Fox ML Infrastructure [UNICODE] Information Security Self-Assessment

This document provides a self-assessment of Fox ML Infrastructure's information security practices. This pre-empts common enterprise security review questions and accelerates procurement processes.

---

1. Executive Summary

Fox ML Infrastructure operates as a zero-data-processing, client-hosted software platform.

- **No client data handling** [UNICODE] Fox ML Infrastructure does not process, store, or transmit client data
- **No vendor infrastructure** [UNICODE] No vendor-hosted servers, databases, or cloud services
- **No vendor access** [UNICODE] No vendor access to client production systems or data
- **Client-controlled security** [UNICODE] All security measures are client-controlled and client-managed

This architecture eliminates most traditional security risks and compliance concerns.

---

2. Data Handling

2.1 No Client Data Processing

Fox ML Infrastructure does not handle client data:

- [OK] **No data storage** [UNICODE] No client data is stored on vendor infrastructure
- [OK] **No data retention** [UNICODE] No client data is retained by the vendor
- [OK] **No data transmission** [UNICODE] No client data is transmitted to vendor systems or third parties
- [OK] **No data access** [UNICODE] Vendor has no access to client production data

See `LEGAL/DATA_PROCESSING_ADDENDUM.md` for detailed data handling practices.

2.2 Client-Controlled Data

All data remains client-controlled:

- [OK] **Client infrastructure** [UNICODE] All data processing occurs on client-owned hardware
- [OK] **Client storage** [UNICODE] All data storage is client-managed
- [OK] **Client access control** [UNICODE] All data access control is client-managed
- [OK] **Client compliance** [UNICODE] Client is responsible for all data compliance requirements

---

3. Infrastructure and Hosting

3.1 No Vendor Infrastructure

Fox ML Infrastructure does not operate infrastructure:

- [OK] **No servers** [UNICODE] No vendor-hosted servers or compute infrastructure
- [OK] **No databases** [UNICODE] No vendor-hosted databases or data storage
- [OK] **No cloud services** [UNICODE] No vendor-managed cloud services or SaaS platforms
- [OK] **No networking** [UNICODE] No vendor-managed networking or network infrastructure

3.2 Client-Hosted Architecture

Software runs entirely on client infrastructure:

- [OK] **Client hosting** [UNICODE] Software is deployed and hosted by the client
- [OK] **Client compute** [UNICODE] All compute resources are client-provided
- [OK] **Client networking** [UNICODE] All networking is client-managed
- [OK] **Client security** [UNICODE] All infrastructure security is client-managed

This eliminates vendor infrastructure security risks.

---

4. Access Control and Credentials

4.1 No Vendor Access

Vendor does not have access to client systems:

- [OK] **No production access** [UNICODE] No vendor access to client production environments
- [OK] **No credentials** [UNICODE] Vendor does not have access to client API keys, credentials, or secrets
- [OK] **No trading accounts** [UNICODE] Vendor does not have access to client trading accounts or financial systems
- [OK] **No remote execution** [UNICODE] No vendor remote execution capability

4.2 Client-Controlled Access

All access control is client-managed:

- [OK] **Client authentication** [UNICODE] Client manages all authentication and authorization
- [OK] **Client credentials** [UNICODE] Client manages all credentials, API keys, and secrets
- [OK] **Client permissions** [UNICODE] Client controls all permissions and access rights
- [OK] **Client monitoring** [UNICODE] Client manages all access monitoring and logging

---

5. Code Delivery and Supply Chain

5.1 Secure Code Delivery

Code is delivered via secure channels:

- [OK] **Private repositories** [UNICODE] Commercial licenses include access to private GitHub repositories
- [OK] **Access controls** [UNICODE] Repository access is controlled via GitHub organization or repository-level permissions
- [OK] **Version control** [UNICODE] All code is version-controlled and tagged
- [OK] **Auditable** [UNICODE] All code changes are auditable via version control

5.2 Supply Chain Integrity

Supply chain security practices:

- [OK] **No telemetry** [UNICODE] No outbound calls or telemetry data collection
- [OK] **No embedded trackers** [UNICODE] No third-party tracking scripts or analytics tools
- [OK] **Explicit dependencies** [UNICODE] All dependencies are explicit and auditable
- [OK] **No hidden code** [UNICODE] No obfuscated or hidden code
- [OK] **Open-source transparency** [UNICODE] Core platform is open-source (AGPL-3.0), enabling full code review

See `LEGAL/SECURITY.md` for detailed supply chain security practices.

