Business Continuity and Disaster Recovery Plan

SOC 1 Type II Document

esm_logo.jpg

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

**9/12/2022**

# Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Business Continuity and Disaster Recovery - SOC 1 Type II Document |
| Project Name: | Business Continuity and Disaster Recovery |
| 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 | November 12, 2022 | 0.1 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document Information ii](#_Toc113894540)

[Revision History iii](#_Toc113894541)

[Table of Contents i](#_Toc113894542)

[Scope 1](#_Toc113894543)

[Terms and Definitions 2](#_Toc113894544)

[Nexelus Security System (NSS) 2](#_Toc113894545)

[Security Domains 2](#_Toc113894546)

[Nexelus Staff 2](#_Toc113894547)

[Network Services 2](#_Toc113894548)

[Business Continuity and Disaster Recovery 4](#_Toc113894549)

[Business Continuity Plan 5](#_Toc113894550)

[Significant Business Disruptions (SBD) 5](#_Toc113894551)

[Assumptions 5](#_Toc113894552)

[Disaster Recovery Plan 7](#_Toc113894553)

[Nexelus Office 7](#_Toc113894554)

[Key Staff 7](#_Toc113894555)

[Recovery Time Objective (RTO) 7](#_Toc113894556)

[Recovery Point Objective (RPO) 7](#_Toc113894557)

[Maximum Tolerable Outage (MTO) 7](#_Toc113894558)

[Critical Business Services 8](#_Toc113894559)

[Business Continuity and Disaster Recovery Management Team 8](#_Toc113894560)

[Plan Maintenance Procedure 8](#_Toc113894561)

[Disaster Recovery Steps 9](#_Toc113894562)

[Restore Servers in Azure 10](#_Toc113894563)

[A. Create new Servers 10](#_Toc113894564)

[B. Recover Databases 10](#_Toc113894565)

[C. Recover Web Application (Web Server): 11](#_Toc113894566)

# 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):

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

### Nexelus Staff

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

### Network Services

Network services required by our network infrastructure are as follow:

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

# 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 city where Nexelus Office is located.
* 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 within 48 hours after the incident as work from home option.
* Make same office operational or move to alternate office location within 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 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. It is also involved in software development and software support services. Both 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:

* All critical resources have Laptops and Desktops with Nexelus provided VPN connection for Server Access.
* Access to TFS (Server deployed in cloud)
* Access to Web and Database Servers
* One telephone line.
* All critical resources have Internet connection.
* Wired and/or Wireless Local area Network infrastructure.
* Microsoft Windows, Microsoft Office, Visual Studio and Microsoft SQL Server Management Studio are installed and configured on company provided desktops and laptops.

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

If one or more database or application servers crash and become inaccessible for general availability, following steps are performed.

|  |  |  |
| --- | --- | --- |
| 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.