Aberrant Open-ISM™

ISMS DOCUMENT AND RECORDS CONTROL STANDARD

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

PROPRIETARY

Next Scheduled Review		
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

<<Company Name>> maintains an Information Security Management System (ISMS) as a mechanism to ensure that implemented controls related to information security policies and procedures are organized and documented. The ISMS Document and Records Control Standard provides for control over creation, approval, distribution, usage, and updates of documents and records used in the ISMS of <<Company Name>>. All documents and records related to the ISMS shall be covered by this standard.

2 PURPOSE

The purposes of this ISMS Document and Records Control Standard are to:

1. Ensure appropriate creation and updating of documentation;
2. Control documentation for the ISMS;
3. Retain important documents and records for reference and future use;
4. Delete documents and records that are no longer necessary for the proper functioning of the organization;
5. Organize important documents and records for efficient retrieval;
6. Ensure that employees know what documents and records should be retained, the length of their retention means of storage, and when and how they should be destroyed; and
7. Ensure that core values are communicated from executive management to personnel through the ISMS.

Management has implemented controls that are built into the organizational and information security policies and procedures.

3 DOCUMENT CONTROL – INTERNAL DOCUMENTS

<<Company Name>>'s Information Owners are responsible for the control of ISMS documents. ISMS documents are defined as all documents created within <<Company Name>> that relate to the company's security program, or that pertain to compliance with third-party standards related to security or privacy.

3.1 DOCUMENT PROPERTIES

<<Company Name>> stores ISMS documentation digitally. The following information is collect for each document in the control standard:

- A name that accurately describes the subject that it addresses.
- An incremented version number.

- Document State: e.g. 'Draft' or 'Approved.'
- Classification: A classification that aligns with the Data Classification and Record Retention Policy—'Confidential', 'Proprietary', 'Public.'
- Owner: The employee who is responsible for ensuring that the document is update to date.
- Document Type: A rubric that identifies the type of document—e.g. 'Policy' or 'Procedure.'
- Activity: An immutable log of all changes that have been made to the document throughout it's history.

3.2 PUBLISHING A DOCUMENT

Changes to ISMS documents must be reviewed and approved prior to being assigned a version. Documents that are identified as 'Policy' documents must undergo a formalize approval process by the ISMS Governance Committee prior to publishing—e.g. incrementing the version and changing the state of the document to approved. Documents that are identified as 'Procedure' documents do not require ISMS Governance approval prior to publishing, however, the revision author is required to select an additional reviewer to ensure that changes made to the procedure are coherent prior to publishing.

3.3 MANAGERIAL OVERSIGHT

The document owner must review all changes to the document's that he / she is charged with monitoring. Changes that impact ancillary documentation such as flowcharts or customer documentation must be modified to reflect changes made in the ISMS.
Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

3.4 DISTRIBUTION

3.4.1 INTERNAL DISTRIBUTION

<<Company Name>>'s policies and procedures, including the code of ethics and corporate conduct policy and acceptable use policy, are made available to employees through the company's intranet.

Distribution is accomplished electronically through membership in a 'Group' that has been assigned the requisite 'Role.'

3.4.2 EXTERNAL DISTRIBUTION

External users can be granted temporary membership into a group that is able to access documentation based on least privilege. Privileges are revoked based on a time limit.

3.5 ARCHIVAL

Obsolete versions of documents are archived. This allows for a review of differences in the documentation between versions.

4 DOCUMENT CONTROL - EXTERNAL DOCUMENTS

External documents related to the ISMS that are controlled externally, such as certifications, are preserved digitally and made available through the same mechanism used for the distribution of documentation.

5 ISMS DOCUMENT AND RECORD RETENTION

<<Company Name>> will follow the retention periods specified in the Data Classification and Record Retention Policy, all documents and records shall be retained for at least the minimum period as stated in applicable state or federal laws or regulations.

6 ISMS DOCUMENT AND RECORD DESTRUCTION

<<Company Name>>'s Information Owners are responsible for the ongoing process of identifying its documents and records, which have met the required retention period and overseeing their destruction.

7 THIRD PARTY REVIEW

A third-party should perform an independent assessment of the <<Company Name>>'s controls environment annually to assess the effectiveness of internal controls within the environment.

8 COMPLIANCE

Failure on the part of employees to follow this standard can result in civil and criminal sanctions against <<Company Name>>'s and its employees and possible disciplinary action against responsible individuals. <<Company Name>> will annually review these procedures to ensure that they are in compliance with new or revised regulations.

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