# Vendor Security Requirements

**Document ID:** COM-SC-010 **Last Updated:** 2024-02-05 **Owner:** Security & Compliance **Classification:** Internal

---

## Purpose

This document outlines the security requirements for third-party vendors who access, process, store, or transmit NovaTech data or connect to NovaTech systems.

---

## Scope

### Covered Vendors

- SaaS providers
- Infrastructure providers
- Professional services firms
- Contractors with system access
- Subprocessors handling customer data

### Exclusions

- Vendors with no data access (office supplies, etc.)
- One-time purchases without ongoing relationship

---

## Risk Tiering

### Tier 1: Critical

**Criteria:** - Access to customer data - Integration with production systems - Single point of failure potential - Annual spend > $100,000

**Requirements:** Full security assessment, annual review, SLA requirements

**Examples:** Cloud providers, payment processors, core SaaS tools

### Tier 2: High

**Criteria:** - Access to internal confidential data - Integration with internal systems - Significant business dependency - Annual spend $25,000 - $100,000

**Requirements:** Security questionnaire, SOC 2 report, biennial review

**Examples:** HR systems, analytics platforms, dev tools

### Tier 3: Standard

**Criteria:** - Limited data access - No production integration - Easy to replace - Annual spend < $25,000

**Requirements:** Basic security review, contract terms

**Examples:** Productivity tools, design software

---

## Security Requirements by Tier

### Tier 1 Requirements

### Documentation Required

- ☐ SOC 2 Type II report (current)
- ☐ Penetration test results (annual)
- ☐ Security questionnaire (detailed)
- ☐ Business continuity plan
- ☐ Incident response plan

### Technical Controls

| Control | Requirement |
|---|---|
| Encryption at rest | AES-256 or equivalent |
| Encryption in transit | TLS 1.2+ |
| MFA | Required for all access |
| Access logging | Complete audit trail |
| Backup | Daily, encrypted, tested |
| Vulnerability scanning | Weekly minimum |
| Penetration testing | Annual |

### Contractual Terms

- Data Processing Agreement (DPA)
- Security addendum
- SLA with uptime guarantee (99.9%+)
- Incident notification (24 hours)
- Right to audit
- Insurance requirements

### Tier 2 Requirements

### Documentation Required

☐ SOC 2 Type II report OR ISO 27001 certificate
☐ Security questionnaire
☐ Privacy policy review

### Technical Controls

| Control | Requirement |
|---|---|
| Encryption at rest | Required |
| Encryption in transit | TLS 1.2+ |
| MFA | Required for admin access |
| Access logging | Required |
| Vulnerability scanning | Monthly minimum |

### Contractual Terms

- Data Processing Agreement (if applicable)
- Confidentiality terms
- Incident notification (72 hours)

### Tier 3 Requirements

### Documentation Required

☐ Security questionnaire (abbreviated)
☐ Privacy policy review

### Technical Controls

| Control | Requirement |
|---|---|
| Encryption in transit | TLS 1.2+ |
| Password requirements | Industry standard |

### Contractual Terms

- Standard terms of service review
- Confidentiality terms (if data shared)

---

## Assessment Process

### New Vendor Assessment

```
Request Submitted



  Classify Risk
  Tier




  Collect
  Documentation




  Security
  Review





 Approved   Requires
            Remediation
```

Work with
vendor

Contract
Negotiation

Onboard &
Monitor

### Timeline

| Tier | Initial Review | Contract Review | Total |
|---|---|---|---|
| 1 | 10 business days | 5-10 days | 3-4 weeks |
| 2 | 5 business days | 3-5 days | 2-3 weeks |
| 3 | 2 business days | 1-2 days | 1 week |

### Ongoing Monitoring

| Tier | Review Frequency | Activities |
|---|---|---|
| 1 | Annual | Full reassessment, SOC 2 review |
| 2 | Biennial | Questionnaire update, cert review |
| 3 | Triennial | Basic review |

---

## Security Questionnaire

### Core Questions (All Tiers)

1. Do you have a documented information security policy?

2. Do you encrypt data at rest and in transit?
3. How do you manage access control?
4. Do you have an incident response plan?
5. What certifications do you hold (SOC 2, ISO 27001, etc.)?

### Extended Questions (Tier 1-2)

6. Describe your vulnerability management program.
7. How frequently do you conduct penetration tests?
8. What is your business continuity/disaster recovery capability?
9. Do you use subprocessors? If so, how are they assessed?
10. How do you handle customer data deletion requests?
11. What logging and monitoring capabilities do you have?
12. Describe your physical security controls.
13. How are employees trained on security?
14. What is your patch management process?
15. Do you have cyber insurance? What are the coverage limits?

### Technical Assessment (Tier 1)

- Review of architecture documentation
- API security assessment
- Integration security review
- Data flow analysis

---

## Contractual Requirements

### Data Processing Agreement (DPA)

Required for vendors processing personal data: - Processing purposes and scope - Data subject rights support - Subprocessor requirements - Security obligations - Breach notification (without undue delay) - Data deletion/return on termination - Audit rights

### Security Addendum

For Tier 1-2 vendors: - Security control commitments - Compliance maintenance - Change notification - Incident response obligations - Insurance requirements

### Standard Clauses

All vendor contracts: - Confidentiality obligations - Data ownership - Termination rights - Indemnification

---

## Incident Response

### Vendor Incident Notification

Expected notification timelines:

| Tier | Notification | Initial Report | Full Report |
|---|---|---|---|
| 1 | 24 hours | 48 hours | 5 days |
| 2 | 72 hours | 5 days | 10 days |
| 3 | 5 days | 10 days | 15 days |

### NovaTech Response

Upon vendor incident notification: 1. Assess impact to NovaTech/customers 2. Engage incident response team 3. Coordinate with vendor on remediation 4. Notify affected parties if required 5. Document and conduct post-incident review

---

## Exception Process

### Request Exception

1. Submit exception request to Security team
2. Provide business justification
3. Identify compensating controls

### Approval

| Risk Level | Approver |
|---|---|
| Low | Security Manager |
| Medium | CISO |
| High | CISO + VP of affected area |

### Documentation

- Exception reason
- Risk acceptance
- Compensating controls
- Review date

---

## Roles and Responsibilities

### Security Team

- Define requirements
- Conduct assessments
- Approve vendors
- Monitor compliance

### Procurement

- Initiate vendor requests
- Coordinate assessment process
- Negotiate contracts

### Business Owners

- Sponsor vendor relationships
- Provide business justification
- Monitor vendor performance

### Legal

- Review contracts
- Negotiate legal terms
- DPA coordination

---

## Tools and Resources

### Vendor Management

- Vendor inventory: [Internal System]
- Risk assessments: [Security Portal]
- Contract repository: [Legal System]

### Templates

- Security questionnaire
- DPA template
- Security addendum

---

*Related Documents: SOC 2 Overview (COM-SC-001), Data Classification Policy (IT-SEC-005), Procurement Policy (FIN-PROC-001)*