Aberrant Open-ISM™

# ASSET INVENTORY 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 .... 4
2 Scope .... 4
3 Roles & Responsibilities .... 4
4 Asset Inventories .... 5
4.1 Physical Assets .... 5
4.1.1 Change to the Physical Asset Inventory .... 5
4.1.2 Return of Physical Assets / Equipment .... 5
4.2 Intellectual Property .... 6
4.3 Authentication and Authorization Systems .... 6
4.4 Applications and Software .... 6
4.4.1 White-Listed Software .... 6
4.4.2 Potentially Unwanted Software .... 7
4.4.3 Open Source Modules and Libraries Inventory .... 7
4.4.4 Licensed Software Components .... 7
4.4.5 Software Inventory .... 7
4.4.6 Unauthorized and Unsupported Software or Software Components .... 8
4.5 Open Source Libraries and Modules .... 8
4.6 Scripts .... 9
4.6.1 White-Listed Scripts .... 9
4.6.2 White-Listing Scripts .... 9
5 Unauthorized Assets .... 9
6 Non-compliance .... 9
7 Contact Information .... 10
8 Document RACI .... 10
9 License Information .... 11

# 1 OVERVIEW

<<Company Name>> information security program is an Information Security Management System (ISMS) that is implemented to strategically adopt a risk management approach in selecting security controls to mitigate risks to the company's information assets.

This document defines the overall enterprise approach for developing and maintaining an inventory of information assets within the scope of the ISMS, for the purposes of ensuring the completeness of their selection and adequacy of their inclusion.

# 2 SCOPE

The scope of this policy relates to physical or intellectual property (e.g. software, patents, etc.) that falls within the scope of the ISMS Scope of Registration Statement and meet the following criteria:

- Physical or intellectual property owned or leased by <<Company Name>>.
- Has a measurable cost / value that can be assessed.

# 3 ROLES & RESPONSIBILITIES

- **Asset Inventory Custodian(s)** shall ensure that asset inventory information remains up to date and follows enterprise change management procedures. The Chief Technology Officer (CTO) is responsible for maintaining asset inventories for <<Company Name>>. The CTO is by default the primary Asset Inventory Custodian for the company. The CTO is empowered to delegate asset inventory responsibilities to product owners when appropriate.
- **ISMS Manager** reviews the asset categorization criteria for sufficiency after each risk assessment exercise and shall periodically validate asset inventory sources with the respective custodians.

# 4 ASSET INVENTORIES

At a minimum, the following specifications and guidelines MUST be adhered to when carrying out any activities of the security program. An audit of physical assets, intellectual property, and open source software should be performed at least annually by the CTO or by an employee designated by the CTO.

As a strong guideline, the organization should utilize software inventory tooling whenever possible in-lieu of performing manual discovery of installed software, modules, or libraries.

## 4.1 PHYSICAL ASSETS

### 4.1.1 CHANGE TO THE PHYSICAL ASSET INVENTORY

Additions or changes to the physical asset inventory should be performed via change control. When a physical asset is acquired it should be tagged and assigned a unique ID prior to being put to use. Assets added, modified, or removed from the physical asset inventory should be recorded on a centrally located master inventory. Access to modify the master list should be restricted to Asset Inventory Custodians, or employees delegated by the CTO.

The master inventory list of physical assets should have the following information:

- A unique ID that matches the ID of the tag affixed to the physical item.
- Serial number
- Description
- Location
- Status (Awaiting Assignment, In Use, Lost, Stolen, Destroyed) (required)
- Destruction Document (If applicable)
- Police Report Number (if applicable)
- Owner (required)
- Date of the last modification of the entry (required)
- Identity of employee who last modified the entry (required)

#### 4.1.1.1 USE DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) LOGGING TO UPDATE ASSET INVENTORY

Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise’s asset inventory. Review and use logs to update the enterprise’s asset inventory weekly, or more frequently.

### 4.1.2 RETURN OF PHYSICAL ASSETS / EQUIPMENT

The return of physical assets should be performed via change control. Any change in ownership, or asset status, of a physical assets should be recorded in a centrally located master inventory list. Additionally:

- The asset inventory custodian should follow secure disposal (or reuse) of equipment instructions outlined in the Physical Security Policy when applicable.
- In the event equipment contains electronic data the asset inventory custodian should follow guidance on the destruction of electronic media in the Data Classification and Record Retention Policy.

## 4.2 INTELLECTUAL PROPERTY

Intellectual property applies to domain names, patents, etc. owned by <<Company Name>>. The master inventory list of intellectual property assets should have the following information

- Name / Namespace
- Version (if applicable)
- License (if applicable)
- Description (if applicable)
- Location(s)
- Owner (required)
- Date of the last modification of the entry (required)
- Identity of employee who last modified the entry (required)

## 4.3 AUTHENTICATION AND AUTHORIZATION SYSTEMS

Establish and maintain an inventory of authentication and authorization systems, including those hosted on-site or at a remote service provider.

