Third-Party Security Policy Template

Document Control Information

- **Document Title:** Third-Party 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 Third-Party Security Policy establishes [ORGANIZATION NAME]'s requirements for managing information security risks associated with third parties that access, process, store, or transmit organizational information, or provide IT services and products, in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that third-party relationships do not compromise the security of the organization's information assets.

1.2 Scope

This policy applies to: - All third parties that have access to [ORGANIZATION NAME]'s information or information systems - All third parties that process, store, or transmit organizational information - All third parties that provide IT services, products, or solutions - All third-party relationships throughout their lifecycle, from selection to termination - All employees responsible for managing third-party relationships

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Identifying and managing information security risks associated with third-party relationships - Establishing security requirements for third parties based on risk assessment - Implementing appropriate controls to protect information shared with third parties - Monitoring third-party compliance with security requirements - Maintaining secure third-party relationships throughout their lifecycle

2. Third-Party Risk Management

2.1 Risk Assessment

- Third-party security risks shall be assessed before engagement
- Risk assessments shall consider:
  - Type and sensitivity of information accessed by the third party
  - Services provided by the third party
  - Third-party access to systems and networks
  - Regulatory and compliance requirements
  - Potential impact of security incidents involving the third party
  - Third-party security capabilities and controls
- Risk assessments shall be documented and reviewed periodically
- Risk assessment results shall determine security requirements for the third party

2.2 Third-Party Categorization

Third parties shall be categorized based on risk level: - **Critical**: Third parties that have access to highly sensitive information, provide critical services, or have direct access to internal systems - **High**: Third parties that have access to sensitive information or provide important services - **Medium**: Third parties that have limited access to sensitive information or provide non-critical services - **Low**: Third parties that have no access to sensitive information and provide commodity services

2.3 Due Diligence

- Security due diligence shall be performed before engaging with new third parties
- Due diligence shall include assessment of:
  - Security capabilities and controls
  - Compliance with relevant standards and regulations
  - Security certifications (e.g., ISO 27001, SOC 2)
  - Security incident history
  - Financial stability
  - Business continuity capabilities
- Due diligence results shall be documented and considered in third-party selection
- Due diligence depth shall be proportionate to the risk level

3. Third-Party Security Requirements

3.1 General Security Requirements

All third parties shall: - Comply with relevant laws, regulations, and contractual obligations - Implement security controls appropriate to the services provided - Report security incidents that may affect [ORGANIZATION NAME] - Maintain confidentiality of [ORGANIZATION NAME]'s information - Return or securely destroy [ORGANIZATION NAME]'s information upon request or contract termination - Provide security documentation upon request

3.2 Tiered Security Requirements

Security requirements shall be based on third-party categorization:

3.2.1 Critical Third Parties

- Maintain ISO 27001 certification or equivalent
- Provide evidence of regular security assessments
- Implement comprehensive security controls
- Allow [ORGANIZATION NAME] to conduct security audits
- Provide security incident notification within [24] hours
- Maintain detailed security documentation
- Implement business continuity and disaster recovery plans
- Conduct regular security testing
- Provide security metrics and reports

3.2.2 High-Risk Third Parties

- Implement industry-standard security controls
- Provide evidence of security assessments
- Allow [ORGANIZATION NAME] to conduct security reviews
- Provide security incident notification within [48] hours
- Maintain security documentation
- Implement business continuity plans
- Conduct periodic security testing

3.2.3 Medium-Risk Third Parties

- Implement basic security controls
- Complete security questionnaires
- Report security incidents that may affect [ORGANIZATION NAME]
- Maintain basic security documentation

3.2.4 Low-Risk Third Parties

- Comply with general security requirements
- Report significant security incidents

3.3 Specific Security Requirements

Specific security requirements shall be defined based on: - Type of service provided - Type of information accessed - Access methods and technologies used - Regulatory and compliance requirements - Industry-specific requirements

4. Contractual Requirements

4.1 Security Clauses

Third-party contracts shall include: - Clearly defined security requirements - Confidentiality and non-disclosure provisions - Data protection requirements - Intellectual property protection - Right to audit or assess security controls - Security incident reporting requirements - Business continuity requirements - Compliance with laws and regulations - Consequences of non-compliance - Termination provisions for security breaches

4.2 Service Level Agreements

Security-related service level agreements shall include: - Security performance metrics - Security reporting requirements - Response times for security incidents - Patching and vulnerability management timeframes - Availability requirements - Penalties for security-related non-compliance