---

6. Network Security

6.1 No Vendor Network Access

Vendor does not have network access:

- [OK] **No network connections** [UNICODE] Vendor does not establish network connections to client systems
- [OK] **No remote access** [UNICODE] No vendor remote access capability
- [OK] **No VPN access** [UNICODE] No vendor VPN or network access
- [OK] **No data exfiltration** [UNICODE] No capability to exfiltrate data from client systems

6.2 Client-Controlled Networking

All networking is client-controlled:

- [OK] **Client firewalls** [UNICODE] Client manages all firewalls and network security
- [OK] **Client VPN** [UNICODE] Client manages all VPN and remote access
- [OK] **Client monitoring** [UNICODE] Client manages all network monitoring and logging
- [OK] **Client compliance** [UNICODE] Client is responsible for network security compliance

---

7. Encryption and Data Protection

7.1 No Vendor Encryption Requirements

Since vendor does not handle client data:

- [OK] **No encryption at rest** [UNICODE] No vendor encryption at rest requirements (no vendor data storage)

- [OK] **No encryption in transit** [UNICODE] No vendor encryption in transit requirements (no vendor data transmission)
- [OK] **No key management** [UNICODE] No vendor key management requirements (no vendor data access)

7.2 Client Encryption Responsibilities

Client is responsible for encryption:

- [OK] **Client encryption** [UNICODE] Client manages all encryption for data at rest and in transit
- [OK] **Client key management** [UNICODE] Client manages all key management and key storage
- [OK] **Client compliance** [UNICODE] Client is responsible for encryption compliance requirements

---

8. Security Monitoring and Logging

8.1 No Vendor Monitoring

Vendor does not monitor client systems:

- [OK] **No vendor logging** [UNICODE] Vendor does not log client system activity
- [OK] **No vendor monitoring** [UNICODE] Vendor does not monitor client systems or networks
- [OK] **No vendor alerts** [UNICODE] Vendor does not receive alerts from client systems

8.2 Client Monitoring

Client manages all monitoring:

- [OK] **Client logging** [UNICODE] Client manages all system logging and log storage
- [OK] **Client monitoring** [UNICODE] Client manages all system and network monitoring
- [OK] **Client alerts** [UNICODE] Client manages all security alerts and incident response
- [OK] **Client compliance** [UNICODE] Client is responsible for monitoring compliance requirements

---

9. Incident Response

9.1 No Vendor Incident Risk

Since vendor does not handle client data or operate infrastructure:

- [OK] **No vendor data breach risk** [UNICODE] No vendor data breach can expose client data
- [OK] **No vendor security incident** [UNICODE] No vendor security incident can compromise client systems
- [OK] **No vendor downtime** [UNICODE] No vendor-caused downtime (client-hosted software)

9.2 Client Incident Response

Client is responsible for incident response:

- [OK] **Client incident management** [UNICODE] Client manages all security incident response
- [OK] **Client breach notification** [UNICODE] Client is responsible for breach notification requirements
- [OK] **Client remediation** [UNICODE] Client manages all incident remediation and recovery
- [OK] **Client compliance** [UNICODE] Client is responsible for incident response compliance

---

10. Compliance and Certifications

10.1 Vendor Compliance

Fox ML Infrastructure adheres to:

- [OK] **GDPR principles** [UNICODE] Adheres to GDPR principles (even if not legally required as a data processor)
- [OK] **CCPA principles** [UNICODE] Adheres to CCPA principles
- [OK] **Export compliance** [UNICODE] Complies with export control regulations (EAR99 classification)
- [OK] **Security best practices** [UNICODE] Follows security best practices for software development

See `LEGAL/DATA_PROCESSING_ADDENDUM.md` and `LEGAL/EXPORT_COMPLIANCE.md` for compliance details.

