Heimdal®

Cloud Security Policy Template

- **[Company Name]**
- **Version: 1.0**
- **Effective Date: [Date]**
- **Last Reviewed: [Date]**
- **Approved By: [Authorized Person/Role]**

Purpose

This policy aims to establish guidelines and procedures for secure cloud computing practices within [Company Name].

The purpose is to ensure the confidentiality, integrity, and availability of [Company Name]'s data in cloud environments and prevent unauthorized access or loss.

Scope

This policy applies to all employees, contractors, and third-party users accessing or managing cloud services on behalf of [Company Name].

It covers all data, systems, and applications residing in cloud environments, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) solutions.

Roles and Responsibilities

- **Cloud Security Administrator**: Responsible for the configuration, monitoring, and enforcement of security settings in cloud environments.
- **IT Team**: Manages cloud infrastructure and provides support to ensure compliance with security controls.
- **Employees/End Users**: Comply with security policies, report suspicious activities, and protect their credentials.

- **Third-Party Vendors**: Must adhere to this policy and agree to comply with [Company Name]'s security standards.

Policy Requirements

Data Classification and Protection

- All data should be classified according to sensitivity and treated accordingly in the cloud.
- Sensitive data must be encrypted both at rest and in transit.
- Access to sensitive data should be restricted based on the principle of least privilege (POLP).

Access Control

- Multi-factor authentication (MFA) must be enabled for all cloud-based accounts.
- Role-based access control (RBAC) should be implemented, ensuring users have the minimum level of access required.
- Access reviews should be conducted quarterly to ensure that only authorized personnel have access.

Data Storage and Backup

- Data stored in cloud environments should be backed up regularly, with recovery procedures tested semi-annually.
- All backups must comply with data retention policies and be encrypted.

Monitoring and Logging

- Enable logging for all cloud accounts, systems, and applications.
- Regularly review logs to detect unauthorized access or anomalies.
- Use automated tools to monitor for potential security incidents.

Incident Response

- Establish and maintain an incident response plan for cloud-specific threats.
- Define roles and responsibilities during an incident, including communication protocols.
- Conduct cloud-specific incident response drills annually.

Compliance and Legal

- Ensure cloud providers comply with relevant data protection regulations, such as GDPR or CCPA.
- Regularly review contractual agreements with cloud providers to confirm security obligations.

Security Controls

Network Security

- Limit network access using firewalls, VPNs, and segmentation for cloud-based systems.

Application Security

- Ensure applications hosted in the cloud are reviewed and tested for vulnerabilities.
- Enforce secure coding practices and perform regular vulnerability assessments.

Encryption

- Implement strong encryption standards (AES-256) for data at rest and TLS 1.2 or above for data in transit.

Identity and Access Management (IAM)

- Establish IAM policies to manage user identities, privileges, and roles effectively.
- Regularly audit IAM policies for compliance.

Policy Enforcement

Violations of this policy may result in disciplinary action, including termination of employment. Contractors and third-party users found in violation may have their access to [Company Name]'s systems revoked.

Review and Updates

This policy shall be reviewed annually or when significant changes occur in technology, regulations, or business requirements.

Revision History Example

A revision history provides transparency and accountability by documenting any changes or updates made to the policy over time. Be sure to document each policy modification and its rationale.

Example

Version	Revision Date	Author	Description
1.0	02/01/2023	Blake Parker, Cloud Security Admin	Initial version
1.1	06/01/2023	Blake Parker, Cloud Security Admin	Updated training frequency

Acknowledgment

By signing below, you acknowledge that you have read, understood, and agree to comply with the Cloud Security Policy.

Signature: ____________________

Date: ____________________