Nexelus Security Manual

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: | Nexelus 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 |
| Tauseef Shahzad | October 17, 2021 | 0.2 | Added Information and Communication Chapter |
| Tauseef Shahzad | November 15, 2021 | 0.3 | Added Risk Management Policy |
| Arshad Sadal | December 21, 2021 | 0.4 | Added Information and Communication chapter and Vendor Management chapters |

# Table of Contents

Contents

[Document Information ii](#_Toc87954110)

[Revision History iii](#_Toc87954111)

[Table of Contents i](#_Toc87954112)

[Scope 1](#_Toc87954113)

[Reference 1](#_Toc87954114)

[Terms and Definitions 2](#_Toc87954115)

[Security Domains 2](#_Toc87954116)

[Nexelus Staff 2](#_Toc87954117)

[Network Services 2](#_Toc87954118)

[Organization and Management 4](#_Toc87954119)

[Organizational Structure 5](#_Toc87954120)

[Job Role Description 6](#_Toc87954121)

[Acceptable Use Policy 7](#_Toc87954122)

[Code of Conduct Policy 8](#_Toc87954123)

[Personnel Security Policy 9](#_Toc87954124)

[User Identification, Authentication, and Authorization Policy 10](#_Toc87954125)

[Employee Hiring and Screening Process 11](#_Toc87954126)

[Visitor Log policy 12](#_Toc87954127)

[Confidentiality Policy 13](#_Toc87954128)

[Clean Desk Policy 14](#_Toc87954129)

[Risk Management 15](#_Toc87954130)

[Policy 16](#_Toc87954131)

[Procedure for Risk Assessment 17](#_Toc87954132)

[Risk Identifying Procedure 17](#_Toc87954133)

[Identification of Risk Assessment Team 18](#_Toc87954134)

[Frequency of Risk Assessment 19](#_Toc87954135)

[Risk of disclosure/other risks not identified in the asset risk assessment sheet 19](#_Toc87954136)

[Identification of Risk Assessment Team 19](#_Toc87954137)

[Frequency of Risk Assessment 20](#_Toc87954138)

[NEXELUS Objectives for Risk Management 21](#_Toc87954139)

[Risk Treatment Plan 22](#_Toc87954140)

[Goals of Risk Management at Nexelus 22](#_Toc87954141)

[What Benefits Will a Risk Management Plan provide? 22](#_Toc87954142)

[Risk Management Structure and Responsibilities 23](#_Toc87954143)

[Implementation 23](#_Toc87954144)

[Timeframe 24](#_Toc87954145)

[Monitoring and Review 24](#_Toc87954146)

[Control Environment 25](#_Toc87954147)

[Data and Information Sensitivity Policy 26](#_Toc87954148)

[Physical Environment Control 27](#_Toc87954149)

[Data Center Security 27](#_Toc87954150)

[Network Security 28](#_Toc87954151)

[Encrypted Data In Transit 28](#_Toc87954152)

[Endpoint Security 28](#_Toc87954153)

[Vulnerability Management 28](#_Toc87954154)

[Remote Access Policy 28](#_Toc87954155)

[Remote Server Access 28](#_Toc87954156)

[Remote Database Servers 29](#_Toc87954157)

[Office 365 Accounts 29](#_Toc87954158)

[Data Backup Policy 30](#_Toc87954159)

[Backup Procedure 30](#_Toc87954160)

[Data Backup & Recovery Procedure 30](#_Toc87954161)

[Project Content Backup 30](#_Toc87954162)

[E-Mail Backup of Leaving Employee 30](#_Toc87954163)

[Project Content Restore 31](#_Toc87954164)

[How to Restore Outlook Emails 31](#_Toc87954165)

[Legal Framework for Security Policy 32](#_Toc87954166)

[Data Retention Policy 33](#_Toc87954167)

[E-mail Data Retention 33](#_Toc87954168)

[Financial and HR Data Retention 33](#_Toc87954169)

[General Data Retention 33](#_Toc87954170)

[TFS Data Retention 33](#_Toc87954171)

[Source Code Retention 33](#_Toc87954172)

[Information and Communication 34](#_Toc87954173)

[Marking/Classification of Sensitive Information 35](#_Toc87954174)

[Information Media 35](#_Toc87954175)

[Information Access Policy 36](#_Toc87954176)

[Data Handling Policy 37](#_Toc87954177)

[Data Ownership 37](#_Toc87954178)

[Categories 37](#_Toc87954179)

[Owner Responsibilities 37](#_Toc87954180)

[Custodian Responsibilities 37](#_Toc87954181)

[User Responsibilities 37](#_Toc87954182)

[Disposal/Destruction Policy 39](#_Toc87954183)

[Data Access Policy 40](#_Toc87954184)

[Training Policies 41](#_Toc87954185)

[Onboarding of New Employees 42](#_Toc87954186)

[Security and Awareness Training Policy 43](#_Toc87954187)

[Business Continuity and Disaster Recovery 44](#_Toc87954188)

[Business Continuity Plan 45](#_Toc87954189)

[Significant Business Disruptions (SBD) 45](#_Toc87954190)

[Assumptions 45](#_Toc87954191)

[Business Impact Analysis 46](#_Toc87954192)

[Disaster Recovery Plan 47](#_Toc87954193)

[Nexelus Office 47](#_Toc87954194)

[Key Staff 47](#_Toc87954195)

[Recovery Time Objective (RTO) 47](#_Toc87954196)

[Recovery Point Objective (RPO) 47](#_Toc87954197)

[Maximum Tolerable Outage (MTO) 47](#_Toc87954198)

[Critical Business Services 48](#_Toc87954199)

[Business Continuity and Disaster Recovery Management Team 48](#_Toc87954200)

[Plan Maintenance Procedure 48](#_Toc87954201)

[Disaster Recovery Steps 48](#_Toc87954202)

[Restore Servers in Azure 50](#_Toc87954203)

[A. Create new Servers 50](#_Toc87954204)

[B. Recover Databases 50](#_Toc87954205)

[C. Recover Web Application (Web Server): 51](#_Toc87954206)

[Monitoring 56](#_Toc87954207)

[Procedure for Control of Nonconforming Products 57](#_Toc87954208)

[Scope 57](#_Toc87954209)

[Incident Reporting Policy 58](#_Toc87954210)

[Types of Incidents 58](#_Toc87954211)

[Critical Incidents 58](#_Toc87954212)

[Internal Reporting 59](#_Toc87954213)

[External/Client Reporting 59](#_Toc87954214)

[Collection of Evidence 59](#_Toc87954215)

[Problem Management 60](#_Toc87954216)

[Root Cause Analysis 60](#_Toc87954217)

[Knowledge Base 60](#_Toc87954218)

[Communication 60](#_Toc87954219)

[Enforcement 60](#_Toc87954220)

[Internal Audit 61](#_Toc87954221)

[Audit Planning 61](#_Toc87954222)

[Audit Execution 61](#_Toc87954223)

[Audit Reporting 62](#_Toc87954224)

[Follow-up Audit 62](#_Toc87954225)

[Independent Review of SOC Compliance 62](#_Toc87954226)

[Roles and Responsibilities 62](#_Toc87954227)

[General Manager and QA Lead 62](#_Toc87954228)

[Network and Security Manager 63](#_Toc87954229)

[Principal Internal Auditor 63](#_Toc87954230)

[Nexelus Employees 63](#_Toc87954231)

[Classification of Observations and Non-Conformity 63](#_Toc87954232)

[Internal Audit Procedure 63](#_Toc87954233)

[Identification of Nonconformities 63](#_Toc87954234)

[Authorization for NCRs Closing 65](#_Toc87954235)

[Maintenance of Records 65](#_Toc87954236)

[Procedure for Corrective and Preventive Actions 66](#_Toc87954237)

[Scope 66](#_Toc87954238)

[Procedure 66](#_Toc87954239)

# 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 and HiQuSystems 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):

1. 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

# Organization and Management

Organizational Management is a management activity that ensures organizational goals are reached by adequately deploying available resources and processes. Organizational management includes monitoring, planning, organizing, and implementing. These all realize the organization’s ambitions which are translated into predetermined goals and objectives.

## Organization Chart

Diagram

Description automatically generated

## Job Description Manual

Job Description Manual is maintained separately.

Reference:

1. Job Description Manual – HiQuSystems.docx
2. Job Description Manual – Nexelus.docx

## Employee Hiring and Screening Process

An efficient and effective hiring process is a step-by-step process for hiring a new employee, whereby an organization identifies its talent needs, recruits from its talent pool and eventually hires the most qualified candidates.

### Hiring Process

Recruitment process starts as and when a hiring need is identified. In the case of newly formed positions, Department head identifies how the new role aligns with its goals and business plan, keeping the relevant internal teams and employees apprised of the new position at each stage of the hiring process. It’s important that all those involved in the hiring decision agree to the hiring process, steps, and appropriate communication channels.

General Manager decides on how to publicize the new position, both internally and externally; criteria for initial candidate screening; what the interview process will look like; and who will conduct interviews.

