AHCA Florida Health Care Connections (FX)

Disaster Recovery Plan

Version: 001

Date: <Month Day, YYYY (Use the Deliverable Draft or Final Submittal Date)>

Author: <Author>

Submitted To: AHCA FX Program Administration Team

Revision History

Date	Version	Description	Author
M/D/YYYY	001	Disaster Recovery Plan Development Draft Version (Entry)	Your name here
M/D/YYYY	002	Disaster Recovery Plan Final Draft Version (Entry)	Your name here
M/D/YYYY	100	Disaster Recovery Plan Approved Baseline Version (Entry)	Your name here
M/D/YYYY	101	Disaster Recovery Plan Approved Baseline Version Refresh (Entry)	Your name here

Modifications to the approved baseline version (100) of this artifact must be made in accordance with the FX Artifact Management Standards.

Quality Review History

Date	Reviewer	Comments
M/D/YYYY	Your name here	<e.g., Conducted peer review/QC review>

Table of Contents

Table of Exhibits

SECTION 1 INTRODUCTION

1.1 Background

The Florida Agency for Health Care Administration (AHCA or Agency) is adapting to the changing landscape of healthcare administration and increased use of the Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) to improve the administration and operation of the Florida Medicaid Enterprise. The current Florida Medicaid Enterprise is complex; it includes services, business processes, data management and processes, technical processes within the Agency, and interconnections and touchpoints with systems necessary for administration of the Florida Medicaid program that reside outside the Agency. The future of the Florida Medicaid Enterprise integration is to allow the Agency to secure services that can interoperate and communicate without relying on a common platform or technology.

The Florida Medicaid Management Information System (FMMIS) has historically been the central system within the Florida Medicaid Enterprise; functioning as the single, integrated system for claims processing and information retrieval. As the Medicaid program has grown more complex, the systems needed to support the Florida Medicaid Enterprise have grown in number and complexity.

The Medicaid Enterprise System (MES) Procurement Project was re-named Florida Health Care Connections (FX) in the summer of 2018. FX is a multi-year transformation to modernize the current Medicaid technology using a modular approach, while simultaneously improving overall Agency functionality and building better connections to other data sources and programs.

1.2 Purpose

The Disaster Recovery (DR) Plan provides step-by-step procedures to identify, address, and recover from disaster events. It also emphasizes the need to minimize negative impacts to the project and resume normal operations.

1.3 Scope Statement

<This section outlines what is in scope for this deliverable/work product. In large projects with many sub-plans created and referenced from the Project Management Plan, it is necessary to define what the particular document is going to cover. Also important is a description of what is NOT in scope especially if there is any chance to misinterpret what should be included in the document.>

1.4 Goals and Objectives

<The section will list and define the goals and objectives for this plan.>

- Goal #1 – Describe Goal #1. This goal will be accomplished by achieving the following objectives:
  - Objective #1 – Describe objective for reaching goal
  - Objective #2 – Describe additional objective to assist in reaching goal
  - Objective #n – Describe additional objective to assist in reaching goal

1.5 Roles and Responsibilities

The **Exhibit 1-1: Roles and** Responsibilities table below identifies the roles and responsibilities for all the stakeholders involved with deliverable review and approval of the DR Plan.

<Instructions: Specify each major role (not name of the individual) and the major activities related to this document. Examples for roles shown in Exhibit 1-1 below.>

<DO NOT MODIFY or DELETE the header or information provided for this table.>

Role	Responsibility
<Vendor/Project> AHCA Contract Manager	▪ Provide detail on Agency direction concerning future module vendors for integration
<Vendor/Project> Account Manager	▪ Act as the main point of contact with the Agency for day-to-day operations ▪ Accountable for the <Vendor/Project> Project Team's staff including staffing levels, hiring, training assignments, performance evaluations, and issue resolution ▪ Work in collaboration with the Agency, Strategic Enterprise Advisory Services (SEAS) Vendor, and other vendors to support the communications and activities necessary to meet the objectives of the <Project> Project ▪ Accountable for all staff the vendor assigns to complete the requirements under the contract to meet the qualifications needed for the work to which they are assigned ▪ Fulfills the <Vendor > System Owner in the context of the Contingency Plan
<Vendor/Project> Project Manager	▪ Responsible for the quality and timeliness of all deliverables, documentation, and reports as described in the Contract ▪ May act as the Contract Manager handling contract-related activities

