Aberrant Open-ISM™

PROGRAM ROLES

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 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to define the duties, responsibilities, authorities and qualifications required by program roles. Program roles are controls to clearly define employee accountability, and to contribute metrics toward employee performance assessment.

1.2 BACKGROUND

Information Security roles are part of a holistic approach to implementing the process of information security.

1. Roles are performed by individuals
2. An individual will typically fulfill multiple program roles
3. A program role may be fulfilled by multiple individuals
4. Program roles serve as the basis for job descriptions

1.3 DEFINITION OF TERMS: AUTHORITIES

This document delineates sets of authorities for each role. Each authority is characterized by one of the following words:

1. **SHALL** or **MUST** indicates an activity or function which the role is obligated to perform and cannot refuse or delegate
2. **SHOULD** indicates an activity or function for which the role is accountable, although specific performance may be delegated
3. **MAY** indicates an activity or function which the role can perform among its other duties

2 SCOPE

2.1 INDIVIDUALS

These descriptions are relevant to all individuals assigned to perform the described program roles. Roles may be strategic, tactical, or operational in nature.

2.2 SYSTEMS

These descriptions are relevant to all in-scope systems to which program role duties, responsibilities, and authorizations have been ascribed.

2.3 SEGREGATION OF DUTIES

Program roles should support a separation of duties in order to prevent conflicts of interests. Any changes to the responsibilities of any program role should be closely evaluated by the ISMS Governance Committee in order to ensure that segregation of duties is structured into the security program.

2.4 REVIEW

Executive management evaluates the skills and expertise of its members relative to their assigned roles at least annually.

3 GROUPS, COMMITTEES, AND BOARDS

3.1 BOARD OF DIRECTORS

The board of directors should operate independent from management and exercise oversight over the development and performance of internal controls.

3.1.1 RESPONSIBILITIES

1. Ensures the interests of investors are addressed.
2. Oversees the development and performance of internal controls.
3. Approves the strategic direction of the company.
4. Legally responsible for ensuring that the organization complies with the applicable federal, state, and local laws and adheres to its mission.

3.1.2 AUTHORITIES

1. Approves strategic initiatives.
2. Enacts structural changes related to personnel and resources.
3. Inquires into the performance and health of the organization.

3.1.3 QUALIFICATIONS

1. Financial knowledge related.
2. Industry acumen
3. Knowledge of all relevant regulatory standards, frameworks, and applicable laws pertaining to security and privacy.

3.2 ISMS GOVERNANCE COMMITTEE

The ISMS Governance Committee is a working committee comprised of leadership from many of the business functions as defined within its charter. The Committee provides overall governance of the information security program. To avoid conflicts of interest the ISMS Governance Committee should maintain its independence from those that operate the security program.

3.2.1 RESPONSIBILITIES

1. Provide overall governance of the information security program.
2. Maintaining documentation related to Information Policies and Procedures.
3. Maintaining the Scope of Registration and ensuring adherence to scope.
4. Ownership of the implementation of the ISMS, e.g. ensures adherence to documented conventions, etc.
5. Encourage awareness of security efforts and support integration of security into everyday working processes.

3.2.2 AUTHORITIES

1. Must review information security standards.
2. Must review information security program strategic plans.
3. Must review information security program status and associated risk levels.
4. Must review and act upon metrics for efficiency and effectiveness of the information security program.

3.2.3 QUALIFICATIONS

1. Invitation to committee by executive management.
2. Member of any group with assigned information security responsibility.

4 ROLES AND RESPONSIBILITIES

As a guiding principle, roles and responsibilities should avoid conflicts of interest and when possible, should strive towards a strict segregation of duties. To assist with roles and responsibilities related to the ISMS, program roles should be well defined and should be prescriptive. Every effort should be made by executive management to reduce and limit ambiguity in terms of job responsibilities in order to reduce conflict, confusion, and inefficiency.

All employees must be assigned a role at that the start of their employment. An employee's job role is used to determines an employee's access to data and sensitive information. It is a requirement that all employees within the organization adhere to the company's Information Security Policy.

4.1 EXECUTIVE MANAGEMENT

Executive management provides the high-level vision and empowers the <<Company Name>> Information Security Program. As a strong-guideline executive management should respect and empower a culture built around a segregation of responsibilities where executive management focuses on strategic drivers of the business. Whenever possible executive management should delegate operational responsibility to operational management.

4.1.1 RESPONSIBILITIES

1. Provide overall guidance, direction and authority for the Information Security Program and the Information Security Management System (ISMS).
2. Performs an annual review with operational management to assess the effectiveness and performance of the ISMS program within the environment.
3. Periodic assessment of ISMS policies, procedures and other control documents for accuracy and applicability on at least an annual basis.
4. Identification and assessment of enterprise risks that could prevent <<Company Name>>'s objectives from being achieved.
5. Establishment of information security objectives in alignment with the ISMS program.
6. Monitors the effectiveness and performance of internal controls implemented within the environment.

