Monitoring and Compliance

SOC 1 Type II Document

esm_logo.jpg

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

**10/16/2021**

Document Details

# Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Monitoring and Compliance - 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 | 1.0 | Initial Draft |
| Asim Jamil | December 21, 2021 | 1.1 | Review and updated audit planning |

# Table of Contents

Contents

[Document Information ii](#_Toc112749918)

[Revision History iii](#_Toc112749919)

[Table of Contents i](#_Toc112749920)

[Scope 1](#_Toc112749921)

[Terms and Definitions 2](#_Toc112749922)

[Nexelus Security System (NSS) 2](#_Toc112749923)

[Security Domains 2](#_Toc112749924)

[Nexelus Staff 2](#_Toc112749925)

[Network Services 2](#_Toc112749926)

[Monitoring and Compliance 4](#_Toc112749927)

[Management Review Procedure 5](#_Toc112749928)

[Roles and Responsibilities 5](#_Toc112749929)

[Procedure 5](#_Toc112749930)

[Improvements 5](#_Toc112749931)

[Frequency 6](#_Toc112749932)

[Attendance 6](#_Toc112749933)

[Inputs to Management Review Meetings 6](#_Toc112749934)

[Follow up of the Meeting 6](#_Toc112749935)

[Outputs of Management Review Meetings 7](#_Toc112749936)

[Follow up of the Meeting 7](#_Toc112749937)

[Internal Audit 8](#_Toc112749938)

[Audit Planning 8](#_Toc112749939)

[Audit Execution 8](#_Toc112749940)

[Audit Reporting 9](#_Toc112749941)

[Follow-up Audit 9](#_Toc112749942)

[Independent Review of SOC Compliance 9](#_Toc112749943)

[Roles and Responsibilities 9](#_Toc112749944)

[Classification of Observations and Non-Conformity 10](#_Toc112749945)

[Internal Audit Procedure 10](#_Toc112749946)

[Authorization for NCRs Closing 12](#_Toc112749947)

[Maintenance of Records 12](#_Toc112749948)

[Incident Reporting Policy 13](#_Toc112749949)

[Types of Incidents 13](#_Toc112749950)

[Critical Incidents 13](#_Toc112749951)

[Internal Reporting 14](#_Toc112749952)

[External/Client Reporting 14](#_Toc112749953)

[Collection of Evidence 14](#_Toc112749954)

[Problem Management 15](#_Toc112749955)

[Root Cause Analysis 15](#_Toc112749956)

[Knowledge Base 15](#_Toc112749957)

[Communication 15](#_Toc112749958)

[Enforcement 15](#_Toc112749959)

[Procedure for Control of Nonconforming Products 16](#_Toc112749960)

[Scope 16](#_Toc112749961)

[Roles and Responsibilities 16](#_Toc112749962)

[Types of Non-Conformity Reports (NCR) 16](#_Toc112749963)

[Procedure 17](#_Toc112749964)

[Procedure for Corrective and Preventive Actions 19](#_Toc112749965)

[Scope 19](#_Toc112749966)

[Procedure 19](#_Toc112749967)

# 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.
* 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

# Monitoring and Compliance

Nexelus evaluates whether each of each of the defined internal control components, and the principles within each component, are present and functioning as per SOC 1 compliance. The process may be achieved through separate evaluations or ongoing activities. Monitoring also includes initiating appropriate corrective actions.

## Management Review Procedure

The purpose of Management Review is to coordinate and control the activities of SOC 1 and Nexelus Security System being carried out by different functional groups at Nexelus and to review the performance of NSS and standard compliance at regular intervals

### Roles and Responsibilities

NSS Lead prepares the agenda and minutes of the review meetings and is responsible for the follow up of the decisions taken in the meetings to ensure their completion in the specified time frame

### Procedure

Top management of the company has established a Management Review Team. This team will coordinate and control the activities of the Nexelus Security System of their IT services provided by different organizational functions. It will also review and evaluate the performance of the Nexelus Security System.

Scope, policy and objectives for NSS are communicated by making these available on TFS. All employees are instructed to read these documents. Training sessions are also conducted for the awareness of these policies. The policies are also available on Nexelus TFS Server and are displayed in all areas with human resource.

Nexelus top management ensures that a system is created, implemented and maintained in order to adhere to SOC 1 and other standards that it implements at organizational level. This is needed in order to achieve the objectives for NSS and fulfill the business operation objectives.