ROLE	RESPONSIBILITY
<Vendor/Project> Enterprise Architect	▪ Informs the creation of the Contingency Plan ▪ Recommends and participates in activities related to the design, development, and maintenance of the Enterprise Architecture (EA) ▪ Advises and recommends EA strategies, processes, and methodologies ▪ Recommends and participates in the development of architecture blueprints for related systems ▪ Validates the solution is compatible and in compliance with the standards for architecture, integration, and security ▪ Shares best practices, lessons learned, and constantly updates the technical system architecture requirements based on changing technologies, and knowledge related to recent, current, and upcoming products and solutions ▪ Participates in the design and implementation of Information Technology (IT) service management standards, tools, and methodologies
<Vendor/Project> Infrastructure Lead	▪ Provides infrastructure input to the creation of the Contingency Plan ▪ Recommends and participates in activities related to the design, development, and maintenance of the Technical and Network Architecture ▪ Advises and recommends technical architecture strategies, processes, and tools ▪ Validates the solution is compatible and in compliance with the standards for architecture, integration, and security ▪ Shares leading practices, lessons learned, and constantly updates the technical system architecture requirements based on changing technologies, and knowledge related to recent, current, and upcoming products and solutions
<Vendor/Project> Integration Manager	▪ Manage the design, configuration/build, integration, defect management, and implementation of the contract ▪ Provide technical leadership to the <Vendor/Project> Project Team to maintain high quality by developing, establishing, and maintaining best practices ▪ Delegate technical responsibilities and monitor progress of projects ▪ Work closely with the <Vendor/Project> Project Manager during all phases of development life cycle ▪ Conduct regular status meetings with all necessary stakeholders ▪ Research and evaluate a variety of alternative software products and make the necessary recommendations to Agency leadership after thorough testing
<Vendor/Project> Development Lead	▪ Provide technical leadership to the <Vendor/Project> Project Team to maintain high quality by developing, establishing, and maintaining best practices ▪ Assist in the collection, review, and documentation of user's requirements, development of user stories, estimates, and work plans ▪ Lead and organize the packaging and support deployment of releases, fixes, and builds ▪ Research and evaluate a variety of alternative software products and make the necessary recommendations to Agency leadership after thorough testing
Agency and SEAS Deliverable Reviewer	▪ Responsible for deliverable review ▪ Provide input to incorporate Contingency Plan into the Business Impact Assessment (BIA)

Exhibit 1-1: Roles and Responsibilities

<Add more information as needed.>

1.6 Referenced Documents

<List any documents referenced to support this deliverable including any other project plans and or documentation, federal or state authorities, quality standards, state artifacts, and other deliverables relevant to this document. The following is a standard list. Please remove or add as needed.>

- FX Technology Standards Reference Guide
- FX MITA Concept of Operations
- T-1: Data Management Strategy
- S-3: FX Strategic Plan
- P-2: FX Project Management Standards
- FX Artifact Management Standards
- FX <Vendor/Deliverable>: Project Management Plan
- FX <Vendor/Deliverable>: High-Level Technical Design
- FX <Vendor/Deliverable>: System Design Document
- FX <Vendor/Deliverable>: System Design Specification Document
- FX <Vendor/Deliverable>: Configuration Management and Release Management Plan
- FX <Vendor/Deliverable>: Environmental Readiness Review
- FX <Vendor/Deliverable>: Test Plan
- FX <Vendor/Deliverable>: Operations and Maintenance Manual
- CMS Risk Management Handbook (RMH) Chapter 6 Contingency Planning
- CMS Disaster Recovery Plan Checklist

For a definition of terms and acronyms used throughout this document, refer to the FX Projects Glossary located in the FX Projects Repository (FXPR) at FX Hub > Project Glossary.

SECTION 2 DOCUMENT UPDATE PROCEDURES

<Instructions: Provide the procedure for updating this DR Plan.>

Updates to the DR Plan shall be evaluated as new components are added or modified to the FX <Vendor> due to workstreams and/or task orders as well as the approach described in Section 8 *Contingency Plan Maintenance* below. For updates to this deliverable, the <Vendor Name> Vendor shall follow the Document Management Plan outlined in the <Deliverable>: Project Management Plan, *P-2: FX Project Management Standards*, and the FX Artifact Management Standards (AMS).

<Add more information as needed.>

SECTION 3 CONCEPT OF OPERATIONS

<Instructions: Describe the Concept of Operations.>

This Concept of Operations section provides an overview of the FX <Vendor>, an overview of the <# of> phases of the <Vendor's> Contingency Plan (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of the <Vendor's> personnel during a contingency activation.

