Cloud Security Policy Template

Document Control Information

- **Document Title:** Cloud Security Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Cloud Security Policy establishes [ORGANIZATION NAME]'s requirements for the secure use of cloud services in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that cloud services are selected, implemented, and managed in a manner that protects the organization's information assets.

1.2 Scope

This policy applies to: - All cloud services used by [ORGANIZATION NAME], including: - Infrastructure as a Service (IaaS) - Platform as a Service (PaaS) - Software as a Service (SaaS) - Function as a Service (FaaS) - Storage as a Service - Other cloud-based services - All employees, contractors, consultants, and third parties who use cloud services on behalf of the organization - All information stored, processed, or transmitted using cloud services - All cloud service providers engaged by the organization

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Evaluating cloud services for security risks before adoption - Implementing appropriate security controls for cloud services - Ensuring cloud services comply with legal, regulatory, and contractual requirements - Managing cloud service provider relationships securely - Monitoring cloud services for security issues - Maintaining ownership and control of organizational data in the cloud

2. Cloud Service Risk Management

2.1 Risk Assessment

- A risk assessment shall be conducted before adopting any cloud service
- Risk assessments shall consider:
  - Sensitivity and criticality of data to be stored or processed
  - Security capabilities of the cloud service provider
  - Compliance with regulatory requirements
  - Data sovereignty and location requirements
  - Business continuity and disaster recovery capabilities
  - Exit strategy and data portability
- Risk assessment results shall be documented and approved by management
- Risk assessments shall be updated periodically and when significant changes occur

2.2 Cloud Service Classification

Cloud services shall be classified based on: - Criticality to business operations - Sensitivity of data processed or stored - Compliance requirements - Integration with other systems - User base and access requirements

2.3 Cloud Service Provider Evaluation

Cloud service providers shall be evaluated based on: - Security controls and capabilities - Compliance with relevant standards (e.g., ISO 27001, SOC 2) - Industry reputation and experience - Financial stability - Service level agreements - Security incident history - Geographic location of data centers - Subcontractor management

3. Cloud Security Requirements

3.1 Data Security

3.1.1 Data Classification

- Data shall be classified according to the Information Classification Policy
- Cloud usage shall be aligned with data classification requirements
- Highly sensitive data may have additional restrictions for cloud storage

3.1.2 Data Encryption

- Sensitive data shall be encrypted during transmission to and from cloud services

- Sensitive data shall be encrypted at rest in cloud storage
- Encryption keys shall be managed according to the Cryptography Policy
- Where possible, the organization shall maintain control of encryption keys

3.1.3 Data Sovereignty

- Data location requirements shall be identified based on legal and regulatory requirements
- Cloud services shall comply with data sovereignty requirements
- Data transfer across borders shall comply with relevant regulations

3.1.4 Data Retention and Disposal

- Data retention periods shall be defined and implemented
- Data disposal shall be secure and verifiable
- Cloud service providers shall provide evidence of secure data deletion
- Backup and archive data shall be included in retention and disposal procedures

3.2 Identity and Access Management

3.2.1 User Access Management

- Access to cloud services shall follow the principle of least privilege
- User provisioning and de-provisioning processes shall be documented and followed
- Regular access reviews shall be conducted
- Privileged access shall be strictly controlled and monitored
- Where possible, centralized identity management shall be implemented

3.2.2 Authentication

- Strong authentication shall be required for cloud service access
- Multi-factor authentication shall be implemented for:
    - Administrative access
    - Access to sensitive data
    - Remote access to cloud services
- Password policies shall comply with the Password Policy
- Single sign-on should be implemented where appropriate

3.2.3 Federation

- Identity federation shall be implemented where appropriate
- Federation protocols shall be securely configured

- Federation relationships shall be documented and reviewed

3.3 Cloud Infrastructure Security

3.3.1 Network Security

- Network connections to cloud services shall be secured
- Virtual private networks or dedicated connections shall be used where appropriate
- Network traffic shall be monitored and controlled
- Firewalls and security groups shall be properly configured
- Network segmentation shall be implemented in cloud environments

3.3.2 Compute Security

- Virtual machines and containers shall be hardened
- Operating systems and applications shall be kept updated
- Unnecessary services shall be disabled
- Host-based security controls shall be implemented
- Server images and templates shall be securely configured

3.3.3 Storage Security

- Access to storage services shall be restricted
- Shared storage shall be properly secured
- Storage encryption shall be implemented
- Storage access logs shall be maintained
- Backup storage shall be secured

3.4 Application Security

3.4.1 Secure Development

- Cloud applications shall be developed following secure development practices
- Security testing shall be performed before deployment
- Application security controls shall be implemented
- API security shall be addressed
- Secure coding standards shall be followed

3.4.2 Configuration Management

- Cloud services shall be securely configured
- Configuration changes shall follow change management procedures

- Configuration baselines shall be established
- Configuration drift shall be monitored
- Infrastructure as Code shall be securely implemented

4. Cloud Service Provider Management

4.1 Contractual Requirements

- Cloud service contracts shall include security requirements
- Service level agreements shall address security aspects
- Right to audit shall be included where appropriate
- Security incident notification requirements shall be specified
- Data ownership and return shall be clearly defined
- Exit strategy shall be addressed

