Fox ML Infrastructure [UNICODE] Business Continuity Plan (BCP)

> **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 is an internal policy summary provided for informational purposes only and does not create any SLA, guarantee, or obligation. 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 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** [UNICODE] Software runs on client infrastructure, not vendor infrastructure - **Minimal vendor dependencies** [UNICODE] Minimal vendor infrastructure required for operations - **Code delivery** [UNICODE] Primary service is code delivery via private repositories - **Support services** [UNICODE] 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** [UNICODE] Delivery of software code via private repositories
2. **Support services** [UNICODE] Technical support and issue resolution
3. **Licensing management** [UNICODE] Commercial license management and renewals

2.2 Dependencies

Key dependencies:

- **GitHub** [UNICODE] Code repository hosting (primary dependency)
- **Email services** [UNICODE] Email for support and communications
- **Internet connectivity** [UNICODE] Internet access for repository access and communications

- **Computing resources** [UNICODE] Personal computing resources for development and support

2.3 Impact Assessment

Impact of disruptions:

- **Code delivery disruption** [UNICODE] Clients cannot access new code or updates
- **Support disruption** [UNICODE] Clients cannot receive support or issue resolution
- **Licensing disruption** [UNICODE] New licenses cannot be processed

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** [UNICODE] Maintain backup repositories on alternative platforms (GitLab, Bitbucket) - **Local backups** [UNICODE] Maintain local backups of code repositories - **Alternative delivery** [UNICODE] 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** [UNICODE] Maintain alternative email accounts - **Support portal** [UNICODE] Use private repository issues for support (if applicable) - **Phone contact** [UNICODE] 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** [UNICODE] Use alternative internet connections (mobile hotspot, etc.) - **Local operations** [UNICODE] Continue local development and documentation - **Delayed communications** [UNICODE] 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** [UNICODE] Maintain backup computing resources - **Cloud development** [UNICODE] Use cloud-based development environments (GitHub Codespaces, etc.) - **Remote access** [UNICODE] 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** [UNICODE] Rotate credentials immediately - **Access revocation** [UNICODE] Revoke compromised access - **Security monitoring** [UNICODE] Enhanced security monitoring - **Incident response** [UNICODE] 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** [UNICODE] GitHub provides built-in redundancy and backup
- **Local backups** [UNICODE] Periodic local backups of critical repositories
- **Backup repositories** [UNICODE] 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** [UNICODE] Email providers provide built-in redundancy
- **Local email archives** [UNICODE] Local archives of critical email communications
- **Documentation backups** [UNICODE] Documentation of critical communications

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

5.3 Documentation Backups

Documentation backup strategy:

- **Repository storage** [UNICODE] Documentation stored in Git repositories (backed up by GitHub)
- **Local backups** [UNICODE] Local backups of critical documentation
- **Version control** [UNICODE] 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** [UNICODE] Assess the nature and scope of the disruption
2. **Activate backup** [UNICODE] Activate backup repositories or alternative delivery methods
3. **Notify clients** [UNICODE] Notify clients of disruption and recovery actions
4. **Restore service** [UNICODE] Restore code delivery service
5. **Verify functionality** [UNICODE] Verify that code delivery is functioning normally

6.2 Support Services Recovery

Recovery procedures for support services:

1. **Assess disruption** [UNICODE] Assess the nature and scope of the disruption
2. **Activate alternatives** [UNICODE] Activate alternative communication channels
3. **Notify clients** [UNICODE] Notify clients of disruption and alternative channels

4. **Restore service** [UNICODE] Restore support services
5. **Catch up** [UNICODE] Address any support requests that accumulated during disruption

6.3 Licensing Management Recovery

Recovery procedures for licensing management:

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

---

7. Communication During Disruptions

7.1 Client Communication

Communication during disruptions:

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

7.2 Communication Channels

Communication channels:

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

---

8. Testing and Maintenance

8.1 Plan Testing

We test the business continuity plan through:

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

8.2 Plan Maintenance

Plan maintenance:

- **Annual review** [UNICODE] Annual review and update of the business continuity plan
- **Process updates** [UNICODE] Update procedures based on lessons learned and changes
- **Dependency updates** [UNICODE] 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** [UNICODE] Maintain and update the business continuity plan - **Recovery coordination** [UNICODE] Coordinate recovery activities during disruptions - **Client communication** [UNICODE] Communicate with clients during disruptions - **Testing** [UNICODE] Conduct testing and exercises

9.2 External Resources

External resources (if needed):

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

---

10. Limitations and Assumptions

10.1 Limitations

This plan assumes:

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

10.2 Assumptions

Key assumptions:

- **Internet connectivity** [UNICODE] Internet connectivity can be restored within 24-48 hours
- **Cloud service availability** [UNICODE] Cloud services provide 99.9%+ availability
- **Client operations** [UNICODE] 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**
Subject: *Business Continuity Inquiry [UNICODE] Fox ML Infrastructure*

---

12. Related Documents

- `LEGAL/INCIDENT_RESPONSE_PLAN.md` [UNICODE] Incident response plan
- `LEGAL/RISK_ASSESSMENT_MATRIX.md` [UNICODE] Risk assessment matrix
- `LEGAL/SECURITY.md` [UNICODE] Security statement

---

13. Summary

Key Business Continuity Principles:

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

This plan ensures business continuity and operational resilience.