Aberrant Open-ISM™

HUMAN RESOURCE SECURITY 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

This policy sets out the collaborative relationship between the Information Security Program and <<Company Name>>'s Human Resources (HR) business function. The primary reason for this policy is to define job roles within the program and to ensure that competent, qualified individuals are hired to fill the job roles that have been documented. Documented job roles (written job descriptions) will, in turn, become inputs to the Role-Based Access Control model. Another important reason is to communicate the user's responsibilities toward information security within the context of each role.

2 EMPLOYMENT HIRING, SCREENING, AND ONBOARDING

2.1 INTERNAL RECRUITING FUNCTION

<<Company Name>> maintains a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives. The recruiting department also assists with ensuring employees that conduct hiring interviews are sufficiently trained and qualified to conduct interviews.

2.2 JOB DESCRIPTIONS

Roles and responsibilities are defined in written job descriptions and communicated to personnel through the company's intranet. Management reviews job descriptions annually and makes updates, if necessary.

2.3 HIRING INTERVIEWS

<<Company Name>> evaluates the competencies and experience of candidates prior to hiring, and of personnel transferring job roles or responsibilities. Job candidates with previous experience should be able to demonstrate competence on the basis of appropriate education, training, or work experience. All job candidates should be evaluated against job descriptions as part of the hiring process.

This process is integral to ensuring that the individuals hired by the company are qualified to perform the roles and responsibilities outlined in their job description.

2.4 BACKGROUND CHECKS

As a condition of employment with <<Company Name>>, all contractors and employees are required to provide documentation that verifies U.S. work authorization.

Any offer of employment with <<Company Name>> is contingent upon satisfactory completion of a background investigation. Background checks may commence after an offer letter has been generated but must be concluded before the employee’s first day of employment. The background check should include the following:

- Federal Criminal Search: A national search of past criminal behavior such as firearm charges, terrorism, white-collar crimes, financial fraud, tax evasion, etc.
- Employment Verification: Verification of employment at the prospective employee's last two previous employers within the last seven years.
- Bankruptcies, Liens, and Judgments Search: A search for bankruptcies, liens, and judgments.

2.5 REQUIREMENTS PRIOR TO STARTING EMPLOYMENT

For an employee to start at <<Company Name>>, the following information must be completed and be included in the employee’s personnel file:

- Resume
- Application for Employment
- Results of Background Investigation
- Signed Offer Letter that includes language certifying the organization’s responsibilities for information security.
- Proprietary Rights and Information Agreement
- Arbitration Agreement
- Notice to Employee

2.6 FIRST DAY OF EMPLOYMENT

Once the employee has satisfied requirements for employment they are granted logical access to systems based on their job function. Additionally, HR should ensure that the company’s organizational chart is updated to reflect the change in staffing.

New employees must be made aware of the information security policy, their importance to the overall Program, and the implications of not conforming with information security management system requirements. The ultimate aim of familiarizing new employees with the company’s policies, procedures, and directives is to communicate core values that executive management feels are integral to the company’s culture. Toward this end, new employee must read and acknowledge the following policies:

- Acceptable Use Policy
- Code of Ethics
- Code of Conduct

- Communication Policy
- Physical Security Policy

3 MANAGEMENT SUPERVISION AND SECURITY COMPLIANCE

Management must ensure that employees and contractors are aware of and fulfil their information security responsibilities.

3.1 DISCIPLINARY PROCESS

If an employee fails to comply with <<Company Name>> information security policies and procedures, <<Company Name>> will take such disciplinary or preventative action as it deems appropriate. Violations of <<Company Name>>'s information security policies and procedures may result in disciplinary measures including, depending on the individual circumstances, the level of the employee's involvement and knowledge and the severity of the violation:

- Warning or reprimand
- Probation
- Suspension
- Salary reduction
- Bonus reduction or elimination
- Demotion
- Termination

Disciplinary measures may be taken against an employee for:

- Directly violating information security policies and procedures (including failing to report a violation or suspected violation) or any applicable law, rule or regulation.
- Directing others to violate information security policies and procedures or any applicable law, rule or regulation.
- Failing to cooperate with an investigation of a violation, including being untruthful or withholding relevant information.
- Knowingly falsely accusing another employee of a violation.
- Retaliating against a person who reports in good faith a violation or suspected or potential violation, or directly or indirectly encouraging others to do so.

