Backup Policy

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

DOCUMENT CONTROL INFORMATION 2

PURPOSE, SCOPE AND USERS 4

1.1. Purpose 4

1.2. Scope 4

1.3. Users 4

2. REFERENCE DOCUMENTS 4

3. POLICY 4

3.1. Identification of Critical Data 4

3.2. Data to be Backed Up 4

3.3. Backup Frequency 4

3.4. Off-Site Rotation 4

3.5. Backup Storage 4

3.6. Backup Retention 5

3.7. Restoration Procedures & Documentation 5

3.8. Restoration Testing 5

3.9. Expiration of Backup Media 5

3.10. Applicability of Other Policies 5

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 5

5. APPENDICES 5

5.1. Definitions 5

5.2. Enforcement 6

5.3. Revision History 6

Purpose, scope and users

1.1. Purpose

This policy establishes the framework for creating and maintaining backups of critical data within Jadarah Funders Debt Collection Co. It aims to ensure data integrity and availability through systematic backup processes, aligning closely with disaster recovery principles to safeguard against data loss from various threats.

1.2. Scope

Applicable to all data across corporate systems within company, this policy mandates procedures for data backup, storage, and recovery, targeting equipment, files, and server data. Exclusions include land, buildings, and hazardous waste, covered under specific SOPs.

1.3. Users

All employees and departments handling company data, with specific roles for the IT Department, Purchasing Services, and users storing critical data on networked devices.

2. Reference Documents

- **SOP/442.MW:** SOP for Manufacturing Waste Management
- **SOP/715.SHM.SWM:** SOP for Hazardous, Chemical, Radioactive, and Biological Waste Management
- **SOP/442.FC.ASDP:** Asset Scrap Disposal Procedure

3. Policy

3.1. Identification of Critical Data

A formal review will identify data critical to company's operations, prioritizing it for backup.

3.2. Data to be Backed Up

Includes all critical operational data, server operating systems, logs, network device configurations, and selected desktop information, ensuring comprehensive coverage.

3.3. Backup Frequency

Adopts an incremental backup strategy from Monday to Thursday, with full backups every Friday, balancing data security with operational efficiency.

3.4. Off-Site Rotation

Mandates weekly off-site rotation of backup media to safeguard against local disasters, utilizing secure and environmentally controlled facilities.

3.5. Backup Storage

Specifies secure, controlled access storage for backups, with stringent guidelines for on-site and off-site storage, including online backup options.

3.6. Backup Retention

Defines a two-week retention period for both incremental and full backups, aligning with data and industry-specific regulatory requirements.

3.7. Restoration Procedures & Documentation

Requires detailed documentation and regular testing of restoration processes to ensure readiness and effectiveness in data recovery scenarios.

3.8. Restoration Testing

Mandates biannual and change-triggered restoration testing to validate the reliability of the backup and restoration system.

3.9. Expiration of Backup Media

Outlines procedures for monitoring and retiring backup media based on manufacturer's lifespan specifications to maintain data integrity.

3.10. Applicability of Other Policies

Integrates with company's comprehensive security policy framework, ensuring cohesive data protection strategies.

4. Managing records kept on the basis of this document

Documentation related to backup schedules, restoration tests, and media expiration will be systematically managed to ensure compliance and facilitate audits.

Record name	Code	Storage			Responsibility
		Retention time	Location	Protection	

5. Appendices

5.1. Definitions

- **Backup:** The duplication of data to a second location for safeguarding.

- **Backup Media:** Devices used for storing backup data, including tapes, disks, and online storage solutions.
- **Full/Incremental Backup:** Complete versus differential data copying based on changes since the last backup.
- **Restoration:** The process of recovering data from backups to its usable state.

5.2. Enforcement

Violations of this policy will be addressed by the IT Manager and Executive Team, with potential disciplinary actions ranging from access restrictions to termination, and legal action for severe breaches.

5.3. Revision History

Document revisions will be tracked and recorded to reflect policy updates and compliance with evolving data protection standards.