WILEY

Asset Management Policy

1. Introduction

1.1. Policy Purpose:

The purpose of the Asset Management (AST) policy is to ensure that technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal.

1.2. Policy:

Wiley shall protect its assets and data by implementing and maintaining appropriate IT Asset Management (ITAM) business practices across the enterprise.

1.3. Policy Information:

This policy is supported by the following control objectives, standards, and guidelines.

2. Policy

2.1. Asset Inventories

Wiley is required to maintain an inventory of its technology assets that includes, but is not limited to:

(a) Hardware and software inventories, both:
    1. Internally hosted assets; and
    2. Externally hosted assets.
(b) A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices);
(c) List of company-approved products;
(d) Updating the inventory as necessary; and
(e) Where technically feasible, a list of all personnel with access to assets.

The inventory should be updated as an integral part of component installations, removals, and information system updates. Without an inventory, some system components could be forgotten, and be inadvertently excluded from applicable configuration standards. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

2.2. Assigning Ownership of Assets

Wiley's requirements for property accountability include:

(a) All persons entrusted with Wiley property are responsible for its proper use, care, custody, safekeeping, and disposition. Responsibility for items will be assigned in writing.
(b) Persons will not be assigned to a duty that will prevent them from exercising proper care and custody for the property for which they are responsible.
(c) When a person assumes accountability for property that is remotely located, records must be maintained to show the location of the property and the persons charged with its care and safekeeping.
(d) Wiley property will not be used for any private purpose except as authorized by Wiley management.
(e) No Wiley property will be sold, given as a gift, loaned, exchanged, or otherwise disposed of unless specifically authorized by Wiley management and
(f) Property documents shall identify the manufacturer's make, model, and serial number.

Wiley should employ an automated mechanism to help maintain an up-to-date, complete, accurate, and readily available inventory of system components.

2.3. Secure Disposal or Re-Use of Equipment

Data/process owners and asset custodians are required to sanitize media when it is no longer needed for business or legal reasons. Asset custodians are required to destroy media that cannot be sanitized, as follows:

(a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed; or
    1. Secure storage containers must be used for cardholder data that is waiting to be destroyed.
(b) Render data on electronic media unrecoverable so that data cannot be reconstructed.

Data destruction may be performed in-house, or it may be outsourced to a qualified data destruction vendor. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

2.4. Removal of Assets

Authorization must be obtained prior to relocation or transfer of hardware, software, or data to offsite premises. Assets are prohibited from being removed from Wiley facilities without prior management authorization. Prior to the removal of the information system, the following applicable information must be captured:

(a) Make / model / serial # of the asset.
(b) Owner of the asset
(c) Reason the asset is being removed from the facility.
(d) Company and name of representative removing the asset.
(e) Estimated return date for the asset, if applicable

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

3. Revision History:

Document Properties

Policy	Asset management Policy
Last Review Date	21st June, 2024
Approved by	Robyn Wright – CISO & DPO
Classification	**Public** (Can be externally shared)