Vendor Risk Management Policy

Document ID: COM-SEC-025 **Effective Date:** January 1, 2024 **Last Reviewed:** March 2024 **Owner:** Security & Compliance **Applies To:** All Third-Party Vendors

---

Purpose

This policy establishes the framework for assessing, managing, and monitoring risks associated with third-party vendors who have access to NovaTech data, systems, or facilities.

Scope

This policy applies to: - Software-as-a-Service (SaaS) providers - Infrastructure and hosting providers - Professional services firms - Data processors and subprocessors - Consultants with system access - Any third party handling NovaTech or customer data

---

Risk Tiers

Tier 1: Critical

Criteria: - Access to customer data - Access to production systems - Processing sensitive data (PII, financial, health) - Business-critical services (>$100K/year spend)

Examples: AWS, Okta, Salesforce, major data processors

Requirements: - Full security questionnaire - SOC 2 Type II report - Annual on-site or virtual assessment - Continuous monitoring - Contractual security requirements - Annual review

Tier 2: High

Criteria: - Access to internal systems - Access to employee data - Moderate business impact - $25K-$100K annual spend

Examples: HR systems, marketing tools, development tools

Requirements: - Security questionnaire - SOC 2 report (Type I acceptable) - Contractual security terms - Annual review

Tier 3: Medium

Criteria: - Limited system access - No sensitive data access - <$25K annual spend

Examples: Office supplies, professional services (no data access)

Requirements: - Abbreviated security questionnaire - Basic due diligence - Standard contract terms - Biennial review

Tier 4: Low

Criteria: - No system or data access - Transactional relationships

Examples: Catering, facilities, general contractors

Requirements: - Basic background check if on-site - Standard contract terms

---

Vendor Assessment Process

1. Initial Assessment

Requestor responsibilities: 1. Submit vendor request via procurement system 2. Provide business justification 3. Identify data and systems vendor will access 4. Specify contract value and duration

Security team responsibilities: 1. Assign risk tier 2. Send appropriate questionnaire 3. Review responses within 10 business days 4. Document findings

2. Security Questionnaire

Tier 1/2 questions include:

Category	Sample Questions
Governance	Security policies, certifications, incident response
Access Control	Authentication, authorization, privileged access
Data Protection	Encryption, data handling, retention
Network Security	Firewalls, segmentation, monitoring
Application Security	SDLC, vulnerability management, testing
Operations	Logging, backups, disaster recovery
Compliance	Certifications, audits, regulatory compliance
Personnel	Background checks, training, termination

3. Documentation Review

Required documentation by tier:

Document	Tier 1	Tier 2	Tier 3
SOC 2 Type II	Required	Preferred	Optional
SOC 2 Type I	-	Acceptable	Optional
ISO 27001	Preferred	Optional	Optional
Penetration test results	Required	Optional	-
Insurance certificates	Required	Required	Optional
Privacy policy	Required	Required	Required

4. Risk Scoring

Score	Rating	Action
0-30	Low	Approve
31-60	Medium	Approve with conditions
61-80	High	Remediation required
81-100	Critical	Do not approve

Contractual Requirements

Security Terms (Tier 1/2)

All Tier 1 and 2 vendors must agree to:

1. **Data Protection**

- Encryption at rest and in transit
- Data classification compliance
- Data retention and deletion

2. **Access Control**
    - Least privilege access
    - MFA for administrative access
    - Access logging
3. **Incident Response**
    - 24-hour breach notification
    - Cooperation in investigations
    - Root cause analysis
4. **Audit Rights**
    - Annual questionnaire completion
    - Audit and assessment rights
    - Compliance evidence provision
5. **Insurance**
    - Cyber liability insurance
    - Professional liability insurance
    - Coverage minimums based on tier

Data Processing Agreement (DPA)

Required for vendors processing personal data: - GDPR-compliant terms - Sub-processor notification - Data subject request procedures - Data transfer mechanisms

---

Ongoing Monitoring

Continuous Monitoring (Tier 1)

Activity	Frequency
Security rating service	Continuous
Dark web monitoring	Continuous
News and breach alerts	Daily
SOC 2 report review	Annual
Security questionnaire	Annual

Periodic Monitoring (Tier 2/3)

Activity	Tier 2	Tier 3
Security questionnaire	Annual	Biennial
Certification verification	Annual	Biennial
Contract review	Annual	At renewal

Monitoring Tools

- **SecurityScorecard:** External security ratings
- **BitSight:** Third-party risk monitoring
- **OneTrust:** Vendor management platform

Incident Management

Vendor Security Incidents

If a vendor experiences a security incident:

1. **Immediate (within 24 hours)**
   - Vendor notifies NovaTech
   - Security team assesses impact
   - Determine if customer notification needed
2. **Investigation (within 72 hours)**
   - Request incident details
   - Assess data exposure
   - Determine remediation needs
3. **Resolution**
   - Verify remediation complete
   - Update risk assessment
   - Document lessons learned
   - Determine relationship continuity

Escalation Path

Impact	Escalate To
Customer data exposed	CISO, Legal, Executive team
Internal data exposed	CISO, affected department
Service disruption	IT, affected department
Potential breach	CISO, Legal

Vendor Offboarding

When vendor relationship ends:

1. **Data Return/Deletion**
   - Request data return (if applicable)
   - Request certificate of destruction
   - Verify deletion within 30 days
2. **Access Revocation**
   - Revoke all system access
   - Disable API keys and tokens
   - Remove from security groups
3. **Contract Closeout**
   - Confirm final invoicing
   - Document lessons learned
   - Archive vendor file

Roles and Responsibilities

Security Team

- Maintain vendor assessment process
- Review security questionnaires
- Conduct risk scoring
- Monitor vendor security posture
- Manage incidents

Procurement

- Ensure security review before contracting
- Include security terms in contracts
- Track vendor inventory
- Manage renewals

Legal

- Review and negotiate security terms
- Ensure DPA compliance
- Support incident response

Business Owners

- Submit vendor requests
- Provide business justification
- Monitor vendor performance
- Report security concerns

Compliance Requirements

Regulatory Alignment

Regulation	Vendor Requirements
GDPR	DPA, subprocessor management
SOC 2	Vendor management controls
HIPAA	BAA for PHI access
PCI-DSS	Service provider compliance

Audit Evidence

Maintain documentation for: - Vendor inventory - Risk assessments - Security questionnaires - Contracts with security terms - Monitoring records - Incident documentation

---

Exceptions

Exceptions to this policy require: - Written business justification - Compensating controls - CISO approval - Time-limited approval (max 1 year) - Documentation in exception register

---

Training

All employees involved in vendor management must complete: - Vendor risk management training (annual) - Data protection awareness (annual) - Procurement process training

---

Contact

- **Security Team:** security@novatech.com
- **Procurement:** procurement@novatech.com
- **Legal:** legal@novatech.com

Related Documents: Data Classification (IT-SEC-005), Information Security Policy (IT-SEC-001), Privacy Policy (COM-DP-001)