

Fox ML Infrastructure [UNICODE] Security Controls Matrix

This document provides a concise summary of security controls implemented across Fox ML Infrastructure.

This matrix is designed for enterprise security reviews and SOC2-adjacent compliance assessments.

1. Executive Summary

Fox ML Infrastructure implements security controls appropriate for a client-hosted software platform with zero data processing.

Key characteristics: - **Client-hosted architecture** [UNICODE] Software runs on client infrastructure (no vendor infrastructure) - **Zero data processing** [UNICODE] No vendor data collection, storage, or processing - **Minimal attack surface** [UNICODE] Limited vendor infrastructure reduces attack surface - **Defense in depth** [UNICODE] Multiple layers of security controls

2. Access Control

2.1 Authentication

Authentication mechanisms:

- [OK] **GitHub authentication** [UNICODE] Two-factor authentication (2FA) required for repository access
- [OK] **SSH key authentication** [UNICODE] SSH keys for secure repository access
- [OK] **Email authentication** [UNICODE] Standard email authentication for support communications
- [OK] **Credential management** [UNICODE] Strong password policies and credential rotation

Access control principles: - **Principle of least privilege** [UNICODE] Access granted only to minimum required - **Multi-factor authentication** [UNICODE] 2FA required for critical systems - **Regular credential rotation** [UNICODE] Credentials rotated regularly

2.2 Authorization

Authorization mechanisms:

- [OK] **Repository-level permissions** [UNICODE] GitHub repository-level access controls
- [OK] **Role-based access** [UNICODE] Access based on commercial license tier
- [OK] **Client-specific repositories** [UNICODE] Isolated repositories for client-specific code
- [OK] **Read-only access** [UNICODE] Read-only access for certain documentation repositories

Authorization principles: - **Separation of duties** [UNICODE] Clear separation between development and client access - **Access reviews** [UNICODE] Regular review of access permissions - **Immediate revocation** [UNICODE] Immediate revocation upon termination or breach

3. Encryption

3.1 Encryption at Rest

Data encryption at rest:

- [OK] **Client data** [UNICODE] Client data encrypted by client (vendor does not store client data)
- [OK] **Repository encryption** [UNICODE] GitHub provides encryption at rest for repositories
- [OK] **Local backups** [UNICODE] Local backups encrypted (if applicable)
- [OK] **Email encryption** [UNICODE] Email stored in encrypted email systems

Note: Since vendor does not store client data, encryption at rest requirements are minimal.

3.2 Encryption in Transit

Data encryption in transit:

- [OK] **HTTPS/TLS** [UNICODE] All web traffic encrypted via HTTPS/TLS
- [OK] **SSH encryption** [UNICODE] Repository access encrypted via SSH
- [OK] **Email encryption** [UNICODE] Email communications encrypted (TLS)
- [OK] **API encryption** [UNICODE] All API communications encrypted (if applicable)

Encryption standards: - **TLS 1.2+** [UNICODE] Minimum TLS 1.2 for all encrypted communications
- **Strong ciphers** [UNICODE] Strong cipher suites enabled
- **Certificate validation** [UNICODE] Proper certificate validation

4. Logging and Monitoring

4.1 Logging

Logging capabilities:

- [OK] **Repository access logs** [UNICODE] GitHub provides access logs for repository access
- [OK] **Code change logs** [UNICODE] Git provides complete change history
- [OK] **Email logs** [UNICODE] Email systems provide communication logs
- [OK] **Application logs** [UNICODE] Software includes structured logging (client-managed)

Logging principles: - **Comprehensive logging** [UNICODE] Log all significant events - **Structured logging** [UNICODE] Structured log format for parsing - **Log retention** [UNICODE] Retain logs per retention policy - **Log integrity** [UNICODE] Protect logs from tampering

4.2 Monitoring

Monitoring capabilities:

- [OK] **Repository monitoring** [UNICODE] Monitor for unauthorized access or changes
- [OK] **Security alerts** [UNICODE] GitHub security alerts for vulnerabilities
- [OK] **Dependency monitoring** [UNICODE] Monitor dependencies for security vulnerabilities
- [OK] **Client reporting** [UNICODE] Clients can report security concerns

Monitoring principles: - **Continuous monitoring** [UNICODE] Monitor systems continuously - **Alert mechanisms** [UNICODE] Alert on suspicious activity - **Incident response** [UNICODE] Integrate with incident response procedures

5. Secrets Management

5.1 Secret Storage

Secret storage practices:

- [OK] **No hardcoded secrets** [UNICODE] No secrets hardcoded in source code
- [OK] **Environment variables** [UNICODE] Secrets stored in environment variables
- [OK] **Client-controlled** [UNICODE] Clients manage their own secrets
- [OK] **GitHub secrets** [UNICODE] GitHub secrets for CI/CD (if applicable)