4.3 Contract Review

- Contracts shall be reviewed by legal, procurement, and information security
- Security requirements shall be clearly documented
- Contracts shall be reviewed periodically
- Contract changes shall be assessed for security impact
- Contract reviews shall be documented

5. Third-Party Access Management

5.1 Access Principles

- Third-party access shall follow the principle of least privilege

- Access shall be limited to information and systems necessary for service provision
- Access shall be time-limited where appropriate
- Access shall be regularly reviewed and updated
- Access shall be promptly revoked when no longer required

5.2 Access Controls

- Third-party access shall be documented and approved
- Strong authentication shall be required for third-party access
- Multi-factor authentication shall be required for critical systems
- Third-party access shall be logged and monitored
- Privileged access shall be strictly controlled
- Remote access shall use secure methods

5.3 Access Review

- Third-party access shall be reviewed at least quarterly
- Access reviews shall verify continued business need
- Unnecessary access shall be promptly removed
- Access review results shall be documented
- Access review shall be performed by appropriate personnel

6. Third-Party Monitoring and Performance

6.1 Security Monitoring

- Third-party activities shall be monitored for security issues
- Monitoring shall be proportionate to risk and access level
- Monitoring may include:
  - Access logs review
  - Security event monitoring
  - Vulnerability scanning
  - Performance monitoring
  - Compliance monitoring
- Monitoring results shall be regularly reviewed
- Security issues shall be promptly addressed

6.2 Performance Evaluation

- Third-party security performance shall be regularly evaluated
- Evaluation criteria shall include:
  - Compliance with security requirements

    - Security incident response
    - Vulnerability management
    - Security control effectiveness
    - Security improvement initiatives
- Performance evaluations shall be documented and shared with third parties
- Performance issues shall be addressed through improvement plans

6.3 Security Reporting

- Third parties shall provide security reports as required
- Reports may include:
    - Security control status
    - Security incident summary
    - Vulnerability management metrics
    - Compliance status
    - Security improvement activities
- Report frequency shall be based on third-party categorization
- Reports shall be reviewed and issues addressed

7. Third-Party Security Assessment

7.1 Initial Assessment

- Security assessments shall be conducted before engaging critical and high-risk third parties
- Assessments may include:
    - Security questionnaires
    - Documentation review
    - On-site assessments
    - Technical testing
    - Certification verification
- Assessment results shall be documented and considered in third-party selection
- Assessment scope shall be based on risk and services provided

7.2 Ongoing Assessment

- Periodic security assessments shall be conducted based on third-party categorization:
    - Critical third parties: Annually
    - High-risk third parties: Every two years
    - Medium-risk third parties: Upon significant changes
- Assessments shall verify continued compliance with security requirements

- Assessment scope shall be based on risk and changes since the last assessment
- Assessment results shall be documented and issues addressed

7.3 Assessment Methods

Assessment methods may include: - Self-assessment questionnaires - Remote assessments - On-site audits - Technical testing - Third-party assessment reports - Certification verification

8. Information Sharing and Communication

8.1 Information Classification and Handling

- Information shared with third parties shall be classified according to sensitivity
- Information handling requirements shall be communicated to third parties
- Third parties shall implement appropriate controls based on classification
- Sensitive information shall be protected during transmission and storage
- Information sharing shall be documented and approved

8.2 Communication Channels

- Secure communication channels shall be established with third parties
- Communication methods shall be appropriate for information sensitivity
- Emergency contact information shall be maintained
- Communication protocols shall be documented
- Communication effectiveness shall be regularly assessed

8.3 Security Knowledge Sharing

- Security requirements and expectations shall be clearly communicated
- Security awareness materials may be shared with third parties
- Security best practices shall be promoted
- Security concerns shall be promptly communicated
- Knowledge sharing effectiveness shall be assessed

9. Third-Party Security Incident Management

9.1 Incident Reporting

- Third parties shall report security incidents that may affect [ORGANIZATION NAME]
- Reporting timeframes shall be based on third-party categorization and incident severity

- Reporting procedures shall be documented and communicated
- Incident reports shall include required information
- Reporting compliance shall be monitored

9.2 Incident Response

- Incident response procedures shall be established for third-party incidents
- Roles and responsibilities shall be clearly defined
- Communication protocols shall be established
- Escalation procedures shall be documented
- Evidence preservation requirements shall be communicated
- Response effectiveness shall be assessed after incidents

