Aberrant Open-ISM™

DATA RETENTION 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 SCOPE

The <<Company Name>> information security program has as its primary goal the "protection of the confidentiality, integrity, and availability of information in all forms". This standard supports that goal by providing specific instructions on the classification and handling of information across its lifecycle. As such, the primary objective of this document is to educate and inform the reader about information classification, how that classification determines the requisite protections (including guidelines for how long certain records should be kept and how they should be destroyed), and how to avoid unauthorized disclosure of the information either generated by or entrusted to, the care of the organization.

2 PURPOSE

The purpose of this record retention policy is to provide a system for protecting information that is critical to the organization. All workers who may come into contact with confidential information are expected to familiarize themselves with this policy and comply with it.

In addition, the goals of this records retention policy are to:

1. Retain vital records for reference and future use;
2. Delete records that are no longer necessary for the proper functioning of the organization; and
3. Ensure that <<Company Name>> personnel know what documents should be retained, the length of their retention, and when and how they should be destroyed.

3 RECORD RETENTION

This record retention policy provides for the systematic review, retention, and destruction of documents received or created by <<Company Name>>. This standard covers all records and documents, regardless of physical form, contains guidelines for how long certain records should be kept and how records should be destroyed. The standard is designed to ensure compliance with federal and state laws and regulations to eliminate accidental or innocent destruction of records and to facilitate <<Company Name>>'s operations by promoting efficiency and freeing up storage space.

3.1 RECORD RETENTION SCHEDULE

Record retention requirements depend on context. The following table provides required timelines for retention depending on context type. As a guideline, older records that are no longer required for retention should be destroyed because they are no longer required for use and destruction protects the customer's confidentiality.

Confidential data that is no longer required to achieve the purpose for which the data was collected and processed must be purged once it has passed the required length of time that it must be maintained. Regulatory or legislative requirements may supersede this directive.

Context Type	Required Length of Time	Comments
ISM Documentation	Permanent	ISM documentation are kept on a permanent basis unless otherwise noted by the Information Owner.
Press Releases/Public Filings	Permanent	<<Company Name>> should retain permanent copies of all press releases and publicly filed documents under the theory that <<Company Name>> should have its own copy to test the accuracy of any document a member of the public can theoretically produce against <<Company Name>>.
Voicemail	Retention not required.	
Email	7 Years	
Stateful Data	Retention not required.	Meta-data required for user experience.
Operational Data	7 Years	This includes PII and customer operational data.
Log Data	90 days minimum	90 days would be the minimum—this decision should be made based on ROI.
Security Scans	180 days	1 year is preferred.
Security Logs	180 days	
Video Logs	30 days	
Backups	2 weeks	
Vendor Contracts	Contract term plus 7 years	There is no requirement to destroy documentation beyond its required retention period.
Customer Contracts	Contract term plus 7 years	There is no requirement to destroy documentation beyond its required retention period.
Corporate Records	Permanent	Corporate records are kept on a permanent basis unless otherwise noted by the Information Owner.

Personnel Records	6 years following separation	Per Titles 29 and 41 of the Code of Federal Regulations, personnel files (including applications, references, promotion/demotion records, background checks, employee training and rate of pay) should be retained for a period of 6 years following separation.
Financial Records	7 Years	Financial records such as accounting, tax, and, payroll shall be retained 7 years and/or permanently deemed by the Information Owner.
Intellectual Property	Permanent	Development documents and source code are often subject to intellectual property protection in their final form (e.g., patents and copyrights). The documents detailing the development process are of value to <<Company Name>> and are protected as a trade secret, as well as <<Company Name>>'s source code. Development documentation and source code are kept on a permanent basis.

3.2 DESTRUCTION OF DOCUMENTS AND ELECTRONIC MEDIA

<<Company Name>>'s Information Owners are responsible for the ongoing process of identifying its records, which have met the required retention period and overseeing their destruction. Document and electronic media destruction will be suspended immediately, upon any indication of an official investigation or when a lawsuit is filed or appears imminent. Destruction will be reinstated upon conclusion of the investigation.

3.2.1 BACKUP RETENTION

Data stored on backup media should be purged within 48 hours after it has passed its required length of retention.

3.2.2 DESTRUCTION OF DOCUMENTATION

Destruction of financial and personnel-related documents will be accomplished by shredding via a cross-cut shredder.

3.2.3 DESTRUCTION OF ELECTRONIC MEDIA

Destruction of electronic media will be accomplished by using processes that adhere to standards for clearing and sanitizing standard DoD 5220.22-M.

3.2.4 SECURE DISPOSAL OR REUSE OF EQUIPMENT

IT Assets (except personnel owned End User Assets) shall be disposed in accordance with approved methods, which may include: auction, sale, destruction or donation and shall maximize the physical value of the IT Asset and the Company's objectives taking into consideration the security of any data or information that may remain on an IT Asset. The disposal method for assets will be subject to the discretion of the CFO.

Devices slated for disposal will have a label or other indicator affixed to the electronic media to signify that the device has been wiped or degaussed. This will ensure that outside parties will not be able to access any data on the device. All electronic equipment that is disposed of will be recorded in order to keep track of what is still in use and what has been removed from service. The type of device, serial/asset number and location it was formerly in use at will be recorded (please refer to ASSET INVENTORY POLICY). The device will then be removed from the hardware and software inventory and placed in a destroyed equipment inventory.

4 COMPLIANCE

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

5 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

6 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

7 LICENSE INFORMATION