Organization and Management

SOC II Document

esm_logo.jpg

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

**Process Owner: General Manager**

**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: | Organization and Management - SOC 1 Type II Document |
| Project Name: | Organization and Management |
| 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 | September 20, 2022 | 0.1 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc111026493)

[Revision History iii](#_Toc111026494)

[Table of Contents i](#_Toc111026495)

[Scope 1](#_Toc111026496)

[Terms and Definitions 2](#_Toc111026497)

[Nexelus Security System (NSS) 2](#_Toc111026498)

[Security Domains 2](#_Toc111026499)

[Nexelus Staff 2](#_Toc111026500)

[Network Services 2](#_Toc111026501)

[Organization and Management 4](#_Toc111026502)

[Organization Chart 5](#_Toc111026503)

[Job Description Manual 6](#_Toc111026504)

[Employee Hiring and Screening Process 7](#_Toc111026505)

[Hiring Process 7](#_Toc111026506)

[Job Description 7](#_Toc111026507)

[Advertise the Position 7](#_Toc111026508)

[Review Applications 7](#_Toc111026509)

[Phone Interview/Initial Screening 7](#_Toc111026510)

[Applicant Assessment 8](#_Toc111026511)

[Interviews 8](#_Toc111026512)

[Background Check 8](#_Toc111026513)

[Decision 8](#_Toc111026514)

[Reference Check 8](#_Toc111026515)

[Job offer 8](#_Toc111026516)

[Hiring 9](#_Toc111026517)

[Onboarding 9](#_Toc111026518)

[Clean Desk Policy 10](#_Toc111026519)

[Policy 10](#_Toc111026520)

[Code of Conduct Policy 12](#_Toc111026521)

[Personnel Security Policy 13](#_Toc111026522)

[Contracts 13](#_Toc111026523)

[Security Policy Acknowledgement 13](#_Toc111026524)

[Security Education 13](#_Toc111026525)

[Monitoring 13](#_Toc111026526)

[Termination Procedures 13](#_Toc111026527)

[Physical Control Policy 14](#_Toc111026528)

[Policy 14](#_Toc111026529)

[Visitor Log Policy 16](#_Toc111026530)

[Policy 16](#_Toc111026531)

[Risk Management 18](#_Toc111026532)

[Policy 19](#_Toc111026533)

[Procedure for Risk Assessment 20](#_Toc111026534)

[Risk Identifying Procedure 20](#_Toc111026535)

[Identification of Risk Assessment Team 21](#_Toc111026536)

[Frequency of Risk Assessment 22](#_Toc111026537)

[Risk of disclosure/other risks not identified in the asset risk assessment sheet 22](#_Toc111026538)

[Identification of Risk Assessment Team 22](#_Toc111026539)

[Frequency of Risk Assessment 23](#_Toc111026540)

[Nexelus Objectives for Risk Management 24](#_Toc111026541)

[Risk Treatment Plan 25](#_Toc111026542)

[Goals of Risk Management at Nexelus 25](#_Toc111026543)

[What Benefits Will a Risk Management Plan provide? 25](#_Toc111026544)

[Risk Management Structure and Responsibilities 26](#_Toc111026545)

[Implementation 26](#_Toc111026546)

[Timeframe 27](#_Toc111026547)

[Monitoring and Review 27](#_Toc111026548)

[Control Environment 28](#_Toc111026549)

[Management Commitment to SOC 1 29](#_Toc111026550)

[WHAT’S THE PRIMARY PURPOSE OF THIS INITIATIVE? 29](#_Toc111026551)

[Information Security Policy 30](#_Toc111026552)

[Physical Environment Control 31](#_Toc111026553)

[Data Center Security 31](#_Toc111026554)

[Network Security 32](#_Toc111026555)

[Encrypted Data In Transit 32](#_Toc111026556)

[Endpoint Security 32](#_Toc111026557)

[Vulnerability Management 32](#_Toc111026558)

[Remote Access Policy 32](#_Toc111026559)

