Nimonik

Nimonik Business CIP Process & Internal Security Policies Summary (Public)

Document Authorization

____
Steven Herry
Operations Manager

Version:	v1.0
Date of Version:	07/16/2024
Created by:	Steven Herry
Approved by:	Steven Herry
Classification Level:	Public

Hello Dear Customer,

As briefly outlined per our ISMS and Privacy Policy webpages, Nimonik we take IT security very seriously and we are always improving our procedures and processes to maximize our IT robustness and client satisfaction.

At Nimonik, the Chief Executive Officer (CEO), Jonathan Brun, holds the highest authority within the organization and is responsible for ensuring compliance with and implementation of compliance to applicable laws and regulations governing data protection and protection of personal information. Jonathan Brun, CEO is in charge of the protection of personal information. However, Jonathan Brun also delegates this responsibility, in whole or in part, to other members of the organization, such as the Operations Manager or the Risk Manager, to ensure effective management and compliance.

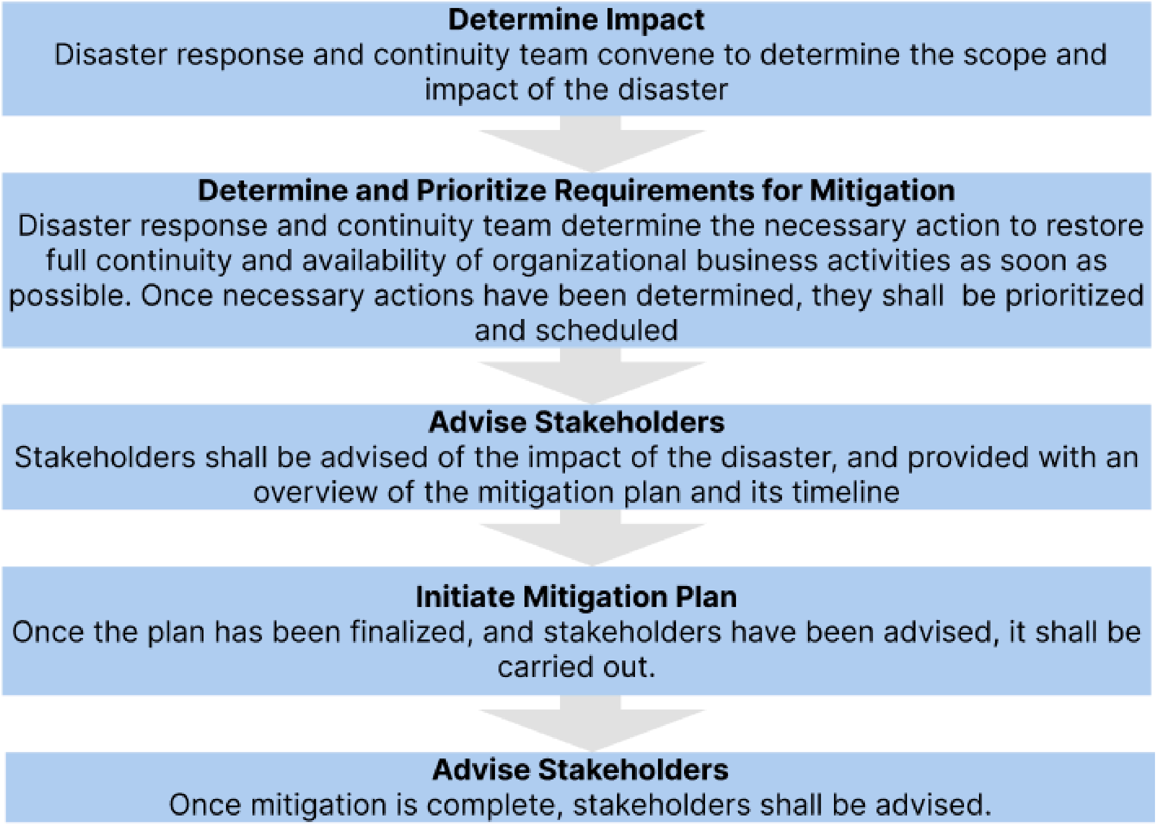
Here's a summary of your business continuity process and internal security policies, tailored for Nimonik's impending ISO certification:

Business Continuity Process

1. **Risk Assessment and Business Impact Analysis (BIA)**:
    - **Identify Risks**: We assess potential threats and vulnerabilities and plan accordingly as per our Risk Management Plan (P-600), our Risk Register (F-800)
    - **Impact Analysis**: We evaluate the impact of these risks on critical business functions and processes.

2. **Developing Business Continuity Strategies**:
    - **Resource Allocation**: As per our Continuity / Disaster Recovery Plan (P-603), we Identify and allocate resources necessary for maintaining and restoring business operations.
    - **Recovery Strategies**: We have put in place solutions for data backup and resource availability and the organization shall coordinate communications, keeping in mind the Incident Response Plan (P-601).

