Fox ML Infrastructure – Incident Response Plan (IRP)

> **Document Hierarchy:** This document is provided for guidance only. In case of any conflict, `COMMERCIAL_LICENSE.md` is the authoritative and controlling document for all commercial licensing terms and obligations, and `LICENSE` (AGPL-3.0) controls for open-source licensing.
>
> **Commercial Licensees Only:** This document applies only to customers with a valid commercial license. AGPL-3.0 users are not eligible for the policies, services, or terms described here.
>
> **No Obligations Created:** This plan does not create any obligation or service commitment. Actual responses depend on Licensor's sole discretion. This document does not grant any license rights. All rights and restrictions are defined solely in `COMMERCIAL_LICENSE.md`.

This document outlines how Fox ML Infrastructure detects, responds to, and recovers from security incidents. This plan is essential for enterprise security reviews and compliance requirements.

---

1. Executive Summary

Fox ML Infrastructure operates as a client-hosted software platform with minimal vendor infrastructure.

Key characteristics: - **No vendor-hosted infrastructure** – No servers, databases, or cloud services operated by vendor - **No client data processing** – Vendor does not process, store, or transmit client data - **Limited incident surface** – Incidents are limited to code delivery and support communications

This plan covers incident detection, response, and notification procedures.

---

2. Incident Types and Classification

2.1 Security Incident Types

Security incidents may include:

- **Code repository compromise** – Unauthorized access to code repositories
- **Credential compromise** – Unauthorized access to vendor credentials or accounts
- **Support system compromise** – Unauthorized access to support systems or email
- **Consulting data breach** – Unauthorized access to consulting engagement data (if applicable)
- **Supply chain compromise** – Compromise of dependencies or third-party services
- **Code integrity issues** – Unauthorized code modifications or tampering

2.2 Severity Levels

Incidents are classified by severity:

Critical (Severity 1)

- **Impact:** Immediate threat to client security or data
- **Examples:** Code repository compromise, credential compromise affecting client access
- **Response time:** Immediate (within 1 hour)
- **Notification:** Immediate notification to affected clients

High (Severity 2)

- **Impact:** Significant security risk but no immediate client data exposure
- **Examples:** Support system compromise, supply chain compromise
- **Response time:** Within 4 hours

- **Notification:** Notification within 24 hours

Medium (Severity 3)

- **Impact:** Limited security risk, no client data exposure
- **Examples:** Minor credential compromise (non-client-facing), code integrity concerns
- **Response time:** Within 1 business day
- **Notification:** Notification within 3 business days

Low (Severity 4)

- **Impact:** Minimal security risk, no client impact
- **Examples:** Suspicious activity that does not result in compromise
- **Response time:** Within 3 business days
- **Notification:** Notification as needed

---

3. Incident Detection

3.1 Detection Methods

We detect incidents through:

- **Code repository monitoring** – Monitoring for unauthorized access or changes
- **Credential monitoring** – Monitoring for suspicious credential usage
- **Support system monitoring** – Monitoring for unauthorized access to support systems
- **Client reports** – Client reports of suspicious activity or security concerns
- **Third-party notifications** – Notifications from GitHub, email providers, or other services
- **Security audits** – Periodic security reviews and audits

3.2 Detection Capabilities

Current detection capabilities:

- **GitHub security alerts** – Automated security alerts from GitHub
- **Email security** – Standard email security monitoring
- **Code review** – Manual code review and security checks
- **Dependency scanning** – Monitoring for vulnerable dependencies

Note: Detection capabilities may evolve as the platform matures.

---

4. Incident Response Team

4.1 Response Team Structure

Incident response is managed by:

- **Primary responder:** Jennifer Lewis (Founder, Fox ML Infrastructure LLC)
- **Contact:** jenn.lewis5789@gmail.com
- **Availability:** Business hours (US Central Time), with best-effort response outside business hours

4.2 Escalation

For critical incidents:

- **Immediate response** – Primary responder addresses immediately
- **External resources** – May engage external security resources if needed

- **Legal counsel** – May engage legal counsel for compliance and notification requirements

---

5. Incident Response Procedures

5.1 Initial Response (0-1 Hour)

Upon detecting an incident:

1. **Immediate containment** – Take immediate steps to contain the incident
2. **Severity assessment** – Assess severity and classify the incident
3. **Documentation** – Document initial findings and timeline
4. **Notification decision** – Determine if immediate client notification is required

5.2 Investigation (1-24 Hours)

Investigation phase:

1. **Evidence collection** – Collect and preserve evidence
2. **Scope determination** – Determine scope of the incident
3. **Impact assessment** – Assess impact on clients and systems
4. **Root cause analysis** – Identify root cause of the incident

5.3 Remediation (24-72 Hours)

Remediation phase:

1. **Remediation actions** – Take actions to remediate the incident
2. **Verification** – Verify that remediation is effective
3. **Prevention measures** – Implement measures to prevent recurrence
4. **Documentation** – Document remediation actions and outcomes

5.4 Post-Incident (72+ Hours)

Post-incident phase:

1. **Incident report** – Prepare incident report
2. **Client notification** – Notify affected clients (if not already done)
3. **Lessons learned** – Conduct lessons learned review
4. **Process improvement** – Update processes and procedures based on lessons learned

---

6. Client Notification

6.1 Notification Requirements

Clients are notified of incidents that:

- **Affect client security** – Incidents that may affect client security or data
- **Require client action** – Incidents that require client action (e.g., credential rotation)
- **Impact code delivery** – Incidents that impact code delivery or repository access
- **Regulatory requirements** – Incidents that require notification per regulatory requirements

6.2 Notification Timeline

Notification timelines by severity:

