Incident Reporting Policy

SOC 2 Document

esm_logo.jpg

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

**10/21/2022**

Document Details

# Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Incident Reporting 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 21, 2022 | 1.0 | Initial Draft |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc117239011)

[Revision History iii](#_Toc117239012)

[Table of Contents i](#_Toc117239013)

[Scope 1](#_Toc117239014)

[Terms and Definitions 2](#_Toc117239015)

[Nexelus Security System (NSS) 2](#_Toc117239016)

[Security Domains 2](#_Toc117239017)

[Nexelus Staff 2](#_Toc117239018)

[Network Services 2](#_Toc117239019)

[Incident Reporting Policy 3](#_Toc117239020)

[Types of Incidents 4](#_Toc117239021)

[Critical Incidents 5](#_Toc117239022)

[Internal Reporting 6](#_Toc117239023)

[External/Client Reporting 7](#_Toc117239024)

[Collection of Evidence 8](#_Toc117239025)

[Problem Management 9](#_Toc117239026)

[Root Cause Analysis 10](#_Toc117239027)

[Knowledge Base 11](#_Toc117239028)

[Communication 12](#_Toc117239029)

[Enforcement 13](#_Toc117239030)

[Procedure for Control of Nonconforming Products 14](#_Toc117239031)

[Scope 14](#_Toc117239032)

[Roles and Responsibilities 14](#_Toc117239033)

[Types of Non-Conformity Reports (NCR) 14](#_Toc117239034)

[Procedure 15](#_Toc117239035)

[Procedure for Corrective and Preventive Actions 17](#_Toc117239036)

[Scope 17](#_Toc117239037)

[Procedure 17](#_Toc117239038)

# 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 implements 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

# 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

1. Incident Management Process

## Types of Incidents

There are number of incidents which can be predicted or anticipated of while operating in software development industry. Some of them are standard and common with other industries. Some of the incidents’ categories are given below.

* Infrastructure failure
* Data loss
* Data theft
* Fire
* Civil unrest (strike, riots, fight, sabotage, and other forms of crime)
* Terrorist activity (bomb blast, bomb alert)
* Physical security breach
* Building damage issues
* Utility failure (Power & Water)
* Service Interruption

## Critical Incidents

Few of the critical incidents and their responsible personnel are as under:

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Incident | Owner (Pakistan) | Owner (USA) |
|  | Network | Shafiq Ahmad | Peter Plakowski |
|  | Infrastructure | Arshad Sadal | Imran Rahman |
|  | Network Hacking | Shafiq Ahmad | Peter Plakowski |
|  | Software Hacking | Tauseef Shahzad | Asim Jameel |
|  | Application Crash | Support ([support@Nexelus.net](mailto:support@nexelus.net)) | |
|  |  |  | |

## Internal Reporting

All the internal incidents, accidents, or hazards at Nexelus are reported on Internal Service Desk on Jira portal. HR, Admin, Accounts, Senior Network Engineer and/or Administrator and General Manager are involved in the Incident Management Team. General Manager is the head of Incident Management Team. All the decisions will be taken after his approval.

* For every incident, the incident is reported on Jira portal, and its related actions and root cause is mentioned over there. However, in case of emergency issues are also fixed on verbal communication and are then logged on Jira later. For more details Change Management Procedure is available.
* It is the duty of the person who witnesses any incident to report it on Jira center.
* It is the responsibility of the incident management team to take appropriate actions against all incidents.
* Admin Manager checks all issues and assigns to concerned individual. Email is sent automatically to the concerned individual, and he/she is then responsible to resolve the issue.
* Though not necessary but a ‘Lesson Learnt Report’ should be prepared.

In case of any legal breach, Incident Management Team will report using information on following:

## External/Client Reporting

For external/client reporting following are used:

* Support center (Jira)
* Emails
* Phone Calls
* Microsoft Teams

External issues include client complaints, suggestions, enhancements, data beach, and/or incidents relating to Nexelus Application and customer Services etc.