### Job Description

Job Description is borrowed from Job Description Manual or new Job Description is developed for a new position. Job description includes a prioritized list of job requirements, special qualifications, desired characteristics, and requisite experience.

### Advertise the Position

Identifying highly qualified potential candidates begins internally. Start, therefore, by notifying current employees of the opening. Advertising the job may stop there if management decides to fill the position internally. If, however, if an external candidate is required, a suitable platform such as Rozee.pk will be used to advertise the job. External publicity may also consist of utilizing a combination of the company’s website and social media platforms, job posting sites like LinkedIn, job fairs, industry publications and events, local newspaper advertisements, and word-of-mouth recruitment. A third party recruiter is also consulted occasionally.

### Review Applications

The review process begins with Human Resource representatives who reviews the applications and eliminate any candidate who does not meet the minimum requirements for the position or the company more generally. Shortlisted applications are then further analyzed by relevant department head(s) and filtered. Once a batch of qualified applications are assembled, HR department initiates the interview process.

### Phone Interview/Initial Screening

Initial interviews typically begin with phone calls with HR representatives. Phone interviews determine if applicants possess the requisite qualifications to fill the position and align with an organization’s culture and values. Phone interviews enable organizations to further pare down the list of candidates while expending company resources efficiently.

### Applicant Assessment

Based on position, each applicant is assigned one or more standardized tests. These exams measure a wide range of variables, including personality traits, problem-solving ability, reasoning, reading comprehension, emotional intelligence, and more.

### Interviews

Early interviews are typically one-on-one, in-person interviews between the applicants and the hiring manager. Early interviews conversations typically focus on applicants’ experience, skills, work history, and availability.

Additional interviews with management, staff, executives, and other members of the organization can be either one-on-one or group interviews with the hiring committee. They may be formal or casual; on-site, off-site, or online via Skype, Google Hangouts, etc. Additional interviews are more in-depth; for example, in interviews between a candidate and multiple members of the hiring team interviewer, each member of the hiring team focuses on a specific topic or aspect of the job to avoid redundancy and ensure an in-depth conversation about the role and the candidates’ qualifications and experience.

HR department inform the candidates that you elect not to request an interview that the search has moved forward and they are no longer under consideration.

Final interviews often include conversations with the company’s general Manager and/or CEO or a more in-depth discussion with an interviewer from an earlier stage in the hiring process. Final interviews are typically extended only to a very small pool of top candidates.

### Background Check

Background checks review candidates’ criminal record, verify employment history and eligibility, and run credit checks. HiQuSystems may also check social media accounts (Facebook, Twitter, etc.) to make sure potential employees are likely to represent the company in a professional manner.

### Decision

After conducting background and reference checks, the HR department identifies their top choice. The HR Department also selects a backup candidate, in case the top choice declines the offer or negotiations fail to produce a signed offer letter. In the event that no candidates meet the hiring criteria, the hiring staff should determine whether or not to start the hiring process over. If so, the hiring staff should discuss whether or not to adjust or alter the hiring process in order to yield more favorable candidates.

### Reference Check

Reference checks verifies any pertinent information shared by the candidate about previous employment--job performance, experience, responsibilities, workplace conduct, etc. A typical question to ask references is “Would you rehire this person?”

### Job offer

Once a top candidate is identified, the General Manager or CEO extends an initial offer. The offer letter includes the position’s salary, benefits, paid time off, start date, working remotely policy, included company equipment and other terms and conditions of employment.

### Hiring

After negotiations, once the candidate accepts the job offer they are hired. An accepted offer letter begins a process of filling out and filing paperwork related to employment.

### Onboarding

The employee workspace is prepared, cleaned, and equipped with the necessary user credentials and equipment before their first day.

HR Department welcomes the new employee and help integrate them in a manner that lays the groundwork for a long-term productive relationship between the employee and HiQuSystems. HR individual introduces the new employee to the team and familiarize him/her with company culture and norms.

The department head or General Manager provides the basic orientation and product overview. A designated resource is assigned to provide necessary onboarding training that is designed for specific role.

## Clean Desk Policy

Clean desk policy is placed to secure the physical security at HiQuSystems. 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 engaged to perform any task for the company.

### Policy

1. Employees are required to secure all sensitive/classified information in their workspace at the completion of the workday and when they are expected to be away from their workspace for an extended or short period of time. This includes both electronic and physical hardcopy information.
2. The Windows lock shall be password protected for reactivation
3. Computer workstations/laptops must be locked (logged out or shut down) when unattended and at the end of the workday. Portable devices like laptops and tablets that remain in the office overnight must be shut down and stored away.
4. Mass storage devices such as CD, DVD, USB drives, or external hard drives must be treated as sensitive material and locked away when not in use.
5. Printed materials must be immediately removed from printers. Printing physical copies should be reserved for moments of absolute necessity. Documents should be viewed, shared and managed electronically whenever possible.
6. All sensitive documents and restricted information must be placed in the designated shredder bins for destruction, or placed in the locked confidential disposal bins.
7. File cabinets and drawers containing sensitive information must be kept closed and locked when unattended and not in use.
8. Passwords must not be written down or stored anywhere in the office.
9. Keys and physical access cards must not be left unattended anywhere in the office.
10. The reception desk can be particularly vulnerable to visitors. This area shall be kept as clear as possible at all times.
11. Individual Personal belongings like bags, books, edibles, etc. shall be kept in drawers.
12. Company provided laptop/tablets/mobile phone should strictly be used for company purpose when working from home. The devices must not be shared with anyone not related to HiQuSystems directly or indirectly.
13. When working from home, the same rules apply to the sensitive and confidential information as of working in office.
14. Server rooms and office areas shall remain locked when they are not in use
15. File cabinets containing Confidential or Internal Use information must be locked when not in use or when not attended.
16. Keys used to access Confidential or Internal Use information must not be left in an unattended work area.
17. Passwords must not be posted on or under a computer or in any other accessible location.

It is the responsibility of each manager, supervisor or lead to ensure enforcement with the policies above. Repeated or serious violations of the clean desk policy can result in disciplinary actions in accordance

## Code of Conduct Policy

Code of conduct is maintained separately in Employee Handbook.

Reference:

1. Employee Handbook

## Personnel Security Policy

The screening is the process of verifying a candidate’s credentials and suitability for the job prior to offering a position in HiQuSystems. Most often this is in the form of a background check. The general idea is to make sure that former criminals are not hired or placed in positions of trust within the organization. But employee screening can take on many different levels, depending on the nature of the organization and the position being screened. The best approach is to check the reference from one or more previous employers. This should provide good information to make determination to hire or leave the candidate.

### Contracts

This is important to have non-disclosure clause in the contract and employee is fully aware of the consequence in case of violation of any clause of the contract and to take action against employees who violate security policies. Controls related to contracts include employment agreements, non-compete agreements, non-disclosure agreements and intellectual property agreements. Contracts are designed to protection intellectual properly from being stolen or lost.

### Security Policy Acknowledgement

Every employee or contractor with access to information must be made aware of the information security policies that apply to them. In most organizations, this includes a high-level “Code of Conduct” as well as acceptable use policies such as Internet Acceptable Use.

The acknowledgement section must make certain that employees formerly acknowledge that they have read and understood the written policies.

### Security Education

The employees must be trained and educated on the basic security information and common threats for breach of data. This is recursive and must be performed periodically.

### Monitoring

Although employees are trusted by the organization, their behavior still must be monitored at some level. The type and level of monitoring depends on many factors, including the sensitivity of the data being used, the overall security posture of the organization, or even government requirements. At a minimum, the organization should monitor all security-related user activity on systems. Many organizations choose to monitor internet and web traffic.

### Termination Procedures

The final essential component of personnel security is having proper termination procedures in place and enforced. Once an employee is no longer employed (or has indicated that they are going to leave), both logical and physical access must be terminated. In addition, the exit process usually involves the return of organizational property such as laptops or access badges.

## Physical Control Policy

Physical Control Policy is placed to secure the physical environment access at HiQuSystems 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.

### Policy

#### Server room

The server room is out of bound for all resources except for Network Administrator/GM Development/General Manager. The server room must be locked all time. The NA will require to visit server room to remove fault on need basis. Such visit is logged in Server Room Access register with date, time, reason, resolution and duration of visit.

Any faulty hardware must be replaced immediately for which NA will raise a request and new hardware will be purchase as per Purchase Policy.

#### Access to office

Access to office is limited to only HiQuSystems employees using biometric access control situated at the main door. Each employee is provided with office key incase biometric system is out of order or management decided to not to use the biometric system in situation like COVID-19.

Its responsibility of the last person to make sure office lights are properly switched off, all windows are closed, and office main door is properly locked.

All visitors must follow the Visitor Log Policy to enter HiQuSystems premises.

#### New resource joining

Upon arrival of new resources, he/she has been issued with HiQuSystesm access card bearing employees picture with name, employment date, and company address with in two working days. This card must be present all the time with an employee and can be checked at the building entrance.