4.1.2 AUTHORITIES

1. Should approve the Information Security Policy
2. Should approve the Information Security Program Charter
3. Should approve the ISMS Governance Committee Charter
4. May appoint members of ISMS Governance Committee (see below)

4.1.3 QUALIFICATIONS

Senior membership in <<Company Name>> management team.

4.2 CHIEF INFORMATION SECURITY OFFICER (CISO)

The Chief Information Security Officer (CISO) and/or their delegate(s) are responsible for information security service delivery.

4.2.1 RESPONSIBILITIES

1. Responsible for information security.
2. Security oversight of the ISMS
3. Continuous improvement of ISMS performance
4. Responsible for monitoring the effectiveness and performance of internal controls implemented within the environment.
5. Leadership of the Incident Management Response Team in order to ensure timely resolution of security incidents.
6. Management of the company's 'Issue Queue' and management of all non-conformities
7. External threat assessment.

4.2.2 AUTHORITIES

1. Required to be a member of the ISMS Committee.
2. Establishes and enforces standards related to conformance to information security.
3. Overarching approval of controls related to security or privacy.
4. Approval and enforcement of security risk assessments.
5. Establishes and enforces standards of technical product security.
6. In charge of the incident management and leadership of the incident response team (IRT) in the event of incident.

4.2.3 QUALIFICATIONS

1. Knowledge of all relevant regulatory standards, frameworks, and applicable laws pertaining to security and privacy.
2. Knowledge of <<Company Name>>'s ISMS program.
3. Awareness of ISMS requirements, processes, and roles.

4.3 CHIEF TECHNOLOGY OFFICER (CTO)

The Chief Technology Officer (CTO) and/or their delegate(s) are responsible for application security and supporting security activities related to the ISMS.

4.3.1 RESPONSIBILITIES

1. Management of the Software Development Lifecycle (SDLC) and implementation of controls related to application security.
2. Performance and monitoring of systems to ensure adherence to internal controls.
3. Prioritizing security and supporting activities of the CISO as it relates to the ISMS.
4. Management of infrastructure support.
5. Supports the activities of the CISO as it relates to the ISMS.
6. Assists with continuous improvement of information security program effectiveness.

4.3.2 AUTHORITIES

1. Required to be a member of the ISMS Committee.
2. Approval and enforcement of controls related to application security.
3. Review and approves technical product security.
4. Backup to the CISO in the event of an incident response issue.

4.3.3 QUALIFICATIONS

1. Knowledge of all relevant regulatory standards, frameworks, and applicable laws pertaining to security and privacy.
2. Knowledge of <<Company Name>>'s ISMS program.
3. Awareness of ISMS requirements, processes, and roles.

4.4 CHIEF COMPLIANCE OFFICER (CCO)

The Chief Compliance Officer (CCO) and/or their delegate(s) are responsible for coordinating with third parties, internal audits, and promoting information security awareness within the company environment.

4.4.1 RESPONSIBILITIES

1. Identification and documentation of non-conformities and missing controls.
2. Coordination of internal audits of manual, automated, preventive, detective, and corrective controls within scope of the ISMS.
3. Adherence to all relevant security and privacy standards; and legal statues.

4. Coordination with external auditors, regulators, and registrars.
5. Management and authority over staff as it relates to adherence to conformance with legal statues or regulatory compliance.
6. Take lead role in overseeing the development and delivery of information security curricula.

4.4.2 AUTHORITIES

1. Required to be a member of the ISMS Committee.
2. Management, coordination, and approval of internal and external audits, and is the ultimate arbiter of audit scope.
3. Approve information security training curricula.
4. Point of contact for outside entities regarding security or privacy.

4.4.3 QUALIFICATIONS

1. Awareness of <<Company Name>>'s ISMS.
2. Awareness of information security requirements.
3. Awareness of roles and role relationships.
4. Ability to develop training curricula and awareness messages.

4.5 DATA PROTECTION OFFICER (DPO)

The DPO is responsible for overseeing data protection strategy and assisting with supporting security activities related to the ISMS

4.5.1 RESPONSIBILITIES

1. Responsible for data protection activities.
2. Supports the activities of the CISO as it relates to the ISMS.
3. Assists with continuous improvement of information security program effectiveness as it related to data protection.
4. Responsible for the education of employees on data protection compliance requirements and training of data processing staff.

4.5.2 AUTHORITIES

1. Required to be a member of the ISMS Committee.
2. Approval of controls related to privacy.

4.5.3 QUALIFICATIONS

1. Knowledge of all relevant regulatory standards, frameworks, and applicable laws pertaining to privacy.
2. Expertise on how personal data is being used and protected.
3. Knowledge of <<Company Name>>'s ISMS program.
4. Awareness of ISMS requirements, processes, and roles.

