Asset Management Policy

SOC 1 Type II Document

esm_logo.jpg

Nexelus USA  
New York, NEW YORK (NY)  
646-558-1950 ext.128

**08/31/2022**

# Document Information

The following table shows the details for document creation, review, approval, and effective date.

| **Category** | **Information** |
| --- | --- |
| Work Product: | Asset Management Policy - SOC 1 Type II Document |
| Product Name: | Nexelus |
| Function Name: | SOC 1 Type II Document |
| Version: | 0.1 |
| Status: | Draft |
| Author(s): | Tauseef Shahzad |
| Reviewer(s): | Asim Jameel |
| Approver(s): | Imran Rahman |
| Control Status: | CONTROLLED, PROTECTED |
| Disclaimer: | This document contains confidential information. Do not distribute this document without prior approval from Nexelus. |

# Revision History

The following table is used for revision details of this document.

| **Author(s)** | **Date** | **Version** | **Description of Change** |
| --- | --- | --- | --- |
| Tauseef Shahzad | August 31, 2022 | 0.1 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc112857462)

[Revision History iii](#_Toc112857463)

[Table of Contents i](#_Toc112857464)

[Scope 1](#_Toc112857465)

[Terms and Definitions 2](#_Toc112857466)

[IT Assets 2](#_Toc112857467)

[IT Assets Register 2](#_Toc112857468)

[Deployable Technology List (DTL) 2](#_Toc112857469)

[Nexelus Security System (NSS) 2](#_Toc112857470)

[Security Domains 2](#_Toc112857471)

[Nexelus Staff 3](#_Toc112857472)

[Asset Management 4](#_Toc112857473)

[Policy 5](#_Toc112857474)

[IT Asset Acquisition 5](#_Toc112857475)

[IT Asset Registration 5](#_Toc112857476)

[IT Asset Identification 5](#_Toc112857477)

[IT Asset Documentation 5](#_Toc112857478)

[IT Asset Governance 6](#_Toc112857479)

[IT Asset Disposal 6](#_Toc112857480)

# Scope

The scope of this document is to define the actions to be taken to protect and preserve technology assets - from physical locks on equipment to inventory tags. In conjunction, policy provides the "asset management mindset". This mindset acknowledges that "technology assets are important to us, and we take them seriously enough to put up with protective controls". To realize all intended benefits, this mindset must be integrated into daily operations and the corporate culture -- and this is achieved through adopted policy.

This policy applies to all employees and non-employees who are owners, custodians or users of Nexelus Assets, or those entities who manage, deploy, or support Nexelus Assets either internally or externally on Microsoft and AWS Cloud Services..

**Reference**

* SSAE-18 SOC 1 Type II – Requirements.pdf
* NIST CF - ID.AM-1,2,3
* ISO 38500 - 5.3, 5.4, 5.5
* ISO 27002-2013 - 8.1, 8.2.3, 11.2.7

# Terms and Definitions

Other than terms and definitions given in SSAE 18 – SOC 1 Type II, following terms and definitions are use in Nexelus Security System (NSS) implementation:

### IT Assets

Any information or operations system, tool, database, application, repository, technical services, hardware and/or device that is used while providing or meeting P&G business activities or business needs, or any technical tool (devices, hardware, etc.) that connects to the P&G internal network directly. For the sake of clarity, these include both Company owned systems, tools, applications, databases, devices, repositories, technical services , (collectively, the “Tools”) and any such Tools procured from third parties. Specific examples of IT Assets include, but are not limited to:

* + Desktop workstations, laptop and mobile computers
  + VOIP & Mobile Phones, network cameras, tablets & handheld devices
  + Printers, copiers, fax machines, scanners, multifunction machine
  + Servers including Virtual Servers, databases including cloud-based resources
  + Application and Middleware Platforms
  + Firewalls, routers, switches
  + Network attached Storage devices and cloud storage
  + Business Applications (including cloud platforms and subscriptions sourced/created internally and/or provisioned by our vendors
  + including layered applications which may include multiple vendors/tools necessary to meet the business need).
  + Software Licenses including entitlements

.

