Nexelus Security Manual

SOC 1 Type II Document

esm_logo.jpg

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

**10/08/2021**

# Document Details

## Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Nexelus Security Manual - 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, 2021 | 0.1 | Initial Draft |
|  |  |  |  |

# Table of Contents

Contents

[Document Details ii](#_Toc84949204)

[Document Information ii](#_Toc84949205)

[Revision History ii](#_Toc84949206)

[Table of Contents i](#_Toc84949207)

[Scope 1](#_Toc84949208)

[Scope 1](#_Toc84949209)

[Reference 1](#_Toc84949210)

[Terms and Definitions 2](#_Toc84949211)

[Security Domains 2](#_Toc84949212)

[Nexelus Staff 2](#_Toc84949213)

[Network Services 2](#_Toc84949214)

[Legal Framework for Security Policy 4](#_Toc84949215)

[Data and Information Sensitivity Policy 5](#_Toc84949216)

[Information Security 6](#_Toc84949217)

[Data Center Security 6](#_Toc84949218)

[Network Security 6](#_Toc84949219)

[Encrypted Data In Transit 6](#_Toc84949220)

[Endpoint Security 6](#_Toc84949221)

[Vulnerability Management 6](#_Toc84949222)

[Sensitive Data and Information Handling 8](#_Toc84949223)

[Marking/Classification of Sensitive Information 8](#_Toc84949224)

[Information Media 8](#_Toc84949225)

[Information Access Policy 8](#_Toc84949226)

[Data Handling Policy 9](#_Toc84949227)

[Data Ownership 9](#_Toc84949228)

[Categories 9](#_Toc84949229)

[Owner Responsibilities 9](#_Toc84949230)

[Custodian Responsibilities 9](#_Toc84949231)

[User Responsibilities 10](#_Toc84949232)

[Clean Desk Policy 10](#_Toc84949233)

[Disposal/Destruction Policy 10](#_Toc84949234)

[Data Access Policy 10](#_Toc84949235)

[Data Backup Policy 11](#_Toc84949236)

[Backup Procedure 11](#_Toc84949237)

[Data Backup & Recovery Procedure 11](#_Toc84949238)

[Project Content Backup 11](#_Toc84949239)

[E-Mail Backup of Leaving Employee 12](#_Toc84949240)

[Project Content Restore 12](#_Toc84949241)

[How to Restore Outlook Emails 12](#_Toc84949242)

[Data Retention Policies 13](#_Toc84949243)

[E-mail Data Retention Policy 13](#_Toc84949244)

[Financial and HR Data Retention Policy 13](#_Toc84949245)

[General Data Retention Policy 13](#_Toc84949246)

[TFS Data Retention Policy 14](#_Toc84949247)

[Source Code Retention Policy 14](#_Toc84949248)

[Security and Awareness Training Policy 15](#_Toc84949249)

# Scope

At Nexelus, security and privacy of your data is one of our key focus points. Data protection is a foundational building block in gaining and maintaining your trust.

Nexelus implement a robust security program spanning from secure system architecture through training and teaching employee’s security and privacy best practices. We believe in creating a culture of security awareness and understanding that security doesn’t have to be difficult.

## Scope

This manual is applicable to all the activities of SSAE 18 (SOC 1 Type 1) at Nexelus as mentioned in this manual.

## 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 ISMS implementation:

### 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 laid by management in line with strategic security needs.

* Network services required by the defined network infrastructure.
* Data Access and Retention Policy
* Acceptable Use Policy
* Clean Desk Policy
* Code of Conduct Policy
* Personnel Security Policy
* User identification, Authentication and Authorization Policy
* Training and Onboarding Policy

### 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

# Legal Framework for Security Policy

Nexelus acknowledges the complexity of legal requirements found in the global networking environment created by the Internet. NEXELUS Security System was drafted to meet, and in some instances exceed the protections found in existing laws and regulations. If any Nexelus Security System component conflicts with existing laws or regulations, this observation must be promptly reported to the management for taking corrective actions.

##### Reference(s):

* Procedure for Compliances and SLA Review

# Data and Information Sensitivity Policy

The Information Security Management System exists for various levels of classification. All documentation will be clearly marked for appropriate access control as defined by its classification and handled in accordance with Nexelus Data Classification and Labeling Sheet.

##### Reference(s):

* Data Handling Policy
* Data Backup Policy
* Data Retention Policy
* Acceptable Encryption and Key Management Policy
* Remote Access Policy
* End User Encryption and Key Management Policy

# Information Security

## Data Center Security

Nexelus cloud-based services and platforms are hosted on Microsoft Azure. Azure datacenters meet security regulations and standards with industry-leading physical and environmental controls. Nexelus solutions benefit from a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations. Azure is compliant with a wide range of standards, laws and regulations including CIS, CSA, various ISO standards, WCAG, SOC 1, SOC 2 and SOC 3.

