Fox ML Infrastructure — Security Statement

This document outlines the security practices and data handling policies for Fox ML Infrastructure. This statement is designed for enterprise buyers, legal departments, and security teams evaluating the platform.

---

1. Client-Hosted Architecture

Fox ML Infrastructure is client-hosted software.
The platform runs entirely within the client's infrastructure and environment.

Implications: - **No vendor-run runtime** — Fox ML Infrastructure does not operate client systems - **No vendor-caused downtime** — Since there is no vendor-hosted service, there is no vendor-caused service interruption - **Client controls all infrastructure** — Clients manage their own hosting, networking, and deployment - **No external dependencies** — The platform operates independently within the client's environment

---

2. Data Handling & Privacy

2.1 No Data Collection

Fox ML Infrastructure does not collect client data.

- No telemetry or usage analytics
- No outbound calls to external services
- No data transmission to vendor systems
- No client data stored on vendor infrastructure

2.2 Client Data Control

All client data remains fully client-controlled.

- Data is stored only in client-approved environments
- Data access is limited to client-defined permissions
- No vendor access to production systems or keys
- Client data is never transferred to vendor systems

2.3 Consulting Engagements

For consulting engagements (separate from licensing):

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

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

---

3. Code Delivery & Supply Chain

3.1 Private Repository Access

Commercial licenses include access to private GitHub repositories.

- Code is delivered via private, client-specific repositories
- Access is controlled via GitHub organization or repository-level permissions
- Code is version-tagged and auditable
- No public exposure of client-specific customizations

3.2 Supply Chain Integrity

Fox ML Infrastructure maintains supply chain integrity.

- **No telemetry** — The platform does not make outbound calls or collect usage data
- **No external dependencies at runtime** — All dependencies are explicit and auditable
- **Open-source transparency** — Core platform is open-source (AGPL-3.0), enabling full code review
- **Version control** — All code is version-controlled and tagged
- **Auditable builds** — Build processes are documented and reproducible

3.3 Dependency Management

- Dependencies are explicitly declared and versioned
- Security updates are provided via patch releases
- Clients can audit all dependencies before deployment
- No hidden or obfuscated code

---

4. Access Control & Credentials

4.1 No Production Access

Fox ML Infrastructure does not access client production systems.

- No vendor access to production environments
- No vendor access to production API keys or credentials
- No vendor access to trading accounts or financial systems
- All deployment and operations are client-controlled

4.2 Credential Handling

For consulting engagements only:

- Credentials are stored only in client-approved secure methods (environment variables, Vault, encrypted key stores)
- Credentials are never hardcoded, logged, or included in source repositories
- Access is limited to the minimum required for the engagement
- Temporary or scoped credentials are preferred when possible

---

5. Security Practices

5.1 Code Security

- **Regular security reviews** — Code is reviewed for security best practices
- **Dependency updates** — Security patches are applied and released via patch versions
- **No hardcoded secrets** — All secrets are externalized to configuration
- **Secure defaults** — Platform ships with secure default configurations

5.2 Deployment Security

- **Client-controlled deployment** — Clients control all deployment processes
- **No vendor deployment access** — Vendor does not deploy to client systems
- **Documented security practices** — Deployment security is documented in client onboarding materials

---

6. Compliance & Auditing

6.1 Auditability

- **Version control** — All code changes are version-controlled and auditable
- **Tagged releases** — All releases are tagged with semantic versioning
- **Change logs** — Enterprise changelog documents all changes (see `CHANGELOG_ENTERPRISE.md`)
- **Documentation** — Security practices are documented and available

6.2 Compliance Support

- **NDA support** — Non-Disclosure Agreements are standard for consulting engagements
- **Data handling policies** — Explicit data handling policies are documented
- **Client-specific compliance** — Client-specific compliance requirements can be addressed in Statements of Work

---

7. Incident Response

7.1 Security Issues

If a security issue is discovered:

- **Immediate notification** — Enterprise and Premium support customers are notified immediately
- **Patch releases** — Security patches are released as patch versions (e.g., `v1.2.0` → `v1.2.1`)
- **Documentation** — Security issues and fixes are documented in release notes

7.2 Reporting Security Issues

To report a security issue:

Email: jenn.lewis5789@gmail.com
Subject: Security Issue — Fox ML Infrastructure

Please include: - Description of the issue - Steps to reproduce (if applicable) - Potential impact assessment - Your contact information

---

8. Third-Party Services

Fox ML Infrastructure does not integrate with third-party vendor services.

- No external API calls (except as configured by the client for data sources)
- No vendor-hosted services
- No third-party analytics or telemetry
- All functionality is self-contained within the client's environment

---

9. Quant Fund & Financial Services Considerations

Additional security considerations for quantitative funds and financial services:

- **No data exfiltration** — Platform does not transmit data outside client environment
- **Auditable codebase** — Full source code is available for security review
- **No vendor access** — Vendor has no access to trading strategies or proprietary algorithms
- **Client-controlled secrets** — All API keys, credentials, and secrets are client-controlled
- **Isolated deployments** — Client-specific repositories keep proprietary code isolated

---

10. Summary

Key Security Principles:

1. **Client-hosted** — No vendor-run services, no vendor-caused downtime
2. **No data collection** — No telemetry, no outbound calls, no data transmission
3. **Client-controlled** — All data, credentials, and infrastructure are client-controlled
4. **Private delivery** — Code delivered via private repositories
5. **Supply chain integrity** — No hidden dependencies, fully auditable
6. **No production access** — Vendor does not access client production systems

This architecture ensures that Fox ML Infrastructure operates as a secure, client-controlled platform with no vendor access to client data or systems.

Contact

For security-related questions or to report security issues:

Jennifer Lewis
Fox ML Infrastructure LLC
Email: **jenn.lewis5789@gmail.com**
Subject: *Security Inquiry — Fox ML Infrastructure*

Related Documents

- `legal/internal/SECURITY_AND_ACCESS_POLICY.md` — Detailed security practices for consulting engagements
- `legal/ENTERPRISE_DELIVERY.md` — Repository structure and delivery model
- `legal/SUPPORT_POLICY.md` — Support tiers and response times
- `legal/SERVICE_LEVEL_AGREEMENT.md` — SLA terms for Enterprise support