[Organization logo]

[Organization name]

IT SECURITY POLICY

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

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

Commented [270012]: To learn more about the structure of this document, read this article:

How to structure the documents for ISO 27001 Annex A controls https://advisera.com/27001academy/blog/2014/11/03/how-to-structure-the-documents-for-iso-27001-annex-a-controls/

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 define clear rules for the acceptable use of the information system and other information assets in [organization name].

This document is applied to the entire scope of the Information Security Management System (ISMS), i.e., to all information systems and other information assets used within the ISMS scope.

Users of this document are all employees of [organization name].

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19, and A.8.23.
- Information Security Policy
- [Information Classification Policy]
- [Incident Management Procedure]
- [Inventory of Assets]
- [Security Procedures for IT Department]
- [Information Transfer Policy]

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

Commented [27A5]: You can find templates for these documents in the ISO 27001 Documentation Toolkit folder "09_Annex_A_Security_Controls".

3. Acceptable use of information assets

Commented [270016]: The extent to which each of the listed items is necessary must be based on the results of risk assessment.

This training will help you raise the security awareness and track the knowledge of your employees: https://training.advisera.com/awareness-session/security-awareness-training/

3.1. Definitions

Information system – includes all servers and clients, network infrastructure, system and application

Information assets – in the context of this Policy, the term *information assets* is applied to

3.2. Acceptable use

3.3. Responsibility for assets

Commented [270017]: Delete this whole item if control A.5.9 is marked as inapplicable in the Statement of Applicability.

3.4. Deletion of information

computer or mobile device.

3.5. Prohibited activities

the performance of the information system, or poses a security threat. It is also prohibited:

- to download image or video files which do not have a business purpose, send e-mail chain
-
-
- [job title]
-
-
- storing and reading data (e.g. USB flash drives) without explicit permission by [job title]; use

3.6. Taking assets off-site

Equipment, information or software, regardless of its form or storage medium, may not be taken off-

granted permission for their removal.

3.7. Return of assets upon termination of contract

3.8. Backup procedure

The user must [specify backup procedure method] all sensitive information stored on his/her computer at least once a day.

3.9. Antivirus/malware protection

[Name of malware software]

3.10. Authorizations for information system use

Users of the information system

Commented [270018]: Delete this whole item if control A.8.10 is marked as inapplicable in the Statement of Applicability.

Commented [270019]: To be deleted if control A.8.19 is marked as inapplicable in the Statement of Applicability.

Commented [2700110]: To be deleted if such a Policy does not exist.

Commented [2700111]: Delete this whole item if control A.7.10 is marked as inapplicable in the Statement of Applicability.

Commented [2700112]:

Commented [2700113]: Delete this whole item if control A.5.11 is marked as inapplicable 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]: For more information about this topic, please 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 [27A16]: Adjust the frequency based on the results of Business Impact Analysis, if one was conducted.

Commented [2700117]: Make sure that this does not interfere with the Security Procedures for IT Department / Backup Policy.

Commented [2700118]: Delete this whole item if control A.8.7 is marked as inapplicable in the Statement of Applicability.

Users may use the information system only [redacted]

Users must not take part [redacted]

3.11. User account responsibilities

The user must not, directly or indirectly, allow another person to use his/her access rights, i.e., username, and must not use another person's username and/or password. The use of group user names is forbidden.

[redacted]

Commented [2700119]: To be deleted if control A.5.17 is marked as inapplicable in the Statement of Applicability.

3.12. Password responsibilities

Commented [2700120]: Delete this whole item if the Password Policy constitutes a separate document.

Commented [2700121]: Delete this whole item if control A.5.17 is marked as inapplicable in the Statement of Applicability.

Users must apply the following good security practices when selecting and using passwords:

- [redacted]
- [redacted]
- [redacted]
- passwords must be changed if there are indications that the passwords or the system may [redacted]
- [redacted]
  - [redacted]
  - [redacted]
    - using at least one uppercase and at least one lowercase alphabetic character
    - using at least one special character
    - [redacted]
    - [redacted]
    - the last three passwords must not be re-used
- passwords must be changed every 3 months
- [redacted]
- [redacted]
- passwords used for private purposes must not be used for business purposes

3.13. Clear desk and clear screen policy

Commented [2700122]: Delete this whole item if the Clear Desk and Clear Screen Policy constitutes a separate document.