The resource is assigned a workstation with all the essentials to perform daily task. The laptop/desktop is assigned to user and Asset Possession form is filed and signed by employee. Then it is employees is responsibility to make sure to keep the hardware in working condition and refrain for physical abuse. The login id/password is created for local network by Network Administrator which is shared with resource and GM.

The resource is required to follow the Clean Desk Policy for security and control.

The laptop is provided to resource for office work and in situation like COVID-19 to work from home. Work from home is allowed in any other situation with prior approval of manager/GM for which an email must be sent to concerned staff.

Any other hardware required to work from home is conditional and resource must take the responsibility of safety and return of the hardware intact. The Asset Possession form is required to be signed by manager/GM.

#### Fire extinguisher

The proper fire extinguishers must be placed at location which is easily accessible in case of fire. The fire extinguishers must conform to the required standards for wood, foam, and computer/laptop materials.

#### Power circuit breaker

Power circuit breaker is located at a place which is easily accessible, and all staff must be made aware to switch of main circuit breaker in case of fire or other emergencies.

## Visitor Log Policy

Visitor Log policy is placed to keep log of all visitor/guests visit HiQuSystems premises. This includes vendors, candidates, employees’ guests and office building personnel.

It is a record book that keeps track of the visitors on site, their identity, the company they represent, who they came to visit, the purpose of coming in, contact details, time in and time out.

The visitor log policy is to adopt a proactive approach to preventing any incident that threatens the security, availability, confidentiality and privacy of customer data and employees

This can be maintained paper based or digital. The paper based logbook must be present at the front desk reception which each visitor must fill in the required information.

### Policy

The logbook must be placed at the front desk reception with a pen all time. It’s the responsibility of the admin manager to make sure each visitor entry is logged in the book and proper information at the time of entry and exit of the visitor. Following is the minimum information required for the visitor logbook:

1. Date

2. Visitor name

3. Company representing

4. Purpose of the visit

5. Visitor card number

6. Time in

7. Time out

8. Comments

The visitor cards are placed at the reception area with each card having its own serial number. After completing the entry in the visitor log, the visitor is assigned a visitor card which he/she must be visible all times.

The visitors are not allowed to enter the server room, storage room, and individual’s workstation.

No visitor is allowed to enter server room for any reason. The visitor will wait at the reception area and wait for the concerned person (Admin) to accompany him to conference room or to GM rooms as required.

Upon conclusion of the visit, the visitor must return the visitor card and time out must be marked on the log.

The policy stands applicable for candidates appearing for interviews.

#### Server room

Server room is restricted area for visitors and employees equally. Only network admin should have access to server room, and it must be logged in the server log book.

Any technician visiting from Internet Service Provider for fixing any issue must be accompanied by concerned staff all time. The network admin will make sure to make an entry the server logbook for the purpose of the visit and time took to conclude the visit.

#### General office area

Any person visiting company for maintenance of the building or hardware repair, must adhere to same policy.

#### Storeroom

Storeroom is out of bond for all employees, and visitors. A separate logbook is required to be maintained for accessing the storeroom. The access to storeroom is restricted to Admin office/GM.

No person can bring along any device, USB device, external hard drive, camera, or laptop, which helps to acquire any information, customer data, or written material from the company premises. All such devices must be kept at the reception area for safe keeping.

It’s the responsibility of GM/Admin manager to make sure the log if maintained properly. This must be verified weekly or as and when deemed necessary.

The logbook must not be left unattended when not in use and must be kept in lock and key.

The GM must validate the logbooks periodically, monthly, for authenticity of the records.

# 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.

## Policy

The execution, development and implementation of remediation programs by Nexelus Security System (NSS) Team for Nexelus informational assets, quality and services. Employees are expected to cooperate fully with any risk assessment being conducted on all informational assets for which they are held accountable. Employees are further expected to work with the Nexelus Security System (NSS) Team in the development of a remediation plan.

## Procedure for Risk Assessment

The risk assessment procedure of Nexelus is as follows:

### Risk Identifying Procedure

Following is the process of identifying the risk on informational assets of Nexelus.

Identification of Informational Assets

NSS Team identifies the informational assets owned by Nexelus. These assets are listed in our Nexelus Asset Register. These assets are divided into following categories:

• Information

• Paper

• People

• Software

• Hardware/ Physical

Each asset is evaluated on the basis of CIA (Confidentiality, Integrity and Availability).

Asset Value = C(onfidentiality) \* I(ntegrity) \* A(vailability).

Each of these asset parameters are assigned criticality values as Low, Medium and High.

Low = 1, Medium = 2, High = 3

If Asset Value is greater 18 then the asset score is 3, If Asset Value is greater than 6 and less than 18 then asset score is 2 else it will be one.

Assets having asset score 2 and 3 are critical to Nexelus.

**Reference**: List of Assets Nexelus

#### Asset Risk Assessment

After having a complete asset register we develop Asset Risk Assessment Workbook. Possible risks associated with each asset and its vulnerabilities are identified. The risk is assessed on the basis of risk probability and its impact on the company. The definitions of Threats and Vulnerabilities are as follow at Nexelus:

**Threats**

Damage or loss to information assets

**Vulnerability**

Weak links that could be exploited by the threats

**Asset risk rating = Asset Score \* Probability \* Impact**

Asset score is derived from the List of Asset. Probability can take following values (High = 3, Medium = 2 and Low =1). The impact can also be categorized as (High = 3, Medium = 2 and Low =1).

For the risk treatment we do one or multiple of the following: Reduction, Avoidance, and Transfer.

**Reduction:**

These are the measures to reduce the occurrence of certain risk at Nexelus assets.

**Avoidance:**

These are the measures taken to avoid or minimize the risk impact on the assets, even if the risk occurs as well.

**Transfer:**

This risk treatment method is used to transfer the risk to any third party to minimize the risk impact.

**Reference:** Asset Risk Assessment

#### Risk Reporting

NSS is responsible to analyze the risk of existing and new purchased informational assets. But the risk can be reported or informed by any employee through email or by any means which are quickest to reach NSS.

#### Acceptance

This technique recognizes the risk and its uncontrollability. Acceptance is a “passive” technique that focuses on allowing whatever outcome to occur without trying to prevent that outcome. This technique is normally used for “low” or “very low” risks where a scope efficient means of reducing the risk is not apparent. With the mutual consent of top management and risk owner’s information security risk acceptance level is decided at medium residual risks which is mathematically presented as 2 in numeric form. The residual risk level which is above 2 or high is required contingency plans which are made accordingly with respect to risk.

#### Risk Sources

Risk sources are interfaces and dependencies of services provided by Nexelus to internal and external stakeholders.

### Identification of Risk Assessment Team

The procedure for risk assessment starts with identification of the team which will analyze the risk levels. Our NSS team has assigned Risk Assessment at Nexelus for its assets in management review meeting to Network Manager. Team selection criteria are as follow:

1. Management side is also involved in risk management.
2. NSS Lead should fulfill the requirements:
3. More than 5 years if experience in network and infrastructure security.
4. More than 2 years job experience in the company.
5. Must be involved in implementation process of NSS.
6. NSS Member should fulfill the following requirements:
7. Must have Lead Implementer in-house training before implementation in company.
8. More than 1-2 years job experience in the company or mandated by General Manager and/or, CEO.
9. Must be from Development, Quality Assurance, HR, or Networks Department.
10. Must be involved in implementation process of NSS.
11. Must have experience to deal with compliances for at least 1 year.

### Frequency of Risk Assessment

It is decided by management that risk assessment will be performed once before internal audit to evaluate all risks against existing and new assets.

### Risk of disclosure/other risks not identified in the asset risk assessment sheet

In case of following disclosures of information, disciplinary action will be taken against the guilty:

1. HR Records
2. Clients’ Data
3. Projects’ Data
4. Other confidential information

### Identification of Risk Assessment Team

The procedure for risk assessment starts with identification of the team which will analyze the risk levels. NSS Team has assigned the duties for Risk Assessment at Nexelus for its assets to Network Manager in management review meeting. Team selection criteria are as follow:

1. Management side is also involved in risk management.
2. NSS Lead should fulfill the requirements:

* Must have Lead Implementer training and certificate.
* More than 2 years job experience in the company.
* Must be from Dev/ QA/ HR department.
* Must be involved in implementation process of ISMS.

1. NSS Member should fulfill the following requirements:

* Must have Lead Implementer in-house training before implementation in company.
* More than 1-2 years job experience in the company or mandated by General Manager/CEO.
* Must be from Development, Quality Assurance, Human Resource or Networks Department.
* Must be involved in implementation process of NSS.
* Must have experience to deal with compliances for at least 1 year.

### Frequency of Risk Assessment

It is decided by management that risk assessment will be performed once before internal audit to evaluate all risks against existing and new assets.