Members of Management Review Team include:

* CEO
* General Manager Development
* General Manager
* Network Manager
* Principal Software Architect

NSS Lead prepares the agenda and minutes of the review meetings and is responsible for the follow up of the decisions taken in the meetings to ensure their completion in the specified time frame.

### Improvements

Nexelus communicates the importance of fulfilling service requirements and a dire need of fulfilling statutory and regulatory requirements along with contractual obligations via email and/or awareness sessions.

Process improvement is a continuous process. The improvements are identified and incorporated through Internal Audits, Management Reviews, organizational objectives and suggestions from all stakeholders.

In case policies and procedures are not followed, it will adversely affect the quality of work and services. This will result in a dissatisfactory service to the customer and/or when the services will not be delivered on time, leading to a loss of clients and business.

### Frequency

The Management Review meetings are conducted on annual basis. This meeting is consolidated for Nexelus Security System and Development System. Unscheduled meetings may be called at any time on the direction of CEO, General Manager, General Manager Development or NSS lead. These meetings might not be on regular basis.

### Attendance

General Manager or CEO chairs the Management Review meeting. CEO may or may not be present in the management review meeting.

Those personnel who are unable to attend may send representatives in their place.

### Inputs to Management Review Meetings

The agenda of the Management Review is prepared by the NSS Lead before the meeting and is distributed to all the members mentioned above via email.

The inputs to management reviews include the following:

1. Review of policy and objectives for NSS
2. The next Internal Audit
3. The status of actions from previous Management Reviews
4. Changes in external and internal issues that are relevant to the Quality, Security and Service Management System.
5. Information on the performance and effectiveness of Nexelus Security System and Nexelus Development and Change Management process, including trends in the extent to which Quality, Service and Security Objectives have been met.
6. Information on NSS Process performance and conformity of products and services.
7. Results and follow-up actions from recent audits.
8. Information on the performance and effectiveness of external providers.
9. The adequacy of resources; current and forecast human, technical, information and financial resource levels; current and forecast human and technical capabilities.
10. The effectiveness of actions taken to address risks, vulnerabilities, threats and opportunities
11. Opportunities for continual improvement.
12. Service and Process Performance and conformity.

### Follow up of the Meeting

NSS Lead is responsible for the follow up of the decisions taken in the meeting to ensure that the decisions are implemented in the time frame specified.

### Outputs of Management Review Meetings

The minutes of the Management Review meetings are prepared by NSS Lead and then distributed to the members. The minutes include decisions related to improvement of the Nexelus Security System, Software Development and Change Management System, and also its processes and product related to customer requirements and resource needs.

The output from the Management Review shall include any decisions and actions related to the following:

* Improvement of the effectiveness of NSS and Development Process
* Update of the Risk Assessment and Risk Treatment Plan
* Modification of procedures and controls that effect information security as necessary to respond to internal or external events that may impact NSS and Development Process, including changes to:
* Business requirements
* Security requirements
* Business processes affecting the existing business requirements
* Regulatory or legal requirements
* Contractual obligations
* Level of risk and/or criteria for accepting risks
* Resource needs
* Improvements to how the effectiveness of controls is being measured

### Follow up of the Meeting

NSS Lead is responsible for the follow up of the decisions taken in the meeting to ensure that the decisions are implemented in the time frame specified.

## Internal Audit

Nexelus maintains a team of auditors to conduct the Internal Audit on regular basis. The Internal Auditors are selected from different organizational functions based on their experience and professional skills. They are then trained on auditing skills by conducting internal training sessions.

Principal Internal Auditor as appointed by company maintains the List of Internal Auditors. The training plan for the auditors is included in the training schedule of Nexelus.

Sometimes Internal Audit is conducted by Nexelus Audit team in the form of a gap analysis.

### Audit Planning

The process for planning an Internal Audit is as follows:

The Principal Internal Auditor discusses Annual Audit Plan in management review meeting and prepares audit schedule, which covers all processes of the SOC in all areas where it is implemented.

The Principal Internal Auditor ensures that all the applicable clauses are audited at least once in a year by trained auditors, chosen from the Nexelus employees.

Principal Internal Auditor assigns qualified auditors that are independent of the activities being audited. The auditors are also assigned different areas to audit periodically to ensure that they do not become too familiar with the activities of a department and a fresh approach is ensured.

