

**Neo Enterprise**

Business Continuity Plan

Dhanashree Salvi

cybersecurity consultant

April 28, 2024

Table of Contents

[1.0 Introduction 2](#_Toc165688589)

[1.1 Objective 2](#_Toc165688590)

[2.0 Business Impact Analysis 3](#_Toc165688591)

[2.1 Business functions 3](#_Toc165688592)

[2.2 Threat Identification 3](#_Toc165688593)

[2.2 Maximum Tolerable Downtime 4](#_Toc165688594)

[2.3 Assets and Resources 5](#_Toc165688595)

[3.0 Strategy Development 6](#_Toc165688596)

[3.1 Continuity Plans and Scenarios 6](#_Toc165688597)

[3.2 Health Crisis/Pandemic 6](#_Toc165688598)

[3.2.1 Implementation Plan 6](#_Toc165688599)

[3.3 Major IT system failure 8](#_Toc165688600)

[3.3.1 Implementation Plan 8](#_Toc165688601)

[3.4 Site Unavailability 9](#_Toc165688602)

[3.4.1 Implementation Plan 9](#_Toc165688603)

[4.0 Training and Awareness 11](#_Toc165688604)

[4.1 Communication 11](#_Toc165688605)

[4.1.2 Emergency Declaration and Resolution 12](#_Toc165688606)

[4.2 BCP Testing and Maintenance Schedule 14](#_Toc165688607)

[4.2.1 Change Control Process 14](#_Toc165688608)

[5.0 Conclusion 15](#_Toc165688609)

[6.0 Revision History Table 16](#_Toc165688610)

[Appendices 17](#_Toc165688611)

[Appendix A – Employee Telephone Lists 17](#_Toc165688612)

[Appendix B – Severity Impact Assessments 18](#_Toc165688613)

[References 19](#_Toc165688614)

Figures and Tables

[Table 1 - Business Function & MTD 4](#_Toc165560321)

[Table 2 - List of Assets and Replacements 5](#_Toc165560322)

[Table 3 - Revision History Table 16](#_Toc165560323)

# 1.0 Introduction

Neo Enterprise is a company based in Princeton, NJ. They have around 100 employees who work both in the office and remotely. Neo Enterprise is known for creating software solutions for businesses. We focus on deep industry expertise and a command of the fast-evolving fields of cybersecurity, cloud computing, business analytics, connectivity, software, and digital engineering.

There are 100 employees as of 04/28/2024.

1. Chief Executive Officer
2. Chief Technology Officer
3. Chief Financial Officer
4. Chief Compliance Officer
5. Secretary (4)
6. Marketing Manager, Sales Manager, HR Manager, Supply Chain Manager, Project Manager(4), Social Media Manager
7. Customer Support Specialist (11)
8. Information Security Analyst (5)
9. Marketing Intern (2)
10. Data Analyst (15)
11. Software Developer Engineer (25)
12. Software Test Engineer (25)

## Objective

The objective of the Business Continuity Plan (BCP) is to coordinate recovery of critical business functions in managing and supporting the business recovery in the event of disruption or disaster. This plan is to be invoked during include short or long-term disasters, and natural or man-made disasters.

# 2.0 Business Impact Analysis

It is critical to ensure that Neo Enterprise can continue to serve its clientele and maintain access to data.

## 2.1 Business functions

Prioritizing essential business functions in a business continuity plan is crucial. The following are key business functions that need to be maintained to ensure operational continuity -

1. **Software Development and Quality Assurance -** This is a core service of Neo Enterprises, therefore it is crucial for ensuring and managing software development processes, including coding, testing, deployment, and ongoing maintenance, to deliver high-quality products and services to clients.
2. **Connectivity Solutions -**Ensuring the continuous operation and availability of critical IT systems, networks, and infrastructure to support internal operations and deliver services to clients.
3. **Cybersecurity Solutions -** Implementing cybersecurity measures to protect clients' digital assets and sensitive information.
4. **Customer Management -**Maintaining client databases, communication channels, and support services to foster strong relationships with clients, address their needs, and ensure customer satisfaction, especially if service may be impacted.