Risk of disclosure/other risks not identified in the asset risk assessment sheet

In case of following disclosures of information, disciplinary action will be taken against the guilty:

* HR Records
* Clients’ Data
* Projects’ Data
* Other confidential information

## Nexelus Objectives for Risk Management

Nexelus is committed to the management of risk to continue to protect its:

1. Customers, clients and stakeholders
2. Employees, and their skills
3. Environment
4. Quality of service
5. Assets and intellectual property
6. Contractual and statutory obligations
7. Image and reputation

Risk management is a key part of improving our business and services to be a leading Organization. Our aim is to achieve best practice in controlling all the risks to which our business is exposed. To achieve this aim, risk management standards will be created, maintained and continually improved. This will involve risk identification and risk evaluation linked to practical and cost-effective risk control measures commensurate with our business.

Risk management is a continuous process demanding awareness and proactive action from all Nexelus employees and outsourced service providers to reduce the possibility and impact of accidents and losses, whether caused by Nexelus or externally. Risk Management is a core responsibility for all managers. Suitable risk management activities will be incorporated into our business planning, operations and the management of our contractors and service providers. The scope of these activities will encompass:

1. Education and training in risk management for staff
2. Developing risk management standards
3. Helping to prioritize and schedule risk control improvements in each of Nexelus business units
4. Reporting to Nexelus Management on risk improvement and compliance

Our challenge for the future is to infuse risk management into our culture, our everyday business operations and those of our contractors and business partners. Everyone’s involvement and support are critical to an effective result.

## Risk Treatment Plan

### Goals of Risk Management at Nexelus

The goals behind introducing Risk Management into Nexelus are three fold:

* To provide an assurance that Nexelus has identified its highest-risk exposures and has taken steps to properly manage these.
* To ensure that Nexelus business planning processes include a focus on areas where risk management is needed.
* To establish a process across Nexelus that will integrate the various risk control measures that Nexelus already has.

### What Benefits Will a Risk Management Plan provide?

Risk Management will assist us to achieve the Nexelus’ corporate objectives by:

* Integrating the various risk control measures that the Nexelus currently uses into one holistic view of what the Nexelus is doing to minimize its risk exposures. This single view will show priorities and any gaps that need to be addressed.
* Implementing a visible, formalized and consistent process for managing the Nexelus’ exposures to risk, thereby supporting continuous improvement in the Nexelus programs and providing an assurance of more effective outcomes.
* Incorporating identified risk management solutions into planning and administrative processes resulting in more structured, accountable and effective business planning and project management.
* Building on existing risk management strategies such as our administrative, engineering, contractual, safety and quality management controls; and
* Encouraging staff and managers to think about risk, and risk management, in their day-to-day work; in program, contractor and project management; and in forward planning activities.

Risk Management will be applied to all the Nexelus activities, including those delivered on the Nexelus behalf by external service providers and project contractors. This will help us to:

* Ensure that the quality and reliability of services and other program outputs are of a very high standard.
* Ensure services meet requirements and are delivered within cost and schedule.
* Protect employees, property, information and all other assets.
* Comply with all legal requirements relative to areas of risk.

## Risk Management Structure and Responsibilities

Management, NSS team and department managers are responsible for managing risk within their span of control, for promoting the application of risk management by contractors, and assisting with the identification of global or broadly based risks that could impact on the Nexelus as a whole.

Management appoints NSS Risk Assessment Team to act as a focal point for communication and coordination of risk assessment, awareness training and risk management assurance.

A team has been established by the Nexelus management and is responsible for:

1. Co-coordinating the regular formal updating of Risk Assessment Workbook and Risk Treatment Plans and compiling a master set.
2. Maintaining corporate risk and risk control information.
3. Ensuring that all relevant risk areas are considered including those emanating from the services of external providers and contractors.
4. Analysis and reporting to the Nexelus Management via meetings or emails.

The identification and review of critical risk areas within the Nexelus and the implementation of the Nexelus Risk Management Plan will also be the subject of internal audit protocols, to be applied by Internal Audit with the oversight and approval of the management.

### Implementation

Nexelus achieves the above requirements by developing suitable analysis and documentation of risks in corporate activities,

1. Identify risks in the immediate work area and of wider impact.
2. Assess the probability of the risk eventuating.
3. Assess the likely impact on the work area and/or organization if the risk occurs.
4. Determine an overall risk rating based on probability and impact.
5. Record any existing controls or strategies which aim to reduce the risk.
6. Determine if the risk exposure is acceptable or not.
7. Determine further action plans and contingency plans to manage the risk where appropriate.
8. Monitoring and reviewing risk in external services, and where appropriate, providing input to contractors’ risk management processes,
9. Periodically reviewing and updating the Risk Assessment Workbook to account for changes in risks and related issues.

Satisfactory risk management is achieved when training has been completed by all relevant personnel, when risk assessment of all critical programs and risk exposures has been concluded.

### Timeframe

All team members have recently received a copy of this Risk treatment Plan containing the Nexelus Policy on Risk Management, guidelines on Risk Management implementation and Nexelus initial Risk Assessment Workbook.

Managers are requested to take the time to discuss the Risk Treatment Plan with their staff to ensure that they are aware of Nexelus Risk Management Policy and their role in implementation of the Risk Management Process.

The timeframe for further development and implementation of risk management within 6 months of initiation of the process.

### Monitoring and Review

The monitoring, review and updating of Registers and Action Plans will be coordinated by the NSS Team, in conjunction with Internal Audit, in line with their responsibilities under this Plan.

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

### Endpoint Security

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

### 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

All users will access remote servers by their individual accounts for logging and tracking purpose. Minimum Access policy will be applied, and users will be provided with RDC access to relevant servers only. All remote server access will be performed using official desktop and laptops only. The communication will be secured using VPN. Two-factor access will be applied on remote desktop access.

No shared passwords will be used to access remote servers.

### Remote Database Servers

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

### Office 365 Accounts

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

## 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.

## Infrastructure Update Policy

This policy ensures that key system changes are properly logged, documented and communicated across your organization so you can more effectively debug issues and respond to incidents as they arise.

[blurbs] What is Infrastructure and Hardware upgrade policy at Nexelus?

# Information and Communication

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.

## Information Access Policy

#### 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 must be 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 must also be 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 15 days. This backup is taken automatically by Azure 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 (i.e. hard disk) which 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 must be 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 will be 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 will keep 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 three 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 | ? |
| 2 | HR Data | ? |
| 3 | Inventory Records | ? |
| 4 | Invoices to customers | ? |
| 5 | Purchase Records | ? |
| 6 | Employee Personal Files | ? |
| 7 | Manuals, User Guides | ? |

### 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 other party) |
|  | Project documentation | 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 |

# Organizational Training Policy

Business growth, performance and effectiveness have always been the focus of organizations implicitly and explicitly embedded in the purpose while devising training programs. Training is basically a planned learning experience designed to bring about permanent change in an individual's knowledge, attitudes, or skills whereas training can also be used as a process for employees’ career development in the long run aiming to accomplish organization development.

Nexelus constantly strives for managing and developing the skill sits, knowledge domain and professional attitude of its human resources by designing different training programs that best suits organizational business needs with special emphasis on employees’ career advancement. As trainings post a huge cost to the books, organizations call for fruit in return. Whether performance goes skyward by the trainings imparted to employees strongly depends on the purpose, design and implementation of the training coupled with organization support in post-training adaptive process

## Scope

The process applies to areas of trainings required for successful accomplishments of functions (projects/operations) run by Nexelus in order to equip employees with skills and knowledge to enhance performance of individuals and positively impact organization growth and success. From training need identification to measuring training effectives, this procedure is defined for compliance and implementation of training where required at Organizational and Project Level.

**Organization Level Trainings Includes:** Required for SOC 1 Type II compliance

**Project Level Trainings Includes:** Required for Domain Knowledge and Technology / Skill Improvement for dedicated teams and specific employee

## Policy

The policy of Nexelus is to ensure that need basis training (both at Organization and Project level) will be arranged to improve the employee’s skills in relevant fields for ensuring and securing organizational objectives by:

* Establishing the criteria for training
* Identifying need and prepare schedule for required training
* Selecting good trainers and provide facility
* Evaluating the effectiveness of training

## Onboarding of New Employees

Training and onboarding process is placed to make sure the newly hired resources is fully aware of the processes followed at HiQuSystems, including, code of conduct, development, deployment, coding standards, and last but not the least, business domain knowledge of Nexelus product.

The training plan is spread over eight weeks. The plan is devised in a way that any new resource is self sufficient to understand the processes and basic business domain knowledge of the product. However, the training of the product does not stop here. It’s a constant learning process and individual is responsible to spend at least 4 hours a week to practice and learn new/advance features of the product. It is manager’s responsibility to make sure that resource spend that much time on the product for at least initial 6 months.

The resource is evaluated every week and gaps and issues are revised, discussed and new targets are set.

At the completion of one month, the resources again evaluated and critical points and issues are highlighted.

After two months of training the resource is evaluated and again gaps/critical points are discussed. If the resource has made good progress the new goals are set by the manager for another month.

If the resource lacks on domain knowledge, then critical points are talked about and resource is tasked to repeat the product domain session and spend extra time to understand the missing links.