### IT Assets Register

A database which stores assets unique identifiers and asset attributes

### Deployable Technology List (DTL)

Deployable technology (hardware, software) means that it is approved for use in Nexelus and by Nexelus employees, all deployable technology is documented in the DTL

### Nexelus Security System (NSS)

All security procedures and policies as defined in this document, and/or other security procedures and policies as defined and implemented at Nexelus.

### Security Domains

The security domain is a discrete logical and / or physical area that is subject to security controls to protect it from all entities outside the domain. For the SOC 1 Type II System the security domain is limited to Nexelus premises.

The location is defined as follows:

* The space within the physical structure bound by, and including, walls, ceiling, floor, doors, and windows.
* All equipment within the physical domain detail mentioned in Asset Identification and Classification Document.

Reference(s):

* Network Security and Access Control Procedure
* Capacity and change Management Procedure

### Nexelus Staff

All personnel employed / contractual engaged by Nexelus are required to follow the policies and procedures as defined in Nexelus Security Manual by management in line with strategic security needs.

# Asset Management

The purpose of the IT Asset Management Policy (the “Policy”) is to protect the company against loss and prevent security incidents, to reduce the company’s risk profile to external and internal pressures, and to minimize security threats, to state commitment to legal compliance and to lower cost and improve productivity through more efficient and effective IT Asset Management. IT Asset Management is a foundational policy which helps support other IT Operations and Information Security policies.

## Policy

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up-to-date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aids in recovery, replacement, anti-criminal, and insurance activities.

Nexelus requires that all IT Assets must be documented and tracked from the day they enter our network or office environment, until after they have been decommissioned.

### IT Asset Acquisition

Hardware and software must be acquired through approved corporate acquisition methods and from approved software distribution channels, adhering to the Vendor Management Policy, and established procurement process by Nexelus Management. Hardware, and software that is acquired must be on the corporate approved IT Asset Register or have an approved exception granted. The IT Asset Register is managed by the Network Security System (NSS) Lead.

### IT Asset Registration

An IT Asset Register is setup, managed, and controlled for an established scope of IT Assets.All IT Assets must be registered within the corporate IT Asset Register.It must beprotected against data loss and alteration by unauthorized persons.

Assets which cost less than ($100/-) shall not be tracked, including computer components such as smaller peripheral devices, video cards, keyboards, or mice. However, assets which store data, regardless of cost, shall be tracked either as part of a computing device or as a part of network attached storage.

### IT Asset Identification

All IT Assets must have a unique assigned ID number from a centrally managed pool or standard. The unique assigned ID number must be maintained throughout the lifecycle of the IT Asset. Violating this Policy may result in disciplinary action, consistent with local laws, up to and including termination. Employees affected by this Policy are expected to read and follow it, directing any questions to NSS Lead and senior management.

### IT Asset Documentation

IT Asset Register must provide capability to track IT Assets based on their ID. The Register must contain all information on IT Asset ownership, purpose, classification, version, location/ portability, details of compliance requirements, licensing details, lifecycle status.

Changes to the IT Asset (transfer, usage, lifecycle, and disposal) with dates must be tracked in the IT Asset Database. Asset ownership information must be maintained to enable governance, escalation, and budget allocation/ reconciliation purposes and in accordance with Records Retention requirements. The NSS Lead is responsible in keeping the IT Asset Register up to date at all times.

### IT Asset Governance

NSS Team ensures that the IT Asset Register is checked regularly (independently, using discovery/ mapping tools) to identify any discrepancy, and is signed off by a senior business leader. IT Assets must enable compliance/ legislation, security, financial and operational efficiency. Formal responsibilities and procedures must be in place to ensure IT Asset data is kept up-to-date and accurate, with satisfactory control of all changes.

### IT Asset Disposal

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus. When disposing of any asset, sensitive data must be removed prior to disposal. NSS Lead shall determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using low level formatting and degaussing techniques. For media storing confidential or student personally identifiable information (PII) that is not being repurposed, disks shall be physically destroyed prior to disposal. IT Assets with residual value to the company must be evaluated for reclamation and re-deployment within the company. Software License IT Assets that are no longer being used must be marked as no longer being leveraged and made available for redeployment. Software Licenses cannot be transferred or provided to external entities without expressed permission granted under the license agreement and the NSS Lead.