DIGIO's. It does not cover personal data of employees.

1. Definitions

1.1 Backup

An information backup is the process of copying critical files from Laptop / Desktop computers to network storage, tape or other backup media such that files may be restored to disk in the event of damage to or loss of data.

Information backup shall also include any data, logs, records, code, technical documentation etc, which is critical to DIGIO

1.2 Restore

The process of bringing offline storage data back from the offline media and putting it on the user laptop / Desktop storage system.

2. Data Backup

2.1 The backup of critical data (Excel, Powerpoint, MSword, Pdf) that resides on individual Desktop and Laptop computers will be backed up by the end user, in Team Drive and/or Official communication tool

2.2 User will be provided with a specified folder / network space where the data can be saved. It is imperative that end-users save their data to the specified folder /or network space outlined in this policy, in order that their data is backed up regularly by IT Support team.

2.3 If the data that need to be backed up is not saved in specified folder / network space then it will not be backed up.

2.4 User Personal Data (Images, Videos, Mp3, Movies) will not be backed up.
Note: IT Infrastructure servers/ applications , HR applications and other white space applications have system specific backup policies for Servers/ applications. These backup policies are documented as a part of Disaster Recovery / Business Continuity Plan.

2.5 Database and Storage data is backed up in "Active-Active" setup, as per real-time mirroring setup in the DIGIO's Cloud Infrastructure. This includes database, audit logs, monitoring logs, stored artefacts
2.6 Code data and information and know-how, including documentation is backed up using central code repositories on a daily basis with auto-save functionality

2.7 Each type of data shall follow a Data/Information Classification and Handling policy that is defined for DIGIO and the retention policy shall be governed by the nature of the data, as per minimum retention policy

3. Email Backup

• DIGIO's uses Google Workspace on Google cloud, where adequate storage space on cloud is provided for archiving and email and document storage.

• Users shall use Online Archive facility to archive their mails on Google cloud storage. User shall not archive their mails locally.

4. Responsibilities

4.1 Department Function Head

Function heads will identify the critical users, considering business requirements, whose data will be backed up.

4.2 IT Infrastructure Team

IT team will take the backup of the data stored by end users on specific folder / network space.
IT Team will ensure that no personal data of employees are stored on specified folder / network space and backed up.
IT will ensure that only word, excel, powerpoint and PDF files are stored on the specified folder / network space and backed up.
IT will take weekly backup of specified folder / network space.

4.3 End User

End user will store and backup only word, excel, powerpoint and PDF files in specified folder / network space.
End User will not store personal data in the specified folder / network space provided by IT.

5. Exit Policy

This section refers to data retention of the employees who leave the organisation.
5.1 IT infrastructure will retain the data for 60 day for the employees who exit the company. Post 60 days the data will be securely archived in the storage

5.2 In case the ex-employee data need to be retain, respective HOD need to intimate and get approval from Head - IT Operation

5.3 Users on their Last Working Day will hand over their Data to his reliever or as directed by his Function Head.
5.4 It is a Department Function Head responsibility to ensure that backup of the users who is going to get relieved by IT Support Team.

5.5 Emails of ex- employees will be archived from email servers after 60 days. In cases where extension of data retention period is required post 60 days, respective HOD need to intimate and get approval from Head- IT Operation .

6. Backup Size

Corporate employees will be assigned by default 5 GB space for backup of their critical documents on specified folder / Network space. Size of documents to be backed up should not exceed 5 GB, employees have to prioritize which documents need to be backed up based on the criticality.

Additional storage space can be requested and shall be provided upon approval of respective Functional heads

7. Incident Reporting

Any person who knows of or suspects a breach of this policy may report it to IT Operation Head, or Corporate Security.

8. Controls

Backups of all essential information and software shall be taken frequently enough to meet business requirements. In this context business requirements shall include all data retention requirements imposed on the business by regulation.

8.1 Backups shall be taken on a regular basis according to a defined and documented cycle.

8.2 Backups shall be protected from loss, damage (including media degradation) and unauthorized

Access.

- Storing them in a fireproof safe on-site, or
- Storing them in restricted access areas, or lockable containers, within suitable climatically controlled locations off-site, and
- Restricting access to authorized staff.

9. Exceptions

Any exceptions to this policy must be authorized in writing by Head- IT Operation / Head- Information Security