Asset Management Policy

Policy Owner: James Pursey

Effective Date: 15th May 2024

Purpose

To identify organizational assets and define appropriate protection responsibilities. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Scope

This policy applies to all Handle Technologies Ltd owned or managed information systems.

Policy

Inventory of Assets

Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be created and maintained.

Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within Handle Technologies Ltd.

Acceptable Use of Assets

Rules for the acceptable use of information, assets, and information processing facilities shall be identified and documented in the *Information Security Policy*.

Loss or Theft of Assets

All Handle Technologies Ltd personnel must immediately report the loss of any information systems, including portable or laptop computers, smartphones, PDAs, authentication tokens (keyfobs, one-time-password generators, or personally owned smartphones or devices with a Handle

Technologies Ltd software authentication token installed) or other devices that can store and process or help grant access to Handle Technologies Ltd data.

Return of Assets

All employees and third-party users of Handle Technologies Ltd equipment shall return all of the organizational assets within their possession upon termination of their employment, contract, or agreement.

Handling of Assets

Employees and users who are issued or handle Handle Technologies Ltd equipment are expected to use reasonable judgment and exercise due care in protecting and maintaining the equipment.

Employees are responsible for ensuring that company equipment is secured and properly attended to whenever it is transported or stored outside of company facilities.

All mobile devices shall be handled in accordance with the Information Security Policy.

Excepting employee-issued devices, no company computer equipment or devices may be moved or taken off-site without appropriate authorization from management.

Asset Disposal & Re-Use

Company devices and media that stored or processed confidential data shall be securely disposed of when no longer needed. Data must be erased prior to disposal or re-use, using an approved technology in order to ensure that data is not recoverable. Or a Certificate of Destruction (COD) must be obtained for devices destroyed by a third-party service.

Please refer to NIST Special Publication 800-88 Revision 1 "Guidelines for Media Sanitization" in order to select which methods are appropriate.

Customer Asset Return

Any physical assets owned by customers shall be promptly returned to the customer following service termination in accordance with the terms of contract or service agreement.

Exceptions

Requests for an exception to this policy must be submitted to the CEO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CEO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	15-May-2024	First Version	James Pursey	James Pursey