Commented [2700123]: To learn more about this topic, please read this article:

Clear desk and clear screen policy and what it means for ISO 27001 https://advisera.com/27001academy/blog/2016/03/14/clear-desk-and-clear-screen-policy-what-does-iso-27001-require/

All information classified as "Internal use," "Restricted," or "Confidential" as specified in the [redacted]

3.13.1. Clear desk policy

If the authorized person is not at his/her workplace, all paper documents, as well as mobile

3.13.2. Clear screen policy

If the authorized person is not at his/her workplace, all sensitive information must be removed from

time (over 30 minutes), the clear screen policy is implemented by logging out of all systems and turning off the workstation.

Information on whiteboards (e.g., those available in meeting rooms) must be cleared when no longer required.

3.13.3. Protection of shared facilities and equipment

Documents containing sensitive information must immediately be removed from printers, fax and

Shared fax machines [specify machines and their location] are protected by [specify the manner of

and the furniture in them must be performed to ensure no [organization name] assets are left behind.

3.14. Internet use

Internet may be accessed only through the organization's local network with appropriate

[Job title] may block access to some Internet pages for individual users, groups of users, or all

Commented [2700124]: Delete this whole item if control A.7.7 is marked as inapplicable in the Statement of Applicability.

Commented [2700125]: Change this reference to "Security Procedures for IT Department" if the "Disposal and Destruction Policy" is integrated to the first document.

Commented [2700126]:

Commented [2700127]: Delete this whole item if control A.7.7 is marked as inapplicable in the Statement of Applicability.

Commented [2700128]:

Commented [2700129]: Delete this item if control A.8.1 is marked as inapplicable in the Statement of Applicability.

Commented [2700130]: E.g. locking the facility, etc.

Commented [2700131]: E.g. locking the facility, etc.

Commented [2700132]: E.g. by locking the facility, use of PIN numbers, access cards, etc.

Commented [2700133]: E.g., more than two weeks.

Commented [2700134]: Include the name of your organization.

may submit a written request to [job title] for authorization to access such pages. The user must not

The user is responsible for all possible consequences arising from unauthorized or inappropriate use of Internet services or content.

3.15. E-mail and other message exchange methods

Message exchange methods other than electronic mail also include download of files from the

In accordance with [Security Procedures for IT Department / Information Transfer Policy], as well as channels, i.e. defines which activities are forbidden.

Users may only send messages containing true information. It is forbidden to send materials with been established or to persons who did not require such information.

Should a user receive a spam e-mail, he/she must inform [job title].

(social networks, forums, etc.), he/she must unambiguously state that it does not represent the organization's viewpoint.

3.16. Copyright

Users must not make unauthorized copies of software owned by the organization, except in cases

3.17. Mobile computing

Commented [2700135]: Delete this whole item if control A.5.14 is marked as inapplicable in the Statement of Applicability.

Commented [2700136]: The media in question may be specified.

Commented [2700137]: The forums and social networks in question may be specified.

Commented [2700138]: To be deleted if such a Policy does not exist.

Commented [2700139]: Delete this whole item if control A.5.32 is marked as inapplicable in the Statement of Applicability.

Commented [2700140]: Delete this whole item if Mobile Device and Teleworking Policy constitutes a separate document.

Commented [2700141]: Delete this whole item if control A.8.1 is marked as inapplicable in the Statement of Applicability.

3.17.1. Introduction

[redacted]
data, no matter where such equipment is used.

The abovementioned equipment may be [redacted]

3.17.2. Basic rules

Special care should be taken when mobile computing equipment is placed in vehicles (including cars, [redacted]

- mobile computing equipment carrying important, sensitive or critical information must not [redacted]
- when using mobile computing equipment in public places, the user must take care that data [redacted]
- [redacted]
- [redacted]
- the person using mobile computing equipment off-premises is responsible for regular back- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- when persons are using their own devices, additional rules that must be applied are defined in the [BYOD Policy]

[Job title] is responsible for training and raising awareness of persons who are using mobile [redacted]

3.18. Teleworking & work from home

3.18.1. Introduction

Teleworking means that information and communication equipment is used to enable employees to [redacted]

Commented [2700142]: Delete this paragraph if control A.7.10 is excluded from the Statement of Applicability.

