Aberrant Open-ISM™

AUDIT POLICY

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

The Internal Audit function reports to the Chief Compliance Officer and operates independently of the Information Security Team. In essence, the Internal Audit function is a check against Information Security to ensure that work is performed as it is documented.

This policy is designed to provide the authority for members of <<Company Name>>'s Internal Audit team to conduct audits on any system within the scope of the security program—this authority also extends to privacy compliance.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources.
- Investigate possible security incidents to ensure conformance to <<Company Name>>'s security policies.
- Monitor user or system activity where appropriate.

2 SCOPE

This policy establishes the audit teams broad authority to operate in area that falls within the scope of the company's ISMS.

3 PERSONNEL

It's imperative that audits are performed by individuals with sufficient knowledge of what is being evaluated. As a result, auditors should have demonstrated experience in performing audits in a particular subject area prior to being given autonomy to run an audit independently. It's is the discretion of the CCO to establish qualifications for audit personnel.

4 RESPONSIBILITY

4.1 AUDITS

The internal audit function is responsible for coordinating the testing and review of business processes, procedures, and systems to ensure that <<Company Name>> is operating in a way that is consistent with our security program. When planning an audit, the internal auditor should account for the following:

- Audit requirements and activities involving checks on operational systems shall be carefully planned and minimize the risk of disruptions to business processes.

- The scope of testing should be limited to those systems and resources specified in the audit plan and agreed to by the resource owner(s).
- Persons performing audit services must document their activities, procedures, findings, and recommendations. Audit documentation and evidence should be stored in a secure location consistent with <<Company Name>>'s data retention policies.
- The scope of the audit limits the auditor's authority. Audit scope is determined by the CCO, or a delegated authority.

4.2 MANAGEMENT REVIEW

Executive management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. The management review shall include consideration of:

- the status of actions from previous management reviews;
- changes in external and internal issues that are relevant to the information security management system;
- feedback on the information security performance, including trends in:
  - nonconformities and corrective actions;
  - monitoring and measurement results;
  - audit results; and
  - fulfilment of information security objectives;
- feedback from interested parties;
- results of risk assessment and status of risk treatment plan; and
- opportunities for continual improvement.

The organization shall retain documented information as evidence of the results of management reviews. The ultimate aim of the audit activity is continuous improvement.

4.3 CONTINUOUS IMPROVEMENT

<<Company Name>>'s Information Security Management System (ISMS) program is based on the Plan – Do – Check – Act (PDCA) cycle, often referred to as a "continuous process improvement" approach. The Internal Audit Team is instrumental in driving the continuous improvement process.

5 AUTHORITY

When requested, and for the purpose of performing an audit, any access needed will be provided to members of <<Company Name>>'s Internal Audit team. This access may include:

- User level and/or system-level access to any computing or communications device.

- Access to information (electronic, hardcopy, etc.) may be produced, transmitted, or stored on <<Company Name>> equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on the company's networks.

6 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

8 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

9 LICENSE INFORMATION