# <Security Standard title>

Date: <Document date>

Version: <Version number for the standard>

Reference: <Company reference for this document>

Approved by: <Name of document approver>

Owned by: <Name of document owner>

Author: <Name of document author>

< This template serves as a foundation for developing specific cloud security standards within an organization. It should be customized and expanded based on the organization's unique requirements, cloud architecture, and risk profile.>

# Introduction

< This section outlines the purpose of the cloud security standard, emphasizing its role in enhancing the security posture of cloud-based services and infrastructure. It explains the importance of establishing clear security benchmarks and practices to protect organizational data and assets in the cloud. >

# Scope of Applicability

< Defines the boundaries of the standard, specifying the cloud services, models (IaaS, PaaS, SaaS), and deployment types (public, private, hybrid) it applies to. It also delineates the organizational units, projects, and technologies covered by this standard.>

# Control statements

<Outline the essential control statements for this standard, organizing them in a clear, sectioned format to enhance readability. Consider using tables to simplify how decisions are presented to the reader. Keep this section focused on the specific control requirements, refraining from including additional information or background context.>

# Roles and responsibilities

< Specify who has the authority to make decisions related to this standard. Identify which organizations are permitted to offer services that meet any of the control requirements outlined in this standard.>

# Compliance monitoring

< Outlines the mechanisms and tools used to monitor compliance with the security standard, including regular audits, reviews, and automated compliance checks. It also specifies the frequency and scope of monitoring activities>

# Background information

< Provides context for the standard, including the rationale behind specific control statements and the alignment of this standard with industry best practices and frameworks. It may also include a summary of relevant threats and vulnerabilities specific to the organization's cloud environment>

# Other relevant documents

<Lists documents that support or are related to this security standard, such as specific policy documents, procedural guidelines, implementation guides, and compliance checklists.>

# Revision history

| Version | Date | Change comments | Author | Approved |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |