Supplier Relationship Security Policy Template

Document Control Information

- **Document Title:** Supplier Relationship 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 Supplier Relationship Security Policy establishes [ORGANIZATION NAME]'s requirements for managing information security risks associated with suppliers and third parties in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that suppliers maintain appropriate security controls to protect the organization's information assets.

1.2 Scope

This policy applies to: - All suppliers, vendors, contractors, and third parties that provide goods or services to [ORGANIZATION NAME] - All suppliers that have access to, process, store, or transmit [ORGANIZATION NAME]'s information - All supplier relationships throughout their lifecycle, from selection to termination - All employees responsible for managing supplier relationships

1.3 Policy Statement

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

2. Supplier Risk Management

2.1 Supplier Risk Assessment

- Suppliers shall be categorized based on the criticality of services provided and access to information
- Risk assessments shall be conducted for all suppliers before engagement
- Risk assessments shall consider:
    - Type and sensitivity of information accessed by the supplier
    - Services provided by the supplier
    - Supplier access to systems and networks
    - Regulatory and compliance requirements
    - Potential impact of security incidents involving the supplier
- Risk assessments shall be documented and reviewed periodically
- Risk assessment results shall determine security requirements for the supplier

2.2 Supplier Categorization

Suppliers shall be categorized as follows: - **Critical**: Suppliers that have access to highly sensitive information, provide critical services, or have direct access to internal systems - **Significant**: Suppliers that have access to sensitive information or provide important services - **Standard**: Suppliers that have limited access to information or provide non-critical services - **Low Risk**: Suppliers that have no access to sensitive information and provide commodity services

2.3 Due Diligence

- Due diligence shall be performed before engaging with new suppliers
- 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 supplier selection

3. Supplier Security Requirements

3.1 General Security Requirements

All suppliers 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 supplier categorization:

3.2.1 Critical Suppliers

- 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 Significant Suppliers

- 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 Standard Suppliers

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

3.2.4 Low Risk Suppliers

- 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

Supplier 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

5. Supplier Access Management

5.1 Access Principles

- Supplier 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

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

5.3 Access Review

- Supplier 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

6. Supplier Monitoring and Performance

6.1 Security Monitoring

- Supplier 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

6.2 Performance Evaluation

- Supplier 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 suppliers

6.3 Security Reporting

- Suppliers 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 supplier categorization

7. Supplier Security Assessment

7.1 Initial Assessment

- Security assessments shall be conducted before engaging critical and significant suppliers
- Assessments may include:
    - Security questionnaires
    - Documentation review
    - On-site assessments
    - Technical testing
    - Certification verification
- Assessment results shall be documented and considered in supplier selection

7.2 Ongoing Assessment

- Periodic security assessments shall be conducted based on supplier categorization:
    - Critical suppliers: Annually
    - Significant suppliers: Every two years
    - Standard suppliers: Upon significant changes
- Assessments shall verify continued compliance with security requirements
- Assessment scope shall be based on risk and changes since the last assessment

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 suppliers shall be classified according to sensitivity

- Information handling requirements shall be communicated to suppliers
- Suppliers shall implement appropriate controls based on classification
- Sensitive information shall be protected during transmission and storage

8.2 Communication Channels

- Secure communication channels shall be established with suppliers
- Communication methods shall be appropriate for information sensitivity
- Emergency contact information shall be maintained
- Communication protocols shall be documented

8.3 Security Knowledge Sharing

- Security requirements and expectations shall be clearly communicated
- Security awareness materials may be shared with suppliers
- Security best practices shall be promoted
- Security concerns shall be promptly communicated

9. Supplier Security Incident Management

9.1 Incident Reporting

- Suppliers shall report security incidents that may affect [ORGANIZATION NAME]
- Reporting timeframes shall be based on supplier categorization and incident severity
- Reporting procedures shall be documented and communicated
- Incident reports shall include required information

9.2 Incident Response

- Incident response procedures shall be established for supplier incidents
- Roles and responsibilities shall be clearly defined
- Communication protocols shall be established
- Escalation procedures shall be documented
- Evidence preservation requirements shall be communicated

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

10. Supplier 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 suppliers shall include security requirements

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

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

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

12. Roles and Responsibilities

12.1 Procurement Department

- Include security requirements in procurement processes

- Ensure security requirements are included in contracts
- Coordinate supplier selection with security input
- Maintain supplier information

12.2 Information Security Team

- Define security requirements for suppliers
- Conduct or review security assessments
- Provide security expertise during supplier selection
- Monitor supplier security compliance
- Respond to supplier security incidents

12.3 Business Owners

- Identify business requirements for supplier relationships
- Ensure suppliers meet business and security requirements
- Monitor supplier performance
- Report security concerns
- Maintain regular communication with suppliers

12.4 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

13. Compliance and Exceptions

13.1 Compliance Monitoring

- Supplier 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

13.2 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

14. Related Documents

- Information Security Policy
- Third-Party Risk Management Procedure
- Supplier Security Assessment Procedure
- Cloud Security Policy
- Data Protection Policy
- Access Control Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

15. Approval

This Supplier Relationship Security Policy is approved by:

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