Warmbox

Asset Management Policy

Effective Date: 02/01/2025

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 Warmbox 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 Warmbox.

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

Return of Assets

All employees and third-party users of Warmbox 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 Warmbox 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.

Exceptions

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

Violations & Enforcement

Any known violations of this policy should be reported to the IT Manager. 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
1.0	01/02/2025	First Version