Nexelus Security Controls

SOC 1 Type II Document

esm_logo.jpg

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

**8/10/2022**

## Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Nexelus Security Controls - 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 | August 8, 2022 | 0.1 | Initial Draft |

## Table of Contents

Contents

[Document Information ii](#_Toc111028852)

[Revision History iii](#_Toc111028853)

[Table of Contents i](#_Toc111028854)

[Scope 1](#_Toc111028855)

[Clean Desk Policy 2](#_Toc111028856)

[Data and Information Security Policy 3](#_Toc111028857)

[Physical Control Policy 4](#_Toc111028858)

[Data Center Security 5](#_Toc111028859)

[Risk Management 6](#_Toc111028860)

[Control Environment 7](#_Toc111028861)

[Network Security Policy 8](#_Toc111028862)

[Legal Framework for Security Policy 9](#_Toc111028863)

[Information Access Policy 10](#_Toc111028864)

[Marking/Classification of Sensitive Information 11](#_Toc111028865)

[Data Handling Policy 12](#_Toc111028866)

[Data Access Policy 13](#_Toc111028867)

[Data Backup Policy 14](#_Toc111028868)

[Data Retention Policy 15](#_Toc111028869)

[Procedure for Communication 16](#_Toc111028870)

[Business Continuity and Disaster Recovery 17](#_Toc111028871)

[Legal Compliances and SLA Review Policy 18](#_Toc111028872)

[Incident Reporting Policy 19](#_Toc111028873)

[Project Management Process Guide 20](#_Toc111028874)

[Release Management Process 21](#_Toc111028875)

[Change Management 22](#_Toc111028876)

## Scope

At Nexelus, security and privacy of your data is one of our key focus points. Information 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 of this document is to list key security policies established and implemented at Nexelus.

**Reference**

SSAE-18 SOC 1 Type II – Requirements

## Clean Desk Policy

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

## Data and 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 the customer 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.

## Physical Control Policy

Physical Control Policy is placed to secure the physical environment access at Nexelus for employees and visitors. The policy ensures the safety of the company hardware, computers, laptops, printers, server rooms, networks, printed materials, company’s financial files and other relevant material deemed necessary for smooth operations of the company.

The policy ensure that each employee is well equipped with required hardware and access to resources required to perform his/her daily tasks effectively and efficiently.

The policy is devised to control theft, loss of company’s intellectual property and financial records at all times. Yet it enables to employees to perform their duties.

## 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.

## Risk Management

Nexelus recognizes the need for risk management to feature as a consideration in strategic and operational planning, day-to-day management and decision making at all levels in the organization.

Nexelus is committed to managing and minimizing risk by identifying, analyzing, evaluating and treating exposures that may impact on the organization achieving its objectives and/or the continued efficiency and effectiveness of its operations. Nexelus will incorporate risk management into its institutional planning and decision-making processes. Risk management is included as a consideration in development, and operational planning as a delegated line management responsibility. Nexelus staff must implement risk management according to relevant legislative requirements and appropriate risk management standards.

Risk assessments can be conducted on any entity within Nexelus or any outside entity that has signed a Third-Party Agreement with Nexelus. RAs can be conducted on any information system, to include services, applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

## 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.

## Network Security Policy

Nexelus Network security Policy focus on preventing the unauthorized use of assets and data handled by the organization. This principle requires organizations to implement access controls to prevent malicious attacks, unauthorized deletion of data, misuse, unauthorized alteration, or disclosure of company information.

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. The network security policy covers following key areas:

* Encrypted Data in Transit
* Endpoint Security
* Vulnerability Management
* Remote Access Policy
* Remote Server Access
* Remote Database Servers
* Office 365 Accounts

## 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

This policy establishes the principles governing access to and dissemination of information products created, collected, maintained, and managed by Nexelus in order to provide the public and Nexelus staff with access to information.

## 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.

## 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. The policy covers following aspects of data handling process:

* Data Ownership
* Categories
* Owner Responsibilities
* Custodian Responsibilities
* User Responsibilities
* Data Disposal/Destruction

## 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.

## 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.

## Procedure for Communication

This procedure covers the communication expectations between the Board of Directors, management, and employees, and between the company and external parties. For instance, Communication between the Board of Directors and management includes regular meetings to discuss company objectives and any relevant objective updates. Effective communication at this level helps the Board of Directors and management execute their roles overseeing internal control structure.