9.3 Incident Investigation

- Security incidents shall be investigated according to their severity
- Root cause analysis shall be performed
- Corrective actions shall be identified and implemented
- Lessons learned shall be documented
- Incident reports shall be maintained
- Investigation results shall be shared as appropriate

10. Third-Party Relationship Termination

10.1 Termination Planning

- Security considerations shall be included in termination planning
- Information and asset return or destruction shall be planned
- Access revocation shall be scheduled
- Knowledge transfer shall be arranged
- Transition to new third parties shall include security requirements
- Termination planning shall be documented

10.2 Termination Activities

- All access rights shall be promptly revoked
- Information and assets shall be returned or securely destroyed
- Confidentiality obligations shall continue after termination
- Termination activities shall be documented
- Compliance with termination requirements shall be verified
- Post-termination security risks shall be assessed

11. Cloud Service Providers

11.1 Cloud Security Requirements

- Cloud service providers shall implement security controls aligned with industry standards
- Data sovereignty and location requirements shall be defined
- Data protection and encryption requirements shall be specified
- Access control and identity management shall be addressed
- Monitoring and logging requirements shall be defined
- Incident response capabilities shall be assessed
- Exit strategy shall be defined

11.2 Cloud Service Agreements

- Cloud service agreements shall include security requirements
- Service level agreements shall address security aspects
- Right to audit shall be included where appropriate
- Data ownership and return shall be clearly defined
- Compliance with regulations shall be addressed
- Exit strategy shall be documented
- Agreement terms shall be regularly reviewed

12. Software and Product Vendors

12.1 Secure Development

- Software vendors shall follow secure development practices
- Secure development requirements shall be specified
- Security testing shall be performed before acceptance
- Vulnerabilities shall be addressed promptly
- Security updates shall be provided in a timely manner
- Secure configuration guidance shall be provided
- Security documentation shall be maintained

12.2 Product Security Assessment

- Products shall be assessed for security before procurement
- Assessment shall include:
    - Security features and capabilities
    - Known vulnerabilities
    - Vendor security practices
    - Support and update policies

    - Compliance with requirements
- Assessment results shall be documented
- Security issues shall be addressed before implementation

13. Outsourced Services

13.1 Outsourcing Security

- Outsourced services shall meet the same security requirements as internal services
- Security responsibilities shall be clearly defined
- Service provider personnel shall meet security requirements
- Service provider facilities shall meet security requirements
- Service provider subcontractors shall be approved
- Service quality and security shall be regularly assessed
- Outsourcing risks shall be regularly reviewed

13.2 Managed Security Services

- Managed security service providers shall meet enhanced security requirements
- Service scope and responsibilities shall be clearly defined
- Performance metrics shall be established and monitored
- Incident response procedures shall be coordinated
- Regular service reviews shall be conducted
- Security effectiveness shall be regularly assessed
- Service improvements shall be implemented

14. Roles and Responsibilities

14.1 Procurement Department

- Include security requirements in procurement processes
- Ensure security requirements are included in contracts
- Coordinate third-party selection with security input
- Maintain third-party information
- Support third-party risk assessments
- Coordinate contract reviews
- Support termination processes

14.2 Information Security Team

- Define security requirements for third parties
- Conduct or review security assessments

- Provide security expertise during third-party selection
- Monitor third-party security compliance
- Respond to third-party security incidents
- Provide security guidance
- Report on third-party security status

14.3 Business Owners

- Identify business requirements for third-party relationships
- Ensure third parties meet business and security requirements
- Monitor third-party performance
- Report security concerns
- Maintain regular communication with third parties
- Support security assessments
- Participate in incident response

14.4 Legal Department

- Review contracts for security and compliance requirements
- Ensure appropriate legal protections are in place
- Advise on regulatory requirements
- Support enforcement of contractual security obligations
- Advise on incident response legal aspects
- Support termination processes
- Provide guidance on legal issues

15. Compliance and Exceptions

15.1 Compliance Monitoring

- Third-party compliance with security requirements shall be regularly monitored
- Non-compliance shall be documented and addressed
- Compliance reports shall be provided to management
- Compliance trends shall be analyzed
- Compliance monitoring methods shall be regularly reviewed
- Compliance effectiveness shall be assessed

15.2 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

16. Related Documents

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

17. Approval

This Third-Party Security Policy is approved by:

Name: _____ Position: _____ Date: _____ Signature: _____