Security and Control Environment

SOC 1 Type II Document

esm_logo.jpg

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

**01/15/2022**

# Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Security and Control Environment - 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 |
| Tauseef Shahzad | October 17, 2021 | 1.0 | Added Data Handling Policy |
| Tauseef Shahzad | January 15, 2022 | 1.1 | Added Data Retention |
| Imran Rahman | August 30, 2022 | 1.2 | Review and few minor edits |

# Table of Contents

Contents

[Document Information ii](#_Toc112769892)

[Revision History iii](#_Toc112769893)

[Table of Contents i](#_Toc112769894)

[Scope 1](#_Toc112769895)

[Terms and Definitions 2](#_Toc112769896)

[Nexelus Security System (NSS) 2](#_Toc112769897)

[Security Domains 2](#_Toc112769898)

[Nexelus Staff 2](#_Toc112769899)

[Network Services 2](#_Toc112769900)

[Control Environment 3](#_Toc112769901)

[Management Commitment to SOC 1 4](#_Toc112769902)

[WHAT’S THE PRIMARY PURPOSE OF THIS INITIATIVE? 4](#_Toc112769903)

[Information Security Policy 5](#_Toc112769904)

[Physical Environment Control 6](#_Toc112769905)

[Data Center Security 6](#_Toc112769906)

[Network Security 7](#_Toc112769907)

[Encrypted Data In Transit 7](#_Toc112769908)

[Endpoint Security 7](#_Toc112769909)

[Vulnerability Management 7](#_Toc112769910)

[Third Party Adons and Connectors 7](#_Toc112769911)

[Data Location and Redundancy 7](#_Toc112769912)

[Remote Access Policy 8](#_Toc112769913)

[Remote Server Access 8](#_Toc112769914)

[Remote Database Servers 8](#_Toc112769915)

[Office 365 Accounts 8](#_Toc112769916)

[Data Storage and Isolation 8](#_Toc112769917)

[Access Management 8](#_Toc112769918)

[Legal Framework for Security Policy 9](#_Toc112769919)

[Information Access Policy 10](#_Toc112769920)

[Marking/Classification of Sensitive Information 11](#_Toc112769921)

[Information Media 11](#_Toc112769922)

[Data Handling Policy 12](#_Toc112769923)

[Data Ownership 12](#_Toc112769924)

[Categories 12](#_Toc112769925)

[Owner Responsibilities 12](#_Toc112769926)

[Custodian Responsibilities 12](#_Toc112769927)

[User Responsibilities 13](#_Toc112769928)

[Data Disposal/Destruction 13](#_Toc112769929)

[Data Access Policy 14](#_Toc112769930)

[Data Backup Policy 15](#_Toc112769931)

[Backup Procedure 15](#_Toc112769932)

[Data Backup & Recovery Procedure 15](#_Toc112769933)

[Project Content Backup 15](#_Toc112769934)

[E-Mail Backup of Leaving Employee 15](#_Toc112769935)

[Data Retention Policy 17](#_Toc112769936)

[E-mail Data Retention 17](#_Toc112769937)

[Financial and HR Data Retention 17](#_Toc112769938)

[General Data Retention 17](#_Toc112769939)

[TFS Data Retention 17](#_Toc112769940)

[Source Code Retention 17](#_Toc112769941)

[Procedure for Communication 18](#_Toc112769942)

[Communication Channels 18](#_Toc112769943)

[Internal Communication 18](#_Toc112769944)

[External Communication 19](#_Toc112769945)

# 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.

**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 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.
* 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

# Control Environment

A control environment is made up of a compilation of an entity’s organizational structure, processes, policies, and standards that are utilized to maintain control across the organization. The board of directors and executive management of a business establish the company culture and attitude regarding the importance of maintaining controls and set the expectations of standards of conduct within the organization.

## Management Commitment to SOC 1

A SOC 1 Type 2 report is an internal control report specifically intended to meet the needs of the Nexelus customers’ management and their auditors, as they evaluate the effect of the Nexelus controls on their own internal controls for financial reporting. The Nexelus SOC 1 report examination will be performed in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 and SSAE-18, therefore it can be used by our customers and their auditors both the US and abroad. These reports will be issued by independent third-party auditors periodically.