- The inventory should be updated as new authentication and authorization systems are added.
- The inventory should be reviewed at least annually to ensure that it is accurate.

## 4.4 APPLICATIONS AND SOFTWARE

### 4.4.1 WHITE-LISTED SOFTWARE

Only approved software can be installed on production systems—e.g. workstations and servers. AppLocker is deployed to ensure that software that is not white-listed is prevented from being installed on production systems.

#### 4.4.1.1 WHITE-LISTING SOFTWARE

Employees may request that software, or licensed software components be added to the Software White-List through change control.

1. Software should be evaluated against cross-cutting system requirements, e.g. SLA, response time performance with two standard deviations, load-testing, etc.
2. The software's license should be reviewed by legal and stored in a centralized location.
3. Deprecated software, or legacy versions of contemporary software should be avoided. In the event it is necessary to use legacy or deprecated software the issue should be documented in the company Issue Queue as an operational exception and given a CVSS score.
4. The software should have an entity that actively supports it—and that can be litigated in the event of a breach of contract.
5. When possible software should be acquired from a reputable source such as a software reseller.

The CTO, or a delegated authority, is authorized to approve software requests. Software that has not been approved is considered unauthorized.

#### 4.4.1.2 BLACK-LISTING SOFTWARE

The CISO, or a delegated authority, can black-list software and mandate the removal of software from production systems.

### 4.4.2 POTENTIALLY UNWANTED SOFTWARE

<<Company Name>> uses Microsoft Intune which is configured to prevent PUA from being downloaded via the internet.

### 4.4.3 OPEN SOURCE MODULES AND LIBRARIES INVENTORY

Perform an open source software inventory of modules and libraries on open source software in the development branch. The inventory should include: the name of the library or module, the version, the hash, the license type, and a CVSS risk score. The open source software inventory should be completed on at least a quarterly basis.

### 4.4.4 LICENSED SOFTWARE COMPONENTS

Perform an inventory of licensed software components in the development branch. The inventory should include: the name of the component, the version, the hash, the license, and a CVSS risk score. The licensed software component inventory should be completed on at least a quarterly basis.

### 4.4.5 SOFTWARE INVENTORY

A catalog of installed software is maintained of all licensed software installed on enterprise assets. The software inventory must include the following attributes for each software entry:

- title;
- publisher;
- initial install/use date;
- business purpose for each entry;
- a Boolean that indicates whether or not the software processes or stores confidential data;
- a Uniform Resource Locator (URL);
- version;
- deployment mechanism (optional);
- SHA1 Hash (optional); and,
- decommission date.

The software inventory should reviewed monthly to ensure that only approved software is installed on <<Company Name>> systems and that approved software is actively supported.

### 4.4.6 UNAUTHORIZED AND UNSUPPORTED SOFTWARE OR SOFTWARE COMPONENTS

On a monthly unsupported software that has not been granted an exception, and unauthorized software must be uninstalled and purged from system images.

#### 4.4.6.1 UNSUPPORTED SOFTWARE

Software that is no longer actively supporter should be removed when feasible. If removal of the software is not feasible it should listed as an operational exceptional, a known vulnerability, on the Issue Queue and assigned a date of remediation.

#### 4.4.6.2 UNAUTHORIZED SOFTWARE

Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.

## 4.5 OPEN SOURCE LIBRARIES AND MODULES

An inventory Open Source libraries of technologies utilized by <<Company Name>> should be maintained by the CTO.

- Name / Namespace
- Version
- License (if applicable)
- Description

- Location(s)
- Owner (required)
- Date of the last modification of the entry (required)
- Identity of employee who last modified the entry (required)

### 4.6 SCRIPTS

Its not uncommon for administrators to sometimes use scripts to perform administration tasks. Scripts are not held in source control and fall outside of the scope of an SDLC.

#### 4.6.1 WHITE-LISTED SCRIPTS

Only approved can be executed on production systems—e.g. workstations and servers.

- Enforcement should be maintained through hash rules, or certificate rules.
- Approved scripts should be held in central location.

#### 4.6.2 WHITE-LISTING SCRIPTS

Employees may request that a script be added to the Script White-List through change control.

1. Software should be evaluated to ensure that it's not doing any malevolent.
2. The software should not hardcode any configuration data.

The CTO, or a delegated authority, is authorized to approve script requests. Software that has not been approved is considered unauthorized.

## 5 UNAUTHORIZED ASSETS

Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

## 6 NON-COMPLIANCE

Failure on the part of employees to follow this policy can result in 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.

## 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<br>Other parties affected by the change |

# 9 LICENSE INFORMATION