Clean Desk Policy

SOC 1 Type II Document

esm_logo.jpg

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

**10/10/2022**

# Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Clean Desk Policy - SOC 1 Type II Document |
| Project Name: | Security Manual |
| 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 | October 10, 2022 | 0.1 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc116983449)

[Revision History iii](#_Toc116983450)

[Table of Contents i](#_Toc116983451)

[Scope 1](#_Toc116983452)

[Terms and Definitions 2](#_Toc116983453)

[Nexelus Security System (NSS) 2](#_Toc116983454)

[Security Domains 2](#_Toc116983455)

[Nexelus Staff 2](#_Toc116983456)

[Network Services 2](#_Toc116983457)

[Clean Desk Policy 4](#_Toc116983458)

# Scope

Clean desk policy is placed to secure the physical security at Nexelus. The policy ensures the confidential information and sensitive materials are stored away and out of sight when custodian of the material is not in the premises/workplace.

The policy is set in place to keep the clean workspace, where confidential and sensitive material about company, clients, vendors, employees, and intellectual property is safe and secured.

The policy applies to employees, contractors, part time employees or any other individual engaged to perform any task for the company.

**Reference**

SSAE-18 SOC 1 Type II – Requirements

# 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:

### 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 and HiQuSystems 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.

### Network Services

Network services required by our network infrastructure are as follow:

* Internet Connectivity from ISP.
* Host based Protection against malware and Virus.
* Web filtering.
* Switches
* Host based Application Control.
* Active Directory
* E-mail Scanning Services.
* Patch management service to update all servers/workstations.
* Application and Database servers.
* Log Management.
* Biometric Access Control
* Office 365

# Clean Desk Policy

1. Employees are required to secure all sensitive/classified information in their workspace at the completion of the workday and when they are expected to be away from their workspace for an extended or short period of time. This includes both electronic and physical hardcopy information.
2. The Windows lock shall be password protected for reactivation
3. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.
4. Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.
5. Printed materials must be immediately removed from printers. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.
6. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction or placed in the locked confidential disposal bins.
7. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
8. Passwords must not be written down or stored anywhere in the office.
9. Keys and physical access cards must not be left unattended anywhere in the office.
10. The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.
11. Individual Personal belongings like bags, books, edibles, etc. shall be kept in drawers.
12. Company provided laptop/tablets/mobile phone should strictly be used for company purpose when working from home. The devices must not be shared with anyone not related to Nexelus directly or indirectly.
13. When working from home, the same rules apply to the sensitive and confidential information as of working in office.
14. Server rooms and office areas shall remain locked when they are not in use
15. File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.
16. Keys used to access Confidential or Internal Use information must not be left in an unattended work area.
17. Passwords must not be posted on or under a computer or in any other accessible location.

It is the responsibility of each manager, supervisor or lead to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance