Business Continuity Policy

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.

Scope

All employees and third-party users.

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

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.

Commitment and Continual Improvement

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

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.

Business Continuity Plans Cover

Roles and responsibilities

Incident Management processes

Business priority of recovery

Information and system back up processes.

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,
- 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.

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.

Business Continuity Testing

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

Disaster Recovery Plans

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

Policy Compliance

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.

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.

Non-Compliance

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

This policy, and matters arising from it are reviewed annually and are the responsibility of Peter James, Director.

Areas of the ISO27001 Standard Addressed

Business Continuity Policy Relevant ISO27001 Controls Mapping

ISO27001:2022	ISO27002:2022	ISO27001:2013/2017	ISO27002:2013/2017
ISO27001:2022 Clause 5 Leadership ISO27001:2022 Clause 5.1 Leadership and commitment ISO27001:2022 Clause 5.2 Policy ISO27001:2022 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2022 Clause 7.3 Awareness	ISO27002:2022 Clause 5 Organisational Controls ISO27002:2022 Clause 5.1 Policies for information security ISO27002:2022 Clause 5.36 Compliance with policies, rules, and standards for information security ISO27002:2022 Clause 5.4 Management Responsibilities ISO27002:2022 Clause 5.29 Information security during disruption ISO27002:2022 Clause 5.30 ICT readiness for business continuity ISO27002:2022 Clause 6 People Controls	ISO27001:2013/2017 Clause 5 Leadership ISO27001:2013/2017 Clause 5.1 Leadership and commitment ISO27001:2013/2017 Clause 5.2 Policy ISO27001:2013/2017 Clause 6.2 Information security objectives and planning to achieve them ISO27001:2013/2017 Clause 7.3 Awareness	ISO27002:2013/2017 Clause 5 Information security policies ISO27002:2013/2017 Clause 5.1 Management direction for information security ISO27002:2013/2017 Clause 5.1.1 Policies for information security ISO27002:2013/2017 Clause 5.1.2 Review of the policies for information security ISO27002:2013/2017 Clause 7 Human resource security ISO27002:2013/2017 Clause 7.2.1 Management Responsibilities ISO27002:2013/2017 Clause 7.2.2 Information security awareness, education, and training ISO27002:2013/2017 Clause 7.2.3 Disciplinary process

	ISO27002:2022 Clause 6.3 Information security awareness, education, and training ISO27002:2022 Clause 6.4 Disciplinary process ISO27002:2022 Clause 8 Technological Controls ISO27002:2022 Clause 8.13 Information Backup ISO27002:2022 Clause 8.14 Redundancy of Information Processing Facilities		ISO27002:2013/2017 Clause 12 Operations Security ISO27002:2013/2017 Clause 12.3 Backup ISO27002:2013/2017 Clause 12.3.1 Information Backup ISO27002:2013/2017 Clause 17 Information security aspects of business continuity management ISO27002:2013/2017 Clause 17.1 Information security continuity ISO27002:2013/2017 Clause 17.1.1 Planning information security continuity ISO27002:2013/2017 Clause 17.1.2 Implementing information security continuity ISO27002:2013/2017 Clause 17.1.3 Verify, review, and evaluate information security continuity ISO27002:2013/2017 Clause 17.2 To ensure availability of information processing facilities. ISO27002:2013/2017 Clause 17.2.1 Availability of information processing facilities