[Organization logo]

[Organization name]

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

INFORMATION TRANSFER POLICY

Commented [270012]: There is no need to write this Information Transfer Policy as a separate document if the same rules are prescribed by the Security Procedures for IT Department.

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

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. TRANSFER OF INFORMATION 3

3.1. ELECTRONIC COMMUNICATION CHANNELS 3

3.2. RELATIONS WITH EXTERNAL PARTIES 3

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. VALIDITY AND DOCUMENT MANAGEMENT 4

1. 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].

2. Reference documents

- ISO/IEC 27001 standard, clause A.5.14
- Information Security Policy
- [Information Classification Policy]
- [Supplier Security Policy]

Commented [27A4]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "05_General_Policies".

3. Transfer of information

3.1. Electronic communication channels

Organization's information may be exchanged through the following electronic communication

[Job title] determines the communication channel that may be used for each type of information,

Commented [270015]: The media in question may be specified.

Commented [270016]:

Commented [270017]:

Commented [270018]:

Commented [270019]: To be deleted if this Policy does not exist.

3.2. Relations with external parties

External parties include various service providers, companies for hardware and software

paper or electronic form (e.g., agreeing to general terms and conditions) and must contain clauses in

- authorizations to access information
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

[illegible]

4. 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	3 years

Commented [2700110]: Alter this record to match the records you already have in your company. If you do not have a similar record, you can create a new one in the format that suits you best.

5. 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.

Commented [2700111]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]
- [illegible]

[job title]
[name]

[signature]

Commented [2700112]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.