Asset Management Policy

Policy Owner: [Job title of policy owner]

Effective Date: [Date you choose, after which there will be consequences for personnel for non-compliance]

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 nexelus.net 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 drawn up and maintained.

Ownership of Assets

Assets maintained in the inventory shall be owned by a specific individual or group within nexelus.net.

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.

Return of Assets

All employees and third-party users of nexelus.net 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 nexelus.net 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.

Exceptions

Requests for an exception to this policy must be submitted to the [approver of requests for an exception to this policy, e.g., IT Manager] for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the [recipient of reports of violations of this policy, e.g., 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	Author	Approved by
[1.0]	[29-Apr-2020]	[First Version]	[OWNER]	[APPROVER]