[Organization logo]

[Organization name]

CLOUD SECURITY POLICY

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

Commented [27A1]: All fields in this document marked by square brackets [ ] must be filled in.

Commented [27A2]: Parts of this document that need to be specified in more detail may be drawn up as separate documents (policies/procedures).

Commented [27A3]: 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 management of cloud environment infrastructure.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e., to all the cloud environment infrastructure and data, as well as to related documentation within the scope.

Users of this document are employees of [organizational unit for cloud environment infrastructure].

Commented [27A4]: Any policies/procedures created to specify in more detail parts of this document.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.12.1.1, A.12.1.3, A.12.4.1, A.12.4.3, A.12.4.4, A.13.1.3, and A.14.2.4
- ISO/IEC 27017 standard, clauses 6.1.1, 9.4.4, 12.1.3, 12.4.1, 12.4.4, 13.1.3, 18.1.2, CLD.6.3.1, CLD.9.5.1, CLD.9.5.2, CLD.12.1.5, CLD.12.4.5, and CLD.13.1.4
- ISO/IEC 27018 standard, clauses 12.4.1 and A.9.2
- Information Security Policy
- [Business Continuity Strategy]
- [Inventory of Assets]
- [Supplier Security Policy]

Commented [27A5]: Delete if such document does not exist.

Commented [27A6]: Delete if such document does not exist.

Commented [27A7]: Delete if such document does not exist.

3. Secure Cloud Environment Management

3.1. Cloud management responsibilities

[Job title] is responsible for managing and controlling the infrastructure, platforms, and services [illegible]

It is therefore necessary that:

- [illegible]
- [job title] identifies the requirements for any utility programs to be used within the cloud [illegible]
- [illegible] will ensure documentation availability]

Commented [27A8]: Examples of responsibilities that can be separated in a cloud environment are:

[illegible]

Commented [27A9]: E.g.: online documentation on a website, paper copy documentation sent to the customer, etc.

- [job title] ensures the alignment between the physical and logical configurations applied in

3.2. Cloud protection responsibilities

[Job title] is responsible for protecting infrastructure, platforms, and services made available in the

- [job title] separates the security responsibilities for both [organization name] and the cloud
- [job title] ensures the availability of cloud environments by [describe controls that will ensure availability]
- units, virtual machines, service protocols, etc.) of the cloud infrastructure by [describe the hardening practices]

Regarding the protection of data in cloud environments, [job title] is responsible for ensuring that

[Job title] is responsible for ensuring the effectiveness of security controls implemented to protect

3.3. Cloud monitoring

be stored. Logs must be kept for all administrators and operators performing activities in cloud environments.

clock synchronization].

Commented [27A10]: E.g.: physical and logical networks, servers, storage units, etc.

Commented [27A11]: Managing IT environments requires a

Commented [27A12]: e.g.: redundancy or contingency of

Commented [27A13]: e.g.: physical/logical resource isolation, firewall policies, static routes, Virtual Local Area Networks, Virtual Machines, etc.

Commented [27A14]: e.g.: restriction to utility programs, disabling unused services, etc.

Commented [27A15]: e.g.: system tests in the development and homologation phases.

Commented [27A16]: The frequency may be specified - e.g. every day, or on certain days of the month, etc.

Commented [27A17]: Controls may be specified - e.g. firewall, intrusion detection systems, etc.

Commented [27A18]: Logs may include user activities,

Commented [27A19]: Delete this text if the organization does not act as a PII cloud processor.

Commented [27A20]: Delete this text if control A.12.4.1 is marked as inapplicable in the Statement of Applicability.

Commented [27A21]: Delete this text if control A.12.4.3 is marked as inapplicable in the Statement of Applicability.

[Job title] is responsible for monitoring the logs of automatically reported faults on a daily basis, as well as [illegible] (reported by users, to analyze why errors occurred and to take appropriate corrective actions. Specific authorizations may be specified for actions in the case of an error, as well as how records of errors are kept).

[illegible] is responsible for regularly reviewing logs in order to monitor the activities of cloud users, administrators, and operators. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [Job title] must be informed about the results of the review.

[Job title] is responsible for regularly reviewing logs related to Personally Identifiable Information (PII) in order to identify unusual behavior over PII handling. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [Job title] must be informed about the results of the review.

[illegible] is responsible for regularly reviewing logs in order to monitor the resources allocated to, and utilized by, each cloud service customer. The review is conducted at intervals prescribed by [job title], who determines and selects the records to be reviewed, and how the implemented review will be recorded. [Job title] must be informed about the results of the review.

[Job title] is responsible to ensure the cloud service customers can log and monitor the use of their cloud services by [describe the technologies used to provide cloud service customer with the functionalities needed for them to log and monitor the use of their cloud services]. These log and monitor capabilities must allow the cloud service customer to access only log data related to the cloud services they use.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
[Security features and level of expected service for cloud services] – 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	5 years after expiration of agreement or provided service
[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

Commented [27A22]: Delete this text if controls A.12.1.3, A.12.4.1 and A.12.4.3 are marked as inapplicable in the Statement of Applicability.

Commented [27A23]: It may be specified that this includes e.g. [illegible]

Commented [27A24]: If necessary, this may be prescribed in [illegible]

Commented [27A25]: Delete this text if controls A.12.4.1 and A.12.4.3 are marked as inapplicable in the Statement of Applicability.

Commented [27A26]: It may be specified that this includes e.g. inclusions, alterations and exclusions.

Commented [27A27]: If necessary, this may be prescribed in [illegible]

Commented [27A28]: e.g.: [illegible]

Commented [27A29]: Delete this text if the organization does not act as a PII cloud processor.

Commented [27A30]: It may be specified that this includes e.g. [illegible]

Commented [27A31]: If necessary, this may be prescribed in [illegible]

Commented [27A32]: Delete this text if control A.12.1.3 is marked as inapplicable in the Statement of Applicability.

Commented [27A33]: Delete this text if controls A.12.1.3, [illegible]

Commented [27A34]: 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.

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 [27A35]: 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]

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

Commented [27A36]: Delete this whole section if your organization does not provide cloud services as a PII processor.

[job title]
[name]

_____
[signature]

Commented [27A37]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.