3. **Business Continuity Plan (BCP) Development**:
    - **Documentation**: As per our Continuity / Disaster Recovery Plan (P-603), we have a comprehensive BCP policy outlining procedures for maintaining business operations during and after a disruption.



Determine Impact
Disaster response and continuity team convene to determine the scope and impact of the disaster

Determine and Prioritize Requirements for Mitigation
Disaster response and continuity team determine the necessary action to restore full continuity and availability of organizational business activities as soon as possible. Once necessary actions have been determined, they shall be prioritized and scheduled

Advise Stakeholders
Stakeholders shall be advised of the impact of the disaster, and provided with an overview of the mitigation plan and its timeline

Initiate Mitigation Plan
Once the plan has been finalized, and stakeholders have been advised, it shall be carried out.

Advise Stakeholders
Once mitigation is complete, stakeholders shall be advised.

- **Roles and Responsibilities**: We define roles and responsibilities for team members during a crisis.
- **Testing**: We conduct annual tests of the effectiveness of the BCP and make necessary adjustments.

4. **Plan Maintenance and Continuous Improvement**:
   - **Regular Reviews**: Review and update the BCP regularly to address new risks and any potential changes in business operations.
   - **Feedback Loop**: Incorporate feedback from drills, incidents, and audits to continuously improve the BCP.

Internal Security Policies

Nimonik has put in place an internal IS / IT Policy (P-602) that all employees must respect.

1. **Information Security Policy (P-602)**:
    - **Data Protection**: Implement measures to protect sensitive data from unauthorized access, disclosure, alteration, and destruction.
    - **Access Control Policy (A-007)**: Restrict access to systems and monitor this via our and data based on roles and responsibilities.

2. **Physical Security Policy (A-008)**:
    - **Access Control**: Secure physical access to the company's premises are limited and controlled by secure Smartlock.
    - **Environmental Controls**: We Ensure appropriate environmental controls (e.g., fire suppression, climate control) are in place.

3. **Security Incident Response Plan (P-601)**:
    - **Incident Identification**: Establish internal and external procedures for detecting and reporting security incidents via our security@nimonik.com email, as well as our Incident & Risk IT and ISMS Reporting Form (F-801) available.
    - **Response and Recovery**: Define steps for responding to incidents, mitigating impact, and recovering systems and data as per our Security Incident Response Plan (P-601) and Law 25 Action Plan 2024 (A-005)

4. **Data Backup and Recovery Policy**:
    - **Backup Procedures**: Nimonik implements regular data backup procedures as per our Continuity / Disaster Recovery Plan (P-603) to ensure data can be restored in case of loss.
    - **Recovery Testing**: We test backup and recovery processes regularly as per our KPI Dashboard to ensure data integrity and availability.

5. **Network Security Policy**:
    - **Intrusion Detection and notification**: We have enabled network segregation as well as set-up Intrusion detection and monitoring via Google Workspace which is ISO compliant.
    - **Password Encryption**: Bitlocker encryption and encryption of sensitive data via 1Password for secure storage

6. **Employee Security Awareness Training**:
    - **Training Programs**: We have recently revamped our IT and ISMS training and conduct regular security awareness training for employees to recognize and respond to security threats.

7. **Personal Information Compliance:**
    - **Access Control**: Restrict access to personal data based on roles and responsibilities as per our Employee and Contractor Accesses (A-011), ensuring only authorized personnel can access sensitive information.
    - **Compliance**: As per our Procedure for Accessing and Disposal of Personal Information (P-00$), Regulatory Compliance Policy (A-005) and Privacy Policy, we adhere to data privacy regulations (e.g., GDPR, CCPA) when handling personal information.

8. **Vendor Management Policy**:
    - **Vendor Assessment**: We evaluate vendors' security practices and ensure they meet Nimonik's security standards as per our Control of External Providers and Supplier Onboarding Policy (P-802), Nimonik Supplier Offboarding Policy (A-018) and Approved Supplier List (F-802).
    - **Contracts and Agreements**: All employees and contractors adhere to security requirements in contracts and agreements.

By adhering to these processes and applying these policies, Nimonik can ensure robust business continuity and maintain high standards of internal security, crucial for obtaining and retaining ISO certification.

How to reach Nimonik about security concerns?

As mentioned above, Nimonik takes security concerns very seriously!

The best way to reach out regarding critical security issues is the following:

Call your Account Executive or our Main Office at +1 888-608-7511.

OR

Send an email to security@nimonik.com and copy (cc) your main point of contact at Nimonik. Additionally you can attach a screenshot or provide any other documentation/links/evidence regarding the issue so that the security team can take appropriate action.

We are happy to announce that our external ISO audit has not found any major unconformities!

Thank you for your support !

Nimonik Inc
info@nimonik.com
+1 888-608-7511

Version History

V 1.0	07/16/2024	Steven Herry	Created Document