10.2 Client Compliance

Client is responsible for:

- [OK] **Regulatory compliance** [UNICODE] All regulatory compliance requirements (e.g., SEC, FINRA, CFTC)
- [OK] **Data compliance** [UNICODE] All data protection and privacy compliance (e.g., GDPR, CCPA)
- [OK] **Security compliance** [UNICODE] All security compliance requirements (e.g., SOC 2, ISO 27001)
- [OK] **Industry compliance** [UNICODE] All industry-specific compliance requirements

---

11. Third-Party Services

11.1 No Third-Party Data Processors

Fox ML Infrastructure does not use third-party data processors:

- [OK] **No subprocessors** [UNICODE] No third-party data processors or service providers
- [OK] **No cloud providers** [UNICODE] No cloud service providers for data storage or processing
- [OK] **No analytics providers** [UNICODE] No analytics or telemetry providers

- [OK] **No data transmission services** [UNICODE] No third-party data transmission services

Since no data processing occurs, no subprocessors are involved.

11.2 Client Third-Party Services

Client may use third-party services:

- [OK] **Client responsibility** [UNICODE] Client is responsible for third-party service security and compliance
- [OK] **Client agreements** [UNICODE] Client manages all third-party service agreements
- [OK] **Client compliance** [UNICODE] Client is responsible for third-party compliance requirements

---

---

13. Security Best Practices

13.1 Code Security

Fox ML Infrastructure follows security best practices:

- [OK] **Secure coding** [UNICODE] Code is developed following security best practices
- [OK] **Dependency management** [UNICODE] Dependencies are managed and updated for security
- [OK] **Security reviews** [UNICODE] Code is reviewed for security issues
- [OK] **No hardcoded secrets** [UNICODE] No secrets are hardcoded in source code

13.2 Documentation

Security practices are documented:

- [OK] **Security statement** [UNICODE] Public-facing security statement (`LEGAL/SECURITY.md`)
- [OK] **Data handling** [UNICODE] Data processing addendum (`LEGAL/DATA_PROCESSING_ADDENDUM.md`)
- [OK] **Compliance** [UNICODE] Export compliance and other compliance documents

---

14. Summary

Key Security Assessment Points:

1. [OK] **Zero data processing** [UNICODE] No client data is processed, stored, or transmitted
2. [OK] **No vendor infrastructure** [UNICODE] No vendor-hosted servers, databases, or cloud services
3. [OK] **No vendor access** [UNICODE] No vendor access to client production systems or data
4. [OK] **Client-controlled security** [UNICODE] All security measures are client-controlled
5. [OK] **Supply chain integrity** [UNICODE] No telemetry, no embedded trackers, fully auditable
6. [OK] **Compliance-ready** [UNICODE] Adheres to GDPR/CCPA principles and export compliance

7. [OK] **Documented practices** [UNICODE] Security practices are fully documented

This architecture eliminates most traditional security risks and accelerates security review processes.

Contact

For questions about information security or to request additional security information:

Jennifer Lewis
Fox ML Infrastructure LLC
Email: **jenn.lewis5789@gmail.com**
Subject: *InfoSec Self-Assessment Inquiry [UNICODE] Fox ML Infrastructure*

Related Documents

- `LEGAL/SECURITY.md` [UNICODE] Security statement and data handling practices
- `LEGAL/DATA_PROCESSING_ADDENDUM.md` [UNICODE] Data processing addendum (zero data processing)
- `LEGAL/EXPORT_COMPLIANCE.md` [UNICODE] Export control compliance
- `LEGAL/ENTERPRISE_CHECKLIST.md` [UNICODE] Enterprise readiness checklist