IT business continuity

**1. Subject**

**1.1 Purpose**

**1.2 Scope**

**1.3 Glossary**

**2. Responsibility**

**3. Documents**

**3.1 Processes and policies**

**3.2 Records**

**4. Requirements of ISO 27001: 2022**

**5. Development**

**5.1 Preparation**

**5.2 Implementation**

**5.3 Verification**

History

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| All | Creation | 01/01/2023 |
| **Page** | **Change** | **Date** |

**1. Subject**

**1.1 Purpose**

The purpose of this procedure during a disruption is to:

* protect information and other associated assets
* ensure the availability of the organization's information and other associated assets

**1.2 Scope**

The scope of the “IT business continuity” procedure applies to all IT systems, applications and data included in our organization’s business continuity plan.

**1.3 Glossary**

BCP – business continuity plan

ISMS - information security management system

ISM – information security manager

IT – information technology

ICT – information and communication technology

**2. Responsibility**

The information security manager (ISM) has the authority to write and update this procedure. He is responsible for its implementation. He has the support of the director.

**3. Documents**

Business continuity plan

Manage security continuity

Business continuity

Backup

Classification and labeling

Redundancy of means

**4. Requirements of ISO 27001: 2022**

A.5.29 Information security during disruption

The organization shall plan how to maintain information security at an appropriate level during disruption.

A.5.30 ICT readiness for business continuity

ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

**5. Development**

**5.1 Preparation**

Information Security's Business continuity plan (BCP) defines how to maintain the organization's critical IT activities during and after a disaster.

Information security objectives applicable to adverse situations are determined in accordance with the results of the analysis of the impact on our business in the event of a crisis or disaster. These objectives are validated by management and recorded in the Business continuity plan (BCP).

Examples of identified risks:

* technical failures of servers, critical communication or network equipment
* human actions (unintentional errors, lack of preparation, abuse of resources, theft, terrorist acts)
* natural disasters (earthquakes, floods, fires)

The assessment and treatment of information security risks contributes to the development of the BCP, in particular by defining critical activities and systems. More details in the Classification procedure.

Information security continuity is built into the Manage security continuity process.

The Backup policy allows us to restore essential data from our systems and applications.

The planning of actions to guarantee the continuity of information and process security in the event of an emergency is based on:

* use information security measures
* ensure support systems and tools
* maintain information security measures during disruptions
* offset measures for information security measures that cannot be maintained during the outage
* understand the risks, their likelihood of occurrence and their impact
* define critical business processes and determine priorities
* identify the assets involved in the critical processes
* clarify business consequences caused by information security incidents
* train and educate staff on information business continuity processes
* select solutions to deal with incidents with a more limited impact, as well as serious incidents that could threaten the viability of the organization
* ensure the safety of personnel and the protection of equipment
* provide the necessary financial, organizational and technical resources
* document information security continuity plans

**5.2 Implementation**

The right team to prepare for and respond to an adverse situation includes people with the necessary authority, experience and skills. This team is appointed by top management to provide timely incident response and maintain information security.

Answers to the following questions are determined:

* who should assess the situation when activating the BCP?
* who to contact?
* when?
* how?
* who is responsible for communication?
* what immediate actions to take?
* what are the critical systems?
* what are the critical services?
* what specific actions to take for extraordinary circumstances?
* what alternative temporary site to set up for critical activities or services?
* what are the recovery steps as soon as possible?
* what are the actions for restoring backups?
* what equipment should be replaced?

The Business continuity plan (BCP) includes the measures necessary to provide the required level of information security continuity for all critical, sensitive and confidential activities.

Examples of measures:

* 30 minutes - meeting of emergency teams
* 120 minutes - assessment of the situation and the damage
* 8 hours - setting up emergency systems
* one week - restore all systems

The organization ensures that:

* an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence
* the business continuity plan, including response and recovery procedures detailing how the organization plans to handle an interruption of ICT services, is:
  + assessed regularly through exercises and tests
  + approved by management
* the business continuity plan includes the following information:
  + performance and capacity specifications to meet business continuity requirements and objectives
  + Time recovery objective of each priority ICT service and restoration procedures for these components
  + recovery point objective of priority ICT resources defined as information and information restoration procedures

ICT continuity management is a key element of business continuity requirements regarding availability to be able to:

* react and recover from an interruption of ICT services, whatever the cause
* ensure that priority business continuity is supported by the required ICT services
* react:
  + before an interruption of ICT services occurs
  + upon detection of at least one incident that may lead to an interruption of ICT services

The Redundancy of means procedure establishes the means to be duplicated to deal with failures, especially if short recovery times are necessary.

**5.3 Verification**

The BCP is updated and tested at least once a year (schedule and resources). The test results are analyzed and evaluated by top management. Updates follow changes in information systems processes, policies, procedures.