References:

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-1>

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2>

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-3>

## Network Security

Nexelus Management is committed to maintaining and improving the security of its environments. Maintaining secure network environments requires continuous attention. We regularly review the services and information accessible on our servers and their security requirements.

Security controls are implemented within networks using a strict access control policy. Access points into the network are blocked apart from those deemed essential or business critical.

## Encrypted Data In Transit

All transmission of data over the internet is communicated via HTTPS. Our services support Transport Layer Security 1.3 encryption, providing the necessary levels of confidentiality, integrity and non-repudiation.

## Endpoint Security

Malware protection suites are installed and managed from a centralized location including monitoring and logging of events.

## Vulnerability Management

Nexelus performs various security tests and audits for the infrastructure and application. Tests include amongst others:

* Static code analysis
* Dynamic code analysis
* Network vulnerability assessment
* Network penetration testing
* Application vulnerability assessment
* Penetration testing of multiple environments and solutions

# Sensitive Data and Information Handling

Data and Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the company without proper authorization. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Nexelus confidential information, this policy also set forth the standards for data labeling.

## Marking/Classification of Sensitive Information

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Confidential" may be written or designated in a conspicuous place on or in the information in question. Even if no marking is present, Nexelus information is presumed to be "Confidential" unless expressly determined to be Nexelus Public information by an Nexelus employee with authority to do so.

### Information Media

#### Hard Copies

1. Hard copies should be marked to identify the data classification.
2. The Document Control Section of documents contains the Classification information, which can have any of the Classification categories.
3. Any document left unmarked, will be considered as NON-SENSITIVE.

#### Documents Of External Origin

Documents of External Origin / Customer Property are not marked physically but have been accounted for in the Data Classification sheet.

#### Soft Copies of Data, Software, and/or Other Information Systems

Soft copies of client requirements, project documentation, Application Code, Database Schema are not marked physically but have been accounted for in the Data Classification sheet.

## Information Access Policy

#### Access

Nexelus employees, contractors, people with a business need to know.

#### Distribution within Nexelus

Standard interoffice mail approved electronic mail and electronic file transmission methods.

#### Distribution outside of Nexelus internal mail

This kind of outbound information will only be sent through Nexelus mail server only. If the data is large, then we will use approved electronic file transmission methods [VPN, sftp, more].

#### Electronic distribution

No restrictions except that it be sent to only approved recipients.

## Data Handling Policy

Data is one of the potentially most valuable and most damage prone assets owned by Nexelus. It is also one of the most intangible assets of ours. Protection of the Confidentiality, Integrity, and Availability of data in all forms and through all life cycles is a cornerstone to a successful Information Security process.

### Data Ownership

Customer Data, and information which has been entrusted to Nexelus, must be protected in a manner commensurate with its data classification label. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems that process it (personal computers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Information must also be consistently protected no matter what its stage in the life cycle from origination to destruction.

### Categories

Nexelus has established three categories, at least one of which applies to each worker. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to data security.

### Owner Responsibilities

Information Owners are the Department Managers, Top Management, or their delegates within Nexelus who bear responsibility for the acquisition, development, and maintenance of production applications which both process customer information and defining the Nexelus infrastructure. All production application system information have a designated Owner. For each type of information, Owners designate the relevant classification level, define which users will be granted access, as well as approve requests for various ways in which the information will be utilized.

### Custodian Responsibilities

Custodians are in physical or logical possession of either Nexelus information or information that has been entrusted to Nexelus. While Support department and Information Technology Department staff members clearly are custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the user is necessarily present along with the custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information owners.

### User Responsibilities

Users are responsible for familiarizing themselves with and complying with all Nexelus policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information. Users are increasingly placed in a position where they must handle information security matters that they did not handle in days gone past. The new security concerned environment forces users to play security roles that they had not previous had to play.

## Clean Desk Policy

A clean desk policy is part of an overall company security strategy. It is, as it states, about keeping your work desk clean. In general, a clean desk policy will mandate that at the end of each working day, that employees clear their desk. This means, for example, securely disposing of Post It notes, keeping written notes in a safe place, and ensuring that any removable media isn’t just lying around. Keep sensitive information from view of unauthorized people;

* Erase whiteboards,
* Do not leave any client data printouts in view on tabletop. It should be kept in drawer while not in use.
* Password protected screen saver must be applied on all desktops with 10 minutes timeout
* No document or its link should be placed on computer Desktop
* Add more clauses..

Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

## Disposal/Destruction Policy

Deposit outdated paper information to Admin manager who will properly destroy it with paper shredder; electronic data should be expunged/ cleared. Reliably erase or physically destroy media.

## Data Access Policy

Access to data is controlled and provided to teams and members with specific business needs. Regular permission review is performed to prevent permission overlap, permission creep or conflict of interests. All data access breaches and loopholes discovered during normal operations, monitoring controls, internal and external audits are escalated and resolved through incident reporting, escalation, and resolution procedure.