4.6 OPERATIONAL MANAGEMENT

Operational Management is comprised of process owners and operational staff.

4.6.1 RESPONSIBILITIES

1. Implementing and operating internal controls within their respective business units.
2. Performing periodic POST HOC assessments at the completion of operational tasks.
3. Monitoring, investigation, and troubleshooting of control failures.
4. Ensuring that business plans and budgets align with the strategic objectives that have been defined by Executive Management.

4.6.2 AUTHORITIES

1. Authority over operational personnel.
2. Authority over operational security.

4.6.3 QUALIFICATIONS

1. Awareness of <<Company Name>>'s ISMS.
2. Awareness of information security requirements.
3. Awareness of roles and role relationships.

4.7 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) MANAGER

This role is the ISMS management framework subject matter expert. This role both directs others to uphold information security requirements and performs activities based on such requirements and the directives of senior management.

4.7.1 RESPONSIBILITIES

1. Enforces operational requirements for the ISMS.
2. Works with the CISO and the CCO to ensure that issues related to the ISMS are resolved in a timely matter.
3. Overarching ownership and maintenance of ISMS documentation.

4. Coordinates audit preparation with the CCO.
5. Supplier security oversight.
6. Information asset oversight.

4.7.2 AUTHORITIES

1. Management of ISMS resources via planning activities coordinated with Executive Management, CISO, CTO, and CCO.
2. Evaluation of system conformance and continuous improvement of the program.

4.7.3 QUALIFICATIONS

1. Awareness of ISO 27001 and ISO 27002.
2. Familiarity with <<Company Name>>'s ISMS program.
3. Awareness of ISMS requirements, processes, and roles.

4.8 SECURITY ARCHITECT

The Security Architect is an individual assigned to implementing the ISMS as it relates to information security.

4.8.1 RESPONSIBILITIES

To implement security based on the ISMS and industry best practices. Responsible for directing network security tasks.

4.8.2 AUTHORITIES

1. Responsible for information security
2. Administration of the network

4.8.3 QUALIFICATIONS

Awareness of relevant security standards, the ISMS and competence in network and information security architecture.

4.9 LEGAL COUNSEL

4.9.1 RESPONSIBILITIES

1. Creates, modifies, and reviews contracts.
2. Supports the activities of the CISO as it relates to the ISMS.
3. Assists with continuous improvement of information security program effectiveness as it related to data protection.

4.9.2 AUTHORITIES

1. Required to be a member of the ISMS Committee.
2. Validates controls related to privacy.

4.9.3 QUALIFICATIONS

1. Knowledge of all relevant regulatory standards, frameworks, and applicable laws pertaining to privacy.
2. Expertise on how personal data is being used and protected.
3. Knowledge of <<Company Name>>'s ISMS program.
4. Awareness of ISMS requirements, processes, and roles.

4.10 INTERNAL AUDITOR

The <<Company Name>> Internal Audit Team shall be responsible for all internal audits. In the event that resources are unavailable during the audit timeframe, the task of performing internal audits will be transferred to an independent third party.

4.10.1.1 RESPONSIBILITIES

Conduct internal audits, either as scheduled or upon request.

4.10.2 AUTHORITIES

1. Identification of non-conformities and opportunities for improvement.
2. Recommendations for continuous improvement.

4.10.3 QUALIFICATIONS

1. Awareness of <<Company Name>>'s ISMS.
2. Awareness of information security and privacy requirements.
3. Awareness of roles and role relationships.

5 THIRD PARTY ROLES

Some functions or responsibilities within the ISMS are dependent on external business relationships. Some of these relationships may be with clients and some may be with parties with specific subject matter expertise. These roles are defined below.

5.1 EXTERNAL SUBJECT MATTER EXPERT (SME)

A party, whether or not operating under contract, with the ability to offer specific expertise not otherwise available within the organization.

5.1.1 RESPONSIBILITIES

Contribution of specialized Awareness.

5.1.2 AUTHORITIES

None.

5.1.3 QUALIFICATIONS

Specialized expertise in a specific subject area or technology.

5.2 CONSULTANT AUDITOR

The <<Company Name>> Internal Audit Team shall be responsible for all internal audits. In the event that resources are unavailable during the audit timeframe, the task of performing internal audits will be transferred to an independent third party.

5.2.1 RESPONSIBILITIES

Conduct internal audits, either as scheduled or upon request.

5.2.2 AUTHORITIES

1. Identification of non-conformities and opportunities for improvement.
2. Recommendations for continuous improvement.

5.2.3 QUALIFICATIONS

Expertise in field of specialization.

6 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

7 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

8 LICENSE INFORMATION