## 2.2 Threat Identification

A threat assessment and audit were conducted previously. The following scenarios were considered -

1. **Cybersecurity Breach -**

Description - A cyber attacker gains unauthorized access to Neo Enterprise's network or systems, compromising sensitive data or disrupting operations.

Possible Causes - Phishing attacks, malware infections, weak passwords, unpatched software vulnerabilities.

Impact -Loss or theft of sensitive data, financial losses due to system downtime, damage to reputation and customer trust, regulatory fines, and legal consequences.

1. **Natural Disaster -**

Description - Neo Enterprise's offices or data centers are affected by a natural disaster, leading to infrastructure damage and disruption of services.

Possible Causes - Severe weather events and earthquakes.

Impact - Physical damage to buildings and equipment, loss of data and hardware, temporary or prolonged business interruptions, financial losses from downtime and recovery efforts.

1. **Insider Threat -**

Description- An employee or contractor intentionally or unintentionally compromises Neo Enterprise's security, data, or operations.

Possible Causes - Malicious actions, irresponsible behavior (clicking on phishing links).

Impact - Data breaches, unauthorized access to systems, loss of intellectual property, disruption of operations, damage to reputation, legal liabilities.

1. **Data Loss -**

Description - Accidental deletion, corruption, or loss of critical data due to system failures, human errors, or malicious actions.

Possible Causes - Hardware failures, software bugs, inadequate backup procedures, improper data handling practices, cyberattacks (ransomware, data breaches).

Impact - Loss of important business data, operational disruptions, compliance violations, financial losses (recovery costs, regulatory fines), damage to reputation.

## 2.2 Maximum Tolerable Downtime

Table 1 outlines the important business functions, and their respective maximum downtime.

|  |  |
| --- | --- |
| Business Function | MTD |
| Software Development and Quality Assurance -[Core service] – Any MTD longer than this could impact client trust and contractual obligations. | 48 hours |
| Connectivity Solutions– If connectivity is disrupted for longer than the MTD then this could impact all the business function. | 72 hours |
| Cybersecurity Solutions -Data must be accessible at all times to ensure services continuity and to maintain client trust. | 24 hours |
| Customer Management– Effective communications and a rapid response is critical to maintaining client relationships. It is crucial to keep projects moving, especially if they are time sensitive. | 48 hours |

Table 1 - Business Function & MTD

## 2.3Assets and Resources

Table 2 outlines the assets that may be harmed in a manmade or a natural disaster. The table also lists alternatives to the physical assets.

|  |  |
| --- | --- |
| Asset | Replacement (if any) |
| Laptops & Computers – 70% of employees have a laptop and remaining are assigned with computers. | Employees will be provided with temporary asset if the issue is not resolved within 24 hours. |
| Mobile Phones – All the leadership management and their secretaries has been provided smart phones for work related purposes. | Employees may use their personal mobile while the company assets are down. Employees will be reimbursed at the current federal rate. |
| Productivity Suite – currently managed by Microsoft (Office365). | Contact IT Help Desk and Microsoft with any issues. |
| Cloud Data Storage – currently managed by Microsoft Azure cloud services. | Contact cloud team and Microsoftwith any issues. |
| Surveillance Camera – Arlo company manages it. | Contact Arlo for a replacement. They will provide with the replacement on the next business day. |

Table 2 - List of Assets and Replacements

# 3.0 Strategy Development

## 3.1 Continuity Plans and Scenarios

It is not possible to think of every scenario. The list below is not an exhaustive list. Additionally, the threat landscape is constantly changing. When a disaster arises, the president or their delegate should consider what is lost as a result of this threat. The current document covers the following -

**Health Crisis/Pandemic -**

Description - Outbreak of a contagious disease (e.g., COVID-19) leading to health-related disruptions, quarantines, remote work mandates, and impacts on workforce availability.

Impact - Reduced workforce capacity, remote work challenges, supply chain disruptions, changes in customer demand, operational slowdowns.

**Major IT System Failure -**

Description - Critical failures in core IT systems, such as ERP systems, databases, or cloud infrastructure, leading to data loss, transaction failures, or service interruptions.

Impact - Business process disruptions, financial losses, customer dissatisfaction, reputational damage, IT recovery and restoration efforts.

**Site unavailability -**

Description -This scenario involves the physical unavailability of office spaces required for business operations. This includes any location used for office work, meetings, or other business functions.