[Remote Server Access 32](#_Toc111026560)

[Remote Database Servers 33](#_Toc111026561)

[Office 365 Accounts 33](#_Toc111026562)

[Legal Framework for Security Policy 34](#_Toc111026563)

[Infrastructure Update Policy 35](#_Toc111026564)

[Information and Communication 36](#_Toc111026565)

[Information Access Policy 37](#_Toc111026566)

[Marking/Classification of Sensitive Information 38](#_Toc111026567)

[Information Media 38](#_Toc111026568)

[Data Handling Policy 39](#_Toc111026569)

[Data Ownership 39](#_Toc111026570)

[Categories 39](#_Toc111026571)

[Owner Responsibilities 39](#_Toc111026572)

[Custodian Responsibilities 39](#_Toc111026573)

[User Responsibilities 40](#_Toc111026574)

[Data Disposal/Destruction 40](#_Toc111026575)

[Data Access Policy 41](#_Toc111026576)

[Data Backup Policy 42](#_Toc111026577)

[Backup Procedure 42](#_Toc111026578)

[Data Backup & Recovery Procedure 42](#_Toc111026579)

[Project Content Backup 42](#_Toc111026580)

[E-Mail Backup of Leaving Employee 42](#_Toc111026581)

[Data Retention Policy 44](#_Toc111026582)

[E-mail Data Retention 44](#_Toc111026583)

[Financial and HR Data Retention 44](#_Toc111026584)

[General Data Retention 44](#_Toc111026585)

[TFS Data Retention 44](#_Toc111026586)

[Source Code Retention 44](#_Toc111026587)

[Procedure for Communication 45](#_Toc111026588)

[Communication Channels 45](#_Toc111026589)

[Internal Communication 45](#_Toc111026590)

[External Communication 46](#_Toc111026591)

[Organizational Training Policy 48](#_Toc111026592)

[Scope 49](#_Toc111026593)

[Policy 50](#_Toc111026594)

[Onboarding of New Employees 51](#_Toc111026595)

[Training Plan 51](#_Toc111026596)

[Training Assessment 57](#_Toc111026597)

[Nexelus Security System Awareness Training 60](#_Toc111026598)

[Five Trust Principles of SOC 1 60](#_Toc111026599)

[Business Continuity and Disaster Recovery 62](#_Toc111026600)

[Business Continuity Plan 63](#_Toc111026601)

[Significant Business Disruptions (SBD) 63](#_Toc111026602)

[Assumptions 63](#_Toc111026603)

[Disaster Recovery Plan 65](#_Toc111026604)

[Nexelus Office 65](#_Toc111026605)

[Key Staff 65](#_Toc111026606)

[Recovery Time Objective (RTO) 65](#_Toc111026607)

[Recovery Point Objective (RPO) 65](#_Toc111026608)

[Maximum Tolerable Outage (MTO) 65](#_Toc111026609)

[Critical Business Services 66](#_Toc111026610)

[Business Continuity and Disaster Recovery Management Team 66](#_Toc111026611)

[Plan Maintenance Procedure 66](#_Toc111026612)

[Disaster Recovery Steps 66](#_Toc111026613)

[Restore Servers in Azure 68](#_Toc111026614)

[A. Create new Servers 68](#_Toc111026615)

[B. Recover Databases 68](#_Toc111026616)

[C. Recover Web Application (Web Server): 69](#_Toc111026617)

[Vendor Management 74](#_Toc111026618)

[Vendor Assessment Policy 75](#_Toc111026619)

[Purchased Product Classification 77](#_Toc111026620)

[Types of Suppliers 78](#_Toc111026621)

[Evaluation of Suppliers 79](#_Toc111026622)

[Supplier Qualification 79](#_Toc111026623)

[How to Include a Supplier in Approved Supplier List 79](#_Toc111026624)

[Supplier Evaluation Form 79](#_Toc111026625)

[Review of Supplier List 80](#_Toc111026626)