Disciplinary action will also apply to managers who, with respect to those employees reporting to them, know that prohibited conduct is contemplated by such employees and do nothing to prevent it, or know that prohibited conduct has been engaged in by such employees and fail to take appropriate corrective action. Managers may also be subject to disciplinary action for their failure to effectively monitor the actions of their subordinates.

In addition, violations of legal and regulatory requirements may carry their own substantial and serious civil and criminal penalties, including fines and imprisonment.

3.2 EMPLOYEE PERFORMANCE AND CONDUCT EVALUATIONS

Performance and conduct evaluations are performed for personnel on an annual basis. Employees are evaluated against their job titles / roles and responsibilities. Employee evaluations are predicated on a letter grade methodology. The employees letter grade and any additional review feedback should be presented to the employee directly. Additionally, the manager should send a copy of the employees evaluation to the employee's <<Company Name>> email address—please see Appendix A.

3.3 DISSEMINATION OF POLICY

<<Company Name>>'s policies and objectives, including changes made to the objectives, are communicated to its personnel through meetings.

3.4 EMPLOYEE OFFBOARDING

When an employee decides to end their employment with <<Company Name>> they should submit a resignation letter addressed to their manager. This communication should be stored for posterity as part of the offboarding process. On the employee's last day offboarding should be initiated to ensure that the employee no longer has access to <<Company Name>>'s systems or resources.

In the event that an employee is terminated for performance reasons the communication shared with the employee should be recorded and the offboarding process should be initiated at the date of termination.

All tasks assigned to offboarding must be completed within 24 hours of the employee's final day of work. Evidence that every step of the offboarding has been completed should be saved for posterity.

The offboarding process should incorporate the following tasks:

- Communicate the employee's departure internally, and if appropriate externally—e.g. with customers or vendors.
- Update all tasks or work items that the employee formerly owned with a new owner.
- Update documents and digital assets to ensure that the employee is no longer listed—e.g. ISM documentation, SOPs, RACIs, etc.
- Recover company assets

- Archive the user in the domain controller and ensure that access or permissions to internal or external systems are revoked.
- Rotate service accounts that the employee had access to.
- Conduct an exit interview and record and disseminate the result.
- Update the company's organizational chart to the reflect the change in staffing.
- Prepare for future reference requests

4 GUIDANCE ON INFORMATION SECURITY TRAINING AND AWARENESS

4.1 NEW HIRE ORIENTATION

1. All new employees, and new contractors or third-party users, who will have access to <<Company Name>> information assets, must complete information security training before being granted access to information and resources in the custody of the organization.
2. Information security training may be either a stand-alone presentation or a module within the New Hire Orientation training materials.
3. Records of training attendance and test results, if any, shall be recorded.
4. Topics presented during new hire training should focus on general information security topics applicable to the entire organization.
5. Training content should include but not be limited to the following:
    1. Security requirements, including password construction, use and expiration
    2. Legal and regulatory compliance requirements
    3. Acceptable use of information assets and resources
    4. Known and potential threats and vulnerabilities related to deployed software
    5. Security event reporting procedures
    6. Contact information for the information security program
6. Training content must be consistent with the security policies of <<Company Name>> and all employees must attend the annual Information Security Awareness Training.
7. Training is mandatory for all <<Company Name>> employees and attendance will be managed by the ISMS Manager and / or Director of HR. In the case that employees do not adhere to this standard; the management team must deploy the corrective action policy.
8. Training materials should be regularly reviewed and updated, at least annually, to ensure such materials remain current with existing information security requirements.

4.2 ADDITIONAL TRAINING FOR SPECIALIZED ROLES

1. Where justified by the user's role and responsibilities, further information security training shall be provided to each user.
2. Additional training shall reflect existing or incoming information security requirements.
3. Records of training attendance and test results, if any, shall be recorded.
4. Training in specialized practices or technologies may be provided by a third party as necessary to meet business needs.
5. Specialized training should be offered, when relevant, to users changing roles within the company.