### Training Plan

There are two training plans in place. Once for QA and Support Team and the other one for Development Team:

#### QA and Support Team Onboarding

Week 1

1. Client Services Protocol

2. Client Items Email

3. JIRA maintenance

4. Basic Nexelus Overview

Week 2

1. Rackspace Protocol

2. Client Services Protocol

3. Client Items Email

4. JIRA maintenance

5. Nexelus Work breakdown Structure

6. SQL Tutorial

Week 3

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. SQL Learning – TSQL

4. SQL Trace

5. Nexelus Level2/Level3 Tables

6. SQL Tutorial

Week 4

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. Troubleshooting (basic overview)

4. SQL Learning – TSQL

5. Databases (basic overview)

6. Crystal Report basic overview

7. SQL Trace

8. Nexelus Level2/Level3 Tables

9. Timesheet

Week 5

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. Troubleshooting (basic overview)

4. SQL Learning – TSQL

5. Crystal Report basic overview

6. SQL Trace

7. Nexelus Level2/Level3 Tables

8. Timesheet, rates

9. Expense Reports

Week 6

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. Troubleshooting (basic overview)

4. SQL Learning – TSQL

5. Crystal Report basic overview

6. SQL Trace

7. Nexelus Level2/Level3 Tables

8. Timesheet, rates, approvals

9. Expense Reports, exp groups, Approvals

10. AMEX Integration Process

Week 7

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. Troubleshooting (basic Items and differentiation between product related items and Report related items)

4. SQL Learning – TSQL

5. Client Deployments/Upgrade (basic overview)

6. Crystal Report advanced overview

7. SQL Trace

8. Web Deployments (basic overview)

9. Nexelus Level2/Level3 Tables

10. Timesheet, rates, approvals

11. Expense Reports, exp groups, Approvals

12. AMEX Integration Process

Week 8

1. Client Items Email - Primary Resource

2. Shared ownership of JIRA for Client Items

3. Troubleshooting (basic Items and differentiation between product related items and Report related items)

4. SQL Learning – TSQL

5. Client Deployments/Upgrade (basic overview)

6. Crystal Report advanced overview

7. SQL Trace

8. Web Deployments (advanced overview)

9. Nexelus Level2/Level3 Tables

10. Timesheet, rates, approvals

11. Expense Reports, exp groups, Approvals

12. AMEX Integration Process

#### Development and DB Team Onboarding

Week 1

Day 1

1. HR related items
2. Introduction to teams
3. Computer access

Day 2

1. Typical Client (ad agency business overview)
2. Nexelus power point presentation (Company Presentation)
3. Demo of the Software

Day 3 & 4

1. Base tables Review (explain each with the business concepts)
2. Show user interface for those base tables
3. Provide access to a test system

Day 5

1. Self Study

Week 2

Day 1

1. Review progress and retention from Previous week
2. Be able to explain any of the base table
3. Be able to show the UI for specific base table
4. Be able to explain the ""business"" logic behind the base table

Day 2

By this time user should be able to use SQL trace to trace calls and is across the company and group rules concept

1. Review Level2/Level3 (WBS)
2. Provide examples - should understand the logic behind Job/Activity Structure

Day 3, 4 & 5

Self Study

1. Understand the relationship between base tables and Level2/Level3 tables
2. Understand the concept about templates
3. Understand how rules affect certain fields (rate tables, Org units, etc.)

Day 5

1. Self Study

Week 3

Day 1

Review progress

1. Rules as it related to Level2, dependency, etc.
2. Provide clear guidance on what the employee will be tested on level2/level3

Day 2

1. Time Sheet Review along with TE table

Day 3

1. Time Sheet Approval
2. Upload & Post"

Day 4 & 5

1. Self Study (Association of fields, Rates and Rules)

Week 4

Day 1

1. Review of Time Sheet
2. Be able to explain flow of Time Sheet
3. Be able to explain Approval criteria

Day 2

1. Expense Report Review with tables
   1. Non CC
   2. CC
   3. Expense Report Items
   4. Rules related to Exp Reports
   5. Payment Types

Day 3

1. Expense Approval Process
2. Upload & Post

Day 4 & 5

1. Self Study (Association of fields, custom fields, Rules and voucher)

Week 5

Day 1

1. Review of Expense Report
2. Be able to explain flow of Expense Report
3. Be able to explain Approval criteria

Day 2

1. Estimate Budget (Types of budget)
2. Overview of Budget templates
3. Overview of regular budget"

Day 3, 4 & 5

1. Self Study of budget along with associated fields & rules

Week 6

Day 1

1. Review of budget section
2. Be able to explain Labor, Expense and Resource budget
3. Be able to explain how rates, tasks, expense types and work function are populated

Day 2

1. Overview of PO and Voucher (Po based and Non PO based voucher)
2. PO Tolerance
3. Self Study

Day 3 & 4

1. Self Study of PO along with fields, rules, linking with Level2/Level3 and budget

Day 4 & 5

1. Self Study of voucher along with fields, rules and linking with PO

Week 7

Day 1

1. Review of PO
2. Review of Voucher

Day 2

1. Overview of Billing & Invoicing
   1. Estimated
   2. Scheduled
   3. Actual
2. Self Study of Billing

Day 3 & 4

1. Self Study of Billing

Day 5

1. Self Study of Job Inquiry, How and when data is populated on this screen

Week 8

Day 1

1. Review of Billing & Invoicing

Day 2

1. Review of Billing & Invoicing
2. Review of Job inquiry (Detail of each section)

Day 3, 4 & 5

1. Review of complete process flow

### Training Assessment

Upon completion of the product training, the resource must be able to participate in product discussion, be able to reproduce test scenario and fix basic level issues.

In third month, the resource must be able learn and demonstrate the product process flow described below:

**Product Process Flow**

1. Go To Job Setup screen
2. Select the client "BERLICLOR"
3. "ZZBILLABLE" template – this is a generic one, additional templates can be defined
4. Save The Job- BERLICOR-13-XXX (not down the job number – copy it)
5. Go to Job resource Management Screen and load the same job
6. Update the data as required on Job resource management screen, Click on Create Revision estimate and update it as required
   1. This is just a sample for RM, without workflow/project plan. Reference Levin’s initiative vs. what we are doing with Chicago initiative
7. Click on the "view estimate" that will redirect to the Job Estimate
8. Enter Time and OOP (billable client)  estimate as per requirement, check the checkboxes on each relevant activity and approve from the grid header icon
9. See defaults loaded for Expense and Studio, this can be based on the template for different type of jobs
10. Now we have estimates, print estimate format, this can be customized
11. From reports – Operational, run the "Estimate Vs. Actual Summary"  for the job ( I suggest copy the Job after the step 3 above)
    1. Drill down to show the Details
12. Go to Job inquiry and show the summary and drill down from there as well
13. On to the billing, “Estimated Billing”
    1. Paste or select the Job, select “Est…” transaction types for each of the drop down for Time, Expenses and Resources
    2. Hit refresh, and perhaps show that each live can be manipulated
    3. Hit refresh again, and use the percent to perhaps bill 25%
    4. Click on Save and Generate Invoice, this should generate the invoice
14. Go To Invoice screen, click search, your invoice should be at the top.
15. Click on the load icon (next to check box on the line) to load the invoice
16. You can click on the drop down to show various different formats
17. Leave the default one as is and click on print and then print as final and then click on post
18. Now go to Job Inquiry and show data
19. Go to Reports  User Reports and print WIP summary for this Job. This ties to the GL
20. Go to Reports  Operational and run the Job status detail report this will show you data in a different format, this also shows the granularity of data
21. Now to the PO Entry
22. Go to PO screen, select vendor i.e.,1Tripo, select  your job
23. Enter PO Amount by selecting the available item in the drop down, save
24. Approve PO, and print it to make it final and active. Note down the PO number (copy it)
25. You can show Job inquiry and Job Status Detail report to show the PO in there as well
26. Now we have PREBILL out and POs issued, let’s assign resources
    1. Create a new revision as this one will be locked since we pushed that version to the estimate/budget. Label it something like “Staffing”
    2. And assign the resources, let’s use Fellows and Jimenez  and few others (as I had used these two in the morning today)
27. Click on the "Assign Resources" and enter data to the selected resource, save
    1. When coming back to the main UI, click on lock revision – this will pin the timesheet line
       1. Switch to one of the assigned resource,
       2. Show the  Workflow gadget
       3. And show the timesheet line (**remember** to go the week that person is scheduled for)
       4. Switch back to yourself
28. GO TO Resource Assignment by Employee (Daily Book), Press search
    1. You can over book people from here as well
    2. You can then show the excel pivot and other burn rate reports that we discussing to address all RM related questions.
29. Now enter some vouchers
    1. Go to Voucher Entry Screen (Under Data Entry), click the new button
    2. In the PO search UP Paste/Select PO000xxx,
    3. Enter Invoice number
    4. Save
    5. Attached a document as a sample (you can show it how it is available in the Job Inquiry as well)
30. Go to the menu click on POST vouchers, hit search, scroll down and your voucher should be the last one, move to the right and post
31. Now you can go to the following to show data
    1. WIP Summary
    2. Job Inquiry
    3. Job Status Detail
    4. Estimate vs. Actual Summary
32. Let’s transfer some time to mimic that we have time entered
33. From under Billing  Posted Transactions
    1. Look up Job “SCRU0113”, click Search
    2. Expand Time panel
    3. And select 3-4 transactions and click on “Transfer” button, select your newly created Job and activity TIME and hit transfer
34. Now let’s do the reconciliation invoice, go to the Generate Invoice Screen (under Billing)
    1. Click on the check box to indicate “apply Pre bill”
    2. Select or paste you job code in From and to boxes for the Job
    3. Generate Invoice
       1. This will generate a reconciliation invoice
       2. Go to the invoice UI and click on Search your invoice should be at the top
       3. Load it, and change the format to cid:image001.png@01CEF279.719248E0, save and print to show this format
       4. Then Select cid:image002.png@01CEF279.719248E0, save and print to show another format.
       5. Print as final and then post
35. Now you should go to the following to show the current status
    1. Job Inquiry
    2. Estimate vs. Actual Summary (click to drill down)
    3. Job Status Detail
    4. WIP Summary

Then you can print the generic utilization report and talk about the same that we had discussed.