## Business Continuity and Disaster Recovery

Business continuity (BC) and disaster recovery (DR) are closely related practices that support an organization's ability to remain operational after an adverse event.

Resiliency has become the watchword for organizations facing an array of threats, from natural disasters to the latest round of cyberattacks.

In this climate, business continuity and disaster recovery (BCDR) have a higher profile than ever before. Every organization, from small operations to the largest enterprises, is increasingly dependent on digital technologies to generate revenue, provide services and support customers who always expect applications and data to be available.

Scope of this section is to define Business Continuity and Disaster Recovery processes.

Diagram

Description automatically generated

*Figure 1: Business Continuity and Disaster Recovery Plan*

## Legal Compliances and SLA Review Policy

The purpose of this set of procedures is to define legal requirements of the organization and identify customer’s need by providing a framework for understanding. It is used to simplify the complex service delivery issues and reduce the areas of conflict among the parties concerned. It encourages dialogue in the event of disputes and eliminates unrealistic expectations.

## Incident Reporting Policy

All incidents, accidents and hazards are reported to designated authorities as defined in the procedure. By doing this Nexelus will keep the record for all the reported incidents, accidents, and hazards. Moreover, we will also learn from these events as to avoid such scenarios in future.

Diagram

Description automatically generated

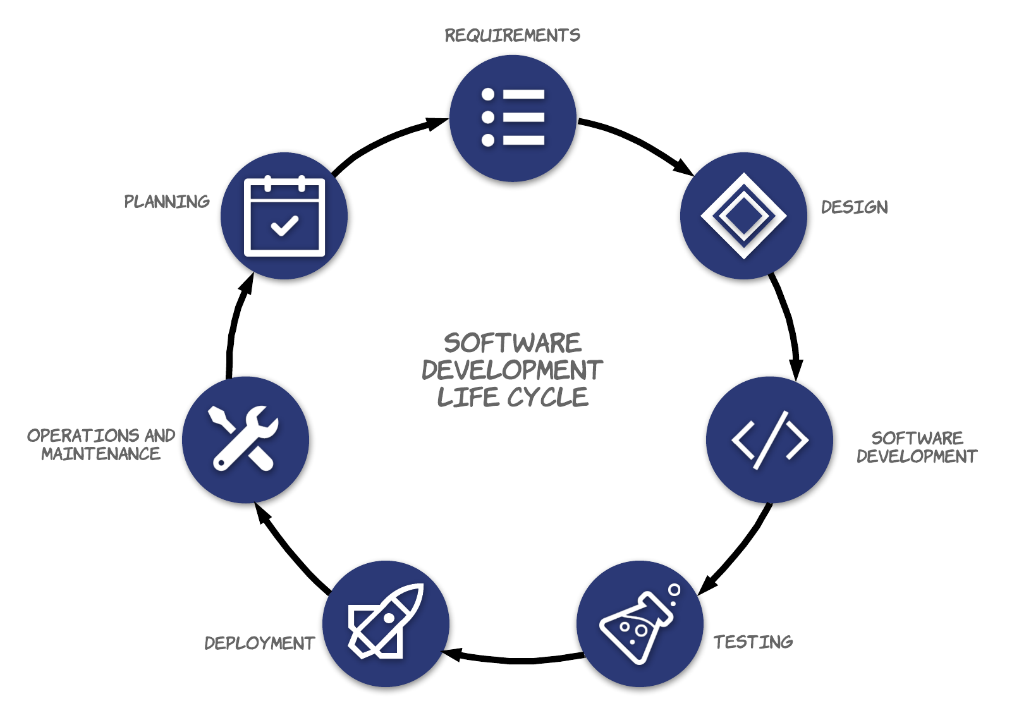
Figure 2: Incident Management Process

## Project Management Process Guide

The purpose of Project Management Process Guide is to establish guidelines for developing realistic plans for project activities, to deliver successful projects across the organization. The guide covers all the project related activities including Project Initiation, Planning, Design, Implementation, Monitor & Control and Closeout all Software Projects produced by Nexelus.

## Release Management Process

Release management oversees all the stages involved in a software release from development and testing to deployment. Release management is required anytime a new product or even changes to an existing product are requested.



*Figure 3: Software Development Life Cycle*

## Change Management

The process for managing application for change in system engineering is the process of requesting, determining accessibility, planning, implementation, and evaluating changes to the system. Its main objective is to support the processing and tracking of changes in a set of interconnected objects.

Diagram

Description automatically generated

*Figure 4: Change Management Process*