[Organization logo]

[Organization name]

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

SECURITY PROCEDURES FOR IT DEPARTMENT

Commented [270012]: Parts of this document that need to be specified in more detail may be drawn up as separate documents (policies/procedures).

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

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].

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31, and A.8.32
- Information Security Policy
- [Disaster Recovery Plan]
- [Mobile Device, Teleworking Policy and Work from Home Policy]
- [Information Classification Policy]
- [Inventory of Assets]
- [Supplier Security Policy]
- [Secure Development Policy]
- [Access Control Policy]

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

3. Operating Procedures for Information and Communication Technology

3.1. Change management

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

1. [illegible]
2. [illegible]
3. [illegible]
4. [job title] is responsible for checking that the change has been implemented in accordance with the requirement
5. [illegible]
6. [illegible]

Commented [270015]: Delete this whole item if control A.8.32 is marked as inapplicable in the Statement of Applicability.

Commented [270016]: Delete this item if the Change Management Policy constitutes a separate document.

Commented [270017]: For more information about this topic, read this article:

How to manage changes in an ISMS according to ISO 27001 A.12.1.2 https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/

Commented [270018]: [illegible]

Commented [270019]: Another way of formulating the steps [illegible]

7. [job title] is responsible for updating the documents (policies, procedures, plans, etc.) that

3.2. Configuration management

[Job title] is responsible for documenting the configuration settings of hardware, software, services,

3.3. Capacity management

3.4. Antivirus protection

3.5. Backup

3.5.1. Backup procedure

Backup copies must be created for all systems identified in the [Business Continuity Strategy] and

backup copies, physical protection for backup copies, encryption, passwords, etc.]

3.5.2. Testing backup copies

Backup copies and the process of their restoration must be tested at least [once every three months]

[Job title] is responsible for testing backup copies. Records of testing backup copies are kept

3.6. Network security management

[Job title] is responsible for managing and controlling the computer networks, for ensuring the

Commented [2700110]: Delete this whole item if control A.8.20 is marked as inapplicable in the Statement of Applicability.

Commented [2700111]: For more information about this topic, read these articles:

• How to manage network security according to ISO 27001 A.13.1
https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/

• Requirements to implement network segregation according to ISO 27001 control A.13.1.3
https://advisera.com/27001academy/blog/2015/11/02/requirements-to-implement-network-segregation-according-to-iso-27001-control-a-13-1-3/

• Network segregation in cloud environments according to ISO 27017
https://advisera.com/27001academy/blog/2016/09/26/network-segregation-in-cloud-environments-according-to-iso-27017/

• Using Intrusion Detection Systems and Honeypots to comply with ISO 27001 A.13.1.1 network controls
https://advisera.com/27001academy/blog/2016/07/04/using-intrusion-detection-systems-and-honeypots-to-comply-with-iso-27001-a-13-1-1-network-controls/

• How to use firewalls in ISO 27001 and ISO 27002 implementation
https://advisera.com/27001academy/blog/2015/05/25/how-to-use-firewalls-in-iso-27001-and-iso-27002-implementation/

Commented [2700112]: Delete this item if the control A.8.6 is not stated as applicable in the Statement of Applicability

Commented [2700113]: Delete this item if the control A.8.7 is not stated as applicable in the Statement of Applicability

Commented [2700114]: Delete this whole item if control A.8.13 is marked as inapplicable in the Statement of Applicability.

Commented [2700115]: Delete this item if the Backup Policy constitutes a separate document.

Commented [2700116]: For more information about this topic, read this article:

Backup policy – How to determine backup frequency
https://advisera.com/27001academy/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

Commented [2700117]:

Commented [2700118]: Backup copies should be stored at

Commented [2700119]: Adjust frequency in accordance with assessed risks.

Commented [2700120]: Delete this whole item if control A.8.20 is marked as inapplicable in the Statement of Applicability.

Commented [2700121]: For more information about this topic, read these articles:

• How to manage network security according to ISO 27001 A.13.1 ... [1]

- to separate the operational responsibility for networks from the responsibility for sensitive
- protection and specify responsibilities and responsible persons]
- to protect equipment connecting to the network from remote locations by [describe the
- to separate development, testing, and operational systems environments
- data leakage

3.7. Network services

[Job title] must define security features and the level of expected services for all network services,

defined in [Supplier Security Policy].

3.8. Data deletion

when no longer required.

equipment].

3.9. Disposal and destruction of equipment and media

reused.

Commented [2700122]:

Commented [2700123]:

Commented [2700124]:

Commented [2700125]: For more information about this topic, read this article:

How to manage the security of network services according to ISO 27001 A.13.1.2
https://advisera.com/27001academy/blog/2017/02/13/how-to-manage-the-security-of-network-services-according-to-iso-27001-a-13-1-2/

Commented [2700126]: If control A.8.10 is marked is

Commented [2700127]: E.g., list specialized tools that must

Commented [2700128]: For more information about this topic, read this article:

Media & equipment disposal – what is it and how to do it in line with ISO 27001
https://advisera.com/27001academy/blog/2015/12/07/secure-equipmentand-media-disposal-according-to-iso-27001/

Commented [2700129]: Delete this item if the Disposal and Destruction Policy constitutes a separate document.

