

# Fox ML Infrastructure — Penetration Testing Statement

This document outlines Fox ML Infrastructure's approach to penetration testing and security assessments.

This statement is essential for enterprise security reviews and SOC2-adjacent compliance.

---

## 1. Executive Summary

**Fox ML Infrastructure recognizes the importance of penetration testing and security assessments for maintaining a strong security posture.**

**Current status:** - **Penetration testing:** Planned for 2026 (timeline to be determined) - **Third-party testing:** Customers may request approval for third-party penetration testing - **Security assessments:** Regular security reviews and vulnerability assessments conducted - **Continuous improvement:** Security practices continuously improved based on assessments

---

## 2. Penetration Testing Approach

### 2.1 Planned Penetration Testing

**Penetration testing is planned for 2026:**

- **Scope:** Code repositories, infrastructure (if applicable), and security controls
- **Frequency:** Annual penetration testing (once established)
- **Methodology:** Industry-standard penetration testing methodologies
- **Third-party engagement:** Engagement of qualified third-party penetration testing firm

**Timeline:** - **Planning:** Q1-Q2 2026 (assessment of requirements and vendor selection) - **Execution:** Q2-Q3 2026 (penetration testing execution) - **Remediation:** Q3-Q4 2026 (remediation of identified issues) - **Reporting:** Q4 2026 (final report and recommendations)

**Note:** Timeline is subject to change based on business priorities and resource availability.

### 2.2 Testing Scope

**Planned penetration testing scope:**

- **Code repositories** — Security assessment of code repositories and access controls
- **Authentication and authorization** — Testing of authentication and authorization mechanisms
- **Network security** — Network security assessment (if applicable)
- **Application security** — Security assessment of software components
- **Infrastructure security** — Infrastructure security assessment (if applicable)

**Exclusions:** - **Client infrastructure** — Client infrastructure is excluded (client-hosted software) - **Client data** — Client data is excluded (vendor does not process client data) - **Third-party services** — Third-party services (GitHub, email) are excluded

---

### **3. Customer-Requested Penetration Testing**

#### **3.1 Third-Party Testing Authorization**

**Customers may request authorization for third-party penetration testing:**

- **Request process** — Customers submit penetration testing requests in writing
- **Authorization required** — Written authorization required before testing
- **Scope definition** — Testing scope must be clearly defined and approved
- **Scheduling** — Testing scheduled to minimize disruption

#### **3.2 Authorization Requirements**

**Authorization requirements:**

- **Written request** — Written request specifying testing scope and methodology
- **Third-party qualifications** — Third-party tester qualifications and certifications
- **Testing methodology** — Detailed testing methodology and approach
- **Timeline** — Proposed testing timeline and schedule
- **Liability and insurance** — Liability and insurance requirements

#### **3.3 Authorization Process**

**Authorization process:**

1. **Request submission** — Customer submits written penetration testing request
2. **Review** — Fox ML Infrastructure reviews request and scope
3. **Authorization** — Written authorization provided (if approved)
4. **Testing execution** — Third-party conducts testing per approved scope
5. **Results sharing** — Testing results shared with Fox ML Infrastructure
6. **Remediation** — Remediation of identified issues (if applicable)

**Response time:** Authorization requests reviewed within 30 days.

#### **3.4 Testing Restrictions**

**Testing restrictions:**

- **No production impact** — Testing must not impact production systems or services
  - **No client data access** — Testing must not access client data
  - **No destructive testing** — No destructive testing without explicit authorization
  - **Compliance** — Testing must comply with applicable laws and regulations
- 

### **4. Security Assessments**

#### **4.1 Regular Security Assessments**

**Regular security assessments conducted:**

- [OK] **Code reviews** — Regular code reviews for security issues
- [OK] **Dependency scanning** — Regular scanning of dependencies for vulnerabilities
- [OK] **Configuration reviews** — Review of security configurations

- [OK] **Access reviews** — Regular review of access permissions

**Assessment frequency:** - **Code reviews** — Continuous (as part of development process) - **Dependency scanning** — Weekly (automated) - **Configuration reviews** — Quarterly - **Access reviews** — Quarterly

## 4.2 Vulnerability Assessments

**Vulnerability assessments:**

- [OK] **Automated scanning** — Automated vulnerability scanning of dependencies
- [OK] **Manual assessment** — Manual security assessment of code and configurations
- [OK] **Third-party assessments** — Third-party security assessments (if applicable)
- [OK] **Client reporting** — Assessment of client-reported security concerns