# Data Backup Policy

Nexelus keeps backup of all the electronic data which will be ready to use in case of any disaster or at time of need. Electronic data includes software & application source code and employee emails.

## Backup Procedure

All Nexelus production, test, and release servers are maintained on Microsoft Azure. Backup for servers is maintained on Microsoft Azure Cloud for last 15 days. This backup is taken automatically by Azure on daily basis and maintained on cloud. The servers can be reconstructed on-the-fly from these backups.

Local Development server backups are maintained on external hard drives by Network Administrator. Data backup log sheet will be updated after each back up by the Senior Network Engineer and verified by the General Manager.

There is one set of our backup media (i.e. hard disk) which is then transferred safely at our offsite data backup location. This data backup site is at sufficient distance away to escape any damage due to any disaster at our main site.

DR Recovery Site Requirements will be asked in case of data backup

## Data Backup & Recovery Procedure

All electronic backups must conform to the following procedures:

* All data, source code files must be adequately and systematically backed up as per our policy.
* One set of backups is made.
* The backup is precisely labeled (folder); we use the date label on which the backup is taken (e.g., [Label]- yyyymmdd).
* The data(s) are kept in order depending on the date of backup taken.
* This will be stored safely at the backup site.
* With every backup taken, Senior Network Engineer updates the backup log.

Reference(s)

* Backup Log

*Log sheet is signed by issuance and receiving authorities.*

## Project Content Backup

It is the responsibility of the Senior Network Engineer to ensure that they have suitable backups of all the projects. The following should be backed up:

* All projects’ data on TFS
* All SOC related data on TFS

## E-Mail Backup of Leaving Employee

Senior Network Engineer is responsible to take immediate backup of e-mails of employee leaving the organization. He will keep that backup/ archive data with other records and maintain ex-employee data on network storage. The information of ex-employee is not available to all employees working in the organization. It can be used with prior permission of General Manager by others in terms of requirements and then Senior Network Engineer will provide this data to them.

## Project Content Restore

In cases where a non-catastrophic issue requires a data restore, the Senior Network Engineer is responsible for performing the restore using backups. Senior Network Engineer will manually restore repository to a prior state if provided a viable backup of project repository.

## How to Restore Outlook Emails

Restoration of email accounts requires a .PST file to be backed up, to restore emails, contacts, and other data from a backup copy of an Outlook PST file:

1. Select File, then Import and Export from the menu in Outlook.
2. Select Import from another program or file.
3. Click Next.
4. Highlight Personal Folder File (PST).
5. Click next again.
6. Now use the Browse button to select the backup copy of the PST file you want to recover from your backup location.
7. Make sure Replace duplicates with items imported is selected.
8. Click Next.
9. Finish the import process with Finish.

# Data Retention Policies

Nexelus Data Retention Policy is intended to define what data should be retained and for how long. The data covered in these guidelines includes, but is not limited to, Administrative, Fiscal, E-mail, General, Temporary, Database Backups, TFS, Source Code, Test Data, Log Files etc.

All employees should familiarize themselves with the data retention policy relevant to them.

There are two broader categories of data (Paper Data and Electronic Data). All paper data will be retained by Admin Office & SOC Team with the approval of General Manager. Network Administrator will ensure all electronic data backup according to data retention policy and hand over the archives to Admin Office & SOC Team for retention on site and off site.

## E-mail Data Retention Policy

Nexelus emails data of all ex-employees are backed up in DVDs and these are kept in storeroom for a period of three years. Current employees’ data email data is resided in Microsoft Office 365 Server.

## Financial and HR Data Retention Policy

Nexelus Financial and HR Record is all information related to revenue and expense for the company. All paper record will have retained by Admin Office for the period of three years. To ensure Financial data secrecy, it is retained by General Manager. A table below explains that which type of data needs to be retained.

|  |  |  |
| --- | --- | --- |
| Item. | Record Types | Retention Period |
| 1 | Financial Data | ? |
| 2 | HR Data | ? |
| 8 | Inventory Records | ? |
| 9 | Invoices to customers | ? |
| 11 | Purchase Records | ? |
| 12 | Employee Personal Files | ? |
| 13 | Manuals, User Guides | ? |

## General Data Retention Policy

Nexelus general record/correspondence covers information that relates to customer interaction and the operational decisions of the business. Admin officer will retain paper data of this category. The individual employee is responsible for electronic data retention of General Correspondence.

## TFS Data Retention Policy

All Data on TFS will be retained from the day it is started.

## Source Code Retention Policy

Source Code data will never be deleted.

# Security and Awareness Training Policy

Nexelus perform various activities to improve the awareness around security and privacy. Some of these include annual awareness training sessions for both security and privacy.