<Add more information as needed.>

3.1 SYSTEM OVERVIEW

<Instructions: Provide a System Overview including Architecture, Infrastructure, Security, Hosting Environments, and Topology.>

3.2 PREVENTIVE MEASURES

<Instructions: Discuss the preventive measures.>

The FX <Vendor's> solution is built with preventive measures to deter, detect, and reduce the risk of failures. These measures are more cost-effective than the declaration of a disaster event and activate the Contingency Plan (CP). These preventive measures can be organized into six perspectives: Data Center, Security, Hardware, Software, Data, and Facility.

<Add more information as needed.>

3.3 DISASTER RECOVERY SYSTEM OVERVIEW

<Instructions: Provide an overview of the DR System.>

3.4 RECOVERY TIERS

<Instructions: Verify and provide information on the recovery tiers and specify the contractual RTO and RPO.>

Exhibit 3 1: CMS Recovery Tiers below depicts the CMS Enterprise Data Center (EDC) recovery tier structure and corresponding Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), which can be used for reference in the enterprise-wide recovery planning.

TIER ZERO	TIER ONE	TIER TWO	TIER THREE	BEST EFFORT
Infrastructure	Hot Site	Warm Site	Bare Meta Site	Cold Site

TIER ZERO	TIER ONE	TIER TWO	TIER THREE	BEST EFFORT
Typical RTO < 4 Hrs	Typical RTO 4-8 Hrs	Typical RTO 8-24 Hrs	Typical RTO 24-72 Hrs	Typical RTO > 72 Hrs
Typical RPO < 15min	Typical RPO 15-60 mins	Typical RPO 1-12 Hrs	Typical RPO 12-24 Hrs	Typical RPO > 24 Hrs

Exhibit 3-1: CMS Recovery Tiers

<Add more information as needed.>

3.5 DISASTER IMPACT CATEGORIES

<Instructions: Describe the disaster impact categories.>

The purpose for identifying types of disasters is to quickly identify the scope of the disaster. There are four impact categories of disasters and multiple impact categories can occur during a single disaster.

- Hardware Impact
- Software Impact
- Data Impact
- Facility Impact

<Add more information as needed.>

3.6 DISASTER TYPE

<Instructions: Describe the disaster types.>

There are three disaster types in accordance with CMS' classification. The three types of disaster that may occur: Type A, Type B or Type C. Each of these are defined by CMS below.

<Add more information as needed.>

3.6.1 TYPE A DISASTER

This level of disaster is one that affects a single application affecting a single line of business. Neither the supporting infrastructure nor the hosting system would be physically damaged or rendered inoperable. The problem is correctable with minimal resources and the recovery teams specified in the FX <Vendor's> Contingency Plan, while placed on alert, may not be activated. The declaration authority for a Type A disaster is the business owner.

3.6.2 Type B Disaster

This type of disaster involves a portion of the enterprise whose impact encompasses multiple applications, systems, or multiple lines of business. A Type B disaster will either affect an entire system with impact to all hosted applications, or a major centrally accessed database, the loss of which affects a significant portion of CMS' mission. The declaration authority for a Type B disaster may be the affected business owners (to include the supporting infrastructure business owner).

3.6.3 Type C Disaster

This Type C disaster will render most of the supporting infrastructure inoperable. Type C disasters will require the transition of all supporting infrastructure functions and services to the alternate processing facility and the implementation of the <Vendor's> Contingency Plan in priority order as directed by the supporting infrastructure and Business Owner.

3.7 Recovery Strategy

<Instructions: Provide the recovery strategy for hardware, software, network, data, and facility.>

3.7.1 Hardware Recovery

<Instructions: Describe the hardware recovery process.>

3.7.2 Software Recovery

<Instructions: Describe the software recovery process.>

3.7.3 Software Recovery Roll Back

<Instructions: Describe the software recovery roll back process.>

When a release deployed into the system fails in critical areas and a work-around is not possible, a release roll back can be performed to roll the system back to the previous stable release and resume the business functions. The new function release can be attempted again once the critical issue is addressed. The roll back approach can vary depending on the release deployment approach.

<Add more information as needed.>

3.7.4 Data Recovery Fix Forward

<Instructions: Describe the data recovery fix forward process.>

When the data is corrupted in the database and the corruption is small scale and the corruption area is not overlaid with new transactional data, then the <vendor system in use> can recover the data from the various locations to allow the data to be fixed.