### WHAT’S THE PRIMARY PURPOSE OF THIS INITIATIVE?

Provide an independent assessment of Nexelus internal controls that are relevant to customers’ internal controls over financial reporting. The assessment includes a description of the controls, the tests performed to assess them, the results of these tests, and an overall opinion on the design and operational effectiveness of the same. Key points of management commitments are:

1. Top management of Nexelus provides evidence of its commitment to planning, establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the Nexelus Security System along with its services by:
2. Establishing and communicating the scope, policy and objectives for security, development and standard compliance
3. Ensuring that the SOC 1 compliant Security and Change management Process is established, implemented, and maintained in order to adhere to the policy, achieve the objectives for SOC 1 requirements.
4. Communicating the importance of fulfilling SOC 1 requirements.
5. Communicating the importance of fulfilling statutory and regulatory requirements and contractual obligations.
6. Ensuring the provision of resources.
7. Conducting management reviews at planned intervals.
8. Ensuring that risks to services are assessed and managed.

## Information Security Policy

Information Security and adherence to security practices in compliance with industry standards adopted by software development industry and information security needs of customers within the framework of Local and Federal Government is one of the top priorities of Nexelus. This is to ensure the protection of its intellectual property from all threats - internal or external, intentional, or accidental and natural disasters. In addition, achieving this goal Nexelus will ensure the following:

* Confidentiality of information assets is ensured, but not limited to third parties, Company Operational, personal, and electronic or electronic communications.
* A Business Continuity Management Framework will be made available and Business continuity plans will be developed to prevent disruption of business operations and to protect critical business processes from the consequences of major failures or disasters. Business continuity plans are maintained and evaluated.
* All information security breaches, real or suspected, will be reported, and investigated by the appropriate authorities.
* Appropriate access controls will be maintained, and data will be protected from unauthorized access. As such but not limited to:
  + Confidentiality, integrity, and availability to information are maintained throughout the process.
  + Access to information and information systems will be met as required by context and supporting business activities.
  + All managers are directly responsible for implementing the Security Policy within their respective departments.
  + Data security is managed through the Nexelus Risk Management framework.
  + It is the responsibility of all staff to adhere to the Security Policy.
* A risk management framework will define risk and its management of all company assets (tangible / intangible and human). Individual risks are assessed and targeted at all risks, using appropriate risk mitigation controls and emergency plans are defined with unacceptable residual risk levels.
* All business assets (tangible / intangible with people) have a safe and secure environment.
* Employees are provided conducive work environment, free from accidental and occupational hazards.
* All employees are trained in information security functions, roles, and responsibilities.
* Physical, sensible, and remote access to all business assets (tangible / intangible), details and tangible locations are monitored and controlled.

## Physical Environment Control

### 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 1.2 an 1.3 encryption, providing the necessary levels of confidentiality, integrity and non-repudiation.

### Endpoint Security

Firewall and 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

### Third Party Adons and Connectors

Nexelus has a vast partner network, including Ad Serving Services such as Google Ads and Microsoft Bing, eSignature integration such as Adobe Sign, as well as integration with third party financial systems. Safeguards for the tools built and implemented by Nexelus partners are established and maintained by the partner. Nexelus does not include these plug-ins and connectors during control performance or application penetration testing and encourages organizations to perform their due diligence on these integrations prior to their use. Any additional information related to the security of these partner plug-ins and connectors should be addressed with the Nexelus partner.

### Data Location and Redundancy

Nexelus applications are hosted both on Microsoft Azure and Amazon Web Services (AWS). These organizations have robust security and privacy programs, and have commitments to encryption, data security, confidentiality and availability that are maintained at standards that meet those established with Nexelus.

Azure and AWS environments are built with resiliency and scale in mind, with the ability to distribute documents and servers between various physical locations within an Azure or AWS region.

### Remote Access Policy

The purpose of this policy is to define the activities associated with the provision of access security for employees and authorized nonemployees working remotely to protect Nexelus Information System, information systems, networks, data, databases, and other information assets from cybersecurity events that may occur while in use by remote workers. Additional policies governing data protection activities will be addressed separately.

The scope of this remote access security policy is all IT systems, software, databases, applications, and network resources needed by the Company to conduct its business, and the access security controls needed to protect those assets when being accessed remotely. The policy is applicable to all Company employees, contractors, and other authorized third-party organizations.

