Asset Management Policy

Nexelus

Purpose

The purpose of this policy is to define requirements for managing and properly tracking assets owned, managed, and under the control of Nexelus through their lifecycle from initial acquisition to final disposal.

Roles and Responsibilities

The following teams have been developed and trained to define, maintain and monitor Asset Management Policy.

- HR & Network Administrator is responsible for all Human Resource and physical inventory is maintained and documented as per policy. The team members also include site leads at each Nexelus work site. The team leader is the Head of HR who reports to the CEO or the partner.
- DevOps is responsible for maintaining asset inventory of all applications, web services, platforms, and their supporting infrastructure in the Cloud. The team leader is the Head of Engineering/Technology.
- Security is responsible for assessing and maintaining cyber security related tools, software, and services. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer/IT Manager.

Policy

Physical and Virtual Asset Standard

Nexelus will ensure the proper management of assets to maximize information security. The following procedures will be enforced as applicable to Nexelus assets to ensure proper maintenance, tracking, monitoring, and handling of assets:

- A detailed asset inventory will be maintained to track and monitor assets.
    - All significant assets will be accounted for on the inventory.
    - Items can be excluded from the inventory if they carry very low purchase/replacement costs (including time and labor needed to install and configure) and pose little or no risk to business operations or compliance status.
- Each significant asset will be associated with an identifier, license, or tag, and proper classification when applicable.

    - Details should include a description of the type of asset, the make/model of the asset, technical specifications, license details, and versions of the software packages or operating systems.
    - Items can be excluded from the inventory if they carry very low purchase/replacement costs (including time and labor needed to install and configure) and pose little or no risk to business operations or compliance status. Assets that contain, store, or handle information, will be classified as per *Data Classification Policy*.
- All copies of media assets will be clearly marked for the attention of the authorized recipient.
    - Temporary or permanent copies of information will be at a level consistent with the protection of the original information.
- Access to each asset will be restricted based on the asset's classification.
- A record of authorized recipients of assets will be established and maintained.
- The disposal/replacement of physical and virtual assets will be tracked, whether it is due to depreciation, expiring leases or agreements, obsolescence/end of support, loss, or other reasons.
- A reporting function will support auditing and monitoring for IT compliance with this standard.

Asset Inventory Standard

An asset inventory process must be in place to support the technological management of critical business processes and to meet legal and regulatory requirements. The inventory process will also support the discovery, management, replacement, and disposal of all assets. It will further facilitate the identification and removal of any illegal or unauthorized software, asset, or processes found in the Nexelus environment. To accomplish these goals, all physical and virtual assets under Nexelus management or control will be listed in an inventory that will include:

- Unique identifier or name of the asset
- Description of the asset
- Purpose of the asset and the role the asset has in supporting critical business processes and in meeting legal or regulatory requirements, if applicable
- Entity responsible for the asset
- Assets that contain sensitive information (e.g., PHI, personal data, etc.) shall be clearly designated as such for the purposes of tracking.
- Classification of the asset, if applicable, as prescribed in the *Data Classification Policy*

Asset Ownership

Nexelus will assign an owner to each asset when the asset is created or transferred to Nexelus. The asset owner can be an individual or an entity with approved management responsibility to control the whole lifecycle of the asset; the asset owner will not necessarily have property rights to the asset.

The asset owner will be responsible for the proper management of the asset over the asset's entire lifecycle, or until a new owner is assigned to the asset. The asset owner will:

- Ensure that assets are inventoried.
- Ensure that assets are appropriately classified and protected.
- Define and periodically review access restrictions and classification to important assets, taking into account applicable access control policies.
- Ensure proper handling when the asset is deleted/destroyed.

Physical Asset Inventory

Nexelus leverages a SaaS-based asset management system, *Drata*, to maintain inventory of all company owned physical computing equipment, including but not limited to:

- Servers
- Workstations
- Laptops
- Printers
- Networking equipment

All company-owned devices are subject to a complete data wipe if deemed necessary, such as in the case of device infection or repurpose. This data wipe will be carried out by the IT manager.

Digital Asset Inventory

Nexelus uses *Drata*'s automated system to query across our cloud-based infrastructure to obtain detailed records of all digital assets, including but not limited to:

- Virtual machines
- Virtual servers
- Virtual repositories
- Security agents
- Source code repositories
- User accounts

Asset Retirement Standard

The information resource owner determines when an asset is no longer needed or is obsolete and can be retired. If the asset to be replaced/retired supports mandatory legal and regulatory requirements of critical business processes, the information resource owner must ensure that any replacement asset can support these processes before the current asset is retired.

Before retiring/replacing any asset that retains data, data retention requirements for all data stored or managed by that asset must be reviewed, and a plan for complying with all applicable data retention requirements must be developed and executed. This is particularly important for assets that manage data subject to legal/regulatory scrutiny. Any data subject to data retention

requirements must be migrated to an appropriate destination and tested for appropriateness, completeness, accessibility and retrievability from the destination before the original data is deleted from the original asset as part of the system retirement process.

