[organization logo]

[organization name]

**INFORMATION TRANSFER POLICY**

|  |  |
| --- | --- |
| 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 3](#_Toc454543519)

[2. Reference documents 3](#_Toc454543520)

[3. Transfer of information 3](#_Toc454543521)

[3.1. Electronic communication channels 3](#_Toc454543522)

[3.2. Physical transfer of Personally Identifiable Information (PII) 3](#_Toc454543523)

[3.3. Relations with external parties 4](#_Toc454543524)

[4. Managing records kept on the basis of this document 4](#_Toc454543525)

[5. Validity and document management 5](#_Toc454543526)

# Purpose, scope and users

The purpose of this document is to ensure the security of information and software when they are exchanged within or outside the organization.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all the information and communication technology and information 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.13.2.1, A.13.2.2
* ISO/IEC 27018 standard, clauses A.9.2, A.9.3, A.10.4, and A.10.5
* Information Security Policy
* [Information Classification Policy]
* [Supplier Security Policy]

# Transfer of information

## 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 available 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].

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| [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 | 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 communication channels used contrary to this document
* number of external parties with which information is exchanged without a signed agreement
* number of business information systems exchanging information without specified security controls

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

[job title]

[name]

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

[signature]