[Criteria of Disqualification of Suppliers 81](#_Toc111026627)

[Re-evaluation of Suppliers 81](#_Toc111026628)

[Purchasing Process 82](#_Toc111026629)

[General Purchase 82](#_Toc111026630)

[Purchasing Information 82](#_Toc111026631)

[Verification and Examination of Purchased Products 82](#_Toc111026632)

[Legal Compliances and SLA Review Policy Procedure 84](#_Toc111026633)

[Disclaimer 85](#_Toc111026634)

[Process 86](#_Toc111026635)

[Service Level Monitoring 86](#_Toc111026636)

[SLA Review Responsibility 87](#_Toc111026637)

[Legal Compliances Review Responsibility 87](#_Toc111026638)

[Regulations of Cryptographic Controls Review and Responsibility 87](#_Toc111026639)

[Technical Compliance Checking 87](#_Toc111026640)

[Monitoring 88](#_Toc111026641)

[Management Review Procedure 89](#_Toc111026642)

[Roles and Responsibilities 89](#_Toc111026643)

[Procedure 89](#_Toc111026644)

[Improvements 89](#_Toc111026645)

[Frequency 90](#_Toc111026646)

[Attendance 90](#_Toc111026647)

[Inputs to Management Review Meetings 90](#_Toc111026648)

[Follow up of the Meeting 90](#_Toc111026649)

[Outputs of Management Review Meetings 91](#_Toc111026650)

[Follow up of the Meeting 91](#_Toc111026651)

[Internal Audit 92](#_Toc111026652)

[Audit Planning 92](#_Toc111026653)

[Audit Execution 92](#_Toc111026654)

[Audit Reporting 93](#_Toc111026655)

[Follow-up Audit 93](#_Toc111026656)

[Independent Review of SOC Compliance 93](#_Toc111026657)

[Roles and Responsibilities 93](#_Toc111026658)

[Classification of Observations and Non-Conformity 94](#_Toc111026659)

[Internal Audit Procedure 94](#_Toc111026660)

[Authorization for NCRs Closing 96](#_Toc111026661)

[Maintenance of Records 96](#_Toc111026662)

[Incident Reporting Policy 97](#_Toc111026663)

[Types of Incidents 97](#_Toc111026664)

[Critical Incidents 97](#_Toc111026665)

[Internal Reporting 98](#_Toc111026666)

[External/Client Reporting 98](#_Toc111026667)

[Collection of Evidence 98](#_Toc111026668)

[Problem Management 99](#_Toc111026669)

[Root Cause Analysis 99](#_Toc111026670)

[Knowledge Base 99](#_Toc111026671)

[Communication 99](#_Toc111026672)

[Enforcement 99](#_Toc111026673)

[Procedure for Control of Nonconforming Products 100](#_Toc111026674)

[Scope 100](#_Toc111026675)

[Roles and Responsibilities 100](#_Toc111026676)

[Types of Non-Conformity Reports (NCR) 100](#_Toc111026677)

[Procedure 101](#_Toc111026678)

[Procedure for Corrective and Preventive Actions 103](#_Toc111026679)

[Scope 103](#_Toc111026680)

[Procedure 103](#_Toc111026681)

# Scope

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.

**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 Nexelus premises.

The location is defined as follows:

* The space within the physical structure bound by, and including, walls, ceiling, floor, doors, and windows.
* All equipment within the physical domain detail mentioned in Asset Identification and Classification Document.

Reference(s):

* Network Security and Access Control Procedure
* Capacity and change Management Procedure

### Nexelus Staff

All personnel employed / contractual engaged by Nexelus are required to follow the policies and procedures as defined in Nexelus Security Manual by management in line with strategic security needs.

### Network Services

Network services required by our network infrastructure are as follow:

* Internet Connectivity from ISP.
* Host based Protection against malware and Virus.
* Web filtering.
* Switches
* Host based Application Control.
* Active Directory
* E-mail Scanning Services.
* Patch management service to update all servers/workstations.
* Application and Database servers.
* Log Management.
* Biometric Access Control
* Office 365

# Organization and Management

## 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 Nexelus. The policy ensures the confidential information and sensitive materials are stored away and out of sight when custodian of the material is not in the premises/workplace.