Secret management principles: - **No secrets in code** [UNICODE] Never commit secrets to repositories - **Secret rotation** [UNICODE] Rotate secrets regularly - **Access control** [UNICODE] Limit access to secrets - **Audit trails** [UNICODE] Audit secret access

5.2 Secret Handling

Secret handling practices:

- [OK] **Secure transmission** [UNICODE] Secrets transmitted securely (encrypted channels)
 - [OK] **No logging** [UNICODE] Secrets never logged
 - [OK] **Client responsibility** [UNICODE] Clients responsible for their own secret management
-

6. Network Security

6.1 Network Segmentation

Network segmentation:

- [OK] **Client-hosted** [UNICODE] Software runs on client networks (vendor has no network access)
- [OK] **No vendor network** [UNICODE] No vendor-managed network infrastructure
- [OK] **Isolated repositories** [UNICODE] Client repositories isolated from each other
- [OK] **No cross-client access** [UNICODE] No network access between client environments

Network security principles: - **Client-controlled** [UNICODE] All network security is client-controlled - **No vendor access** [UNICODE] Vendor has no network access to client systems - **Isolation** [UNICODE] Client environments isolated from each other

6.2 Network Monitoring

Network monitoring:

- [OK] **Client-managed** [UNICODE] Network monitoring is client-managed
- [OK] **No vendor monitoring** [UNICODE] Vendor does not monitor client networks
- [OK] **No data exfiltration** [UNICODE] No capability for data exfiltration

7. Package Integrity

7.1 Code Integrity

Code integrity controls:

- [OK] **Version control** [UNICODE] All code in version control (Git)
- [OK] **Signed commits** [UNICODE] Git commit signing (if applicable)
- [OK] **Tagged releases** [UNICODE] All releases tagged with semantic versioning
- [OK] **Audit trail** [UNICODE] Complete audit trail of all code changes

Code integrity principles: - **Immutable tags** [UNICODE] Release tags are immutable - **Change tracking** [UNICODE] All changes tracked in version control - **Code review** [UNICODE] Code reviewed before release - **Integrity verification** [UNICODE] Verify code integrity before deployment

7.2 Supply Chain Integrity

Supply chain integrity:

- [OK] **Explicit dependencies** [UNICODE] All dependencies explicitly declared
- [OK] **Dependency scanning** [UNICODE] Scan dependencies for vulnerabilities
- [OK] **No telemetry** [UNICODE] No outbound calls or telemetry
- [OK] **No embedded trackers** [UNICODE] No third-party tracking scripts
- [OK] **Open-source transparency** [UNICODE] Core platform open-source (AGPL-3.0)

Supply chain principles: - **Explicit dependencies** [UNICODE] No hidden dependencies - **Vulnerability scanning** [UNICODE] Regular vulnerability scanning - **No external calls** [UNICODE] No unauthorized external calls - **Transparency** [UNICODE] Transparent supply chain

8. Vulnerability Management

8.1 Vulnerability Detection

Vulnerability detection:

- [OK] **Dependency scanning** [UNICODE] Scan dependencies for known vulnerabilities
- [OK] **Code review** [UNICODE] Code review for security issues
- [OK] **Security alerts** [UNICODE] GitHub security alerts
- [OK] **Client reporting** [UNICODE] Clients can report vulnerabilities

8.2 Vulnerability Response

Vulnerability response:

- [OK] **Immediate assessment** [UNICODE] Assess vulnerabilities immediately
- [OK] **Patch releases** [UNICODE] Release security patches promptly
- [OK] **Client notification** [UNICODE] Notify clients of security issues
- [OK] **Incident response** [UNICODE] Follow incident response procedures

Vulnerability management principles: - **Rapid response** [UNICODE] Respond to vulnerabilities rapidly - **Patch management** [UNICODE] Release patches promptly - **Client communication** [UNICODE] Communicate with clients transparently - **Continuous improvement** [UNICODE] Continuously improve vulnerability management

9. Incident Response

9.1 Incident Detection

Incident detection:

- [OK] **Monitoring** [UNICODE] Continuous monitoring for security incidents
- [OK] **Client reports** [UNICODE] Client reports of security concerns
- [OK] **Third-party notifications** [UNICODE] Notifications from service providers
- [OK] **Security audits** [UNICODE] Periodic security reviews

9.2 Incident Response

Incident response:

- [OK] **Incident response plan** [UNICODE] Documented incident response plan
- [OK] **Response procedures** [UNICODE] Clear response procedures
- [OK] **Client notification** [UNICODE] Timely client notification
- [OK] **Remediation** [UNICODE] Effective remediation procedures

See [LEGAL/INCIDENT_RESPONSE_PLAN.md](#) for detailed incident response procedures.

