[organization logo]

[organization name]

**OPERATING PROCEDURES FOR INFORMATION AND COMMUNICATION TECHNOLOGY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 4](#_Toc454543138)

[2. Reference documents 4](#_Toc454543139)

[3. Operating Procedures for Information and Communication Technology 4](#_Toc454543140)

[3.1. Change management 4](#_Toc454543141)

[3.2. Backup 5](#_Toc454543142)

[3.2.1. Backup procedure 5](#_Toc454543143)

[3.2.2. Testing backup copies 5](#_Toc454543144)

[3.2.3. Backup information to cloud service customers 5](#_Toc454543145)

[3.3. Network security management 5](#_Toc454543146)

[3.4. Network services 6](#_Toc454543147)

[3.5. Cloud services 6](#_Toc454543148)

[3.5.1. Cloud management responsibilities 6](#_Toc454543149)

[3.5.2. Cloud protection responsibilities 7](#_Toc454543150)

[3.6. Disposal and destruction of equipment and media 7](#_Toc454543151)

[3.6.1. Equipment 7](#_Toc454543152)

[3.6.2. Paper media 8](#_Toc454543153)

[3.6.3. Cloud computing environment 8](#_Toc454543154)

[3.6.4. Erasure and destruction records; commission for the destruction of data 8](#_Toc454543155)

[3.7. Information transfer 8](#_Toc454543156)

[3.7.1. Electronic communication channels 8](#_Toc454543157)

[3.7.2. Physical transfer of Personally Identifiable Information (PII) 9](#_Toc454543158)

[3.7.3. Relations with external parties 9](#_Toc454543159)

[3.8. System monitoring 9](#_Toc454543160)

[3.8.1. General monitoring 9](#_Toc454543161)

[3.8.2. Cloud environment monitoring 10](#_Toc454543162)

[4. Managing records kept on the basis of this document 10](#_Toc454543163)

[5. Validity and document management 12](#_Toc454543164)

# Purpose, scope and users

The purpose of this document is to ensure correct and secure functioning of information and communication technology.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology, as well as to related documentation within the scope.

Users of this document are employees of [organizational unit for information and communication technology].

# Reference documents

* ISO/IEC 27001 standard, clauses A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
* ISO/IEC 27017 standard, clauses 11.2.7, 12.1.2, 12.1.3, 12.3.1, 12.4.1, and 12.4.3
* ISO/IEC 27018 standard, clauses 11.2.7, 12.1.4, 12.3.1, 12.4.1, 13.2.1, A.9.2, A.10.4, A.10.5, and A.10.6
* Information Security Policy
* [Business Continuity Strategy]
* [Mobile Device and Teleworking Policy]
* [Information Classification Policy]
* [Inventory of Assets]
* [Supplier Security Policy]

# Operating Procedures for Information and Communication Technology

## Change management

Each change to operational or production systems must be made in the following way:

1. change may be proposed by [specify job functions]
2. change must be authorized by [job title], who must assess its justification for business and potential negative security impacts
   1. relevant change that affects cloud services must be communicated by [job title] to their respective cloud service customers, so they can provide their evaluation to complement the [job title]’s change assessment
3. changes must be implemented by [job title]
4. [job title] is responsible for checking that the change has been implemented in accordance with the requirement
5. [job title] is responsible for testing and verifying the system's stability – the system must not be put into production before thorough testing has been conducted
6. implementation of changes must be reported to the following persons: [list all necessary job titles]

Change records are kept [provide the name of the form, or describe a different method for recording changes].

## Backup

### Backup procedure

Backup copies must be created for all systems identified in the [Business Continuity Strategy] and with the frequency specified in that document.

[job title] is responsible for backing up the information, software and system images. [If necessary, describe the technology used for making backup copies, specify responsibilities for individual activities, locations for storing backup copies, physical protection for backup copies, encryption, passwords, etc.]

Logs of the backup process are automatically created on systems where the backup copy is made.

### Testing backup copies

Backup copies and the process of their restoration must be tested at least [once every three months] by implementing the data restore process on [identify the server where the data restore is carried out], and checking that all data has been successfully recovered.

[job title] is responsible for testing backup copies. Records on testing backup copies are kept [describe record form – on paper or in electronic form, is there is a prescribed form, etc.].

### Backup information to cloud service customers

[job title] is responsible to provide to the cloud service customers the following information regarding the backup of their information:

* customer responsibilities on backup and restore procedures
* scope and schedule of backups performed on customer’s data
* time schedule and conditions for data restore
* technology used for making backup copies
* locations for storing backup copies
* physical and logical protection applied on backup copies
* any capabilities that are available to allow cloud service customers to perform backup operations by themselves
* [list here other information the organization deems as relevant or is required by contract]

## Network security management

[job title] is responsible for managing and controlling the computer networks, for ensuring the security of information in networks, and for protecting the services connected to the networks from unauthorized access. It is therefore necessary:

* to separate the operational responsibility for networks from the responsibility for sensitive applications and other systems
* to protect sensitive data passing over the public network by [describe the technology used for protection and specify responsibilities and responsible persons]
* to protect sensitive data passing over wireless networks by [describe the technology used for protection and specify responsibilities and responsible persons]
* to protect equipment connecting to the network from remote locations by [describe the technology used for protection and specify responsibilities and responsible persons]
* to segregate traffic coming in from mobile devices, set up unique firewall policies, static routes, Virtual Local Area Networks, etc.
* to ensure the availability of network services by [describe controls which will ensure availability]
* [job title] must regularly monitor and test implemented controls

## Network services

[job title] must define security features and the level of expected services for all network services, whether these services are provided in-house or outsourced – such requirements should be documented with service providers.