Commented [2700143]: To be deleted if control A.7.9 is marked as inapplicable in the Statement of Applicability.

Commented [27A44]: E.g., weekly access of the organization's server and synchronization of the patches and system settings

Commented [27A45]: E.g., by enforcing installation of the tool for antimalware protection and synchronization of the updates at least once per week, by accessing the organization's network

Commented [27A46]: E.g., by accessing the organization's network and performing automatic/manual backup according to the document that specifies backup

Commented [27A47]: E.g., by establishing secure a communication channel using VPN for encrypting data

Commented [27A48]: Specify the type of information stored on portable computers that should be encrypted according to your organization's practices.

E.g. Entire hard disk, sensitive files, files classified as confidential

Commented [27A49]: E.g., through virtual disk encryption, volume encryption, or file/folder encryption

Commented [27A50]: If your organization [redacted]

Commented [27A51]: If your organization [redacted]

Commented [52]: To be deleted in case usage of employees' own devices is not allowed.

Commented [27A53]: You can use the following Security Awareness Training to train your employees: https://training.advisera.com/awareness-session/security-awareness-training/

Commented [27k54]: To learn more about this topic, please read this article:

How to apply information security controls in teleworking according to ISO 27001 https://advisera.com/27001academy/blog/2017/03/22/how-to-apply-information-security-controls-in-teleworking-according-to-iso-27001/

Commented [2700155]: Delete this whole item if control A.6.7 is marked as inapplicable in the Statement of Applicability.

Commented [2700156]: Delete this whole item if the Mobile Device and Teleworking Policy constitutes a separate document.

Teleworking must be authorized by [job title]

Commented [2700157]:

3.18.2. Additional rules for teleworking

All persons performing teleworking must follow the rules for mobile computing defined in section

- the physical location where teleworking is performed must be protected by
- prevention of unauthorized access by persons living or working at the location where the
- return of data and equipment in the case of termination of employment must be implemented in accordance with section 3.7 of this policy
- activities specifically allowed for employess when performing teleworking]

Commented [27A58]:

Commented [27A59]: E.g., uninterruptable power supply, alternative communication links, etc.

Commented [27A60]: In case the Clear Desk and Clear Screen Policy is implemented as part of the IT Security Policy, then change this reference to "section 3.13 of this policy"

Commented [27A61]:

Commented [27A62]: E.g., participating in meetings with the

Commented [2700163]: You can delete this text if there are no specific forbidden activities for employees.

Commented [27A64]: E.g., changing configurations on network devices, etc.

Commented [27A65]: You can delete this text if there are no specific allowed activities for employees.

3.19. Monitoring the use of information and communication systems

All data which is created, stored, sent or received through the information system or other

Users agree that authorized persons from the organization may access all such data, and that access

3.20. Incidents

Each employee, supplier or third person who is in contact with data and/or systems of [organization

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time

Commented [2700166]: Please 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.

[Authorizations for software installation, use of Java applications and Active X controls, use of cryptographic tools, download of program code from external media, installing peripheral devices] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years
[Authorization for taking assets off-site] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years
[Authorization for access to selected Internet pages] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years
[Decision on how each data type may be exchanged] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years
[Decision on how messages containing business-relevant data should be stored] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years
[Authorization for teleworking] – electronic form	[intranet folder]	[job title]	Records cannot be edited; only [job title] has the right to store such records	Records are stored for a period of 3 years

Commented [2700167]: Adjust as appropriate.

Commented [2700168]: Adjust as appropriate.

Commented [2700169]: Adjust as appropriate.

Commented [2700170]: Adjust as appropriate.

Commented [2700171]: Adjust as appropriate.

Commented [2700172]: Adjust as appropriate.

Only [job title] can grant other employees access to the any of the abovementioned documents.

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 [2700173]: 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 [2700174]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.