Backup

**1. Subject**

**1.1 Purpose**

**1.2 Scope**

**1.3 Glossary**

**2. Responsibility**

**3. Documents**

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

**5. Development**

History

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

**1. Subject**

**1.1 Purpose**

The purpose of this procedure is to enable recovery after loss of data or systems.

**1.2 Scope**

The scope of the “Backup” procedure applies to people who have access to tools for backing up information, software and systems.

**1.3 Glossary**

ISM – information security manager

**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**

Backup of information

Backup plan

Incident management plan

Business continuity plan

Information security with suppliers

Classification plan

Deletion of information

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

A.8.13 Information backup

Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

**5. Development**

The Information backup policy establishes data retention requirements.

Adequate backup facilities are in place to ensure that all essential data and software can be recovered following an incident, failure or loss of storage media.

The Backup plan establishes how the organization will back up information, software and systems according to the Information backup policy.

The Backup plan takes into account the following elements:

* produce accurate and complete records of backup copies according to documented activities
* consider:
  + business requirements
  + information security requirements
  + the criticality of the information
  + backup frequency
* store backups in a safe and secure remote location
* give the backup information an appropriate level of physical and environmental protection according to the standards applied at the main site
* regularly test backup media to ensure they can be used in an emergency
* test the ability to restore backed up data on an independent test system and not by overwriting the original storage medium
* protect backups using encryption based on identified risks (data confidentiality)
* ensure inadvertent data loss is detected before backup

Operational activities monitor backup execution and address scheduled backup failures to ensure backup completeness.

Backup measures for individual systems and services are regularly tested to ensure they meet the Incident management plan and Business continuity plan.

In the case of critical systems and services, backup measures include all information, applications and system data necessary to restore the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of information, applications and systems are made on a scheduled basis, cf. the Information security with suppliers file.

The retention period for backed up information is established according to the Classification plan. The record of deletions is kept in the Deletion information file and takes into account applicable laws and regulations.