**Assessment methodology:** - **OWASP Top 10** — Assessment against OWASP Top 10 vulnerabilities - **Industry standards** — Assessment against industry security standards - **Best practices** — Assessment against security best practices

---

## 5. Remediation and Follow-Up

### 5.1 Remediation Process

**Remediation process:**

1. **Issue identification** — Security issues identified through testing or assessment
2. **Severity assessment** — Severity of issues assessed (Critical, High, Medium, Low)
3. **Remediation planning** — Remediation plan developed
4. **Remediation execution** — Issues remediated per plan
5. **Verification** — Remediation verified through retesting
6. **Documentation** — Remediation documented

**Remediation timelines:** - **Critical issues** — Remediated within 7 days - **High issues** — Remediated within 30 days - **Medium issues** — Remediated within 90 days - **Low issues** — Remediated within 180 days

### 5.2 Follow-Up Testing

**Follow-Up testing:**

- **Retesting** — Retesting of remediated issues
- **Verification** — Verification that remediation is effective
- **Continuous monitoring** — Continuous monitoring for recurrence

---

## 6. Reporting and Disclosure

### 6.1 Testing Reports

**Penetration testing reports include:**

- **Executive summary** — High-level summary of findings
- **Methodology** — Testing methodology and approach
- **Findings** — Detailed findings and vulnerabilities
- **Risk assessment** — Risk assessment of identified issues
- **Remediation recommendations** — Recommendations for remediation
- **Appendices** — Supporting documentation and evidence

## 6.2 Report Distribution

**Report distribution:**

- **Internal** — Reports distributed internally for review and remediation
- **Client sharing** — Reports may be shared with clients upon request (subject to confidentiality)
- **Public disclosure** — Public disclosure only if required by law or if issues are publicly known

## 6.3 Disclosure Policy

**Disclosure policy:**

- **Responsible disclosure** — Follow responsible disclosure practices
  - **Client notification** — Notify clients of critical issues immediately
  - **Public disclosure** — Public disclosure only after remediation (if applicable)
  - **Regulatory reporting** — Report to regulatory authorities if required
- 

## 7. Continuous Improvement

### 7.1 Process Improvement

**Process improvement:**

- **Lessons learned** — Learn from penetration testing and security assessments
- **Process updates** — Update security processes based on findings
- **Tooling enhancements** — Enhance security tooling based on recommendations
- **Training** — Security training based on identified gaps

### 7.2 Maturity Progression

**Security maturity progression:**

- **Current state** — Regular security assessments and vulnerability scanning
  - **Near-term** — Annual penetration testing (planned for 2026)
  - **Long-term** — Continuous penetration testing program
  - **Advanced** — SOC2 certification (if applicable)
- 

## 8. Compliance and Standards

### 8.1 Testing Standards

**Penetration testing follows:**

- **OWASP Testing Guide** — OWASP Testing Guide methodology
- **PTES** — Penetration Testing Execution Standard (if applicable)
- **Industry best practices** — Industry-standard penetration testing practices
- **Regulatory requirements** — Compliance with regulatory requirements

## 8.2 Tester Qualifications

Penetration testers must have:

- **Certifications** — Relevant security certifications (e.g., OSCP, CEH, GPEN)
  - **Experience** — Experience in penetration testing and security assessments
  - **References** — Professional references and track record
  - **Insurance** — Professional liability insurance
- 

## 9. Contact

For penetration testing requests or questions:

**Jennifer Lewis**

Fox ML Infrastructure LLC

Email: [jenn.lewis5789@gmail.com](mailto:jenn.lewis5789@gmail.com)

Subject: *Penetration Testing Request — Fox ML Infrastructure*

For authorization requests, include: - Testing scope and methodology - Third-party tester qualifications - Proposed timeline - Liability and insurance information

---

## 10. Related Documents

- `legal/SECURITY.md` — Security statement
  - `legal/INCIDENT_RESPONSE_PLAN.md` — Incident response plan
  - `legal/SECURITY_CONTROLS_MATRIX.md` — Security controls matrix
  - `legal/INFOSEC_SELF_ASSESSMENT.md` — Information security self-assessment
- 

## 11. Summary

Key Penetration Testing Principles:

1. **Planned testing** — Annual penetration testing planned for 2026
2. **Third-party authorization** — Customers may request authorization for third-party testing
3. **Regular assessments** — Regular security assessments and vulnerability scanning
4. **Rapid remediation** — Rapid remediation of identified issues
5. **Continuous improvement** — Continuous improvement based on findings
6. **Responsible disclosure** — Responsible disclosure of security issues

This statement demonstrates commitment to security and provides transparency for enterprise security reviews.