Aberrant Open-ISM™

DATA RECOVERY POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 OVERVIEW

The Data Recovery Policy establishes formal procedures to ensure that data is reliably available in the event of a technical incident.

2 PURPOSE

The ultimate aim of this policy is to ensure that customer data is available in the event of technical incident can be recovered with minimal loss and disruption to business operations.

3 SCOPE

This document relates to all data used across the organization.

4 SERVICE LEVEL AGREEMENT, UPTIME, AND RTO / RPO

As per <<Company Name>>'s Service Level Agreement (SLA) with its clients we honor a Service Level Agreement where services are provided under normal business hours. <<Company Name>> supports an uptime of 99.95% annually—24 hours should also be our maximum acceptable outage (MAO) duration. Internally, we target a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of 4 hours. Our recovery objectives accounts for a catastrophic loss of services or equipment at our host facility. Aberrant provides an uptime portal that allows customers to subscribe to alerts and review historical uptime data. The page can be viewed at <<Uptime Website>>.

The company should establish a minimum Service Level Agreement or Service Level Objective for each application and service utilized by the business. Data repositories that are critical to the business, or that are leveraged by other system should be held to a higher standard than non-critical systems.

Recovery Time Objectives (RTO)s and Recovery Point Objectives (RPO)s should be established for systems that hold data. For systems that hold email or other sensitive data an archive must be maintained that complies with legal or regulatory requirements. Requirements should align with the company's Data Retention Policy.

5 PROTECTION OF RECOVERY DATA

Data used for recovery, e.g. backups, servers images, etc., should be available in the event of a system outage. This may require that backups are stored in separate regional datacenters, offsite at third party locations, or held in escrow.

- Recovery data should be encrypted at rest as per the company's Encryption Policy.
- Backup Testing should be performed in accordance with the Business Continuity and Disaster Recovery Policy.

6 INFORMATION BACKUPS

6.1 FILE SHARES AND IMAGES

Backups of file shares and images are completed nightly. Backup retention is set at 30 days.

6.2 DATABASE BACKUPS

- Full backups of our database are executed nightly. Period snapshots of transaction logs a performed every five minutes. Database backups are held for 7 days.
- In the event that a backup job fails, the backup tool sends an alert to the SRE team. The failure is investigated and resolved on a timely basis.
- Backup should be stored on encrypted storage media.

6.3 OFFSITE BACKUPS

Offsite DB backups and file backups are encrypted and stored in an off-site location. Offsite backups are retained for two weeks.

7 BACKUP RESTORATION TESTING

- Backup restoration tests should be performed at least annually on all system that hold customer data, or proprietary data.
- A backup test should be considered a failure if it cannot meet stated RPO and RTO objectives.

8 DATA RESTORATION

8.1 RESTORATION REQUESTS

Requests for the restoration of an archived backup should be made directly to IT Operations. Backups restored into non-production environments must have PII elided. Requests are handled on an ad-hoc basis.

8.2 RECOVERY FROM AN INCIDENT

Recovery from an incident falls with the scope of the Incident Response Procedure.

9 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

10 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

11 LICENSE INFORMATION