## Nexelus Security System Awareness Training

Every employee and stakeholder of an organization can be a potential target, and every online activity performed by them carries a degree of risk. Building a strong cybersecurity program is a blend of people, processes, and technology. Within that, people are the soft target who are often exposed to exponential levels of security threats. That is why information security awareness and training should be an organization’s top priority.

Cyber Security Awareness and Training Program should never be underestimated. The awareness and training program is a process that focuses on educating employees and stakeholders about various security threats prevailing in the industry and ways to deal with them. The program demonstrates the best security practices to be adopted for safeguarding sensitive data and assets of the organization.

The program involves educating employees and providing information related to the tactics adopted by hackers to compromise the security of a company’s client data. Not just that, the program conducted should talk about the organization’s security policies and procedures that should be followed by every employee.

The program educates employees about the controls in place that are enforced to safeguard sensitive data. Security awareness training should include sharing techniques of securing email, techniques to prevent falling prey to phishing, and fake messages, insider threats, securing mobile devices, physical security, malware, social engineering, Wi-Fi security, reporting incidents, whistle blowing, etc.

All employees should be aware of Organization and Management Policies as defined for SOC compliance. The training includes following areas:

### Five Trust Principles of SOC 1

SOC 1 compliance requires “The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.” SOC 1 compliance also requires your organization to achieve the following 5 trust principles:

#### 1. Security

The security section of a SOC 1 audit examines both the physical and electronic forms of security in use.

#### 2. Availability

Are your customers able to access the system as per contractual specifications?

#### 3. Processing Integrity

If a company offers financial or e-commerce transactions, audit reports should include details on controls designed to safeguard transactions.

#### 4. Confidentiality

Are there any restrictions on how data is shared? Include how data is stored, transferred, and accessed as well as adherence procedures for privacy policies.

#### 5. Privacy

Unlike confidentiality, this area focuses on how your organization collects and uses customer information. Your privacy policy must align with actual operational procedures.

# 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

## Business Continuity Plan

Nexelus Business Continuity Policy is to respond to significant business disruptions by safeguarding employees’ lives and company property, quickly recovering, and resuming its operations by restoring its critical business services, protecting all the company’s information and records, and allowing our customers to transact business.

If we determine we are unable to continue our business, we will assure customers prompt access to their information held with Nexelus.

### Significant Business Disruptions (SBD)

Nexelus Business Continuity Plan anticipates two kinds of SBDs, internal and external.

#### Internal SBDs

These internal disruptions affect only our company’s ability to communicate and do business, such as a fire in our building, hardware or software failure or sudden death of an employee.

#### External SBDs

These prevent the overall operation of the markets or several companies to operate and continue their operations. Examples include terrorist attack, a city flood, a wide-scale earthquake, or a regional disruption (civil unrest or War). Our response to an external SBD relies more heavily on other organizations and systems such as Law Enforcement Agencies (Police, FIA), Fire brigade, Rescue 1122 or National Disaster Response Unit.

#### Approval and Execution Authority

General Manager is responsible for approving and executing this plan. He/she is also responsible for conducting the annual review during annual review meeting for SOC Compliance. This approval and execution authority personnel can be changed in case the existing person leaves the company or as Per Top Management decisions in annuals review meetings.

### Assumptions

The Business Continuity Plan is predicted on the validity of the following four assumptions:

* The situation that causes the disaster is localized to the data processing facility of operations and system in the building or space housing the functional area; or to the communication systems and networks that support the functional area. It is not a general disaster, such as an earthquake or flood affecting a major portion of Islamabad Pakistan.
* It should be noted that the plan would still be functional and effective, if third party restores relevant services, for example, electricity services, water and building management etc.
* The plan is based on the availability of the hot sites or the backup resources. The accessibility of these or equivalent backup resources, is a vital requirement.
* The plan is a document that reflects the changing environment and requirements of the Nexelus. Therefore, the plan requires the continued allocation of resources to maintain and to keep it in a constant state of readiness.

The Business Continuity Plan also provides its objectives, gains Senior Management support, and allocates the necessary time and resources to develop, exercise and maintain the plan. The following are the main objectives of the plan.

* Minimizing interruptions to business/service operations.
* Resuming critical operations within a specified time after a disaster.
* Assuring clients/customers that their interests and business are protected, to gain their confidence.
* Limiting the severity of the disruption.
* Expediting the restoration of services.
* Establishing awareness, so that management and staff understand the implications of a disaster upon services.
* A brief study of Business Impact Analysis, regarding Nexelus operations, and corporate customers businesses.

## Disaster Recovery Plan

Nexelus Disaster Recovery (DR) plan is in place with the following objectives:

* In case of any significant business disruption, we will resume our critical business services within 48 hours from the decision to invoke disaster recovery.
* Nexelus recovery point objective is to restore our last period-end data, that is our last weekly backup.

A disaster is defined as an incident which results in the loss of computer processing at the Nexelus site to the extent that relocation to the alternate office location must be considered. A disaster can be a result from several accidental, malicious, or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures.

The primary objective of this Disaster recovery Plan is to ensure the continued operation of identified business critical systems in the event of a disaster. Since Development, QA and Production environments are hosted in Microsoft Azure, which is SOC compliant, there is no need to procure and deploy new servers for alternate location. This ensures that client operations will remain operational in case of a disaster. However, for back-office operations and development, following goals have been set:

### Nexelus Office

* To be operational at the alternate office location within six working days after the incident.
* To operate at the alternate office location for up to one month.
* To reinstate Nexelus facilities in the main Nexelus premises within the maximum working standby period.
* To minimize the disruption to Nexelus business.

### Key Staff

* Key staff is identified, and provided appropriate equipment to operate from home
* Appropriate security policies are in place for selected staff to work from home.

### Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption), to avoid unacceptable consequences associated with a break in business continuity.

### Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) refers to the amount of data at risk. It is determined by the amount of time between data protection events and reflects the amount of data that potentially could be lost during a disaster recovery

### Maximum Tolerable Outage (MTO)

Additionally, there is an additional measure; the Maximum Tolerable Outage (MTO). The MTO is the maximum time that our business will survive from the disruption or interruption in critical business services.

Nexelus can survive without its critical business services for a maximum of one business day. In case of any incident BCDR (Business Continuity and Disaster Recovery) Team will conduct the impact analysis to evaluate the recovery time. If this recovery time is more than our MTO time, we will initiate our Disaster Recovery Plan.

### Critical Business Services

Nexelus manages client applications in cloud using Microsoft Azure Services. [blurbs]

It is also involved in software development and software support services. Both of these are our critical services and reason for offshore office. For this purpose, we need the following assets, data (source code) infrastructure, development and OS software and personnel to carry on and continue our business. These critical requirements of our business are as follows:

* Access to TFS (Server deployed in cloud).
* At least one Server Machine.
* At least one Internet connection.
* One telephone line.
* Wired and/or Wireless Local area Network infrastructure.
* xxx computers with installed OS, Microsoft Office, Visual Studio and Microsoft SQL Server Management Studio.

As part of our BCP and disaster recovery plan we will designate a backup site ready to use in case of any SBD (significant business disruption).

### Business Continuity and Disaster Recovery Management Team

NSS Team also acts as Nexelus Business Continuity Management Team consists of following personnel:

* CEO
* General Manager
* General Manager (Development)
* Senior System Architect
* Senior Network Engineer
* QA Lead

NSS Team will have an electronic copy of this plan stored on their respective Microsoft OneDrive account, so that in case of emergency they can use it for guidance.