If the network services are outsourced, then the requirements must be specified in the agreement as defined in [Supplier Security Policy].

## Cloud services

### Cloud management responsibilities

[job title] is responsible for managing and controlling the infrastructure, platforms, and services made available in the cloud environments, defining security features and the level of expected services for all cloud services, whether these services are provided in-house or outsourced – such requirements should be documented with service providers.

It is therefore necessary that:

* [job title] separates the operational responsibilities for both [organization name] and the cloud service customers regarding the cloud environments (infrastructure, applications, services, and data)
* [job title] identifies the requirements for any utility programs to be used within the cloud environment
* [job title] ensures the availability of documentation needed by the Cloud Service Customers so they can properly fulfill their cloud environment responsibilities by [describe controls that will be used to ensure documentation availability]
* [job title] ensures the alignment between the physical and logical configurations applied in the cloud environment by [describe or refer to the policy/procedure use to configure logical elements of the cloud infrastructure that possess a physical counterpart]

### Cloud protection responsibilities

[job title] is responsible for protecting infrastructure, platforms, and services made available in the cloud environments from unauthorized access and loss of integrity or availability.

It is therefore necessary that:

* [job title] separates the security responsibilities for both [organization name] and the cloud service customers regarding the cloud environments (infrastructure, applications, services, and data)
* [job title] protects the access and use of utility programs within the cloud environment by [describe the technology and methods used for protection]
* [job title] ensures the availability of cloud environments by [describe controls that will ensure availability]
* [job title] enforces cloud environment segregation between tenants in the cloud service customers’ environment and between cloud service customers’ environment and the [organization name]’s internal administrative environment by [describe the methods and technologies used for segregation]
* [job title] enforces hardening practices in physical and logical components (e.g.: storage units, virtual machines, service protocols, etc.) of the cloud infrastructure by [describe the hardening practices]

Regarding the protection of data in cloud environments, [job title] is responsible for ensuring that cloud customer data needed in test procedures, especially Personally Identifiable Information (PII), is handled through proper technical and organizational measures proportional to the risk involved in such test procedures.

[job title] is responsible for ensuring the effectiveness of the security controls implemented to protect cloud environments and the information stored and processed by them, by means of regular monitoring and testing of implemented controls.

## Disposal and destruction of equipment and media

All data and licensed software stored on mobile storage media (e.g. on CD, DVD, USB flash drive, memory card, etc.; but also on paper) and on all equipment containing storage media (e.g. computers, data storage, mobile phones, network equipment, etc.) must be erased or the medium destroyed before it is disposed of or reused.

The person responsible for erasing data / destroying media must inform the owner of the asset in question about erasing/destroying, and the asset owner must update the Inventory of Assets.

### Equipment

[job title] is responsible for checking and erasing data from equipment, unless the Information Classification Policy prescribes differently. Data must be erased [describe the technology used for erasing data from media in the equipment], but if the process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed. In situations where there is no certainty that an equipment stores Personally Identifiable Information (PII) or not, the equipment must be handled as though it stores PII. Mobile storage media

[job title] is responsible for erasing data from mobile storage media, unless the Information Classification Policy prescribes differently. Data must be erased [describe the technology used for erasing data from media], but if the erasure process is not secure enough considering the sensitivity of the data, then the storage medium must be destroyed. In situations where there is no certainty that equipment stores Personally Identifiable Information (PII) or not, the mobile storage media must be handled as though it stores PII.

### Paper media

Employees of the organization handling individual documents are responsible for destroying paper documents, unless the Information Classification Policy prescribes differently. Paper documents are destroyed by paper shredders.

### Cloud computing environment

Considering the cloud computing environment (e.g., virtual applications, databases, etc.), data must be erased [describe the technology used for erasing data in cloud computing environment], but if the erasure process is not secure enough considering the sensitivity of the data, then the procedures for erasing data from equipment in section 3.1 must be followed.

In situations where there is no certainty that a cloud computing environment stores Personally Identifiable Information (PII) or not, the virtual storage media must be handled as if it stores PII.

### Erasure and destruction records; commission for the destruction of data

Records of erasure/destruction must be kept for all data classified as "Restricted" and "Confidential." Records must include the following information: information about the media, date of erasure/ destruction, method of erasure/destruction, person who carried out the process.

All information classified as "Confidential" must be erased/destroyed in the presence of a commission consisting of persons authorized to access the information in question.

All information classified as "PII" must be erased/destroyed according the documents [list the procedures agreed between the organization and it cloud service customers].

