Fox ML Infrastructure [UNICODE] 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** [UNICODE] Security assessment of code repositories and access controls
- **Authentication and authorization** [UNICODE] Testing of authentication and authorization mechanisms
- **Network security** [UNICODE] Network security assessment (if applicable)
- **Application security** [UNICODE] Security assessment of software components
- **Infrastructure security** [UNICODE] Infrastructure security assessment (if applicable)

Exclusions: - **Client infrastructure** [UNICODE] Client infrastructure is excluded (client-hosted software) - **Client data** [UNICODE] Client data is excluded (vendor does not process client data) - **Third-party services** [UNICODE] 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** [UNICODE] Customers submit penetration testing requests in writing
- **Authorization required** [UNICODE] Written authorization required before testing
- **Scope definition** [UNICODE] Testing scope must be clearly defined and approved
- **Scheduling** [UNICODE] Testing scheduled to minimize disruption

3.2 Authorization Requirements

Authorization requirements:

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

3.3 Authorization Process

Authorization process:

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

Response time: Authorization requests reviewed within 30 days.

3.4 Testing Restrictions

Testing restrictions:

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

---

4. Security Assessments

4.1 Regular Security Assessments

Regular security assessments conducted:

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

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

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

4.2 Vulnerability Assessments

Vulnerability assessments:

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

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

---

5. Remediation and Follow-Up

5.1 Remediation Process

Remediation process:

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

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

5.2 Follow-Up Testing

Follow-Up testing:

- **Retesting** [UNICODE] Retesting of remediated issues
- **Verification** [UNICODE] Verification that remediation is effective
- **Continuous monitoring** [UNICODE] Continuous monitoring for recurrence

---

6. Reporting and Disclosure

6.1 Testing Reports

Penetration testing reports include:

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

6.2 Report Distribution

Report distribution:

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

6.3 Disclosure Policy

Disclosure policy:

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

---

7. Continuous Improvement

7.1 Process Improvement

Process improvement:

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

7.2 Maturity Progression

Security maturity progression:

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

---

8. Compliance and Standards

8.1 Testing Standards

Penetration testing follows:

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

8.2 Tester Qualifications

Penetration testers must have:

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

---

9. Contact

For penetration testing requests or questions:

Jennifer Lewis
Fox ML Infrastructure LLC
Email: **jenn.lewis5789@gmail.com**
Subject: *Penetration Testing Request [UNICODE] 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` [UNICODE] Security statement
- `LEGAL/INCIDENT_RESPONSE_PLAN.md` [UNICODE] Incident response plan
- `LEGAL/SECURITY_CONTROLS_MATRIX.md` [UNICODE] Security controls matrix
- `LEGAL/INFOSEC_SELF_ASSESSMENT.md` [UNICODE] Information security self-assessment

---

11. Summary

Key Penetration Testing Principles:

1. **Planned testing** [UNICODE] Annual penetration testing planned for 2026
2. **Third-party authorization** [UNICODE] Customers may request authorization for third-party testing
3. **Regular assessments** [UNICODE] Regular security assessments and vulnerability scanning
4. **Rapid remediation** [UNICODE] Rapid remediation of identified issues

5. **Continuous improvement** [UNICODE] Continuous improvement based on findings
6. **Responsible disclosure** [UNICODE] Responsible disclosure of security issues

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