### Plan Maintenance Procedure

Ensuring that the plan reflects ongoing changes to the resources is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updated plan; and training the personnel. The Business Continuity Management members are responsible for this comprehensive maintenance task. The NSS Team members will make sure that the plan undergoes a more formal review every Six months to confirm the incorporation of all changes since the previous quarter. Annually, the NSS Team members initiate a complete review of the plan, which could result in major revisions to this document. These revisions will be updated and distributed to all NSS Team members. The BCP plan is a live document and requires updates as soon as there are changes and will include a mechanism for induction of new services.

### Disaster Recovery Steps

[blurbs]

|  |  |  |
| --- | --- | --- |
| Info | Description | Details |
| Access to Azure Portal | You will need Azure portal access to spin up new servers |  |
| Access to Backup server images |  |  |
| DB Back Source Folder | Folder path with Database backups. |  |
| DB Destination Folder | Folder path on new DB server where we will copy the backup. This folder should be accessible by SQL server where we are restoring backups. |  |
| Application Files Source Folder | Folder path where Application / Document files are backed up. |  |
| Application Files Destination Folder | Folder path where application files will be copied to restore. |  |
| DB Server IP Address | IP Address of new DB server. This will be required when updating Database connection settings for Web Application. |  |
| Web Server IP Address | This will be required when creating shared folder for GP files. |  |
| SFTP Details | Make sure you have access to SFTP setup details. |  |
| SQL Script to create Databases. | Will be referenced as Nexelus\_dr\_recovery\_create\_all\_databases in this document. |  |
| SQL Script to restore database. | Will be referenced as Nexelus\_dr\_recovery\_restore\_databases in this document. | This SP should take one parameter as below. 1- Backup path: This SP will get backups for all databases from this path and will restore all databases. |
| Update Script to update Server name, uid/pwd for all databases. | This Script will update DB server name, user id and password for all databases. Question is, do we need to use separate users for all clients the same way we are doing, or we can use “sa” for all users for disaster recover. in any case, we must create this script to do this automatically, rather than doing it manually. For now, let’s assume we will use “sa” for all clients. Nexelus\_dr\_recovery\_update\_database\_credentials will be referenced in this document. | This SP will take 2 parameters. user ID and password. |

## Restore Servers in Azure

[blurbs]

### A. Create new Servers

Login to Azure Portal.

1. Spin up new Servers.
2. Restore Server Images:
   1. Restore Database server Image.
   2. Restore Web Server Image.
3. Copy source Files**.**
   1. Copy files from source folder to Destination Folders.

### B. Recover Databases

* 1. RDC to new DB Server.
  2. Open Microsoft SQL Server Management Studio (MSMS) and step c. to k. for each company database.
  3. **Create New** Databases for All company using steps below
     1. Click on “New Query” in MSMS
     2. Copy SQL Script from “Nexelus\_dr\_recovery\_create\_all\_databases “ in New Query Window.
     3. Run the script by pressing F5.
        1. This will create databases for All clients.
  4. **Restore Full Backup.**
     1. Clear Query Window
     2. Copy SQL Script from “Nexelus\_dr\_recovery\_restore\_databases“ in New Query Window.
     3. Provide Backup folder path as parameter.
     4. Run the script by pressing F5.
        1. This will restore databases for All clients based on backup.
  5. **Restore partial backup**
  6. **Update Database credentials:**
     1. Clear Query Window
     2. Copy SQL Script from “Nexelus\_dr\_recovery\_update\_database\_credentials“ in New Query Window.
     3. Provide user ID and password as parameters.
     4. Run the script by pressing F5.
        1. This Script will update user id and password for all client enterprise databases in pdm\_company\_site table.
  7. Share Folder for Format and GP posting.

C. Recover Web Application (Web Server):  
Restoring web server image will restore all applications and required configurations. However, we will have to perform following tasks once Web Server Image is restored.

1. **Update Application’s Web.Config.  
   Please note:** You need to perform this step for all client applications.  
   * 1. Open IIS Manager.
     2. Click on Server name to expand the node.
     3. Click on “Site” nodes to expand it.
     4. Click on client application node you are working with to expand it.
     5. Right click on Web folder and select Explore.
        1. Graphical user interface, text, application

           Description automatically generated
        2. Graphical user interface, application

           Description automatically generated
     6. This will open windows explorer.
     7. Search for Web.Config in opened folder.
     8. Open web.config in notepad.
     9. Search for “databaseserver\_esment” in web.config and update existing values with new database server, user Id and password.
     10. Text, letter

         Description automatically generated
     11. Search for “connectionStrings” in web.config.
     12. Replace old database name, user/pwd with new DB server, UID and password.
         1. Graphical user interface, text, application

            Description automatically generated
2. **Update Report Server Web.Config.**You need to perform this step for every report server for every client.  
   We can also write a small application/ Script to update these values automatically. Will discuss this later.
   * 1. Right Click on reportServer Application in IIS and click Explore
     2. Graphical user interface, text, application

        Description automatically generated
     3. This will open windows explorer where report server files are stored.
     4. Search for Web.Config in notepad.
     5. Update highlighted values with new values for database server, userid /pwd.
        1. Text, letter

           Description automatically generated
3. Update File folder Credentials in App pool (If needed) [Asif Azim to fill]
5. **Verification Process.**
   1. Open application for any Client.
   2. Login Into application using default user credentials.
   3. Navigate through different User Interfaces.
   4. Pint few reports to verify report server is working.
   5. For Media clients only.
      1. Open Client Profile.
      2. Load Any client.
      3. Go to integrations Section.
      4. Open Look up for Google Ads account.
      5. Press refresh button.
         1. System should prompt those accounts has been refreshed.
   6. Go to database server.
   7. Open query manager.
   8. Go to link Servers and Expand “172.16.8.224” Node to make sure Hstar Connection is working.
      1. Graphical user interface, text, application, chat or text message

         Description automatically generated

Open GP for Hy and Login into GP to make sure GP is working.

# Vendor Management

The purpose of the vendor Management Procedure is to select vendors based on their ability and to examine the items purchased to meet the requirements of the company, to make sure that purchased product conforms to specified requirements, and to ensure that purchase order clearly defines the product ordered.

## Vendor Assessment Policy

The policy is devised to cater for all types of vendors, hardware, technical services, or any other contract pertaining to our business. Vendor may by engaged to provide hardware, continuously supply the consumables for smooth operations of the office or can be engaged in the development activity as and when required.

#### Experience

Find out the history of vendor and years of business. The vendor must have relevant experience and well-trained staff in the relevant field. The vendor must provide details of past ventures, contracts completed, and list of individuals engaged in the contract.

#### Customers

The vendor should have and must provide on request list of customers and contact information. It is best to check the after-sale support and service about the vendor.

#### Key personnel

Talk/meet with representative involved in the business transaction. Get the cv’s of individuals to be engaged in any development project and/or activity.

#### Geographical location

It is important to find out if the vendor has on office within the city and It is equally important to find out if the vendor has branch in Karachi or has a liaison vendor which can provide services in Karachi.

#### Capacity

Find out if the vendor has the capacity to fulfill the current and future business requirement.

#### Quality and service commitment

Find out quality of after sale support and service. This can be validated through the customers directly hence it is important to get the list of customers. Ensure the vendor has sufficient resources to provide the quality support and service.

Ensure if the vendor can deliver high levels of quality and service throughout the life of the contract. Making sure the vendor has dedicated team or account manager to respond to questions or queries.

#### Standard Compliance

Find out if the vendor has achieved any standard compliance certification essential to your business and how they adhere to standards to conduct the business. Prefer the vendor having attained the certification. Measure the culture that emphasis on continuously improving quality and business practices.

#### Price

Price is one of the key factors for any business contract. The price must include details like, taxes, after sale support cost, discounts, and terms of sales. No hidden cost be part of actual price.

#### Delivery

Making sure the vendor has good record of making deliveries on time and has good reputation of meeting deadlines and commitment. Delays can cause damage to project hence vendor must make sure to keeping his promise and meeting crucial timelines.

#### Communication

Make sure vendor can attend regular meetings, or on demand for long term contracts to provide the accurate status of the contract.

## Purchased Product Classification

Purchased products are of three types of major categories:

* Commercial off-the-shelf software
* Computer and communication hardware
* Stationery and other general items

Purchase responsibility is as under:

* Admin Manager is responsible for stationery and other general items.
* Network Administrator is responsible for commercial off-the-shelf software and computer and communications hardware.

An item requisition form is filled by concerned person and approved by General Manager then forwarded to Admin requesting supply/purchase. First the required item is checked for availability in stock. In case of unavailability the item is sourced from the market.

General Manager will make sure that purchases of the value of Rs.X,XXX.XX and above are approval by the CEO through email or telephonic conversation.

## Types of Suppliers

The following types of suppliers are associated with the company:

|  |  |
| --- | --- |
| **Supplier** | **Used for** |
| Supplier 1 | For Computer related hardware/software |
| Supplier 2 | For Networking (Cables, etc.) |
| Supplier 3 | For Office equipment (stationary Items and general items etc.) |
| Supplier 4 | For Providing Services like consultancy service of all types, certification service of all types, repair and periodic maintenance, services of computer, fax, telephone, photocopiers, printers, scanners etc. |

## Evaluation of Suppliers

Following procedure is adopted to evaluate the suppliers and supply of items to Nexelus. A simple supplier history is maintained for all suppliers.