### Remote Server Access

Authorized users access remote servers by their individual accounts for logging and tracking purpose. Minimum Access policy is applied, and authorized users are provided with RDC access to relevant servers only. All remote server access will be performed using official desktop and laptops only. The communication is secured using VPN. The VPN only be installed and configured on company owned laptops and desktops. If employees want to use personal devices with VPN access, then General Manager needs to provide a written approval. Two-factor access is applied on remote desktop access.

No shared passwords is used to access remote servers.

### Remote Database Servers

Authorized employees have limited Database access through their individual database user login credentials. Remote Desktop access is provided to Database Manager and general Manager only. Remote Desktop and Database access is available through VPN. Two-factor access is applied on remote desktop access.

### Office 365 Accounts

All office 365 accounts are secured using strong password and two-factor authentication using SMS or Microsoft authenticator as secondary authentication method.

### Data Storage and Isolation

Nexelus does not store customer data on unencrypted portable media like laptop computers, external hard drives, USB drives, or other portable devices. Customer data is always stored properly -- encrypted at rest in our backend databases or object stores in Microsoft Azure cloud service provider. Data from one customer cannot be accessed by another customer.

### Access Management

Access to production systems and data is restricted to vetted, authorized personnel. Personnel access is established based on roles, using the principle of least privilege and requires multiple factors to authenticate. Access to data is logged and monitored.

## 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.

## Information Access Policy

Information and Asset Access Controls and Policies 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

#### 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.

## 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 Classification Sheet 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.

## 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 are 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 is also 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:

1. Owner
2. Custodian
3. 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 has 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.

### Data Disposal/Destruction

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 Access Register is maintained for data access classification and assignment to resources.

## 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 30 days. This backup is taken automatically by Azure services 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 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 are 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 is 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/she keeps 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.

## Data Retention Policy

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

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

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 seven 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 | 7 Years |
| 2 | HR Data | 7 Years |
| 3 | Invoices to customers | 7 Years |
| 4 | Purchase Records | 7 Years |
| 5 | Employee Personal Files | 7 Years |

### General Data Retention

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

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

### Source Code Retention

Source Code data will never be deleted.

## Procedure for Communication

### Communication Channels

Modes of official communication are segregated by internal and external communication modes.

#### Channel for Internal Communication:

* Meetings
* Training sessions
* E-Mails
* Computer network
* Telephone
* Microsoft Teams
* TFS
* Service Desk (JIRA)

#### Channel for External Communication:

* E-Mails
* Meetings
* Telephone
* Conference Calls
* Microsoft Teams
* GoToMeeting
* Nexelus Website
* Support Center

### Internal Communication

All the policies related to Nexelus Security System along with the importance of their requirements are communicated via email and are placed on Microsoft Teams. The central repository is maintained on Microsoft Team Foundation Server (TFS).

The policies and procedures for Nexelus Security System are made available on the Team Foundation server. Furthermore, training and awareness sessions are conducted for the effective communication.

Communication channels are devised to communicate the following to the team members of a project:

* All the communication activities within a project will be circulated.
* Project Directory Structure will be maintained to keep record and track of all communication activities.

Personnel at all levels are encouraged to report problems or nonconformities related to Internal Support Management System on Jira and offer suggestions on how to improve performance via service desk.

Every team communicates with others team via managers or Lead. Within team communication is done via meetings and emails etc.

### External Communication

Following table shows external communication related details:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | What  (Service Components, Projects & Software related Communication) | Who  (The liaison person or POC from Nexelus) | When | How  (Media) | Whom  (The liaison person or POC from other party) |
|  | Product or Project documentation | Product or Project Owner | On need basis/ defined frequency | Email | Client POC |
|  | Process related Documents | NSS Team/ NSS Lead | As and when a process is created or modified | Email/ Nexelus Website | External Stakeholders |
|  | Vendor Communication | Network Engineer/ Sr. Network and System Administrator/ Admin Manager | On need basis | Email/ Phone | Vendor POC |
|  | Media | CEO, General Manager | On need basis | Interview/ Press Briefing | Media Personnel |
|  | Legal | Legal Advisor | On need basis after approval from CTO | Letter/ Email | Legal Panel |
|  | Authorities | General Manager/HR Manager | On need basis | Email/ Phone/ Fax | POC |
|  | Services related communication | Service Owner | On need basis | Email/Phone | Customer POC |
|  | Issues | Project Manager/ Process Owners | On need basis | Support Center | Customer POC |