## Information transfer

### Electronic communication channels

Organization's information may be exchanged through the following electronic communication channels: e-mail, download of files from the Internet, transfer of data via [provide names of specialized communication systems], telephones, fax machines, SMS text messages, portable media, and forums and social networks.

[job title] determines the communication channel that may be used for each type of information, and possible restrictions regarding permissions to use the communication channels, i.e. defines which activities are forbidden.

In addition to controls prescribed by the Information Classification Policy, [job title] prescribes additional controls for each type of data and communication channel, based on risk assessment results. In situations involving cloud service customers’ information, [job title] also must consider the cloud service agreements clauses to prescribe security controls.

### Physical transfer of Personally Identifiable Information (PII)

PII under the organization's responsibility may be exchanged through the following physical ways: [describe here the methods for physical transfer].

According to the situation, [job title] describes, among the abovementioned available options, the physical way that may be used for specific PII transfers, and possible restrictions.

In addition to controls prescribed by the Information Classification Policy, [job title] must ensure the proper record of the following information about a PII transfer:

* the physical media used
* the authorized sender/recipients
* the incoming and outgoing date and time

Additionally, based on risk assessment results, [job title] must prescribe additional controls.

### Relations with external parties

External parties include various service providers, companies for hardware and software maintenance, companies handling transactions or data processing, clients, etc.

Before exchanging information and/or software with any external party, an agreement must be signed, which is the responsibility of [job title]. The agreement may be in paper or electronic form (e.g. agreeing to general terms and conditions) and must contain clauses in line with the risk assessment, including at least the following:

* method of identification of the other party
* authorizations to access information
* ensuring non-repudiation
* technical standards for data transfer
* incident response
* labeling and handling sensitive information
* copyright

Agreements with external parties must be drawn up according to the [Supplier Security Policy].

## System monitoring

### General monitoring

Based on the risk assessment results, [job title] decides which logs will be kept on which systems and for which systems, and how long they will be stored. Logs must be kept for all administrators and system operators on sensitive systems.

[job title] is responsible for monitoring the logs of automatically reported faults on a daily basis, as well as to register faults reported by users, to analyze why errors occurred and to take appropriate corrective actions. [Specific authorizations may be specified for actions in the case of an error, as well as how records of errors are kept.][job title] is responsible for regularly reviewing logs in order to monitor the activities of users, administrators and system operators. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [job title] must be informed about the results of the review.

### Cloud environment monitoring

Based on the risk assessment results, and Customer’s Cloud Service Agreements, [job title] decides which logs will be kept about cloud environments’ access and use, resource allocation and utilization, and about changes to Personally Identifiable Information (PII), and how long they will be stored. Logs must be kept for all administrators and operators performing activities in cloud environments.

[job title] is responsible to ensure correct clock synchronization between Cloud Service Customers’ local clocks and [organization name]’s cloud services’ clocks by [describe the technology used for clock synchronization].

[job title] is responsible for regularly reviewing logs related to Personally Identifiable Information (PII) in order to identify unusual behavior over PII handling. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [job title] must be informed about the results of the review.

[job title] is responsible for regularly reviewing logs in order to monitor the resources allocated to, and utilized by, each cloud service customer. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [job title] must be informed about the results of the review.

[job title] is responsible to ensure the Cloud Service Customers can log and monitor the use of their cloud services by [describe the technologies used to provide Cloud Service Customer with the functionalities needed for them to log and monitor the use of their cloud services]. These log and monitor capabilities must allow the cloud service customer to access only log data related to the cloud services it uses.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
| [Name of change record] – in electronic form | [intranet folder name] | [job title] | Once created, the record cannot subsequently be changed | 3 years |
| [Decisions about the communication channels used for specific types of information, restrictions, forbidden activities] – electronic form | [intranet folder name] | [job title] | Once created, the record cannot subsequently be changed | 3 years |
| [Backup process logs] – electronic form | System executing the backup procedure | [job title] | Logs are read-only; they cannot be deleted or edited | Logs are stored for a period of 1 year |
| [Records of testing backup copies] – paper or electronic form | [name of filing folder/cabinet] | [job title] | Only [job title] has the right to access such records | Records are stored for a period of 1 year |
| [Security features and level of expected service for network services] – electronic and paper form | [job title]'s computer, [name of filing folder/cabinet] | [job title] | Only [job title] has the right to access such records | 5 years after expiration of agreement or provided service |
| [Security features and level of expected service for cloud services] – electronic and paper form | [job title]'s computer, [name of filing folder/cabinet] | [job title] | Only [job title] has the right to access such records | 5 years after expiration of agreement or provided service |
| [Erasure/destruction records] – in paper form | [name of filing folder/cabinet] | [job title] | The cabinet is locked; the keys are kept by [job functions] | Records are stored for a period of 5 years |
| [Records of log reviews] – in electronic and paper form | [job title]'s computer, [name of filing folder/cabinet] | [job title] | Only [job title] has the right to access such records | Records are stored for a period of 5 years |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number of incidents related to the secure functioning of ICT systems
* number of incidents due to unclear responsibilities for the functioning of ICT systems

Previous versions of this document must be stored for a period of 5 years, unless specified otherwise by legal or contractual requirement.

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]