### Supplier Qualification

Criteria for including suppliers in the approved Supplier List if applicable:

* Brand representation
* Quality provided
* Market credibility
* Delivery time
* Reasonability of the rates quoted.
* Warranties

### How to Include a Supplier in Approved Supplier List

Management is the final authority for the selection of Suppliers. Admin Manager, or Network Administrator visits or calls the potential supplier, conducts a supplier evaluation and fills Supplier Evaluation Form. If the supplier meets the acceptable criteria, then recommends him as an Approved Supplier for the company. After approval, he assigns code number and category to the approved supplier(s). Finally, the supplier history file is updated, and its name is added in the Approved Supplier List.

### Supplier Evaluation Form

Following list of questions will be used to filter the vendors and to choose the suitable vendor. Answering yes or no sheet will be used for all the vendors selected for the required task/contract. A minimum of three, and maximum five, vendors must be picked and compared to select one vendor. Each question carries 1 or 0 (Yes/No) mark and any vendor attain maximum numbers will be awarded the contract.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Screening criteria | Vendor 1 | Vendor 2 | Vendor 3 |
| 1 | Does the vendor have relevant experience for the required task? |  |  |  |
| 2 | Is the vendor in business for more than 3 years? |  |  |  |
| 3 | Is the vendor in business for more than 5 years? |  |  |  |
| 4 | Does the vendor have sound reputation in the market? |  |  |  |
| 5 | Does the vendor have office in the city? |  |  |  |
| 6 | Does the vendor have office in Karachi city? |  |  |  |
| 7 | Does the vendor have sufficient staff to complete the contract |  |  |  |
| 8 | Does the vendor provide support within 24 hour’s time? |  |  |  |
| 9 | Does the customers reference check is positive? |  |  |  |
| 10 | Does the vendor carry any flagship product or represent any international brand? |  |  |  |
| 11 | Did the vendor provide enough information to establish the understanding of the project/requirement |  |  |  |
| 12 | Did vendor furnish detail breakdown of the price? |  |  |  |
| 13 | Does the vendor provide after sale support for 6 months? |  |  |  |
| 14 | Does the vendor provide after sale support for 12 months? |  |  |  |
| 15 | Does the vendor provide the required information, literature, documents, or any other material required for the task/contract? |  |  |  |
| 16 | Was the vendor quotation lowest? |  |  |  |
|  | Total points==============🡺 |  |  |  |

**Note:** *The vendor screen must be supported by all the relevant documents to support the selection of the vendor, including scope of the contract, breakdown of the cost, bio data of the personnel involved in the project, and any other document that can help to finalize the vendor.*

### Review of Supplier List

Admin Manager and Network Administrator are responsible for maintaining the supplier history file of the relevant category and reviewed by Admin Manager then approved by General Manager the final supplier list on annual basis. (Can be more often which depends upon the item type and need). The supplier history file contains the following:

* Supplier Evaluation Forms
* Purchase Order / Work Order
* Goods Receipt Register
* Corrective / Preventive Action (if any)

All the venders in approved supplier list have their own approved sub-vendors and they maintain their SLA with them.

### Criteria of Disqualification of Suppliers

On review of the Supplier history file, the supplier can be disqualified if he fails to meet the requirements on repeated instances, the defect advice note is maintained for such purposes.

### Re-evaluation of Suppliers

Approved suppliers are periodically re-evaluated every year based on their performance measured at agreed service level. However, the re-evaluation can be event driven.

For monitoring of SLA please refer to **“Legal Compliances and SLA Review Policy Procedure”**

## Purchasing Process

#### Purchase Demand

Depending on the nature of purchase, its demand is initially raised by HR Manager/Sr. Network Engineer through Item Requisition Form and takes approval from the ED/GMA&HR (If and when needed).

#### Quotations

Quotations are invited from approved suppliers via e-mail and telephonic conversation or fax for the purchasing of amounts Rs.50, 000/- and above. Comparative statement is prepared by relevant responsible person. After completion of all activities, relevant person will submit approved quotation to Accounts Manager for payment.

#### Purchase Order Approval

Accounts Manager is responsible for making the purchase order, and then CEO/General Manager approves the purchase order. Purchase order will be generated only for items worth Rs.XX,XXX/- and above.

### General Purchase

Urgently required General Store items like stationery, computer parts, office equipment, small engineering items, food and refreshment items etc. are purchased by Admin Manager from selected suppliers. Admin Manager uses Requisition Form for approval from General Manager and after purchasing he is responsible to maintain inventory of Stock and issue the items as and when required/requested.

### Purchasing Information

It is the responsibility of Admin Manager to assure that purchasing documents contain data clearly describing the product ordered, including where applicable:

* Supplier Number
* Purchase Order Number
* Date of Demand
* Quality
* Unit, type, class, grade or other precise identification
* Precise identification of the product ordered, such as product name and or product number.

### Verification and Examination of Purchased Products

Depending on the nature of the products, the verification and examination activities are performed by:

* Network Administrator (network department for Hardware/Software related items)
* Admin Manager for other items

Rejected items will return to the supplier after physical examination of the products and informs the supplier accordingly for return or replacement of the rejected items and inform management verbally about verification results and examination results are recorded in asset test form.

**Examination at Nexelus Premises**: network Manager, and/or NSS Lead will fill Asset Test Form after examining the new purchased assets before implementation or use. This form can also use for existing assets in case of any change.

**Verification at Supplier’s Premises**: In case purchased products are to be verified at supplier’s premises concerned person contacts supplier for necessary verification arrangements.

# Service Level Agreements

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.

## Disclaimer

Neither party shall be liable to the other in any manner whatsoever if it is unable to perform any of its obligations under this Agreement due to any cause beyond its reasonable control including but not limited to acts of God, war or national emergency, riots, civil commotion, fire, explosion, flood, epidemic, lock-outs (whether or not by that party), strikes and acts/orders of Government, or other competent authorities or interruption or inability in obtaining supplies or services from third parties.

## Process

It is the policy to provide guidance to all stakeholder regarding services provided by Nexelus. It will be reviewed by management on an annual basis. Changes in content will be handled by General Manager and HR after consulting with legal advisor.

This process is contingent upon each party knowing and fulfilling their responsibilities and generating an environment conducive to the achievement and maintenance of targeted service levels according to required legal requirements of organization.

### Service Level Monitoring

The success of service level agreements depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.

* Service factors must be meaningful, measurable and monitored constantly. Actual levels of service are to be compared with agreed target levels on a regular basis by bothparties. In the event of a discrepancy between actual and targeted service levels both parties are expected to identify and resolve the reason(s) for any discrepancies in close co-operation.
* Service level monitoring will be performed by stakeholder*.* Reports will be produced as and when required and forwarded to the Nexelus contact.
* Service level monitoring and reporting is performed on response times for faults, which can include in agreement’s Criteria
* SLA Should include information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships.
* For information and communication technology services, requiring that suppliers propagate organization’s security requirements throughout the supply chain if suppliers subcontract of parts of information and communication technology service provided to the organization.
* For information and communication technology products, requiring the suppliers propagate appropriate security practices throughout the supply chains if these products include components purchased from suppliers.
* Implement a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements.
* Implementing a process for identifying product service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsource aspects of procedure or service components to other suppliers.
* Obtaining assurance that critical components and their origin can be traced throughout the supply chain.
* Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features.
* Defining rules for sharing of information regarding the supply chain any potential issues and components among the organization and suppliers.
* Implementing specific process for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to supplier no longer being in the business or supplier no longer providing these components due to technology advancements.

### SLA Review Responsibility

The following persons are responsible for SLA review:

* General Manager responsible for any change or review suggested by concerned bodies (departments) regarding SLA.
* In case of general purchasing, General Management is responsible to review the SLAs.
* For network related devices, assets, services and equipment, Network Manager/Network Administrator are responsible for the review of SLAs.

### Legal Compliances Review Responsibility

General Manager and Legal Advisor are responsible to review the information security management related legal compliances. For this purpose, we have SLA with our legal advisor to deal with data protection and violation acts done by any one from Nexelus. We have copies of these laws as well in records which are available on following links:

<http://www.cyberlawpakistan.com/>

<http://www.serl.pk/?p=aW1wb3J0YW50X2xhd3MucGhw>

### Regulations of Cryptographic Controls Review and Responsibility

General Manager, NSS Lead, and Legal Advisor are responsible to review the regulations regarding cryptographic tools used in other development of any software/hardware or for implementation of any software/hardware by Nexelus. As per policy, the responsibilities lie on above mentioned heads, for ensuring that none of the local or international applicable laws are breached while using cryptographic tools and technologies.

### Technical Compliance Checking

Technical compliance checking (Penetration testing and vulnerability assessment) is performed on annual basis or when network major change occurs. This testing is performed by specialized and competent external resources.

# Monitoring

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

MR/ISMR 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.