<Add more information as needed.>

3.7.5 Data Recovery Restore

<Instructions: Describe the data recovery restore process.>

3.7.6 Facility Recovery Alternate Site

<Instructions: Describe the recovery alternate site facility.>

3.7.7 Facility Recovery Remote Working

<Instructions: Describe the facility for recovery remote working, if applicable.>

3.7.8 Cutover To DR Site

<Instructions: Describe the cutover to the DR site process.>

3.8 Business Impact

<Instructions: Verify and provide information on the business impact.>

In a typical IT system, the business owners would establish the essential functions, process, and applications that are critical to the Agency.

The foundation of all recovery planning is the prioritization of business processes and functions. The Maximum Tolerable Downtime (MTD) is calculated by each business process and function.

<Add more information as needed.>

3.9 Recovery Team Roles and Responsibilities

<Instructions: Verify and provide information on the recovery team roles and responsibilities.>

The <Vendor’s> Contingency Plan establishes several roles for the FX <Vendor’s> recovery and reconstitution support. Individuals or teams assigned to roles have been trained to respond to a contingency event affecting the FX <Vendor>. The **Exhibit 3-2: Team Roles and** Responsibilities table below lists the recovery team roles and their responsibilities. Each of the roles should be filled with a primary resource and an alternate resource.

<Example roles shown in table below.>

ROLE	RESPONSIBILITY
<Vendor> CP Director (<Vendor> System Owner)	▪ Provide overall management responsibility for the <Vendor> system and availability
<Vendor> CP Coordinator / <Vendor> CP Testing Lead	▪ Provide oversight of recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate ▪ During routine testing, provide oversight and coordination of the recovery testing and trainings
<Vendor> Business Owner (Agency Business Owner)	▪ Provide oversight responsibility from the Agency for the <Vendor> system
<Vendor> Operations and Maintenance (O&M) Point of Contact (PoC) / Service Delivery Manager (SDM)	▪ Provide oversight of service delivery of Tier 3 operation teams, serve as the point of contact to the Tier 3 operation teams on the shift
<Vendor> CP Recovery Team Network	▪ Provide triage and recovery operation support from network perspective
<Vendor> CP Recovery Team Database	▪ Provide triage and recovery operation support from database perspective
<Vendor> CP Recovery Team Middleware	▪ Provide triage and recovery operation support from middleware perspective
<Vendor> CP Recovery Team Security	▪ Provide triage and recovery operation support from security perspective

Exhibit 3-2: Team Roles and Responsibilities

SECTION 4 ACTIVATION AND NOTIFICATION

<Instructions: Verify and provide information on the activation and notification phase.>

The Activation and Notification Phase defines initial actions taken once the FX <Vendor> system disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the <Vendor's> Contingency Plan. At the completion of the Activation and Notification Phase, the Recovery Team shall be prepared to perform recovery measures.

<Add more information as needed.>

4.1 Activation Criteria

<Instructions: Verify and provide information on the activation criteria. Describe the steps to activate the Contingency Plan.>

4.2 Notification Procedures

<Instructions: Verify and provide information on the notification procedures. Define who can declare a disaster. Define the notification process.>

4.3 Outage Assessment Procedures

<Instructions: Verify and provide information on the outage assessment procedures.>

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, as well as any damage and expected recovery time.

<Add more information as needed.>

4.4 Decision To Declare A Disaster

<Instructions: Verify and provide information on the decision to declare a disaster and define who can declare a disaster.>

When the team concludes that the only effective recovery strategy is to cutover to the DR site, a formal decision to declare a disaster should be considered. The following checklist can help pre-validate the decision. The **Exhibit 4-1: Disaster Decision** Checklist below lists the questions to be considered prior to declaring a disaster.

Checklist Consideration	Yes / No Answer
Are all the major components in the <Vendor's> production environment down?	▪ Yes/No

Checklist Consideration	Yes / No Answer
Is the issue unrelated to the application software?	▪ Yes/No
Is the component issue critical to the <Vendor’s> production operation?	▪ Yes/No
Did we confirm the hardware recovery fix forward is not able to resolve this issue?	▪ Yes/No
Did we confirm the software recovery work-around is not able to resolve this issue?	▪ Yes/No
Did we confirm the software recovery roll back is not able to resolve this issue?	▪ Yes/No
Did we confirm the data recovery fix forward is not able to resolve this issue?	▪ Yes/No
Did we confirm the data recovery restore is not able to resolve this issue?	▪ Yes/No
Is the facility issue unrelated to the production data center?	▪ Yes/No

Exhibit 4-1: Disaster Decision Checklist

Once the disaster is declared, the time of this declaration would be marked for calculation of time lapsed in the later stages.

If the incident is related to a security data breach, the Agency security incident notification procedures shall be followed instead of the standard notification process.