Reference(s):

* Support Center (Jira)

## Collection of Evidence

This activity depends upon the place of occurrence of an incident. If it is in the premises of Nexelus then it is the responsibility of NSS Team to collect the evidence and maintain records for it. If the incident occurs in the building, then it is the duty of Manager Admin to keep the records of incident evidence. Moreover, in case of a major disaster, NSS Team can make joint effort with Manager Admin to collect and save the evidence.

## Problem Management

Every incident has a root cause. Root cause is basically the problem. For problem management that root cause is analyzed and entered in the history of every issue. The root cause is also mentioned in the knowledge base.

## Root Cause Analysis

Following tools can be used for the root cause analysis (RCA) of problems:

* Brainstorming
* FTA (Fault Tree Analysis)

## Knowledge Base

Report is generated for all the issues which are reported on service desk. This report becomes the knowledge base for the period for which report is generated. Currently, it is planned twice a year. It is the responsibility of Network Administrator and/or Admin Manager to write root cause and solution in the knowledge base. If the issue is repeated and is of the sort that it can be then it is promoted to the status of problem. For each problem permanent fix is recommended and implemented by the concerned department. The effectiveness of the fix is checked and then it is marked closed in the knowledge based. Those problems which are accepted by management as a normal problem are also marked in the knowledge base.

An incident has a root cause that root cause is analyzed and entered on service desk and is present in knowledge base as well.

## Communication

Communication with stake holders is conducted by using communication channels as mentioned in communication procedure.

## Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Procedure for Control of Nonconforming Products

This procedure provides a system for:

1. Evaluating the root cause of defects and eliminate the nonconformity
2. Evaluating projects, policies, procedures and other related documents and processes
3. Creating/suggesting a permanent solution that prevents recurrence of problems in procedure, applies to the review and subsequent disposition of non-conforming product.

### Scope

This procedure applies to all activities related to identifying and eliminating non-conformities in products, projects, policies, processes, equipment’s etc.

### Roles and Responsibilities

#### General Manager, Department Managers

The General Manager, and Department Managers will be informed about the NCRs by the NSS Lead. They will provide appropriate suggestions for resolutions and assist in root cause analysis and preventive and corrective actions.

The Department Manager will also make sure that relevant customer complaints are appropriately handled and resolved. Support Center (Jira) is used for client issues, complains, suggestions and incidents.

The General Manager will also make sure that all security, quality and service-related complaints are properly handled and resolved.

#### Network Manager

The Network Manager will review and resolve the network, hardware and application software non-conformities.

#### NSS Lead

Nexelus Security System (NSS) lead shall maintain the record of NCRs and close the NCRs after verification of the appropriate action taken. The NSS Lead shall also ensure that all NCRs are properly handled and resolved.

The NSS Lead will conduct the root cause analysis on the NCR in collaboration with relevant personnel and fill the details on the NCR.

#### Nexelus Employees

This procedure applies to all the employees of Nexelus shall report all non-conformities whenever they encounter any.

### Types of Non-Conformity Reports (NCR)

NCRS can be defined as follows:

#### Major Nonconformity

Fails to satisfy the requirements of SOC 1 and/or other implemented standards at Nexelus or Systematic failures to carry out an activity.

#### Minor Nonconformity

Satisfies the requirements of SOC 1 and/or other implemented standards but fails to satisfy the Organization’s own internal Standards, Procedures, Policies, Manuals or Non-Systematic failures.

#### Observation

An area of weakness that could be improved or be given any suggestions for improvement.

### Procedure

#### Identification of Nonconformities

In software development, non-conforming items are identified at the following stages:

* At receiving inspection stage of hardware items.
* During an audit activity (Internal Audit).
* Management Review
* By general observation of any employee of Nexelus.

##### Purchased Products

Three types of non-conformances are normally found in purchase items received in the company

* Totally rejected (all types of hardware & software)
* Re-workable by supplier
* Acceptable with some concession- depending upon the nature of the purchased or acquired product.

In all the above cases the receiver fills the Defect Advice Note and sends it to Administration Manager, who subsequently fills in the rest of the portion of the same note for onward dispatch to the concerned supplier. A copy of all filled Defect Advice Notes is also kept for reference and record. Further details may be found in Procurement Procedure.

