Aberrant Open-ISM™

WORKSTATION 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 PURPOSE

The purpose of this policy is to provide guidance for workstation security for <<Company Name>> workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met. UIT does not deal with personal health information, for the purpose of this document we will use Sensitive Information (SI).

2 SCOPE

This policy applies to all <<Company Name>> employees, contractors, workforce members, vendors and agents with a <<Company Name>>-owned or personal-workstation connected to the <<Company Name>> network.

3 POLICY

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including sensitive information (SI) and that access to sensitive information is restricted to authorized users.

3.1 USE OF WORKSTATIONS

Workforce members using workstations shall consider the class of the information, including sensitive information (SI) that may be accessed and minimize the possibility of unauthorized access.

3.2 PHYSICAL AND TECHNICAL SAFEGUARDS FOR WORKSTATIONS

<<Company Name>> will implement physical and technical safeguards for all workstations that access electronic sensitive information to restrict access to authorized users.

3.2.1 MALWARE PROTECTION

1. Anti-malware software must be deployed on all workstations.
2. Ensure that automatic updates are configured for anti-malware signature.

3.2.2 DOMAIN CONTROLLER

Workstations should be joined to a domain that leverages centralized policies and role-based access control.

3.2.3 IMPLEMENT AND MANAGE A FIREWALL ON END-USER DEVICES

Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

3.2.4 REMOVABLE MEDIA

1. Disable autorun and autoplay auto-execute functionality for removable media.
2. Anti-malware software to automatically scan removable media is required.

3.2.5 ENABLE ANTI-EXPLOITATION FEATURES

Enable anti-exploitation features on workstations and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

3.2.6 HARD DRIVE ENCRYPTION

Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.

3.2.7 LEAST PRIVILEGE

User Access Control should be turned on by default.

3.2.8 REMOVE UNNECESSARY APPLICATIONS AND SERVICES

Uninstall or disable unnecessary services and software, such as an unused file sharing service, web application module, or service function.

3.2.9 OPERATING SYSTEM PATCH MANAGEMENT

Perform operating system updates on workstations through automated patch management on a monthly, or more frequent, basis.

3.2.10 APPLICATION PATCH MANAGEMENT

Perform application updates on workstations through automated patch management on a monthly, or more frequent, basis.

3.2.11 INSTALLED SOFTWARE REVIEW

On a monthly basis an installed software report is generated which lists the software installed on workstations.

- Software installed on workstations is evaluated by InfoSec personnel against the Acceptable Use Policy and a list of software that is approved for installation on <<Company Name>> workstations.
- Software that violates the Acceptable Use Policy or that is unauthorized must be removed prior to the generation of the next installed software review via a change control ticket.

3.3 PORTABLE END USER DEVICES

3.3.1 REMOTE WIPE

Enterprise data should be remotely wiped from enterprise-owned portable end-user devices when a device has been lost or stolen, or when an individual no longer supports the enterprise. Personal mobile devices used for work must have the company's MDM installed as per the Acceptable Use Policy.

3.3.2 SEPARATE ENTERPRISE WORKSPACES ON MOBILE END-USER DEVICES

Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.

4 POLICY COMPLIANCE

4.1 COMPLIANCE MEASUREMENT

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 EXCEPTIONS

Any exception to the policy must be approved by the Infosec team in advance.

4.3 NON-COMPLIANCE

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

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