[Company]

BUSINESS CONTINUITY POLICY

Business continuity management

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Business Continuity Policy

3.1 Purpose

The purpose of this policy is business continuity management and information security continuity. It addresses threats, risks and incidents that impact the continuity of operations.

3.2 Scope

All employees and third-party users.

All devices used to access, process, transmit or store company information.

3.3 Principle

The Business Continuity Policy requires:

People's safety to be our first priority. Always.

The framework is based on industry best practice and the business continuity standard ISO 22301 Business Continuity Management.

3.4 Commitment and Continual Improvement

The company is committed to the development and the continual improvement of the business continuity process, plans and system.

3.5 Business Impact Analysis

Business continuity is based on a documented business impact analysis and risk assessment.

3.6 Business Continuity Plans

The company has documented procedures for responding to a disruptive incident and how it will continue or recover its activities within a predetermined timeframe. Such procedures address the requirements of those who will use them.

3.6.1 Business Continuity Plans Cover

Roles and responsibilities

Incident Management processes

Business priority of recovery

Information and system back up processes.

3.6.2 Business Continuity Plans Contain

The business continuity plans collectively contain

- defined roles and responsibilities for people and teams having authority during and following an incident,
- a process for activating the response,
- details to manage the immediate consequences of a disruptive incident giving due regard to
    1. the welfare of individuals
    2. strategic, tactical, and operational options for responding to the disruption, and
    3. prevention of further loss or unavailability of prioritized activities
- details on how and under what circumstances the organization will communicate with employees and their relatives, key interested parties and emergency contacts,
- how the organization will continue or recover its prioritized activities within predetermined timeframes,
- details of the organization’s media response following an incident, including
    1. a communications strategy
    2. preferred interface with the media,
    3. guideline or template for drafting a statement for the media, and
    4. appropriate spokespeople.
- a process for standing down once the incident is over.

Each plan shall define

- purpose and scope,

- objectives,
- activation criteria and procedures,
- implementation procedures,
- roles, responsibilities, and authorities,
- communication requirements and procedures,
- internal and external interdependencies and interactions,
- resource requirements, and
- information flow and documentation processes.

3.7 Recovery

The company has documented procedures to restore and return business activities from the temporary measures adopted to support normal business requirements after an incident.

3.8 Business Continuity Testing

Business continuity plans are tested at least annually and / or when significant change occurs.

3.9 Incident and Business Continuity Reporting and Escalation

An incident management process is in place followed.

Business continuity incidents are additionally recorded and tracked in a register.

Business continuity incidents are additionally reported to the Management Review Team.

3.10 Disaster Recovery Plans

Technical recovery plans for disaster recovery are in place and tested.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.