Impact -Impact on customer service, communication channels, and loss of potential sales opportunities.

## 3.2 Health Crisis/Pandemic

## 3.2.1 Implementation Plan

In case of a pandemic, the following actions need to be taken.

**Implement Remote Work Infrastructure**

**Who**– IT Department (IT Manager, IT Support Team) will set-up Infrastructure

**What** - Set up remote access tools (VPN, remote desktop solutions) and ensure employees have necessary equipment (laptops, secure internet connections).

**When** - Before a health crisis occurs and as soon as a crisis is anticipated.

**How** - Configure VPNs, provide remote access training, establish communication channels (email, chat, video conferencing).

**Where** - IT department configures systems remotely, employees work from their homes or designated remote locations.

**Develop and Communicate Remote Work Policies**

**Who** - HR Department (HR Manager) will communicate and develop policies and procedures.

**What** - Create policies for remote work expectations, attendance tracking, cybersecurity guidelines, and data protection measures.

**When** - Before remote work implementation and ongoing updates as needed.

**How** - Draft policy documents, conduct training sessions, distribute guidelines through company intranet/email.

**Where** - HR department develops policies, employees access guidelines electronically.

**Ensure Business Operations Continuity**

**Who** - Department Heads (Marketing Manager, Sales Manager, Project Manager, etc.) will ensure the business continuity.

**What** - Identify critical business functions and develop continuity plans for each department.

**When** - Before and during a health crisis.

**How** - Prioritize key tasks, allocate resources, cross-train employees, establish backup processes.

**Where** - Department heads coordinate plans within their teams and communicate updates virtually.

**Enhance Communication Channels**

**Who** - Communications Team (Communications Manager) will establish, enhance the communication channels.

**What**- Establish clear communication protocols, update contact lists, and create a crisis communication plan.

**When** - Before and during a health crisis.

**How** - Set up emergency notification systems, conduct regular updates through email, intranet, and other channels.

**Where**- Communications team manages communication platforms, employees access information remotely.

**Monitor Employee Well-being**

**Who** - HR Department (HR Manager, Employee Relations Team) will monitor the employee’s well-being.

**What** - Implement wellness checks, mental health support programs, and flexible work arrangements.

**When** - Throughout the health crisis and recovery period.

**How** - Conduct regular check-ins, provide resources for stress management, promote work-life balance.

**Where** - HR department coordinates wellness initiatives, employees access support resources remotely.

## 3.3Major IT system failure

### 3.3.1 Implementation Plan

**Identify Critical Systems and Dependencies**

**Who** - IT Department (Systems Analyst, IT Managers) will be responsible for identifying dependencies and critical system.

**What** - Identify critical IT systems, applications, and dependencies across departments.

**When** - Regularly as part of IT asset management and risk assessments.

**How** - Conduct interviews, review documentation, and use IT management tools to map dependencies.

**Where** - IT department analyzes systems and dependencies within the organization.

**Develop Redundancy and Backup Plans**

**Who** - IT Department (Infrastructure Team, Backup Administrators) will be responsible for developing backup plans.

**What**- Implement redundancy measures, backup solutions, and data recovery plans for critical systems.

**When** - Before any major system failure and regularly updated.

**How** - Set up redundant servers, cloud backups, scheduled backups, and test data recovery procedures.

**Where** - IT department configures redundancy and backup systems in data centers or cloud platforms.

**Establish Incident Response Team**

**Who**-Information Security Analyst will establish incident response team.

**What**- Form an incident response team with clear roles, responsibilities, and escalation procedures.

**When** - Before a major IT system failure occurs and during incident response.

**How** - Define incident severity levels, create response playbooks, conduct training and simulations.

**Where** - Incident response team coordinates virtually or in designated incident response areas.

**Implement Business Continuity and Recovery Plans**

**Who** - IT Department, Department Heads (IT Managers, Department Managers) will oversee and implement continuity and recovery plans.