Commented [2700130]: Delete this whole item if controls A.7.10 and A.7.14 are marked as inapplicable in the Statement of Applicability.

Commented [2700131]:

Commented [2700132]:

The person responsible for

Commented [2700133]: Delete this item if control A.5.9 is marked as inapplicable in the Statement of Applicability.

3.9.1. *Equipment*

Commented [2700134]: Delete this section if control A.7.14 is not applicable

[Job title] is responsible for checking and erasing data from equipment, unless the Information

Commented [2700135]:

Commented [2700136]:

3.9.2. *Mobile storage media*

Commented [2700137]:

[Job title] is responsible for erasing data from mobile storage media, unless the Information

Commented [2700138]: Delete this section if control A.7.10 is not applicable.

Commented [2700139]: To be deleted if such a policy does not exist.

3.9.3. *Paper media*

Commented [2700140]: Delete this section if control A.8.10 is not applicable.

Employees of the organization handling individual documents are responsible for destroying paper

Commented [2700141]: To be deleted if such a policy does not exist.

Commented [2700142]: Or specify some other technology.

3.9.4. *Erasure and destruction records; commission for the destruction of data*

Commented [2700143]: Adapt to confidentiality levels used in the organization.

destruction, method of erasure/destruction, person who carried out the process.

3.10. Information transfer

Commented [2700144]: Delete this item if the Information Transfer Policy constitutes a separate document.

3.10.1. *Electronic communication channels*

Commented [2700145]: The media in question may be specified.

Commented [2700146]:

Commented [2700147]: The forums and social networks in question may be specified.

which activities are forbidden.

Commented [2700148]:

Commented [2700149]: To be deleted if this Policy does not exist.

results.

3.10.2. *Relations with external parties*

maintenance, companies handling transactions or data processing, clients, etc.

line with the risk assessment, including at least the following:

- method of identification of the other party

3.11. Handling the source code

in the [Access Control Policy].

3.12. Use of utility programs

3.13. System monitoring

Based on the risk assessment results, [job title] decides which logs will be kept on which systems and

errors are kept.]

must be informed about the results of the review.

Commented [2700150]: Delete this item if the control A.8.4 is not stated as applicable in the Statement of Applicability.

Commented [2700151]:

Commented [2700152]: Delete this section if the control A.8.18 is not stated as applicable in the Statement of Applicability.

Commented [27A53]:

Commented [2700154]: To learn more about this topic, read this article:

Logging and monitoring according to ISO 27001 A.12.4
https://advisera.com/27001academy/blog/2015/11/23/logging-and-monitoring-according-to-iso-27001-a-12-4/

Commented [2700155]:

Commented [2700156]: Delete this text if control A.8.15 is marked as inapplicable in the Statement of Applicability.

Commented [2700157]: Delete this text if control A.8.15 is marked as inapplicable in the Statement of Applicability.

Commented [2700158]: Delete this text if control A.5.7 is marked as inapplicable in the Statement of Applicability.

Commented [2700159]: Delete this text if control A.8.12 is marked as inapplicable in the Statement of Applicability.

Commented [2700160]: Delete this text if control A.8.15 is marked as inapplicable in the Statement of Applicability.

Commented [2700161]:

Commented [2700162]: Delete this text if control A.5.7 is marked as inapplicable in the Statement of Applicability.

Commented [2700163]: Delete this text if control A.8.12 is marked as inapplicable in the Statement of Applicability.

Commented [2700164]:

Commented [2700165]: Delete this text if control A.8.15 is marked as inapplicable in the Statement of Applicability.

Commented [2700166]: Delete this text if control A.8.8 is marked as inapplicable in the Statement of Applicability.

[job title] is responsible for monitoring applied configurations on devices and systems against

Commented [2700167]: Delete this text if control A.8.8 is marked as inapplicable in the Statement of Applicability.

Commented [2700168]: Delete this text if control A.8.8 is marked as inapplicable in the Statement of Applicability.

3.14. External threat monitoring

Commented [2700169]: Delete this section if the control A.5.7 is not stated as applicable in the Statement of Applicability

[job title] is responsible for monitoring suppliers,

4. Managing records kept on the basis of this document

Commented [2700170]: Alter these records to match what you already have in your company. If you do not have similar records, you can create new ones in the format that suits you best.

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] –	[job title]'s computer,	[job title]	Only [job title] has the right to access such records	5 years after expiration of agreement

electronic and paper form	[name of filing folder/cabinet]			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

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 [2700171]: 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]

[job title]
[name]

_____
[signature]

Commented [2700172]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.