4.2 Compliance Requirements

- Cloud services shall comply with relevant regulations
- Compliance responsibilities shall be clearly defined
- Evidence of compliance shall be obtained and reviewed
- Compliance gaps shall be addressed
- Compliance status shall be regularly monitored

4.3 Vendor Management

- Cloud service providers shall be included in the supplier management program
- Performance shall be regularly reviewed
- Security issues shall be promptly addressed
- Communication channels shall be established
- Relationship managers shall be assigned

5. Cloud Security Operations

5.1 Monitoring and Logging

5.1.1 Security Monitoring

- Cloud services shall be monitored for security events
- Monitoring shall cover:
  - Access attempts and authentication events
  - Administrative activities
  - Configuration changes
  - Data access and modification

    - System performance and availability
- Alerts shall be configured for suspicious activities
- Monitoring data shall be protected from tampering

5.1.2 Logging

- Logs shall be collected from cloud services
- Log retention periods shall be defined
- Logs shall be protected from unauthorized access and modification
- Log analysis shall be performed regularly
- Log correlation shall be implemented where possible

5.2 Vulnerability Management

5.2.1 Vulnerability Assessment

- Cloud environments shall be included in vulnerability assessments
- Vulnerability scanning shall be performed regularly
- Vulnerabilities shall be prioritized and remediated
- Vulnerability management responsibilities shall be defined
- Vulnerability trends shall be analyzed

5.2.2 Patch Management

- Cloud systems shall be patched according to the Patch Management Policy
- Patching responsibilities shall be clearly defined
- Patch testing shall be performed before deployment
- Emergency patching procedures shall be established
- Patch compliance shall be monitored

5.3 Incident Response

5.3.1 Incident Detection and Reporting

- Cloud security incidents shall be promptly detected and reported
- Incident response procedures shall include cloud-specific scenarios
- Cloud service providers shall report security incidents affecting the organization
- Incident reporting channels shall be established

5.3.2 Incident Investigation

- Cloud forensic capabilities shall be established

- Evidence collection procedures shall be documented
- Investigation tools shall be available
- Cloud service providers shall cooperate with investigations
- Chain of custody shall be maintained

6. Business Continuity and Disaster Recovery

6.1 Continuity Planning

- Cloud services shall be included in business continuity plans
- Recovery time objectives and recovery point objectives shall be defined
- Dependencies on cloud services shall be documented
- Alternative processing capabilities shall be identified
- Continuity plans shall be tested regularly

6.2 Backup and Recovery

- Critical data in cloud services shall be backed up
- Backup strategy shall be documented
- Backup verification shall be performed regularly
- Recovery procedures shall be documented and tested
- Backup responsibilities shall be clearly defined

6.3 Exit Strategy

- Exit strategies shall be developed for cloud services
- Data export capabilities shall be verified
- Alternative providers or solutions shall be identified
- Exit costs shall be estimated
- Exit testing shall be performed where feasible

7. Cloud Security Awareness and Training

7.1 User Training

- Cloud security awareness training shall be provided to all users
- Training shall cover:
    - Secure use of cloud services
    - Data protection requirements
    - Access control responsibilities
    - Incident reporting procedures
    - Compliance requirements
- Training shall be updated as cloud services evolve

- Training effectiveness shall be measured

7.2 Administrator Training

- Cloud administrators shall receive specialized training
- Training shall cover:
  - Secure configuration
  - Monitoring and incident response
  - Compliance requirements
  - Service-specific security features
  - Emerging cloud security threats
- Certification shall be encouraged where appropriate
- Knowledge sharing shall be promoted

8. Compliance and Audit

8.1 Regulatory Compliance

- Cloud services shall comply with applicable regulations
- Compliance requirements shall be documented
- Compliance shall be regularly assessed
- Compliance gaps shall be addressed
- Regulatory changes shall be monitored

8.2 Security Assessments

- Cloud services shall be included in security assessments
- Assessment scope and frequency shall be based on risk
- Assessment results shall be documented and tracked
- Remediation actions shall be implemented
- Assessment methodologies shall be appropriate for cloud environments

8.3 Audit

- Cloud services shall be included in audit scope
- Audit rights shall be established with cloud service providers
- Audit evidence shall be collected and maintained
- Audit findings shall be addressed
- Audit logs shall be protected

9. Roles and Responsibilities

9.1 Management

- Approve cloud security policy
- Ensure adequate resources for cloud security
- Review cloud security status regularly
- Approve high-risk cloud services
- Support cloud security initiatives

9.2 Information Security Team

- Develop and maintain cloud security standards
- Conduct cloud risk assessments
- Review cloud service security
- Monitor cloud security compliance
- Respond to cloud security incidents

9.3 IT Department

- Implement cloud security controls
- Configure cloud services securely
- Monitor cloud services
- Maintain cloud documentation
- Support cloud security assessments

9.4 Cloud Users

- Follow cloud security procedures
- Protect access credentials
- Report security incidents
- Use cloud services appropriately
- Participate in security awareness training

10. Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

11. Related Documents

- Information Security Policy

- Data Protection Policy
- Access Control Policy
- Supplier Relationship Security Policy
- Business Continuity Policy
- Incident Management Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

12. Approval

This Cloud Security Policy is approved by:

Name: _______________________ Position: _____________________ Date: ________________________ Signature: ____________________