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: | 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

[Document Details ii](#_Toc84586728)

[Document Information ii](#_Toc84586729)

[Revision History ii](#_Toc84586730)

[Table of Contents 1](#_Toc84586731)

[ISMS Manual 3](#_Toc84586732)

[Introduction 3](#_Toc84586733)

[Scope 3](#_Toc84586734)

[Reference 3](#_Toc84586735)

[Terms and Definitions 3](#_Toc84586736)

[Security Domains 3](#_Toc84586737)

[Nexelus Staff 4](#_Toc84586738)

[Network Services 4](#_Toc84586739)

[Legal framework for SOC 1 Type II 4](#_Toc84586740)

[Data Classification 5](#_Toc84586741)

[Context of the organization 5](#_Toc84586742)

[Understanding organization and its context 5](#_Toc84586743)

[Support and Services 5](#_Toc84586744)

[Nexelus Functions 5](#_Toc84586745)

[IT Security 5](#_Toc84586746)

[Understanding the needs and expectation of interested parties 5](#_Toc84586747)

[Determining the Scope of the Information Security Management System 5](#_Toc84586748)

[Nexelus Security System 5](#_Toc84586752)

[Leadership 6](#_Toc84586753)

[Leadership and Commitment 6](#_Toc84586754)

[Planning 6](#_Toc84586755)

[Support 6](#_Toc84586756)

[Resources 6](#_Toc84586757)

[NEXELUS's Top Management has formed "SOC Monitoring Team" for the establishment, implementation, maintenance, and continual improvement of the information security management system. 6](#_Toc84586758)

[Competence 6](#_Toc84586759)

[Awareness 7](#_Toc84586760)

[Communication 7](#_Toc84586761)

[Operation 7](#_Toc84586762)

[Performance Evaluation 8](#_Toc84586763)

[Monitoring, Measurement, Analysis and Evaluation 8](#_Toc84586764)

[Improvement 8](#_Toc84586765)

[Nonconformity and Corrective Action 8](#_Toc84586766)

[Continual Improvement 8](#_Toc84586767)

# ISMS Manual

## Introduction

[blurbs]

## 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.

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.
* Customer Data Protection

##### Reference(s):

* Network Security and Access Control Procedure
* HR Management Procedure
* Data and Information Sensitivity Policy Procedure

### 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 on multiple levels.
* Patch management service to update all servers/workstations.
* Application and Database servers.
* Log Management.
* Biometric Access Control
* Office 365

##### Reference(s):

* Network Security and Access Control Procedure
* Capacity and Change Management Procedure
* Data and Information Sensitivity Policy Procedure

### Legal framework for SOC 1 Type II

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 Classification

The documentation that comprises the Information Security Management System will exist under 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):

* Procedure for Control of Documents and Records
* Data and Information Sensitivity Policy Procedure

## Context of the organization

### Understanding organization and its context

Nexelus determines its external and internal issues that are relevant to its purpose and that effect its ability to achieve the intended outcome of its information security management system.

#### Support and Services

[blurbs]

#### Nexelus Functions

Services provided by Nexelus are mentioned in Service Catalogue.

#### IT Security

### Understanding the needs and expectation of interested parties

##### Reference(s)

* Context of Organization

### Determining the Scope of the Information Security Management System



##### Reference(s)

* Statement of Applicability

### Nexelus Security System

The Nexelus Security System is based on the overall business risks of Nexelus. The Nexelus Security System is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to Nexelus management and stakeholders.

Other relevant documents within the Nexelus Security System are:-

* Policies
* Procedures / Standards
* Asset Risk Assessment
* Statement of Applicability
* Network Security and Access Control Procedure
* Information Security Audit Schedule and Logs
* Internal Audit Process
* Templates

## Leadership

### Leadership and Commitment

[Text]

##### Reference(s)

* Job Description Manual

## Planning

## Support

## 

### Resources

NEXELUS's Top Management has formed "SOC Monitoring Team" for the establishment, implementation, maintenance, and continual improvement of the information security management system.

### Competence

Nexelus ensures that all the personnel who are assigned the responsibility defined for SOC 1 compliance are competent to perform the required tasks by;

1. Identifying the appropriate personnel to perform the tasks as per ISMS policies and procedures.
2. By providing appropriate training to the ISMS team through internal and external means to satisfy the ISMS needs.
3. By regular monitoring and evaluation of actions taken for preventive and corrective steps and
4. By maintaining all records of personnel’s records and qualifications.

##### Reference(s)

* HR Management Procedure
* JD Manual

### Awareness

[Blurbs]

### Communication

Nexelus determines the need for internal and external communications relevant to the information security management system including:

1. On what to communicate.
2. When to communicate.
3. With whom to communicate.
4. Who shall communicate;
5. The processes by which communication shall be affected.

## Operation

## Performance Evaluation

### Monitoring, Measurement, Analysis and Evaluation

##### Reference(s)

* Management Review Procedure

## Improvement

### Nonconformity and Corrective Action

When nonconformity occurs, Nexelus takes action to eliminate the cause of nonconformities associated with the implementation and operation of the Nexelus Security System in order to prevent recurrence on a regular basis according to the following procedure:

1. React to the nonconformity, and as applicable:

* Take action to control and correct it; and
* Deal with the consequences.

1. Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

* Reviewing the nonconformity.
* Determining the root causes of the nonconformity.
* Determining if similar nonconformities exist, or could potentially occur.

1. Implement any action needed.
2. Review the effectiveness of any corrective action taken; and
3. Make changes to the Nexelus Security System, if necessary.

##### Reference(s)

* Internal Audit Procedure
* Management Review Procedure

### Continual Improvement

Nexelus continually improves the suitability, adequacy, and effectiveness of the information security management system, following the PDCA model shown in Section Process Approach of this manual, through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and management reviews.