##### Software Development

In the disposition of the non-conformities of software products developed in the company, attention is paid to the following aspects

* Any discovered problems are recorded using the TFS.
* Areas impacted by any modifications are identified & retested. The record of the testing is logged in the TFS.
* Sometimes changes are required to be made to the software product for improvement in design or due to prevention of potential bugs. These changes are recorded in the Change Request Form.

##### Audit Non-Conformity

Any nonconformity uncovered during the audit activity is regarded as the Audit Nonconformity. Audit nonconformities are logged and reported using the NCR. Corrective and preventive actions taken on the NCRs are logged. The NCRs are closed after verification and analysis of the appropriate actions taken. The NCRs are closed and maintained by the NSS Lead.

##### Network/Equipment Nonconformity

Users can submit requests for their problems on the service desk on Jira. The Network Manager responds to user’s requests or complaint in timely manner and adds history for the problem.

##### Quality Management System Nonconformity

Any activity not according to the documented procedures of the NSS will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. NSS Lead will be responsible to keep the record of NCR.

##### Nexelus Security System Nonconformity

Any activity not according to the documented policies and procedures of the NSS will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. NSS Lead will be responsible to keep the record of NCR.

##### Service Management System Nonconformity

Any activity that is not in accordance with documented policies and procedures of the NSS will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. NSS Lead will be responsible to keep the record of NCR.

#### Authorization for NCRs Closing

All closed NCRs are submitted to NSS Lead for record and closure.

#### Maintenance of Records

Records related to non-Conforming activities are maintained by NSS Lead.

## Procedure for Corrective and Preventive Actions

This procedure provides system and instructions to assign responsibilities for initiating, requesting, implementing, and checking the effectiveness of corrective and preventive actions.

### Scope

This procedure applies to preventing and correcting nonconformities related to components, finished products, and the Quality Assurance, Service Management, and Information Security Management Systems. This procedure affects all other departments and functions in the company.

### Procedure

Procedures for corrective and preventive actions are given below:

#### Corrective Action

Corrective actions will be taken to correct existing problems (problems that have occurred). These may include problems involving the product, process, or equipment.

1. Principal Internal Auditor and Support Departments will send details of the nonconformities including customer complaint to concerned person for resolution. The concerned person will conduct the relevant corrective actions to ensure that all nonconformities are removed. Details of these actions will be recorded in the Corrective and Preventive Action (CPA) columns of the NC log.
2. The performed actions will be audited/ reviewed by Principal Internal Auditor and/or other assigned personnel to assess the effectiveness of the corrective actions.
3. In case the action was effective, the NC will be closed. Otherwise, the details will be entered in the CPA including “Reasons for Ineffectiveness” and “Next Target Action”. Till the corrective/preventive actions are declared as effective, the audit/review will be continuously conducted. Once the corrective/preventive actions are considered as effective, the NC will be closed.
4. This action can be implemented for all types of nonconformities that occur before and after the internal audit.

#### Preventive Actions

Preventive actions will be taken to prevent potential problems or to avoid from reoccurrence of any issue. These may include potential problems in the product, process, or equipment.

1. Any existing and potential problems may be identified in purchased products, unreleased/released software products, network, equipment, SOC Compliance, Service Management System, and Information Security Management System.
2. These problems may be identified through general observation, inspection, audits, management reviews and customer feedback.
3. Root cause analysis of the existing problem will be recorded on the NC log.
4. A follow-up audit may be conducted after which the relevant details will be entered in the NC log and appropriate action will be taken.
5. The performed actions will be audited/reviewed by Principal Internal Auditor and/or other assigned personnel to assess the effectiveness of the preventive actions.
6. In case the action was effective, the NC will be closed, otherwise the details will be entered in the CPA columns of the NC log including “Follow up”. Till the corrective/preventive actions are declared as effective, the audit/review will be continuously conducted. Once the preventive actions are considered as effective, the NC will be closed.
7. This action can be implemented for all types of nonconformities that occur before and after the internal audit.
8. CPA columns of the NC log will be filled against major problems which required protecting future issues. It is not necessary that all IRF or NCs must have CPAs.