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 Team (CTO, Systems Manager). All executive leadership shall be informed of 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. Either the CTO or the Head of Engineering is responsible for the recovery of Nexelus technical environments. If the CEO, CTO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the General Manager Development 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 infrastructure and systems.

HR or the Facilities is responsible for ensuring the physical safety of all personnel and environmental safety at each physical location. The team members also include site leads at each work site. The team leader reports to the CEO, partner, or the General Manager.

Systems Manager and DevOps are 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 CTO or the Head of Engineering/Technology. This team 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 Head of Engineering/Technology.

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 relocate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete.

Nexelus' software development organization has the ability to work from non public location with Internet access and does not require an office provided Internet connection.

Application Service Event Recovery

Nexelus maintains a 24/7 hotline to provide real time updates and informs customers of the status of each service. Any reported or detected downtime is followed by an email sent by the support team to inform customers.

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 some services on Amazon Web Services (AWS).

All employees and contractors of Nexelus work remotely within the United States All employees and contractors of Nexelus work in a hybrid model of working from the office and home in Pakistan.

II. Data Collection

Data was collected through email. Nexelus also has a 24/7 hotline where customers can report system down incident

STEP 1. Determine Process and System Criticality

Microsoft Office 365 and Azure environments are critical systems to maintain business operation.

Outage Impacts and Estimated Downtime

Nexelus SaaS product is hosted on Microsoft Azure. Nexelus maintains a 24/7 hotline for customers to report if the system is down. Nexelus maintains SLA with its clients as follows:

System Availability: NEXELUS shall have the System available for access and to which the COMPANY can access the SYSTEM, its features, functions, and capabilities and under normal operating performance standards, 99.9% of the time each month, excluding any Scheduled Downtime as defined below ("System Availability"). NEXELUS is responsible for connectivity up to and including the point where NEXELUS's hosting facility enters the Internet. NEXELUS will credit CUSTOMER's account 5% of the prorated monthly fee for each 60 minutes of system downtime ("Downtime"), excluding Scheduled Downtime, up to 100% of the prorated monthly fee.

Downtime is measured from the time of COMPANY's notice to NEXELUS of the issue, or otherwise, if sooner, upon discovery by NEXELUS of the issue, and until system availability is restored. COMPANY is not entitled to a credit if the event giving rise to the credit would not have occurred but for COMPANY's material breach of the Agreement.

Notwithstanding anything in this Agreement to the contrary, the maximum total credit for failure of NEXELUS to meet the System Availability guarantee under this Agreement for any calendar month shall not exceed 100% of COMPANY's prorated monthly fees for the Hosted System, and credits that would be available but for this limitation will not be carried forward to future months.

Scheduled Downtime: To maintain this level of availability, NEXELUS proactively performs routine maintenance and system upgrades on a scheduled basis ("Scheduled Downtime"). NEXELUS currently reserves the following scheduled Downtime periods:

Period: Monthly

Reason: Systems Maintenance

Duration: 6 Hours

The actual timing of above Scheduled Downtime can be adjusted based on mutual agreement to avoid system downtime during COMPANY's heavy usage hours. In no case is scheduled downtime to occur without advanced notice or during COMPANY's normal business operating hours.

In any event, both NEXELUS and COMPANY will mutually agree upon specific reserved Scheduled Downtime periods, except for release related downtime which will be determined by NEXELUS (provided NEXELUS provides at least 5 days prior written notice to COMPANY). Notwithstanding the foregoing, all downtime to the System (whether Scheduled Downtime or otherwise) shall be scheduled so as to minimize interference with or disruption to COMPANY's business operations.

System Priorities: On occasion, exceptional circumstances may arise when it is necessary to perform essential planned maintenance outside the time periods defined above and even within the COMPANY's primary hours of operation. Such maintenance will be undertaken only when NEXELUS believes in good faith it to be necessary to prevent an even more serious and disruptive unplanned loss of service.

Wherever and whenever possible a minimum of 24 hours written notice will be given in advance of such a service interruption and in any event shall not occur more frequently than once per calendar month. This provision in no ways limits or alleviates NEXELUS's obligation to meet System Availability as described herein.

STEP 2. Identify Resource Requirements

Identify the resources that are needed 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	Microsoft Windows	Web Server Environment
Database Servers	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 resources and identify the expected time for recovering the resource following a "worst case" (complete rebuild/repair or replacement) disruption.

Priority	System Resource / Component	RTO
1	Servers and other items to bring Nexelus System Online	24 Hours
2	Source Code	48 Hours
3	Developer Workstation	24 Hours

Any alternate strategies to meet expected RTOs can be identified to shorten the recovery time.