Penetration Testing Policy

Document ID: COM-SC-020 **Effective Date:** January 1, 2024 **Last Updated:** February 2024 **Owner:** Information Security **Classification:** Internal

---

Purpose

This policy establishes requirements for conducting penetration testing to identify security vulnerabilities in NovaTech systems before they can be exploited by malicious actors.

Scope

This policy applies to: - All NovaTech production systems - Customer-facing applications - Internal applications and infrastructure - Cloud infrastructure - Third-party integrations

---

Testing Requirements

Mandatory Testing

Test Type	Frequency	Scope
External penetration test	Annual	All external-facing systems
Internal penetration test	Annual	Internal network and systems
Web application testing	Annual + after major releases	All customer-facing apps
API security testing	Annual + after major releases	All public APIs
Cloud security assessment	Annual	AWS, GCP, Azure environments

Trigger-Based Testing

Additional testing required for: - Major system changes or new deployments - After significant security incidents - New product launches - Acquisition of new systems - Compliance requirements (SOC 2, etc.)

Testing Types

External Penetration Testing

Objective: Identify vulnerabilities accessible from the internet

Scope: - Public-facing websites - APIs - VPN endpoints - Email systems - DNS infrastructure

Methodology: 1. Reconnaissance 2. Vulnerability scanning 3. Exploitation attempts 4. Privilege escalation 5. Lateral movement (if applicable)

Internal Penetration Testing

Objective: Identify vulnerabilities from inside the network

Scope: - Internal networks - Active Directory - Internal applications - Database servers - File shares

Methodology: 1. Assume compromised endpoint 2. Network discovery 3. Vulnerability identification 4. Privilege escalation 5. Access to sensitive data

Web Application Testing

Objective: Identify application-level vulnerabilities

Focus Areas: - OWASP Top 10 - Authentication/authorization flaws - Input validation - Session management - Business logic flaws - API security

Social Engineering (Optional)

Objective: Test human security awareness

Types: - Phishing simulations - Vishing (phone-based) - Physical security testing

Requirements: - HR and Legal approval - No punitive action for employees - Training follow-up

---

Authorized Testing Partners

Approved Vendors

Testing must be conducted by approved vendors: - Primary: SecureAudit Inc. - Secondary: CyberDefense Partners - Tertiary: RedTeam Security

Vendor Requirements

Approved vendors must have: - Industry certifications (CREST, OSCP, CEH) - Professional liability insurance ($5M minimum) - Non-disclosure agreement - Background checks on testers - Proven track record

Selecting a New Vendor

1. Security team identifies candidates
2. RFP process with security criteria
3. Vendor security assessment
4. Legal review of contract
5. CISO approval

Pre-Test Requirements

Authorization

Testing requires: 1. **Written authorization** from CISO 2. **Scope document** defining systems to test 3. **Rules of engagement** defining methods 4. **Communication plan** for emergencies 5. **Legal sign-off** for new vendors

Rules of Engagement

Define for each test: - In-scope systems (IPs, domains, applications) - Out-of-scope systems (production customer data, etc.) - Allowed techniques - Prohibited actions - Testing windows - Escalation contacts

Notification

Notify (as appropriate): - IT Operations (for monitoring awareness) - Cloud provider (if required by agreement) - Relevant system owners - Do NOT notify widely (to maintain test validity)

During Testing

Communication

- Daily status updates to security team
- Immediate notification of critical findings
- Emergency contact available 24/7
- Document all activities

Emergency Procedures

If testing causes service impact: 1. Tester stops immediately 2. Notifies security team 3. IT Operations investigates 4. Determine if testing-related 5. Resume only with approval

Finding Classification

Severity	Description	Example
Critical	Immediate exploitation risk	Remote code execution
High	Significant vulnerability	SQL injection, auth bypass
Medium	Moderate risk	XSS, information disclosure
Low	Minor risk	Missing headers, verbose errors
Informational	Best practice	Recommendations

Post-Test Requirements

Report Contents

Penetration test reports must include: - Executive summary - Detailed findings with evidence - Risk ratings - Affected systems - Reproduction steps - Remediation recommendations - Positive findings (what worked well)

Report Handling

- Reports classified as **Confidential**
- Distributed on need-to-know basis
- Stored in secure document repository
- Retained for 7 years

Remediation

Severity	Remediation Timeline
Critical	24-72 hours
High	7 days
Medium	30 days
Low	90 days
Informational	Best effort

Verification

- Critical/High findings require retest
- Retest within 30 days of remediation
- Document verification results

Internal Testing

Bug Bounty Program

NovaTech operates a bug bounty program: - Platform: HackerOne - Scope: Public-facing applications - Rewards: $100 - $10,000 based on severity

Security Team Testing

Internal security team conducts: - Continuous vulnerability scanning - Ad-hoc penetration testing - Red team exercises - Purple team exercises

Developer Testing

Developers should: - Use SAST tools during development - Run DAST scans in staging - Address security findings before release - Follow secure coding guidelines

---

Cloud-Specific Requirements

AWS Testing

- Notify AWS via support case (not required for most tests)
- Stay within NovaTech-owned resources
- No testing of AWS infrastructure itself
- Document any AWS service disruptions

GCP Testing

- Review GCP Acceptable Use Policy
- Stay within NovaTech projects
- No testing of GCP infrastructure

Azure Testing

- Review Azure penetration testing rules
- Stay within NovaTech subscriptions
- No testing of Azure infrastructure

Prohibited Activities

Testing must NOT: - Access customer production data - Cause denial of service (unless specifically authorized) - Modify production data - Test systems without authorization - Use zero-day exploits without approval - Conduct social engineering without HR approval - Test third-party systems without their consent

---

Compliance Integration

SOC 2

Annual penetration testing supports: - CC6.1: Security testing - CC7.1: Vulnerability management

ISO 27001

Supports: - A.12.6: Technical vulnerability management - A.14.2: Security testing

PCI DSS (if applicable)

- Requirement 11.3: Penetration testing
- Annual external testing
- Internal testing after changes

Metrics and Reporting

Track Metrics

- Number of tests conducted
- Findings by severity
- Mean time to remediate
- Retest pass rate
- Trend analysis

Quarterly Report

Security provides quarterly summary to: - Executive team - Audit committee - Relevant stakeholders

---

Roles and Responsibilities

CISO

- Approve testing scope and vendors
- Review critical findings
- Report to executive team

Security Team

- Coordinate testing activities
- Track remediation
- Maintain vendor relationships

System Owners

- Provide system information
- Implement remediations
- Verify fixes

Engineering Teams

- Remediate findings
- Participate in verification
- Implement preventive measures

Exceptions

Exceptions to this policy require: 1. Written request with justification 2. Risk assessment 3. CISO approval 4. Compensating controls 5. Time-limited exception

---

Related Documents

- Vulnerability Management Policy (IT-SEC-030)
- Incident Response Plan (IT-SEC-010)
- Security Best Practices (IT-SEC-001)
- Third-Party Security Requirements (COM-SC-010)

Questions

Contact: security@novatech.com

Last Review: January 2024 Next Review: January 2025