System Hardening Standards

Device Best Practices and Hardening Standards

- Manufacturer-provided hardening and best practice guides will be employed to ensure all device installation is properly guarded from vulnerabilities and unauthorized attempts to access the systems.
- Vendor supplied defaults, including usernames, passwords, and any other common settings that may result in unauthorized attempts to access the systems, will be changed in accordance with hardening guides.
- Insecure and unnecessary communication protocols are disabled.
- Local passwords, when required, will be randomly generated and securely stored in the approved password management system.
- Current patches will be installed.
- Malware protection will be implemented.
- Logging will be enabled.
- Two-factor authentication should be used whenever available/supported on the device platform.

Infrastructure Configuration and Maintenance

- Internal Workstation and Server Patching
    - Operating system patches/upgrades are evaluated periodically.
    - Operating system and security patches/upgrades are installed based on their criticality.
    - Operating system patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
- Internal Infrastructure Patching
    - Infrastructure (routers, switches, virtual hosts, etc.) patches/upgrades are evaluated as they come available from vendors.
    - Infrastructure patches/upgrades are installed based on their criticality.
    - Infrastructure patches/upgrades are reviewed and approved via a lab environment when possible/practical.
    - Infrastructure patches/upgrades are installed during off-peak hours to minimize the disruption to business processes.
    - When applicable, redundant systems are patched/upgraded one device at a time to ensure no impact to shared services.
    - Networking hardware/software updates follow the regular change management procedures.
- Infrastructure Support Documentation
    - A network diagram is available to all appropriate service personnel and is kept current.

    - Configuration standards for the setup of all infrastructure devices are in place and are formally documented as necessary.
- Endpoint Security/Threat detection
    - Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).
    - Antivirus and anti-malware tools are configured to automatically receive updates, run scans and alert appropriate personnel of viruses or malware.

Capacity Management

Capacity requirements of systems will be identified in line with the business criticality of a concerned system.

- System tuning and monitoring will be applied to ensure and improve (when needed) the availability and efficiency of systems.
- Detective controls will be put in place to indicate problems as they occur.
- Projections of future capacity requirements will account of new business and system requirements and current and projected trends in the company's information processing capabilities.
- To mitigate bottlenecks and dependence on key personnel presenting a threat to system security or services, managers must monitor the utilization of key system resources, identify trends in usage, and account for any resources that may have a long procurement lead times or high costs.

Providing sufficient capacity will be achieved by increasing capacity or by reducing demand. This includes:

- Deletion of obsolete data (disk space)
- Decommissioning of applications, systems, databases, or environments
- Optimizing batch processes and schedules
- Optimizing application logic or database queries
- Denying or restricting bandwidth for resource-hungry services if these are not business critical (e.g. video streaming)
- Managing capacity demand
- Provisioning new server instances when capacity thresholds are met.

Management of Media

Removable Media

For the proper management of removable media, the following steps will be taken, when applicable:

- Authorization will be required for removing media from Nexelus facilities or assets, when necessary and practical.
    - A record of the removal will be kept for an audit trail.

- Contents of any reusable media being retired, replaced, will be made unrecoverable.
- All media will be stored and secured in accordance with manufacturers' specifications.
- Cryptographic techniques should be used to protect data on removable media to maintain integrity and confidentiality.
- Media degradation will be mitigated by transferring stored data to fresh media before becoming unreadable.
- Coincidental data damage or loss will be mitigated by making multiple copies of valuable data on separate media.
- Removable media drives will only be enabled if there is a business reason for it.
- Transfer of information to removable media will be monitored.

Physical Media Transfer

For the protection of media containing information during transport, the following steps will be taken, when applicable:

- Reliable transport/couriers will be used.
    - Management-approved list of authorized couriers
    - Procedures to verify identification of couriers.
- Packaging of media will be sufficient to protect the contents from any physical damage during transport and in accordance with any manufacturers' specifications.
- Transfers will be logged with information.
    - Information about content of the media
    - Type of protection applied.
    - Time of transfer to transport custodian
    - Time of receipt at destination
- A separate log or a clearly defined section of the overall record shall be designated specifically for media containing ePHI.

Return of Assets Upon Termination

- The termination process includes the return of all previously issued physical and electronic assets owned by or entrusted to Nexelus, as outlined in the *Employment Terms and Conditions*, and *Asset Management Policy*.
- If Nexelus equipment was purchased by an employee or third-party user, or personal equipment was used, all relevant information must be transferred to Nexelus and securely erased from the equipment.
- Unauthorized copying of information by employees and contractors will be monitored and controlled during the termination period.

Disposal of Media

The steps for the secure disposal of media containing confidential information will be proportional to the sensitivity of that information. The following guidelines will be applied accordingly:

- Identification of items that require disposal.
- Use of appropriate third-party collection and disposal services in accordance with the *Vendor Management Policy*.
- Secure disposal by incineration or shredding, or erasure of data for use by another application within the company.
- Risk assessment of damaged media to determine disposal or repair.
- Whole-disk encryption to mitigate risk of disclosure of confidential information, in line with Nexelus *Encryption Policy*.
- Logging each disposal to maintain an audit trail.