10. Business Continuity

10.1 Backup and Recovery

Backup and recovery:

- [OK] **Repository backups** [UNICODE] GitHub provides repository redundancy
- [OK] **Local backups** [UNICODE] Local backups of critical repositories
- [OK] **Email backups** [UNICODE] Email systems provide redundancy
- [OK] **Documentation backups** [UNICODE] Documentation in version control

10.2 Business Continuity

Business continuity:

- [OK] **Business continuity plan** [UNICODE] Documented business continuity plan
- [OK] **Recovery procedures** [UNICODE] Clear recovery procedures
- [OK] **RTO/RPO targets** [UNICODE] Defined recovery time and point objectives
- [OK] **Client communication** [UNICODE] Communication during disruptions

See [LEGAL/BUSINESS_CONTINUITY_PLAN.md](#) for detailed business continuity procedures.

11. Compliance and Audit

11.1 Compliance

Compliance controls:

- [OK] **GDPR principles** [UNICODE] Adheres to GDPR principles
- [OK] **CCPA principles** [UNICODE] Adheres to CCPA principles
- [OK] **Export compliance** [UNICODE] Complies with export control regulations
- [OK] **Data protection** [UNICODE] Data protection and privacy controls

11.2 Audit

Audit controls:

- [OK] **Audit trails** [UNICODE] Complete audit trails of all activities
 - [OK] **Documentation** [UNICODE] Comprehensive security documentation
 - [OK] **Access logs** [UNICODE] Access logs for audit purposes
 - [OK] **Change logs** [UNICODE] Change logs for code and configuration
-

12. Security Controls Summary

12.1 Control Categories

Security controls by category:

Category	Controls	Status
Access Control	Authentication, Authorization, Credential Management	[OK] Implemented
Encryption	Encryption at Rest, Encryption in Transit	[OK] Implemented
Logging & Monitoring	Logging, Monitoring, Alerting	[OK] Implemented
Secrets Management	Secret Storage, Secret Handling	[OK] Implemented
Network Security	Network Segmentation, Network Monitoring	[OK] Client-Controlled
Package Integrity	Code Integrity, Supply Chain Integrity	[OK] Implemented
Vulnerability Management	Vulnerability Detection, Vulnerability Response	[OK] Implemented
Incident Response	Incident Detection, Incident Response	[OK] Implemented
Business Continuity	Backup and Recovery, Business Continuity	[OK] Implemented
Compliance & Audit	Compliance, Audit	[OK] Implemented

12.2 Control Effectiveness

Control effectiveness:

- **High effectiveness** [UNICODE] Access control, encryption, logging, package integrity
 - **Medium effectiveness** [UNICODE] Vulnerability management, incident response
 - **Client-dependent** [UNICODE] Network security, secrets management (client-controlled)
-

13. Continuous Improvement

13.1 Security Enhancements

Security enhancements:

- **Regular reviews** [UNICODE] Regular security reviews and assessments
- **Process improvements** [UNICODE] Continuous improvement of security processes
- **Tooling enhancements** [UNICODE] Enhance security tooling and monitoring
- **Training** [UNICODE] Security training and awareness (if applicable)

13.2 Maturity Progression

Security maturity:

- **Current state** [UNICODE] Appropriate for client-hosted software platform
 - **Future enhancements** [UNICODE] SOC2 certification (if applicable), enhanced monitoring
 - **Scalability** [UNICODE] Controls designed to scale with business growth
-

14. Contact

For security controls questions:

Jennifer Lewis

Fox ML Infrastructure LLC

Email: jenn.lewis5789@gmail.com

Subject: *Security Controls Inquiry* [UNICODE] Fox ML Infrastructure

15. Related Documents

- **LEGAL/SECURITY.md** [UNICODE] Security statement
 - **LEGAL/INFOSEC_SELF_ASSESSMENT.md** [UNICODE] Information security self-assessment
 - **LEGAL/INCIDENT_RESPONSE_PLAN.md** [UNICODE] Incident response plan
 - **LEGAL/BUSINESS_CONTINUITY_PLAN.md** [UNICODE] Business continuity plan
-

16. Summary

Key Security Controls:

1. [OK] **Access Control** [UNICODE] Strong authentication and authorization
2. [OK] **Encryption** [UNICODE] Encryption at rest and in transit
3. [OK] **Logging & Monitoring** [UNICODE] Comprehensive logging and monitoring

4. [OK] **Secrets Management** [UNICODE] Secure secret storage and handling
5. [OK] **Network Security** [UNICODE] Client-controlled network security
6. [OK] **Package Integrity** [UNICODE] Code and supply chain integrity
7. [OK] **Vulnerability Management** [UNICODE] Vulnerability detection and response
8. [OK] **Incident Response** [UNICODE] Documented incident response procedures
9. [OK] **Business Continuity** [UNICODE] Backup and recovery procedures
10. [OK] **Compliance & Audit** [UNICODE] Compliance and audit controls

This matrix provides a comprehensive summary of security controls for enterprise security reviews.