Business Continuity and Disaster Recovery (BC/DR)

Policy Owner: [Job title of policy owner]

Effective Date: [Date you choose, after which there will be consequences for personnel for non-compliance]

Purpose

The purpose of this business continuity plan is to prepare nexelus.net in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame.

Scope

All nexelus.net IT systems that are business critical. This policy applies to all employees of nexelus.net and to all relevant external parties, including but not limited to nexelus.net consultants and contractors.

The following scenarios are excluded from the BC/DR plan scope:

- Loss of availability for a production hosting service provider (i.e., [production hosting service provider, e.g., AWS])
- Loss of availability of nexelus.net satellite offices (these will be considered incidents)

In the event of a loss of availability of a hosting service provider, the [driver of the response, e.g., VP of Global Support] will confer with the [assistants for the response, e.g., IT Manager and executive staff] to determine an appropriate response strategy.

Policy

In the event of a major disruption to production services and a disaster affecting the availability and/or security of the nexelus.net office, senior managers and executive staff shall determine mitigation actions.

A disaster recovery test, including a test of backup restoration processes, shall be performed on an annual basis.

Continuity of information security shall be considered along with operational continuity.

In the case of an information security event or incident, refer to the Incident Response Plan.

Alternate Work Facilities

If the nexelus.net office becomes unavailable due to a disaster, all staff shall work remotely from their homes or any safe location.

Communications and Escalation

Executive staff and senior managers should be notified of any disaster affecting nexelus.net facilities or operations.

Communications shall take place over any available regular channels including [list your company's regular communication channels, e.g., Slack, email, phone and online meeting tools].

Key contacts shall be maintained on the on-call schedule and key contacts: [link to wiki page that lists out key contacts]

Roles and Responsibilities

Role	Responsibility
IT Manager	The IT Manager shall lead BC/DR efforts to mitigate losses and recover the corporate network and information systems.
Departmental Heads	Each department head shall be responsible for communications with their departmental staff and any actions needed to maintain continuity of their business functions. Departmental heads shall communicate regularly with executive staff and the IT Manager.
Managers	Managers shall be responsible for communicating with their direct reports and providing any needed assistance for staff to continue working from alternative locations.
VP of Global Support	The VP of Global Support, in conjunction with the CEO and CFO shall be responsible for any external and client communications regarding any disaster or business continuity actions that are relevant to customers and third parties.
VP of Engineering	The VP of Engineering, in conjunction with the VP of Global Support, shall be responsible for leading efforts to maintain continuity of nexelus.net services to customers during a disaster.
Chief HR Officer	The CHRO shall be responsible for internal communications to employees as well as any action needed to maintain physical health and safety of the workforce. The CHRO shall work with the IT Manager to ensure continuity of physical security at the nexelus.net office.

Continuity of Critical Services

Procedures for maintaining continuity of critical services in a disaster can be found in Appendix A.

Strategy for maintaining continuity of services can be seen in the following table:

KEY BUSINESS PROCESS	CONTINUITY STRATEGY
Customer (Production) Service Delivery	Rely on AWS availability commitments and SLAs
IT Operations	Not dependent on HQ. VPN is redundant between HQ and Colo. Critical data is backed up to alternate locations.
Email	Utilize Gmail and its distributed nature, rely on Google's standard service level agreements.
Finance, Legal and HR	All systems are vendor-hosted SaaS applications.
Sales and Marketing	All systems are vendor-hosted SaaS applications.

Plan Activation

This BC/DR shall be automatically activated in the event of the loss or unavailability of the nexelus.net office, or a natural disaster (i.e., severe weather, regional power outage, earthquake) affecting the larger [describe the location of your company's headquarters, e.g., San Francisco, CA] region.

Version	Date	Description	Author	Approved by
[1.0]	[29-Apr-2020]	[First Version]	[OWNER]	[APPROVER]

Appendix A - Business Continuity Procedures by Scenario

Business Continuity Scenarios

HQ Offline (power and/or network)

- CRM, Telephony, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT unaffected
- HQ Staff offline (30-60 minutes)
- Remote Staff unaffected (US)

Procedure:

1. HQ Staff relocate to home offices (30-60 minutes)
2. Verify Telephony, CRM, & Email Connectivity at home offices (10 minutes)
3. Remotely resume normal operations

Colo Offline (power and/or network)

- CRM, Telephony, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT Offline
- Production Database offline (redundant)
- HQ Staff unaffected
- Remote Staff unaffected (US)

Procedure:

1. Notify Customer Base that proactive monitoring is offline
2. Normal operations continue

Disaster Event at HQ (Sunnyvale & Santa Clara)

- CRM, Telephony, Video Conferencing/Screen Share & Corp Email unaffected
- SUPPORT offline
- HQ Staff offline (variable impact)
- Remote Staff unaffected (US)

Procedure:

1. Activate Remote Staff (US)
2. Notify Customer Base of impaired functions & potential delays
3. Commandeer Field Resources for Critical Response (SE Teams)

SaaS Tools Down

- CRM, Telephony, Video Conferencing/Screen Share, or Corp Email Affected
- SUPPORT partially affected (no new cases, manual triage required))
- HQ Staff unaffected
- Remote Staff unaffected (US)

Procedures:

Telephony Down

1. Notify Customer Base to use Support Portal or Email
2. Support Staff use Mobile Phones and/or Land Lines as needed

Email Down (Gmail/Corp Email)

1. Support Staff manually manage ‘case' related communications
2. Support Staff use alternate email accounts as needed (Hotmail)

CRM Down

1. Notify Customer Base that CRM is down
2. Activate ‘Spreadsheet' Case Tracking (Google Sheets)
3. Leverage ‘Production' Database for Entitlements, Case History, Configuration data.

Video Conferencing/ScreenShare Down (Zoom)

1. Support Staff utilize alternate service as needed