- **Critical (Severity 1):** Immediate notification (within 1 hour)

- **High (Severity 2):** Notification within 24 hours
- **Medium (Severity 3):** Notification within 3 business days
- **Low (Severity 4):** Notification as needed

6.3 Notification Content

Notifications include:

- **Incident description** – Description of the incident
- **Impact assessment** – Assessment of impact on clients
- **Remediation actions** – Actions taken to remediate the incident
- **Client actions** – Actions clients should take (if any)
- **Contact information** – Contact information for questions

6.4 Notification Channels

Notifications are sent via:

- **Email** – Primary notification channel (to commercial license contacts)
- **Private repository** – Notifications posted in private repositories (if applicable)
- **Support channels** – Notifications via support email (if applicable)

---

7. Containment and Remediation

7.1 Containment Actions

Immediate containment actions may include:

- **Credential rotation** – Rotate compromised credentials immediately
- **Access revocation** – Revoke unauthorized access
- **Repository lockdown** – Temporarily restrict repository access (if needed)
- **Support system lockdown** – Temporarily restrict support system access (if needed)

7.2 Remediation Actions

Remediation actions may include:

- **Security patches** – Apply security patches or updates
- **Configuration changes** – Update security configurations
- **Access controls** – Strengthen access controls
- **Monitoring enhancements** – Enhance monitoring and detection capabilities

7.3 Verification

Remediation is verified through:

- **Testing** – Testing to verify remediation effectiveness
- **Monitoring** – Enhanced monitoring to detect recurrence
- **Review** – Security review to ensure no residual risks

---

8. Communication and Reporting

8.1 Internal Communication

Internal communication:

- **Incident log** – Maintain incident log with timeline and actions
- **Status updates** – Regular status updates during incident response
- **Documentation** – Document all actions and decisions

8.2 External Communication

External communication:

- **Client notifications** – Notify affected clients per notification requirements
- **Public disclosure** – Public disclosure only if required by law or if incident is publicly known
- **Regulatory reporting** – Report to regulatory authorities if required

8.3 Incident Reports

Incident reports include:

- **Incident summary** – Summary of the incident
- **Timeline** – Timeline of events
- **Impact assessment** – Assessment of impact
- **Remediation actions** – Actions taken to remediate
- **Prevention measures** – Measures to prevent recurrence
- **Lessons learned** – Lessons learned and process improvements

---

9. Recovery and Business Continuity

9.1 Recovery Procedures

Recovery procedures:

- **System restoration** – Restore systems to normal operation
- **Access restoration** – Restore normal access controls
- **Verification** – Verify that systems are operating normally
- **Monitoring** – Enhanced monitoring during recovery period

9.2 Business Continuity

Business continuity measures:

- **Code delivery** – Code delivery continues via private repositories
- **Support services** – Support services continue (may be temporarily limited during incident)

Note: Since software is client-hosted, client operations are not affected by vendor incidents.

---

10. Prevention and Improvement

10.1 Prevention Measures

Prevention measures include:

- **Security best practices** – Follow security best practices for code and systems
- **Access controls** – Strong access controls and credential management
- **Monitoring** – Continuous monitoring for suspicious activity
- **Security reviews** – Periodic security reviews and audits

10.2 Process Improvement

Process improvement:

- **Lessons learned** – Conduct lessons learned reviews after incidents
- **Process updates** – Update processes and procedures based on lessons learned
- **Training** – Security training and awareness (if applicable)
- **Tooling** – Enhance security tooling and monitoring capabilities

---

11. Testing and Exercises

11.1 Incident Response Testing

We test incident response through:

- **Tabletop exercises** – Periodic tabletop exercises to test response procedures
- **Scenario planning** – Planning for various incident scenarios
- **Process review** – Regular review of incident response procedures

11.2 Improvement Based on Testing

Testing results inform:

- **Process improvements** – Updates to incident response procedures
- **Tooling enhancements** – Enhancements to detection and response tooling
- **Training needs** – Identification of training needs

---

12. Compliance and Legal

12.1 Regulatory Compliance

We comply with:

- **Data breach notification laws** – Comply with applicable data breach notification requirements
- **Regulatory reporting** – Report incidents to regulatory authorities if required
- **Contractual obligations** – Comply with contractual notification obligations

12.2 Legal Considerations

Legal considerations:

- **Legal counsel** – Engage legal counsel for compliance and notification requirements
- **Documentation** – Maintain documentation for legal and compliance purposes
- **Preservation** – Preserve evidence for legal proceedings (if applicable)

---

13. Contact

For incident reporting or questions:

Jennifer Lewis
Fox ML Infrastructure LLC
Email: **jenn.lewis5789@gmail.com**
Subject: *Security Incident Report – Fox ML Infrastructure*

For critical incidents, use subject line: *URGENT: Security Incident – Fox ML Infrastructure*

---

14. Related Documents

- `LEGAL/SECURITY.md` – Security statement and practices
- `LEGAL/DATA_PROCESSING_ADDENDUM.md` – Data processing addendum (zero data processing)
- `LEGAL/BUSINESS_CONTINUITY_PLAN.md` – Business continuity plan

---

15. Summary

Key Incident Response Principles:

1. **Rapid detection** – Detect incidents quickly through monitoring and client reports
2. **Immediate containment** – Contain incidents immediately to prevent escalation
3. **Thorough investigation** – Investigate incidents thoroughly to understand scope and impact
4. **Effective remediation** – Remediate incidents effectively and verify effectiveness
5. **Timely notification** – Notify clients promptly per severity and requirements
6. **Continuous improvement** – Learn from incidents and improve processes

This plan ensures effective incident response and client protection.