4.3 INFORMATION SECURITY AWARENESS ACTIVITIES

1. The Information Security Program shall prepare a series of awareness notices, each addressing a specific topic within the realm of information security.
2. Topics selected should be easily covered in a relatively brief message or meeting format.
3. Topics should be timely, focused on a specific area applicable to the general user population, and may be selected in response to recent events or popular concerns.
4. Awareness messages should be delivered on an as needed basis.
5. Awareness messages should include an invitation to contact the Information Security Program for help or guidance, and include contact information for the appointed message responder.
6. Other activities should be considered to further reinforce awareness of information security. Some examples:

    1. Lunch discussions of information security topics and events, internal and external
    2. Random inspections of working areas for violations of the clear desk and clear screen requirements, with violators "cited" for infractions
    3. Articles in the employee newsletter to educate on information security topics.

4.4 ANNUAL TRAINING AND REINFORCEMENT OF SECURITY EDUCATION

4.4.1 OVERVIEW

<<Company Name>> has established a formal policy and supporting training regarding information security responsibilities. The training will be evaluated and updated to reflect current security trends on an annual basis for ensuring its adequacy and relevancy regarding the organization's needs and goals. This policy is to be implemented annually and the provisions below set forth the framework for information security responsibilities.

1. The CISO, or a delegate, must conduct mandatory annual security awareness training for all employees and contractors.
2. Security training topics may be based on current events, known or upcoming changes in information security requirements, or reminders of topics covered during the previous year.
3. Course attendance shall be recorded within the user's employment record.
4. Test results, if any, shall also be recorded for each user.

4.4.2 TRAINING TOPICS

The training program will include the following material and relevant topics:

4.4.2.1 POLICY REVIEW

On an annual basis employees and contractors should be re-familiarized with the:

- Acceptable Use Policy
- Code of Ethics
- Code of Conduct
- Communication Policy
- Physical Security Policy
- Change Control Policy;
- Roles and responsibilities of personnel within the organization with respect to the ISMS;
- System access, including provisioning and de-provisioning activities, password complexity rules and requirements, remote access rights, and system administrative rights;
- Network access and monitoring, such as network user, network administrative rights, network monitoring, logging and reporting, anti-virus, patch management network maintenance and the protection of the network (DDoS, worms, malicious code, unknown email and attachments);
- Media backup, transport and logging activities;
- Software licensing issues;

4.4.2.2 SOCIAL ENGINEERING ATTACKS

Workforce members should be familiar and trained on how to recognize and foil social engineering attacks such as:

- phishing / spear-phishing;
- wire fraud;
- invoice fraud;
- pre-texting, and
- tailgating.

4.4.2.3 AUTHENTICATION BEST PRACTICES

Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.

4.4.2.4 DATA HANDLING BEST PRACTICES

Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely. They should also be refamiliarized with Data Classifications, and the Data Retention policy.

4.4.2.5 CAUSES OF UNINTENTIONAL DATA EXPOSURE

Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

4.4.2.6 RECOGNIZING AND REPORTING SECURITY INCIDENTS

Workforce members should be trained so that they are able to recognize a potential security incident and be able to report such an incident in a timely manner.

4.4.2.7 UNDERSTANDING SECURITY UPDATES

The workforce should understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.

4.4.2.8 USE OF INSECURE NETWORKS

Workforce members should be informed about the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.

4.4.3 ANNUAL POLICY REVIEW

Personnel are required to re-review and acknowledge the following policies on an annual basis:

- Code of Ethics
- Code of Conduct
- Acceptable Use
- Communication Policy

Evidence of the review should be recorded for each user.

5 ROLES AND RESPONSIBILITIES

Roles and responsibilities are defined by job title. Job titles incorporate written job descriptions that are versioned and available to employees digitally. Job titles are also used for the purpose of salary benchmarking and access management automation.

Executive management should review job titles and job responsibilities at least annually to ensure that titles and descriptions align with contemporary standards.

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

This work is licensed under a Creative Commons Attribution-NonCommercial-No Derivatives 4.0 International Public License (the link can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode)

To further clarify the Creative Commons license related to the Open-ISM™ content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to Aberrant, Inc., and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the Open-ISM, you may not distribute the modified materials. Users of the Open-ISM framework are also required to refer to (http://www.aberrant.io/open-ism/license) when referring to the Open-ISM to ensure that users are employing the most up-to-date guidance. Commercial use of the Open-ISM is subject to the prior approval of Aberrant, Inc.

APPENDIX A: PERFORMANCE REVIEW TEMPLATE

Copy and fill out the template for employee reviews.

Employee Name		
Date of Hire		
Date of Evaluation		
Date of Previous Evaluation		
Review Grade		
Written Review		