2024

JJIF Data Backup Policy

CONFIDENTIAL

Created by

Document owners	**Role**
P. Schouten	Administration Director

Document Version Management

Version	**Date**	**Author**	**Description**
1.0	10-04-2024	P. Schouten	Initial document

Table of Contents

1. Policy Statement

JJIF recognizes the importance of protecting organizational data from loss due to errors, corruption, or disasters. The purpose of this Data Backup Policy is to ensure that all critical data is backed up in a secure and retrievable manner.

2. Scope

This policy applies to all staff members, contractors, and third-party service providers of JJIF who handle organizational data. It covers all data stored on JJIF cloud storage, workstations, laptops, mobile devices, and any other electronic media that contain organizational data.

3. Objectives

- To maintain and protect the integrity and availability of organizational data.
- To ensure timely restoration of data in the event of data loss.
- To comply with regulatory and legal requirements regarding data preservation and security.

4. Data Classification

Data must be classified into categories based on criticality and sensitivity:

- **Critical Data**: Data essential for the operation of the organization and whose loss would cause significant impact.
- **Sensitive Data**: Data that includes personal, confidential, or proprietary information.
- **Non-sensitive Data**: Data that can be made public without any repercussions.

5. Backup Requirements

- Critical Data must be backed up at least once every 24 hours.
- Sensitive Data must be backed up at least once every 48 hours.
- Non-sensitive Data should be backed up at least once per week.

6. Backup Methods

- Automated Backups: Scheduled backups using automated software to minimize human error.
- Offsite Backups: Storage of backup data at a geographically separate location to protect against local disasters such as Microsoft OneDrive or Dropbox.
- Onsite Backups: Additional onsite storage for quick access and restoration.

7. Storage Media

- Data must be stored on encrypted, secure storage media.

8. Data Retention

- Backup data must be retained according to the JJIF Data Retention Policy.
- Critical data backups must be stored for a minimum of 8 weeks.
- Other data backups should be retained as deemed necessary based on their classification.

9. Testing and Restoration

- Backup procedures must be tested regularly to ensure data integrity and successful restoration.
- A log of all backup testing activities and their outcomes must be maintained.

10. Responsibilities

- IT Department: Responsible for implementing the backup procedures and ensuring compliance with this policy.
- JJIF Data Protection Officer: Oversight and regular audits of the backup processes.
- All staff: Compliance with backup procedures and reporting any issues with data backup systems.

11. Incident Response

In the event of data loss, the JJIF Data Protection Officer must be notified immediately to initiate data recovery procedures according to the Incident Response Plan.

12. Policy Compliance

Violations of this policy may result in disciplinary action.

13. Amendment

This policy may be amended as necessary to reflect changes in technology, operations, or legal requirements.

14. Approval and Implementation

This policy is approved by the board of directors of the JJIF and is effective immediately.