This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the outlined image.

Cybersecurity Business Continuity Policy Template

Choose Classification

DATE:	Click here to add date
VERSION:	Click here to add text
REF:	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>’s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual’s full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual’s full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This policy aims to define the detailed cybersecurity requirements related to <organization name>'s business continuity in order to minimize the cybersecurity risks resulting from internal and external threats in <organization name> and to preserve confidentiality, integrity and availability.

The requirements in this policy are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all information and technology assets in <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1- General Requirements

1-1 Continuity of Cybersecurity systems and procedures at <organization name> must be ensured.

1-2 Assessment of risks that may affect business continuity of <organization name> must be performed.

1-3 Vulnerabilities must be addressed to avoid incidents that may affect business continuity of <organization name>.

1-4 Legal and regulatory requirements related to business continuity at <organization name> must be defined.

1-5 Cybersecurity incident response plans that may affect business continuity of <organization name> must be developed.

1-6 Supply chain continuity plans must be included in <organization name>'s business continuity plans.

1-7 Disaster Recovery Plans must be developed.

1-8 High risk cybersecurity incidents must be included as a rationale for activating Business Continuity Plan at <organization name>.

1-9 Communication means dedicated for the cybersecurity team must be included and documented in <organization name>, both internal and external means.

1-10 Roles and responsibilities of business continuity related parties in <organization name> must be defined.

1-11 Implementation and monitoring plans for cybersecurity responsibilities and actions during disasters and until conditions return to normal must be developed.

1-12 Identity and Access on all systems and data hosted on the disaster recovery site of <organization name> must be managed to ensure they are not being accessed by unauthorized persons.

1-13 Implementation of Cybersecurity Controls must be ensured as per <organization name> and NCA requirements such as (ECC-1:2018, CSCC-1:2019) and best global practices at <organization name> DRC environment.

1-14 Use KPI to ensure continuous improvement and proper and effective use of cybersecurity business continuity requirements.

2- Critical Systems and Cloud Computing Systems

2-1 Business Impact Analysis must be conducted to define critical systems in <organization name> and copy them to the disaster recovery site.

2-2 <Organization name>'s critical systems must be included in the disaster recovery plans.

2-3 Disaster recovery centre for critical systems must be established.

2-4 Periodic tests must be conducted to ensure effectiveness of disaster recovery plans for <organization name> critical systems at least once a year.

2-5 Requirements for periodic backup of critical systems must be defined to the recovery centre.

2-6 Disaster recovery and business continuity procedures related to cloud computing must be developed, implemented and include the relevant requirements in <organization name> contracts and agreements with third parties and cloud service providers.

2-7 Annual Live DR Test for critical systems must be conducted, whenever possible.

Roles and Responsibilities

1- **Policy Owner:** <head of the cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <business continuity function>, <IT function>, and <cybersecurity function>

4- **Policy Compliance Measurement**: <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this policy on a regular basis.

2- All personnel at <organization name> must comply with this policy.

3- Any violation of this policy may be subject to disciplinary action as per <organization name>'s procedures.