### Audit Execution

The process of audit execution is as follows

1. Approximately a week prior to the planned audit, Principal Internal Auditor distributes the audit schedule to all relevant Managers to ensure their availability on the date of the scheduled audit. Moreover, this schedule is communicated through all the relevant Managers in the SOC Compliance meeting.
2. Principal Internal Auditor informs the auditee about the timings of audit in advance. If any changes in timings are desired, auditors make adjustment on the day of the audit in the brief opening meeting with auditee.
3. The auditors conduct audit on sample basis, which is informed to auditee in the brief opening meeting.
4. During the audit, the auditor only asks questions from the persons performing the tasks and uses suitable language for auditee.
5. During the audit, the auditors can use their own designed checklist. Checklist consists of leading questions, which ensure no area of the department is left out.
6. The auditor uses the audit checklist as a reference document and notes down all the observations on it. Audit findings/observations may be noted on a single paper.
7. The auditors also use the Checklist to identify non-conformances observed during the audit and transfer these on the Non-Compliance Report (NCR), which is presented to the auditee by the auditor.
8. To see whether relevant records of operations and inspections conform to standard and specifications, results of the process/operation activity are selected, and their record is traced backwards.
9. NCR remains with the auditee and/or departmental representative until the closing of non-conformance(s) raised during the audit. After closing of all non-conformances NCR are submitted to MR for record.
10. The NCR must be signed by the lead auditor and the auditee.
11. Principal Internal Auditor maintains Internal Audit Logbook to efficiently monitor the progress and follow up of Internal SOC Compliance Audit results.

Independent audit will be conducted by the consulting team (if available) with6 month intervals as required by SOC standard.

### Audit Reporting

After the completion of audit, the auditors submit their findings (observations, NCRs) to Principal Internal Auditor, who compiles all these findings and prepares the Internal Audit Report. It includes the summary of the audit, audit non-conformities and observations observed.

### Follow-up Audit

A follow-up audit is conducted to check the effective implementation of the corrective action proposed during the actual audit. This audit is conducted on or after the date agreed upon during the original audit. During this process due consideration will be given to the corrective actions suggested during the initial audit. For the follow-up audit, corrective and preventive actions are used as a reference which is also part of NCR.

### Independent Review of SOC Compliance

QA team has been designated to perform Internal Audits independently and objectively as required by checklist of Internal Audit. This audit will be performed as per audit plan on regular intervals as required by SOC and other security standards in place at Nexelus.

### Roles and Responsibilities

#### General Manager and QA Lead

The CEO, General Manager, and QA Lead will be informed about the NCRs by the Principal Internal Auditor. They will provide appropriate suggestions for resolutions and assist in root cause analysis and preventive and corrective actions.

The Development Manager will also make sure that customer complaints are appropriately handled and resolved as logged in Support Center to deals with client-side issues.

A separate JIRA repository for Internal Support is being setup to manage and track internal issues, complaints, suggestions, and incidents.

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

#### Network and Security Manager

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

#### Principal Internal Auditor

The Principal Internal Auditor shall maintain the record of NCRs and close the NCRs after verification of the appropriate action taken. The Principal Internal Auditor shall also ensure that all NCRs are properly handled and resolved.

The Principal Internal Auditor 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. NCRS can be defined as follows:

### Classification of Observations and Non-Conformity

#### Major Nonconformity

Fails to satisfy the requirements of Soc Compliance or Systematic failures to carry out an activity.

#### Minor Nonconformity

Satisfies the requirements of SOC Compliance 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.

### Internal Audit Procedure

#### Identification of Nonconformities

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

1. At receiving inspection stage of hardware items.
2. During an audit activity (Internal Audit).
3. Management Review
4. 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

1. Totally rejected (all types of hardware & software)
2. Re-workable by supplier
3. 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 Products

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

1. Any discovered problems are recorded using the Internal Support Center.
2. Areas impacted by any modifications are identified & retested. The record of the testing is logged in the Internal Support Center.
3. 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 Principal Internal Auditor.

#### Network/Equipment Nonconformity

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

#### SOC Compliance Nonconformity

Any activity not according to the documented procedures of the SOC Standard 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. Internal Support Center will be responsible to keep the record of NCR.

#### Information Security Management System Nonconformity

Any activity not according to the documented policies and procedures of the ISMS 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. Principal Internal Auditor will be responsible to keep the record of NCR.

#### Service Management System Nonconformity

Any activity that is not in accord to the documented policies and procedures of the Nexelus Security Policy 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. Principal Internal Auditor will be responsible to keep the record of NCR.

### Authorization for NCRs Closing

All closed NCRs are submitted to Principal Internal Audit for record and closure.

### Maintenance of Records

Records related to Non-Conformance activities will be maintained

## 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 Products

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.