**What** - Execute business continuity plans, activate backup systems, and restore services to minimize downtime.

**When** - Immediately after identifying a major IT system failure.

**How** - Follow predefined recovery procedures, restore data from backups, test system functionality.

**Where** - IT department conducts recovery operations in data centers or cloud environments.

## 3.4Site Unavailability

### 3.4.1 Implementation Plan

**Activate Backup Site**

**Who** - IT Department (IT Manager, System Administrators) will set up backup sites.

**What** - Activate the backup site or mirror server to host the company website and essential services.

**When** - Immediately upon detecting site unavailability.

**How** - Use automated failover systems or manual switching to redirect traffic to the backup site.

**Where** - IT team manages and monitors the backup site remotely or at an off-site data center.

**Monitor Site Performance**

**Who** - IT Department (Monitoring Team) will monitor site performance.

**What**- Continuously monitor the performance and availability of the backup site.

**When** - Throughout the duration of the site unavailability.

**How** - Use monitoring tools to track site uptime, response times, and user interactions.

**Where** - Monitoring team operates from the IT department or a central monitoring center.

**Investigate Root Cause**

**Who** - IT Security and Operations Teams will perform the root cause analysis.

**What** - Investigate the root cause of the site unavailability (e.g., server failure, DDoS attack, network issues).

**When** - Concurrently with site recovery efforts.

**How** - Analyze server logs, network traffic, and security alerts to identify and mitigate the issue.

**Where** - IT teams collaborate within the IT department or a dedicated incident response center.

**Implement Redundancy Measures**

**Who** - IT Infrastructure Team will implement redundancy measures.

**What** - Enhance redundancy for critical systems, implement load balancing, and optimize server configurations.

**When** - After resolving the site unavailability issue and during downtime maintenance windows.

**How** - Configure failover systems, distribute traffic across multiple servers, and conduct regular system audits.

**Where** - IT team performs infrastructure enhancements within data centers or cloud environments.

# 4.0 Training and Awareness

At Neo Enterprise, training and awareness plan for Business Continuity includes comprehensive programs aimed at educating employees on how to respond effectively to emergency situations. For cyber-attacks, training modules cover recognizing phishing attempts, reporting suspicious emails or activities promptly, practicing good password hygiene, and identifying malware signs. In the event of a cyber incident, employees are trained on proper incident reporting procedures and escalation paths to our IT Security team.

Training also includes evacuation procedures, assembly points, emergency contact information, and roles and responsibilities during crisis situations. Employees are educated on using emergency communication channels such as mobile alerts, internal messaging platforms, and designated emergency contact persons within the organization and external emergency services if needed. Regular drills and simulations reinforce these procedures, ensuring employees are prepared to act swiftly and effectively during emergencies, safeguarding both their safety and company assets.

## 4.1 Communication

Communication Plan for Business Continuity at Neo Enterprise -

1. **Leadership Team (CEO, CTO, CFO, CCO) -**
   1. Responsible for overall decision-making during emergencies.
   2. Authorized to speak with law enforcement, media, clients, and the public as per established protocols.
   3. Internal communication through secure channels and regular updates to all employees.
2. **Secretary -**
   1. Acts as a central point of contact for internal communications and relays messages from the leadership team to employees.
   2. Supports coordination efforts and ensures timely dissemination of critical information.
3. **Department Managers (Marketing, Sales, HR, Supply Chain, Project, Social Media) -**
   1. Communicate with their respective teams regarding safety protocols and operational instructions.
   2. Coordinate with the leadership team for external communications, as necessary.
4. **Customer Support Specialist -**
   1. Communicates with clients regarding service disruptions, alternative solutions, and updates during emergencies.
   2. Directs client inquiries to appropriate departments or designated spokespersons as needed.
5. **Information Security Analyst, Software Developers, Software Test Engineers, Data Analyst -**
   1. Collaborate to address IT-related incidents, system downtime, data breaches, or cyber-attacks.
   2. Maintain communication channels for technical updates and recovery progress to relevant stakeholders.
6. **Marketing Intern, Social Media Manager -**
   1. Coordinate with the marketing team and leadership for external messaging on social media platforms.
   2. Monitor and respond to public inquiries or concerns during emergencies, following established guidelines.

**Before an Incident -**

* 1. Conduct regular training sessions and drills to familiarize employees with emergency protocols and communication procedures.
  2. Ensure contact lists, emergency response plans, and communication channels are up to date.

**During an Incident -**

* 1. Activate the crisis management team and follow established incident response protocols.
  2. Communicate regularly with employees, providing updates, safety instructions, and status reports.

