[organization logo]

[organization name]

**CLOUD SECURITY POLICY**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Abdullah | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc454535230)

[2. Reference documents 3](#_Toc454535231)

[3. Secure Cloud Environment Management 3](#_Toc454535232)

[3.1. Cloud management responsibilities 3](#_Toc454535233)

[3.2. Cloud protection responsibilities 4](#_Toc454535234)

[3.3. Cloud monitoring 4](#_Toc454535235)

[4. Managing records kept on the basis of this document 5](#_Toc454535236)

[5. Validity and document management 5](#_Toc454535237)

# 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].

# 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]

# Secure Cloud Environment Management

## Cloud management responsibilities

[job title] is responsible for managing and controlling the infrastructure, platforms, and services made available in the cloud environments, defining security features and the level of expected services for all cloud services, whether these services are provided in-house or outsourced – such requirements should be documented with service providers.

It is therefore necessary that:

* [job title] separates the operational responsibilities for both [organization name] and the cloud service customers regarding the cloud environments (infrastructure, applications, services, and data)
* [job title] identifies the requirements for any utility programs to be used within the cloud environment
* [job title] ensures the availability of documentation needed by the Cloud Service Customers so they can properly fulfill their cloud environment responsibilities by [describe controls that will ensure documentation availability]
* [job title] ensures the alignment between the physical and logical configurations applied in the cloud environment by [describe or refer to the policy/procedure used to configure logical elements of the cloud infrastructure that possess a physical counterpart]

## Cloud protection responsibilities

[job title] is responsible for protecting infrastructure, platforms, and services made available in the cloud environments from unauthorized access and loss of integrity or availability.

It is therefore necessary that:

* [job title] separates the security responsibilities for both [organization name] and the cloud service customers regarding the cloud environments (infrastructure, applications, services, and data)
* [job title] protects the access and use of utility programs within the cloud environment by [describe the technology and methods used for protection]
* [job title] ensures the availability of cloud environments by [describe controls that will ensure availability]
* [job title] enforces cloud environment segregation between tenants in the cloud service customers’ environment and between the cloud service customers’ environment and [organization name]’s internal administrative environment by [describe the methods and technologies used for segregation]
* [job title] enforces hardening practices in physical and logical components (e.g.: storage 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 cloud customer data needed in test procedures, especially Personally Identifiable Information (PII), is handled through proper technical and organizational measures proportional to the risk involved in such test procedures.

[job title] is responsible for ensuring the effectiveness of security controls implemented to protect cloud environments and the information stored and processed there, by means of regular monitoring and testing of implemented controls.

## Cloud monitoring

Based on the risk assessment results, and the Customer’s Cloud Service Agreements, [job title] decides which logs will be kept about cloud environments’ access and use, about resources allocation and utilization, and about changes on Personally Identifiable Information (PII) and how long they will be stored. Logs must be kept for all administrators and operators performing activities in cloud environments.

[job title] is responsible for ensuring correct clock synchronization between cloud service customers’ local clocks and [organization name]’s cloud services’ clocks by [describe the technology used for clock synchronization].

[job title] is responsible for monitoring the logs of automatically reported faults on a daily basis, as well as registering faults 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.]

[job title] 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.

[job title] 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.

# 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 |

# 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.

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

* number of incidents related to the secure functioning of cloud environment infrastructure
* number of incidents due to unclear responsibilities for the functioning of cloud environment infrastructure

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

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]