**Business Continuity Plan**

**Nexelus**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Purpose**

This policy establishes procedures to recover Nexelus following a disruption in conjunction with the *Disaster Recovery Plan*.

**Policy**

Nexelus policy requires that:

* A plan and process for business continuity, including the backup and recovery of systems and data, must be defined and documented.
* The Business Continuity Plan shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the process.
* Security controls and requirements must be maintained during all Business Continuity Plan activities.

**Roles and Responsibilities**

This Policy is maintained by the Nexelus Security Officer and Privacy Officer. All executive leadership shall be informed of any and all contingency events.

**Line of Succession**

The following order of succession ensures that decision-making authority for the Nexelus Business Continuity Plan is uninterrupted. The CEO is responsible for ensuring the safety of personnel and the execution of procedures documented within this Plan. The Head of Engineering is responsible for the recovery of Nexelus technical environments. If the CEO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Business Operations Lead shall function as that authority or choose an alternative delegate.

**Response Teams and Responsibilities**

The following teams have been developed and trained to respond to a contingency event affecting Example Corporation infrastructure and systems.

HR & Facilities is responsible for ensuring the physical safety of all Example Corporation personnel and environmental safety at each Example Corporation physical location. The team members also include site leads at each Example Corporation work site. The team leader is the Head of HR who reports to the CEO.

DevOps is responsible for assuring all applications, web services, platforms, and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.

Security is responsible for assessing and responding to all cybersecurity related incidents according to Example Corporation Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the Business Continuity Plan succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any, and all contingency events.

**Policy**

**Business Impact Analysis (BIA)**

The BIA will help identify and prioritize system components by correlating them to the business processes that the system supports. It will allow for the characterization of the impact on the processes if the system becomes unavailable. The BIA has three steps:

* **Determine business processes and recovery criticality.** Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
* **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
* **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.
* See Appendix A for the BIA breakdown.

**Work Site Recovery**

In the event a Nexelus facility is not functioning due to a disaster, employees will work from home or locate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete.

Nexelus’s software development organization has the ability to work from any location with Internet access and does not require an office provided Internet connection.

**Application Service Event Recovery**

Nexelus maintains a status page to provide real time updates and inform customers of the status of each service. The status page is updated with details about an event that may cause service interruption / downtime. Nexelus’s status page:

**<STATUS PAGE URL>**

**APPENDIX A**

**Business Impact Analysis**

**I. System Description**

Nexelus runs most of its operations on Microsoft Azure. The specific services used are Virtual Machines for running Web Servers on Microsoft Windows as well as Microsoft SQL Server Database,

Nexelus runs completely on Amazon Web Services (AWS). The specific services used are EC2 for running servers, RDS for managing databases, S3 for storing unstructured data, CloudWatch/CloudTrail for logging and monitoring, AWS Textract for OCR services.

Nexelus Corporation has no physical office locations and has no business partnerships or system interconnections with the networks of other organizations. All employees and contractors of Nexelus Corporation work remotely within the United States and Pakistan.

Users of Nexelus access the platform by using standard web browsers and navigating to dev.azure.com. There, users are able to login to their account where they can view support dashboard, sync source code with Microsoft DevOps. Users primarily reside in United States and Pakistan.

**II. Data Collection**

Data was collected through email questionnaires sent to the individuals responsible for these business processes.

**STEP 1. Determine Process and System Criticality**

Identify the specific business processes that depend on or support the information system, using input from users, managers, business process owners, and other internal or external points of contact.

|  |  |
| --- | --- |
| **Business Process** | **Description** |
| Employee Onboarding | Employee Onboarding is the process of getting new employees set up within Example Corporation It is the responsibility of Human Resources. |
| Recruiting | Recruiting is the process of finding and interviewing potential new employees for Example Corporation It is the responsibility of Human Resources. |
| Legal Services | Legal Services encompasses functions such as contract review, regulation analysis, and legal counsel. Legal Services are the responsibility of the Legal department. |
| Development Process | Nexelus development is the process of building out new functionality or improving existing functionality for Nexelus. Development of Nexelus product is the responsibility of the Development Department. |
| Support Process | Support is provided to customers over direct phone calls, and through email. All support history is maintained on Microsoft Azure DevOps Dashboard |

|  |  |
| --- | --- |
|  |  |

**Outage Impacts**

Impact categories and values characterize levels of severity to the company that would result for that particular impact category, if the business process could not be performed. These impact categories and values are samples and should be revised to reflect what is appropriate for the organization.

|  |  |  |  |
| --- | --- | --- | --- |
| **Impact** | **High** | **Moderate** | **Low** |
| Cost | > $500,000 | $100,001 - $499,999 | < $100,000 |
| Customer Satisfaction | Loss of greater than 10% of customers | Loss of between 1% - 9% | Loss of little to no customers |
| Legal Impact | Organization is deemed non-compliant with laws or regulations | Organization agrees to unfavorable contract | Contract review is delayed |
| Data Loss | > 10,000 records lost | 100 - 9,999 records lost | 100 or less records lost |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Process** | **Impact Category** | | | | |
|  | **Cost** | **Customer Satisfaction** | **Legal Impact** | **Data Loss** | **Overall Impact** |
| Employee Onboarding | Low | Low | Low | Low | Low |
| Recruiting | Low | Low | Low | Low | Low |
| Legal Services | Moderate | Low | Moderate | Low | Moderate |
| Software Development | Moderate | Low | Low | High | High |
| Support Services | Moderate | High | Low | Low | High |

**Estimated Downtime**

Downtime factors resulting from a disruptive event will be estimated by working directly with business process owners, departmental staff, managers, and other stakeholders. The following downtime categories will be considered:

* **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time managers are willing to accept for a business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on:
  + Selection of an appropriate recovery method; and
  + The depth of detail which will be required when developing recovery procedures, including their scope and content.
* **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.
* **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, to which business process data must be recovered (given the most recent backup copy of the data) after an outage.

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Process** | **MTD** | **RTO** | **RPO** |
| Employee Onboarding | 4 Weeks | 6 Weeks | 6 Weeks |
| Recruiting | 4 Weeks | 6 Weeks | 6 Weeks |
| Legal Services | 1 Week | 72 Hours | 72 Hours |
| Software Development | 1 Day | 2 Days | 2 Days |
| Support Services | 1 Day | 2 Days | 2 Days |

**STEP 2. Identify Resource Requirements**

Identify the resources that compose <system name> in support of business processes, including hardware, software, and other resources such as data files.

|  |  |  |
| --- | --- | --- |
| **System Resource/Impact** | **Platform/OS/version** | **Description** |
| Source Code | Microsoft DevOps | Source Code for Nexelus |
| Web Servers | Azure Virtual Machine / Microsoft Windows | Web Server Environment |
| Database Servers | Azure Virtual Machine / Microsoft Windows / Microsoft SQL Server | Database Server Environment |
| Developer Workstations | Microsoft Windows / Microsoft Visual Studio | Development Workstation Environment |

**STEP 3. Identify Recovery Priorities for System Resources**

List the order of recovery for <system name> resources, and identify the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption. A system resource can be software, data files, servers, or other hardware and should be identified individually or as a logical group.

|  |  |  |
| --- | --- | --- |
| **Priority** | **System Resource / Component** | **RTO** |
| 1 | Servers | 24 Hours |
| 2 | Source Code | 48 Hours |
| 3 | Developer Workstation | 24 Hours |

Any alternate strategies in place to meet expected RTOs will be identified, including backup or spare equipment and vendor support contracts.