**After an Incident -**

* 1. Conduct post-incident reviews to assess communication effectiveness and identify areas for improvement.
  2. Communicate lessons learned, recovery progress, and follow-up actions to employees, clients, and stakeholders.

### 4.1.2 Emergency Declaration and Resolution

Emergency Declaration and Resolution Plan for Neo Enterprise -

**Emergency Declaration -**

The power to declare an emergency is with the CEO or an appointed senior executive in their absence, such as the CTO or CFO. In the case of specific types of emergencies, the information security analyst may initiate the emergency declaration process in sconsultation with senior management.

**Criteria for Declaration -**

1. A significant disruption to critical business operations or services.
2. Threats to employee safety, such as natural disasters, physical security breaches, or health emergencies.
3. Breaches of cybersecurity leading to data loss, unauthorized access, or system compromise.

**Emergency Resolution -**

The CEO, in coordination with the leadership team, holds the authority to declare the end of an emergency.The information security analyst, in the case of cybersecurity incidents, works with the IT team and senior management to confirm resolution and system stability.

**Criteria for Resolution -**

1. Restoration of critical business functions or services to an acceptable operational level.
2. Mitigation of safety threats and assurance of employee well-being.
3. Successful containment and remediation of cybersecurity incidents with verified system integrity.
4. Compliance with legal and regulatory requirements related to incident reporting and resolution timelines.

**Process for Declaration and Resolution -**

Upon identification of an emergency situation, designated personnel assess the severity and impact. If warranted, the CEO or designated senior executive formally declares the emergency. Immediate communication is initiated with relevant authorities, including employees and clients.

The emergency response team implements predefined mitigation and recovery measures to address the emergency's effects. Regular status updates are provided to the leadership team and stakeholders throughout the resolution process. Once the criteria for resolution are met, the CEO or designated authority formally declares the end of the emergency. Post-incident analysis and documentation are conducted to capture lessons learned and improve future response capabilities.

## 4.2 BCP Testing and MaintenanceSchedule

Below are planned maintenance and testing plan for BCP -

1. **Annual Updates -**

a. **Relevant Personnel -** All employees, led by the CEO.

b. **Activities -**

i. Review and update contact information and communication plans.

ii. Review and update critical business processes, recovery strategies, and priorities.

iii. Conduct a full-scale review of the BCP, including risk assessments and lessons learned from the previous year.

iv. Schedule and plan training sessions or awareness programs related to the BCP.

c. **Documentations -** Update and maintain the BCP documentation, including contact lists, recovery procedures, and training materials.

1. **Bi-annual Tests -**

a. **Relevant Personnel -** All employees, led by the CEO.

b. **Activities -**

i. Conduct tabletop exercises simulating various disaster scenarios and crisis responses.

ii. Perform functional tests of critical systems, communication channels, and backup solutions.

c. **Documentations -** Document test results, identify gaps or areas for improvement, and update the BCP accordingly.

1. **Quarterly Reviews -**

a**. Relevant Personnel -** All employees, led by the CEO.

b. **Activities -**

i. Review incident reports and recovery actions taken since the last review.

ii. Conduct spot checks on critical processes or systems to ensure readiness.

* 1. **Documentations -** Document review findings, track progress on action items, and update risk assessments as needed.

## 4.2.1 Change Control Process

The change control process ensures that all changes to this plan are properly vetted and documented. The change control process consists of -

1. Proposed changes are submitted through formal change requests to the Information Security Analyst, detailing the nature, scope, justification, and potential impact of the change.
2. The Change Management Board evaluates each change request to assess feasibility, risks, and alignment with business objectives, granting formal authorization for approved changes. The change request could require approval from the CTO and the Legal Advisor if compliance is involved.
3. Approved changes should be scheduled for implementation. Detailed implementation plans are developed, outlining steps, resources, and timelines. Changes are executed according to plan, with coordination from the Change Coordinator.
4. Progress is monitored throughout implementation, with regular updates provided to stakeholders. Post-implementation reviews assess effectiveness and identify lessons learned.
5. Comprehensive documentation is maintained for each change, including requests, approvals, plans, and reviews. Changes are formally closed once successfully implemented and validated.
6. Employees and other internal stakeholders are then notified once the timeline approaches. Notification occurs via an emailed link to a webpage that outlines the changes with an “I acknowledge” button.
7. If the changes impact external parties, then they are notified via a link to a webpage that outlines the changes with an “I acknowledge” button.
8. Previous versions are then archived, and the revision history table is updated to reflect the newest version number.
9. Lessons learned from post-implementation reviews are used to refine and improve the change control process over time, ensuring its effectiveness and efficiency.