The policy is set in place to keep the clean workspace, where confidential and sensitive material about company, clients, vendors, employees, and intellectual property is safe and secured.

The policy applies to employees, contractors, part time employees or any other individual 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 Nexelus 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

The primary goal of Nexelus Code of Conduct is to foster inclusive, collaborative and safe working conditions for all nexelus.net staff. As such, nexelus.net is committed to providing a friendly, safe and welcoming environment for all staff, regardless of gender, sexual orientation, ability, ethnicity, socioeconomic status, or religion (or lack thereof).

This code of conduct outlines our expectations for all nexelus.net staff, as well as the consequences for unacceptable behavior.

### Culture and Citizenship

A supplemental goal of this Code of Conduct is to increase open citizenship by encouraging participants to recognize the relationships between our actions and their effects within Nexelus culture.

**Be welcoming**. We strive to be a company that welcomes and supports people of all backgrounds and identities. This includes, but is not limited to members of any race, ethnicity, culture, national origin, color, immigration status, social and economic class, educational level, sexual orientation, gender identity and expression, age, size, family status, political belief, religion, and mental and physical ability.

**Be considerate**. Your work at nexelus.net will be used by other people, and you in turn will depend on the work of others. Any decision you take will affect users and colleagues, and you should take those consequences into account when making decisions.

**Be respectful**. Not all of us will agree all the time, but disagreement is no excuse for poor behavior and poor manners. We might all experience some frustration now and then, but we cannot allow that frustration to turn into a personal attack. It's important to remember that a company where people feel uncomfortable or threatened is neither productive nor pleasant. Nexelus staff should always be respectful when dealing with other personnel as well as with people outside of Nexelus employment.

### Acceptable and Expected Behavior

The following behaviors are expected and requested of all nexelus.net staff:

* Participate in an authentic and active way. In doing so, you contribute to the health and longevity of nexelus.net.
* Exercise consideration and respect in your speech and actions at all times.
* Attempt collaboration before conflict.
* Refrain from demeaning, discriminatory, or harassing behavior and speech.
* Be mindful of your surroundings and of your fellow participants. Alert nexelus.net leaders if you notice a dangerous situation, someone in distress, or violations of this Code of Conduct, even if they seem inconsequential.
* Remember that nexelus.net events may be shared with members of the public and Nexelus customers; please be respectful to all patrons of these locations at all times

### Unacceptable Behavior

The following behaviors are considered harassment and are unacceptable within our community:

* Violence, threats of violence or violent language directed against another person.
* Sexist, racist, homophobic, transphobic, ableist or otherwise discriminatory jokes and
* language.
* Posting or displaying sexually explicit or violent material.
* Posting or threatening to post other people's personally identifying information ("doxing").
* Personal insults, particularly those related to gender, sexual orientation, race, religion, or
* disability.
* Inappropriate photography or recording.
* Inappropriate physical contact. You should have someone's consent before touching them in any manner.
* Unwelcome sexual attention. This includes sexualized comments or jokes; inappropriate touching, groping, and unwelcome sexual advances.
* Deliberate intimidation, stalking or following (online or in person).
* Advocating for, or encouraging, any of the above behavior.
* Repeated harassment of others. In general, if someone asks you to stop, then stop.
* Other conduct which could reasonably be considered inappropriate in a professional setting.

## 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 Nexelus. 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 Nexelus for employees and visitors. The policy ensures the safety of the company hardware, computers, laptops, printers, server rooms, networks, printed materials, company’s financial files and other relevant material deemed necessary for smooth operations of the company.

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

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

### 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 Nexelus 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 Nexelus premises.

#### New resource joining

Upon arrival of new resources, he/she has been issued with Nexelus 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 Nexelus 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.