

# Fox ML Infrastructure — Business Continuity Plan (BCP)

This document outlines how Fox ML Infrastructure maintains business operations and recovers from disruptions.

This plan is essential for enterprise risk management and procurement reviews.

---

## 1. Executive Summary

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

**Key characteristics:** - **Client-hosted software** — Software runs on client infrastructure, not vendor infrastructure - **Minimal vendor dependencies** — Minimal vendor infrastructure required for operations - **Code delivery** — Primary service is code delivery via private repositories - **Support services** — Support services provided via email and private repositories

**This plan covers business continuity, recovery objectives, and operational resilience.**

---

## 2. Business Impact Analysis

### 2.1 Critical Business Functions

**Critical business functions:**

1. **Code delivery** — Delivery of software code via private repositories
2. **Support services** — Technical support and issue resolution
3. **Licensing management** — Commercial license management and renewals
4. **Consulting services** — Consulting engagements (if applicable)

### 2.2 Dependencies

**Key dependencies:**

- **GitHub** — Code repository hosting (primary dependency)
- **Email services** — Email for support and communications
- **Internet connectivity** — Internet access for repository access and communications
- **Computing resources** — Personal computing resources for development and support

### 2.3 Impact Assessment

**Impact of disruptions:**

- **Code delivery disruption** — Clients cannot access new code or updates
- **Support disruption** — Clients cannot receive support or issue resolution
- **Licensing disruption** — New licenses cannot be processed
- **Consulting disruption** — Consulting engagements may be delayed

**Note:** Since software is client-hosted, client operations continue even if vendor services are disrupted.

---

### 3. Recovery Objectives

#### 3.1 Recovery Time Objectives (RTO)

**RTO targets by function:**

- **Code delivery:** 24 hours
- **Support services:** 48 hours
- **Licensing management:** 72 hours
- **Consulting services:** 72 hours

#### 3.2 Recovery Point Objectives (RPO)

**RPO targets:**

- **Code repositories:** 0 hours (GitHub provides backup and redundancy)
- **Support communications:** 24 hours (email backup)
- **Licensing records:** 24 hours (local backup)

**Note:** RPO is minimal since most data is stored in cloud services (GitHub, email) with built-in redundancy.

---

### 4. Risk Scenarios and Mitigation

#### 4.1 Scenario 1: GitHub Service Disruption

**Scenario:** GitHub is unavailable or compromised.

**Impact:** Code delivery disrupted.

**Mitigation:** - **Backup repositories** — Maintain backup repositories on alternative platforms (GitLab, Bitbucket) - **Local backups** — Maintain local backups of code repositories - **Alternative delivery** — Deliver code via alternative methods (direct file transfer, if needed)

**Recovery:** Switch to backup repositories or alternative delivery methods.

**RTO:** 24 hours

#### 4.2 Scenario 2: Email Service Disruption

**Scenario:** Email services are unavailable.

**Impact:** Support and communications disrupted.

**Mitigation:** - **Alternative email** — Maintain alternative email accounts - **Support portal** — Use private repository issues for support (if applicable) - **Phone contact** — Provide phone contact for critical issues (if applicable)

**Recovery:** Switch to alternative communication channels.

**RTO:** 48 hours

### 4.3 Scenario 3: Internet Connectivity Loss

**Scenario:** Internet connectivity is lost.

**Impact:** All online services disrupted.

**Mitigation:** - **Alternative connectivity** — Use alternative internet connections (mobile hotspot, etc.) - **Local operations** — Continue local development and documentation - **Delayed communications** — Resume communications when connectivity is restored

**Recovery:** Restore internet connectivity or use alternative connectivity.

**RTO:** 24-48 hours

### 4.4 Scenario 4: Personal Computing Resource Loss

**Scenario:** Personal computing resources are unavailable (hardware failure, etc.).

**Impact:** Development and support activities disrupted.

**Mitigation:** - **Backup hardware** — Maintain backup computing resources - **Cloud development** — Use cloud-based development environments (GitHub Codespaces, etc.) - **Remote access** — Use remote access to alternative computing resources

**Recovery:** Switch to backup or cloud-based computing resources.

**RTO:** 24-48 hours

### 4.5 Scenario 5: Credential Compromise

**Scenario:** Vendor credentials are compromised.

**Impact:** Repository access and services may be compromised.

**Mitigation:** - **Credential rotation** — Rotate credentials immediately - **Access revocation** — Revoke compromised access - **Security monitoring** — Enhanced security monitoring - **Incident response** — Follow incident response procedures

**Recovery:** Rotate credentials and restore secure access.

**RTO:** 4-24 hours (depending on severity)

---

## 5. Backup and Redundancy

### 5.1 Code Repository Backups

**Code repository backup strategy:**

- **GitHub redundancy** — GitHub provides built-in redundancy and backup
- **Local backups** — Periodic local backups of critical repositories
- **Backup repositories** — Backup repositories on alternative platforms (GitLab, Bitbucket)

**Backup frequency:** Continuous (GitHub), periodic (local backups)

## 5.2 Email and Communications Backups

Email backup strategy:

- **Email provider redundancy** — Email providers provide built-in redundancy
- **Local email archives** — Local archives of critical email communications
- **Documentation backups** — Documentation of critical communications

**Backup frequency:** Continuous (email provider), periodic (local archives)

## 5.3 Documentation Backups

Documentation backup strategy:

- **Repository storage** — Documentation stored in Git repositories (backed up by GitHub)
- **Local backups** — Local backups of critical documentation
- **Version control** — All documentation is version-controlled

**Backup frequency:** Continuous (GitHub), periodic (local backups)

---

# 6. Recovery Procedures

## 6.1 Code Delivery Recovery

Recovery procedures for code delivery:

1. **Assess disruption** — Assess the nature and scope of the disruption
2. **Activate backup** — Activate backup repositories or alternative delivery methods
3. **Notify clients** — Notify clients of disruption and recovery actions
4. **Restore service** — Restore code delivery service
5. **Verify functionality** — Verify that code delivery is functioning normally

## 6.2 Support Services Recovery

Recovery procedures for support services:

1. **Assess disruption** — Assess the nature and scope of the disruption
2. **Activate alternatives** — Activate alternative communication channels
3. **Notify clients** — Notify clients of disruption and alternative channels
4. **Restore service** — Restore support services
5. **Catch up** — Address any support requests that accumulated during disruption

## 6.3 Licensing Management Recovery

Recovery procedures for licensing management:

1. **Assess disruption** — Assess the nature and scope of the disruption
  2. **Access records** — Access licensing records from backups
  3. **Resume processing** — Resume license processing and renewals
  4. **Notify clients** — Notify clients of any delays
  5. **Verify records** — Verify that licensing records are complete and accurate
-

## 7. Communication During Disruptions

### 7.1 Client Communication

**Communication during disruptions:**

- **Immediate notification** — Notify clients immediately of significant disruptions
- **Status updates** — Provide regular status updates during recovery
- **Recovery timeline** — Provide estimated recovery timeline
- **Alternative channels** — Provide information about alternative channels (if applicable)

### 7.2 Communication Channels

**Communication channels:**

- **Email** — Primary communication channel
  - **Private repositories** — Notifications in private repositories (if applicable)
  - **Support portal** — Support portal or issue tracking (if applicable)
- 

## 8. Testing and Maintenance

### 8.1 Plan Testing

**We test the business continuity plan through:**

- **Tabletop exercises** — Periodic tabletop exercises to test recovery procedures
- **Scenario planning** — Planning for various disruption scenarios
- **Process review** — Regular review of business continuity procedures

### 8.2 Plan Maintenance

**Plan maintenance:**

- **Annual review** — Annual review and update of the business continuity plan
  - **Process updates** — Update procedures based on lessons learned and changes
  - **Dependency updates** — Update dependencies and mitigation strategies as needed
- 

## 9. Roles and Responsibilities

### 9.1 Business Continuity Coordinator

**Primary responsibility:** Jennifer Lewis (Founder, Fox ML Infrastructure LLC)

**Responsibilities:** - **Plan maintenance** — Maintain and update the business continuity plan - **Recovery coordination** — Coordinate recovery activities during disruptions - **Client communication** — Communicate with clients during disruptions - **Testing** — Conduct testing and exercises

## 9.2 External Resources

External resources (if needed):

- **GitHub support** — GitHub support for repository issues
  - **Email provider support** — Email provider support for email issues
  - **Legal counsel** — Legal counsel for compliance and contractual matters
- 

## 10. Limitations and Assumptions

### 10.1 Limitations

This plan assumes:

- **Client-hosted software** — Software runs on client infrastructure (not affected by vendor disruptions)
- **Cloud service reliability** — Cloud services (GitHub, email) provide high availability
- **Single-person operation** — Current operation is single-person (may change as business grows)

### 10.2 Assumptions

Key assumptions:

- **Internet connectivity** — Internet connectivity can be restored within 24-48 hours
  - **Cloud service availability** — Cloud services provide 99.9%+ availability
  - **Client operations** — Client operations continue independently of vendor services
- 

## 11. Contact

For business continuity questions or to report disruptions:

**Jennifer Lewis**

Fox ML Infrastructure LLC

Email: [jenn.lewis5789@gmail.com](mailto:jenn.lewis5789@gmail.com)

Subject: *Business Continuity Inquiry — Fox ML Infrastructure*

---

## 12. Related Documents

- `legal/INCIDENT_RESPONSE_PLAN.md` — Incident response plan
  - `legal/RISK_ASSESSMENT_MATRIX.md` — Risk assessment matrix
  - `legal/SECURITY.md` — Security statement
- 

## 13. Summary

Key Business Continuity Principles:

1. **Minimal dependencies** — Minimal vendor infrastructure dependencies
2. **Client independence** — Client operations continue independently
3. **Backup and redundancy** — Backup and redundancy for critical services
4. **Rapid recovery** — Rapid recovery objectives (24-72 hours)
5. **Clear procedures** — Clear recovery procedures for each scenario
6. **Regular testing** — Regular testing and maintenance of the plan

**This plan ensures business continuity and operational resilience.**