[Organization logo]

[Organization name]

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

STATEMENT OF APPLICABILITY

Commented [270013]: To learn how to write the Statement of Applicability, read this article:

Statement of Applicability in ISO 27001 – What is it and why does it matter? https://advisera.com/27001academy/knowledgebase/the-importance-of-statement-of-applicability-for-iso-27001/

Commented [270014]: 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.

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

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 which controls are appropriate to be implemented in [organization name], the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of [organization name] who have a role in the ISMS.

2. Reference documents

- ISO/IEC 27001 standard, clause 6.1.3 d)
- Information Security Policy
- Risk Assessment and Risk Treatment Methodology
- Risk Assessment and Risk Treatment Report

3. Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.5.1	Policies for information security					

Commented [27A5]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "05_General_Policies".

Commented [27A6]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

Commented [27A7]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

Commented [270018]: To learn more about ISO 27001 Annex A controls, take a look at this book:

ISO 27001 Annex A Controls in Plain English
https://advisera.com/books/iso-27001-annex-controls-plain-english/

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of [redacted]

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.5.6	Contact with special interest groups				[job title] is responsible for monitoring [list names of interest groups and security forums]	
[redacted]						

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700114]: Different interest groups may be assigned to different job functions, depending on specialization of work.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.5.10	Acceptable use of [redacted]				[IT Security Policy], [Information Classification Policy]	
A.5.11	Return of assets				[IT Security Policy], [Supplier Security Policy]	
A.5.12	[redacted]				[Information Classification Policy]	
A.5.13	[redacted]				[Information Classification Policy]	
[redacted]						

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: [redacted]

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	Status
[redacted]					
[redacted]					
[redacted]					
A.5.28	Collection of evidence				Management Procedure]

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700115]: Write this only if business continuity management is included in ISO 27001.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
A.5.32	Intellectual property rights				[IT Security Policy]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.5.33	Protection of records				[Procedure for Document and Record Control], [Secure Development Policy]	
[redacted]	[redacted]				[redacted]	
[redacted]	[redacted]				[redacted]	
[redacted]	[redacted]				[redacted]	
A.5.37	Documented operating procedures				[Security Procedures for IT Department]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
[redacted]						
A.6.5	of employment				employment	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700116]: E.g., checking the CV, contacting former employers, checking criminal records, financial status, etc.

Commented [2700117]: See the list of free security awareness videos here: https://training.advisera.com/awareness-session/security-awareness-training/

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
[redacted]						
A.7.2	Physical entry				are controlled [describe how]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700118]: E.g., offices, archives, warehouses, data centers, etc.

Commented [2700119]: E.g., with walls, alarm systems and video monitoring.

Commented [2700120]: E.g., access cards, security guards, etc.

Commented [2700121]: E.g., with walls, alarm systems and video monitoring.

Commented [2700122]: E.g., back door to your office or warehouse.

Commented [2700123]: E.g., with walls, alarm systems and video monitoring, material inspections.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	Status
[redacted]					

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700124]: E.g., with video monitoring, security guard.

Commented [2700125]: E.g., alarm monitoring center of a security company, employees' phone, etc.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	Status
[redacted]					

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700126]: E.g., server room.

Commented [2700127]: E.g., UPS, power generator, etc.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[illegible]	[illegible]	[illegible]	Status
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
A.8.1	User endpoint devices				Policy]	
A.8.2	Privileged access rights				[Access Control Policy]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [illegible]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700128]: E.g., cable protectors, securing holes and pass-throughs, protective pipes, etc.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
A.8.11	Data masking				Development Policy]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.8.12	Data leakage prevention				[Information Classification Policy], [IT Security Policy], [Security Procedures for IT Department]	
[redacted]						

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)	[redacted]	[redacted]	[redacted]	Status
A.8.23	Web filtering				[IT Security Policy], [Security Procedures for IT Department]	
[redacted]						
A.8.33	Test information				[Secure Development Policy]	

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: [redacted]

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]: [redacted]

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

ID	Controls according to ISO/IEC 27001	Applicability (YES/NO)				Status
A.8.34	Protection of information systems during audit testing				[Internal audit procedure]	

4. Acceptance of Residual Risks

Treatment Table as the source.]

No.	Name of asset						

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, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.

considered:

Commented [2700113]: Indicate the status of implementation - e.g. "Planned," "Partially implemented," "Fully implemented."

Leave blank if the control is marked as inapplicable.

Commented [2700110]: They should be defined for each of your controls and made measurable if possible; however, you can also copy objectives listed in clauses categories in Annex A.

Leave blank if the control is marked as inapplicable.

Commented [2700111]: To learn more about control objectives, read this article:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [2700112]:

Commented [270019]: Based on risk assessment results, contractual and legal obligations.

Commented [2700129]: Acceptance of residual risks must be in accordance with the Risk Assessment and Risk Treatment Methodology.

Commented [2700130]: Delete this text and the table if there are no residual risks with values 3 and 4.

Commented [2700131]: This is only a recommendation; adjust frequency as appropriate.

[job title]
[name]

[signature]

Commented [2700132]: Statement of Applicability needs to be approved by risk owners or by top management on the behalf of risk owners.

Commented [2700133]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.