# 5.0 Conclusion

The Business Continuity Plan for Neo Enterprise encompasses a range of critical components designed to ensure the organization's resilience in the face of various disruptions. By addressing scenarios such as natural disasters, cybersecurity breaches, site unavailability, and health crises, the plan outlines specific strategies and tasks to maintain continuity of operations, protect critical assets, and safeguard employee well-being. Key elements include remote work infrastructure readiness, communication protocols, data backup and recovery procedures, and cross-functional collaboration among departments.

By proactively identifying vulnerabilities, establishing clear roles and responsibilities, and regularly testing and updating the plan, Neo Enterprise demonstrates a commitment to operational excellence, customer trust, and long-term sustainability in the face of disruptions, ultimately ensuring business continuity and resilience in an ever-changing environment.

# 6.0 Revision History Table

The table below includes the revision history for this document.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Changes |
| v 0.1.0 | Dhanashree Salvi | 04.28.24 | First draft |
| v 0.2.0 | Dhanashree Salvi | 04.29.24 | Updated Implementation Plan |
| v 1.0.0 | Dhanashree Salvi | 05.01.24 | Presented documents to CEO, and made changes requested |
| v 2.0.0 | Dhanashree Salvi | 05.04.24 | Version approved by CEO |

Table 3 - Revision History Table

# Appendices

## Appendix A – Employee Telephone List

|  |  |  |  |
| --- | --- | --- | --- |
| Employee | Title/Function | Office Phone # | EMAIL |
| Amy Santiago | Chief Executive Officer (CEO) | +1 2739797639 | Walter@neo.com |
| Jake Peralta | Chief Technology Officer (CTO) | +1 8362649341 | Jake@neo.com |
| Walter White | Chief Financial Officer (CFO) | +1 8354710873 | Amy@neo.com |
| James Blunt | Chief Compliance Officer (CCO) | +1 6382904739 | James@neo.com |
| Dave Cooper | Secretary | +1 2846378321 | Dave@neo.com |
| Fire, Police, Emergency |  | **911** |  |

Table 4–Employee Telephone Lists

## Appendix B –Severity Impact Assessment

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | Severity of Impact | | | | | | |
|  | | | ***Least ------>*** | | ***to ------>*** |  | **Greatest** | **Comment** |
|  | **Impact Area** | | **1** | **2** | **3** | **4** | **5** |  |
| 1 | **Major IT system failure** | |  | **2** |  |  |  |  |
| 2 | **Inoperative Financial Controls** | |  |  |  | **4** |  |  |
| 3 | **Loss of Customers** | |  |  |  |  | **5** |  |
| 4 | **Increases in Liability** | |  |  |  | **4** |  |  |
| 5 | **Loss of Public Image** | |  |  |  | **4** |  |  |
| 6 | **Customer Liability & Relations** | |  |  |  |  | **5** |  |
| 7 | **Staff Resignations** | | **1** |  |  |  |  |  |

Table 5–Severity Impact Assessments

# References

1. <https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/business-continuity-planning.pdf>
2. <https://www.capgemini.com/in-en/insights/research-library/the-importance-of-business-continuity-during-times-of-upheaval/>
3. https://www.capgemini.com/wp-content/uploads/2017/07/bc\_continuity\_whitepaper.pdf
4. <https://www.caloes.ca.gov/PlanningPreparednessSite/Documents/Business%20Continuity%20Plan%20Template%20Ver.%201.0.docx>
5. <https://www.digitalcarehub.co.uk/resource/creating-and-testing-a-business-continuity-plan-for-data-and-cyber-security/>
6. <https://www.enisa.europa.eu/publications/example-bcp-template>
7. <https://my.interactive.com.au/rs/590-NET-294/images/BC-2019-04-23-Business%20Continuity%20Plan%20Template.pdf>