# <Security Policy title>

Date: <Policy date>

Version: <Version number for the policy>

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 foundational document to be customized and expanded based on the specific needs and requirements of the organization, ensuring comprehensive coverage of all aspects of cloud security governance.>

# Introduction

<This section provides an overview of the cloud security policy, including its objectives and the importance of security in cloud environments. It outlines the intent to protect the organization's data and assets in the cloud and ensure compliance with relevant laws and regulations.>

# Scope of Applicability

<Defines the environments, technologies, and scenarios to which this policy applies. This may include all types of cloud services (IaaS, PaaS, SaaS), cloud deployment models (public, private, hybrid, community), and any associated cloud-based information systems and technologies.>

# Target audience

<Specifies the individuals and groups within the organization who must adhere to this policy. This typically includes employees, contractors, third-party service providers, and any other personnel who access or manage the organization's cloud resources.>

# Policy Statements

<The main contents of the policy expressing the rules that the target audience must adhere to withing the scope of applicability.
This can, for example, include:
Data security, Identity and access management, Infrastructure security, Incident response, compliance, Business continuity and Disaster recovery.>

# Roles and responsibilities

<Explain, using the RACI model, all the roles involved and who has the authority to make decisions related to this policy. If these roles are detailed in other documents, please refer to them. Ensure that individuals in these roles are informed of their responsibilities and that these expectations are included in their job descriptions.>

# Compliance metric objectives

<Describe the key performance indicators (KPIs) and metrics used to measure compliance with the cloud security policy, such as the number of incidents detected, response times, and audit results.>

# Other relevant documents

< Lists additional documents and resources that support the cloud security policy, such as specific procedural guidelines, technical standards, and incident response plans.>

# Revision history

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