Nexelus Security Manual

SOC 1 Type II Document

esm_logo.jpg

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

**10/08/2021**

# 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 |
|  |  |  |  |

# Table of Contents

Contents

[Document Details ii](#_Toc85721104)

[Document Information ii](#_Toc85721105)

[Revision History ii](#_Toc85721106)

[Table of Contents i](#_Toc85721107)

[Scope 1](#_Toc85721108)

[Scope 1](#_Toc85721109)

[Reference 1](#_Toc85721110)

[Terms and Definitions 2](#_Toc85721111)

[Security Domains 2](#_Toc85721112)

[Nexelus Staff 2](#_Toc85721113)

[Network Services 2](#_Toc85721114)

[Legal Framework for Security Policy 4](#_Toc85721115)

[Data and Information Sensitivity Policy 5](#_Toc85721116)

[Physical Environment Control 6](#_Toc85721117)

[Data Center Security 6](#_Toc85721118)

[Network Security 6](#_Toc85721119)

[Encrypted Data In Transit 6](#_Toc85721120)

[Endpoint Security 6](#_Toc85721121)

[Vulnerability Management 6](#_Toc85721122)

[Remote Access Policy 8](#_Toc85721123)

[Access Controls and Policies 9](#_Toc85721124)

[Marking/Classification of Sensitive Information 9](#_Toc85721125)

[Information Media 9](#_Toc85721126)

[Information Access Policy 9](#_Toc85721127)

[Data Handling Policy 10](#_Toc85721128)

[Data Ownership 10](#_Toc85721129)

[Categories 10](#_Toc85721130)

[Owner Responsibilities 10](#_Toc85721131)

[Custodian Responsibilities 10](#_Toc85721132)

[User Responsibilities 11](#_Toc85721133)

[Clean Desk Policy 11](#_Toc85721134)

[Disposal/Destruction Policy 11](#_Toc85721135)

[Data Access Policy 11](#_Toc85721136)

[Data Backup Policy 12](#_Toc85721137)

[Backup Procedure 12](#_Toc85721138)

[Data Backup & Recovery Procedure 12](#_Toc85721139)

[Project Content Backup 12](#_Toc85721140)

[E-Mail Backup of Leaving Employee 13](#_Toc85721141)

[Project Content Restore 13](#_Toc85721142)

[How to Restore Outlook Emails 13](#_Toc85721143)

[Data Retention Policy 14](#_Toc85721144)

[E-mail Data Retention 14](#_Toc85721145)

[Financial and HR Data Retention 14](#_Toc85721146)

[General Data Retention 14](#_Toc85721147)

[TFS Data Retention 15](#_Toc85721148)

[Source Code Retention 15](#_Toc85721149)

[Security and Awareness Training Policy 16](#_Toc85721150)

[Business Continuity Plan 17](#_Toc85721151)

[Significant Business Disruptions (SBD) 17](#_Toc85721152)

[Internal SBDs 17](#_Toc85721153)

[External SBDs 17](#_Toc85721154)

[Approval and Execution Authority 17](#_Toc85721155)

[Assumptions 17](#_Toc85721156)

[Business Impact Analysis 18](#_Toc85721157)

[Disaster Recovery Plan 19](#_Toc85721158)

[Nexelus Office 19](#_Toc85721159)

[Key Staff 19](#_Toc85721160)

[Recovery Time Objective (RTO) 19](#_Toc85721161)

[Recovery Point Objective (RPO) 19](#_Toc85721162)

[Maximum Tolerable Outage (MTO) 20](#_Toc85721163)

[Critical Business Services 20](#_Toc85721164)

[Business Continuity and Disaster Recovery Management Team 20](#_Toc85721165)

[Plan Maintenance Procedure 20](#_Toc85721166)

[Incident Reporting Policy 22](#_Toc85721167)

[Types of Incidents 22](#_Toc85721168)

[Critical Incidents 22](#_Toc85721169)

[Internal Reporting 23](#_Toc85721170)

[External/Client Reporting 23](#_Toc85721171)

[Collection of Evidence 24](#_Toc85721172)

[Problem Management 24](#_Toc85721173)

[Root Cause Analysis 24](#_Toc85721174)

[Knowledge Base 24](#_Toc85721175)

[Communication 24](#_Toc85721176)

[Enforcement 25](#_Toc85721177)

# 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.

## Scope

This manual is applicable to all the activities of SSAE 18 (SOC 1 Type 1) at Nexelus as mentioned in this manual.

## 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 ISMS implementation:

### 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):

* 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 laid by management in line with strategic security needs.

* Network services required by the defined network infrastructure.
* Data Access and Retention Policy
* Acceptable Use Policy
* Clean Desk Policy
* Code of Conduct Policy
* Personnel Security Policy
* User identification, Authentication and Authorization Policy
* Training and Onboarding Policy

### 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

# 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.

##### Reference(s):

* Procedure for Compliances and SLA Review

# Data and Information Sensitivity Policy

The Information Security Management System exists for various levels of classification. All documentation will be clearly marked for appropriate access control as defined by its classification and handled in accordance with Nexelus Data Classification and Labeling Sheet.

##### Reference(s):

* Data Handling Policy
* Data Backup Policy
* Data Retention Policy
* Acceptable Encryption and Key Management Policy
* Remote Access Policy
* End User Encryption and Key Management Policy

# 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.

# Access Controls and Policies

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.

## 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.

## 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.

## 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 Owner, Custodian, and 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.

## Clean Desk Policy

A clean desk policy is part of an overall company security strategy. It is, as it states, about keeping your work desk clean. In general, a clean desk policy will mandate that at the end of each working day, that employees clear their desk. This means, for example, securely disposing of Post It notes, keeping written notes in a safe place, and ensuring that any removable media isn’t just lying around. Keep sensitive information from view of unauthorized people;

* Erase whiteboards,
* Do not leave any client data printouts in view on tabletop. It should be kept in drawer while not in use.
* Password protected screen saver must be applied on all desktops with 10 minutes timeout
* No document or its link should be placed on computer Desktop
* Add more clauses..

Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

## Disposal/Destruction Policy

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.

## Project Content Restore

In cases where a non-catastrophic issue requires a data restore, the Senior Network Engineer is responsible for performing the restore using backups. Senior Network Engineer will manually restore repository to a prior state if provided a viable backup of project repository.

## How to Restore Outlook Emails

Restoration of email accounts requires a .PST file to be backed up, to restore emails, contacts, and other data from a backup copy of an Outlook PST file:

1. Select File, then Import and Export from the menu in Outlook.
2. Select Import from another program or file.
3. Click Next.
4. Highlight Personal Folder File (PST).
5. Click next again.
6. Now use the Browse button to select the backup copy of the PST file you want to recover from your backup location.
7. Make sure Replace duplicates with items imported is selected.
8. Click Next.
9. Finish the import process with Finish.

# 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 | ? |
| 8 | Inventory Records | ? |
| 9 | Invoices to customers | ? |
| 11 | Purchase Records | ? |
| 12 | Employee Personal Files | ? |
| 13 | 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.

# Security and Awareness Training Policy

Nexelus perform various activities to improve the awareness around security and privacy. Some of these include annual awareness training sessions for both security and privacy.

# 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.

## Business Impact Analysis

[Blurbs]

# 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 and Visual 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

Nexelus Security 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

Nexelus Security 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. According to this, every Six months the Nexelus Security Team members make sure that the plan undergoes a more formal review to confirm the incorporation of all changes since the previous quarter. Annually, the Nexelus Security 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 Nexelus Security 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.

# 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 Nexelus Security 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, Nexelus Security 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.