

Fox ML Infrastructure — 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** — Fox ML Infrastructure does not process, store, or transmit client data
- **No vendor infrastructure** — No vendor-hosted servers, databases, or cloud services
- **No vendor access** — No vendor access to client production systems or data
- **Client-controlled security** — 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** — No client data is stored on vendor infrastructure
- [OK] **No data retention** — No client data is retained by the vendor
- [OK] **No data transmission** — No client data is transmitted to vendor systems or third parties
- [OK] **No data access** — 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** — All data processing occurs on client-owned hardware
 - [OK] **Client storage** — All data storage is client-managed
 - [OK] **Client access control** — All data access control is client-managed
 - [OK] **Client compliance** — 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** — No vendor-hosted servers or compute infrastructure
- [OK] **No databases** — No vendor-hosted databases or data storage

- [OK] **No cloud services** — No vendor-managed cloud services or SaaS platforms
- [OK] **No networking** — No vendor-managed networking or network infrastructure

3.2 Client-Hosted Architecture

Software runs entirely on client infrastructure:

- [OK] **Client hosting** — Software is deployed and hosted by the client
- [OK] **Client compute** — All compute resources are client-provided
- [OK] **Client networking** — All networking is client-managed
- [OK] **Client security** — 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** — No vendor access to client production environments
- [OK] **No credentials** — Vendor does not have access to client API keys, credentials, or secrets
- [OK] **No trading accounts** — Vendor does not have access to client trading accounts or financial systems
- [OK] **No remote execution** — No vendor remote execution capability

4.2 Client-Controlled Access

All access control is client-managed:

- [OK] **Client authentication** — Client manages all authentication and authorization
 - [OK] **Client credentials** — Client manages all credentials, API keys, and secrets
 - [OK] **Client permissions** — Client controls all permissions and access rights
 - [OK] **Client monitoring** — 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** — Commercial licenses include access to private GitHub repositories
- [OK] **Access controls** — Repository access is controlled via GitHub organization or repository-level permissions
- [OK] **Version control** — All code is version-controlled and tagged
- [OK] **Auditable** — All code changes are auditable via version control

5.2 Supply Chain Integrity

Supply chain security practices:

- [OK] **No telemetry** — No outbound calls or telemetry data collection
- [OK] **No embedded trackers** — No third-party tracking scripts or analytics tools
- [OK] **Explicit dependencies** — All dependencies are explicit and auditable
- [OK] **No hidden code** — No obfuscated or hidden code
- [OK] **Open-source transparency** — 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** — Vendor does not establish network connections to client systems
- [OK] **No remote access** — No vendor remote access capability
- [OK] **No VPN access** — No vendor VPN or network access (except for consulting engagements, if applicable)
- [OK] **No data exfiltration** — No capability to exfiltrate data from client systems

6.2 Client-Controlled Networking

All networking is client-controlled:

- [OK] **Client firewalls** — Client manages all firewalls and network security
 - [OK] **Client VPN** — Client manages all VPN and remote access
 - [OK] **Client monitoring** — Client manages all network monitoring and logging
 - [OK] **Client compliance** — 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** — No vendor encryption at rest requirements (no vendor data storage)
- [OK] **No encryption in transit** — No vendor encryption in transit requirements (no vendor data transmission)
- [OK] **No key management** — No vendor key management requirements (no vendor data access)

7.2 Client Encryption Responsibilities

Client is responsible for encryption:

- [OK] **Client encryption** — Client manages all encryption for data at rest and in transit
 - [OK] **Client key management** — Client manages all key management and key storage
 - [OK] **Client compliance** — 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** — Vendor does not log client system activity
- [OK] **No vendor monitoring** — Vendor does not monitor client systems or networks
- [OK] **No vendor alerts** — Vendor does not receive alerts from client systems

8.2 Client Monitoring

Client manages all monitoring:

- [OK] **Client logging** — Client manages all system logging and log storage
 - [OK] **Client monitoring** — Client manages all system and network monitoring
 - [OK] **Client alerts** — Client manages all security alerts and incident response
 - [OK] **Client compliance** — 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** — No vendor data breach can expose client data
- [OK] **No vendor security incident** — No vendor security incident can compromise client systems
- [OK] **No vendor downtime** — No vendor-caused downtime (client-hosted software)

9.2 Client Incident Response

Client is responsible for incident response:

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

10. Compliance and Certifications

10.1 Vendor Compliance

Fox ML Infrastructure adheres to:

- [OK] **GDPR principles** — Adheres to GDPR principles (even if not legally required as a data processor)
- [OK] **CCPA principles** — Adheres to CCPA principles
- [OK] **Export compliance** — Complies with export control regulations (EAR99 classification)
- [OK] **Security best practices** — 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** — All regulatory compliance requirements (e.g., SEC, FINRA, CFTC)
 - [OK] **Data compliance** — All data protection and privacy compliance (e.g., GDPR, CCPA)
 - [OK] **Security compliance** — All security compliance requirements (e.g., SOC 2, ISO 27001)
 - [OK] **Industry compliance** — 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** — No third-party data processors or service providers
- [OK] **No cloud providers** — No cloud service providers for data storage or processing
- [OK] **No analytics providers** — No analytics or telemetry providers
- [OK] **No data transmission services** — 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** — Client is responsible for third-party service security and compliance
 - [OK] **Client agreements** — Client manages all third-party service agreements
 - [OK] **Client compliance** — Client is responsible for third-party compliance requirements
-

12. Consulting Engagements

12.1 Limited Data Access (Consulting Only)

For consulting engagements only (separate from licensing):

- [OK] **NDA required** — All consulting engagements require a Non-Disclosure Agreement
- [OK] **Limited scope** — Data access is limited to the minimum required for the engagement
- [OK] **Client-controlled** — All data access uses client-approved secure methods
- [OK] **No retention** — Client data is deleted upon project completion unless written authorization is provided

See `legal/internal/SECURITY_AND_ACCESS_POLICY.md` for detailed consulting security practices.

13. Security Best Practices

13.1 Code Security

Fox ML Infrastructure follows security best practices:

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

13.2 Documentation

Security practices are documented:

- [OK] **Security statement** — Public-facing security statement (`legal/SECURITY.md`)
 - [OK] **Data handling** — Data processing addendum (`legal/DATA_PROCESSING_ADDENDUM.md`)
 - [OK] **Access policy** — Security and access policy for consulting (`legal/internal/SECURITY_AND_ACCESS_POLICY.md`)
 - [OK] **Compliance** — Export compliance and other compliance documents
-

14. Summary

Key Security Assessment Points:

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

Related Documents

- `legal/SECURITY.md` — Security statement and data handling practices
- `legal/DATA_PROCESSING_ADDENDUM.md` — Data processing addendum (zero data processing)
- `legal/internal/SECURITY_AND_ACCESS_POLICY.md` — Security and access policy for consulting
- `legal/EXPORT_COMPLIANCE.md` — Export control compliance
- `legal/ENTERPRISE_CHECKLIST.md` — Enterprise readiness checklist