The <Vendor Name> Vendor shall follow the Agency’s security incident disaster declaration and notification procedures provided by the Agency.

<Add more information as needed.>

SECTION 5 RECOVERY

<Instructions: Verify and provide information on the recovery process.>

The recovery process provides formal recovery operations that begin after the <Vendor's> Contingency Plan has been activated, outage assessments have been completed (if possible), personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, the FX <Vendor> shall be recovered to a trusted state that is functional and capable of performing business functions.

<Add more information as needed.>

5.1.1 Sequence Of Recovery Activities

<Instructions: Verify and provide information on the sequence of recover activities.>

5.1.2 Recovery Procedures

<Instructions: Verify and provide information on the recovery procedures.>

5.1.3 Recovery Escalation Notices / Awareness

<Instructions: Verify and provide information on the recovery escalation notices/awareness process.>

SECTION 6 RECONSTITUTION

<Instructions: Verify and provide information on the reconstitution process.>

Reconstitution is the process by which recovery activities are completed and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the plan.

<Add more information as needed.>

6.1 Validation Data Testing

<Instructions: Verify and provide information on the validation data testing process.>

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely.

<Add more information as needed.>

6.2 Validation Functionality Testing

<Instructions: Verify and provide information on the validation functionality testing process.>

Validation functionality testing is the process of verifying that the FX <Vendor's> functionality has been tested and the system is ready to return to normal operations.

<Add more information as needed.>

6.3 Recovery Declaration

<Instructions: Verify and provide information on the recovery declaration process.>

Upon successfully completing testing and validation, the <Vendor> CP Coordinator shall formally declare recovery efforts complete and that the FX <Vendor's> system has returned to a trusted state and is in normal operations. The FX <Vendor's> business and technical Points of Contact (PoC) shall be notified of the declaration by the <Vendor> CP Coordinator.

<Add more information as needed.>

6.4 Notifications (Users)

<Instructions: Verify and provide information on the notification of users.>

Upon return to normal system operations the required FX stakeholders shall be notified.

<Describe the notification process and stakeholders. Add more information as needed.>

6.5 Data Backup

<Instructions: Verify and provide information on the data backup process.>

As soon as reasonable following recovery, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups.

<Add more information as needed.>

6.6 Event Documentation

<Instructions: Verify and provide information on the event documentation process.>

It is important that all recovery events be well-documented including actions taken, problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this <Vendor's> Contingency Plan.

<Add more information as needed.>

6.7 Return To Primary Site

<Instructions: Verify and provide information on the return to primary site process.>

6.8 Post Mortem

<Instructions: Verify and provide information on the post mortem process.>

After the system is successfully returned to the primary site, the Recovery Team members shall conduct a post mortem meeting. This meeting shall go over the recovery log and discuss the following topics:

- What went right?
- What went wrong?
- What shall be done differently next time?

<Add more information as needed.>

SECTION 7 TESTING AND TRAINING

<Instructions: Verify and provide information on the testing and training process.>

7.1 Testing Approach

<Instructions: Verify and provide information on the testing approach.>

The <Vendor's> Contingency Plan shall be tested annually. The testing shall be coordinated and monitored by the <Vendor> CP Coordinator and the <Vendor> O&M Team.

<Add more information as needed.>

7.1.1 Load/Performance Test

<Instructions: Verify and provide information on the load/performance test process.>

A load or performance test is executed in the DR environment and validates the system performance under normal and anticipated peak load conditions.

<Add more information as needed.>

7.1.2 Failover Test

<Instructions: Verify and provide information on the failover test process.>

7.2 Training Approach

<Instructions: Verify and provide information on the training approach process.>

DR training should be directed to two groups within the <Vendor's> organization. The first group is the personnel who are members of one (or more) of the recovery teams. The second group is the management personnel.

<Add more information as needed.>

7.2.1 Recovery Team Training

<Instructions: Verify and provide information on the Recovery Team training.>

7.3 Testing Outcomes Reporting

<Instructions: Verify and provide information on testing outcomes reporting process.>

It is important that all testing events be well-documented, including actions taken and problems encountered, and lessons learned during the testing.

<Add more information as needed.>

SECTION 8 CONTINGENCY PLAN MAINTENANCE

<Instructions: Verify and provide information on the Contingency Plan maintenance process.>

8.1 Maintenance Approach

<Instructions: Verify and provide information on the maintenance approach process.>

The <Vendor> O&M Team has the overall responsibility to maintain the <Vendor's> Contingency Plan. The <Vendor's> Contingency Plan should be updated and maintained on an agreed upon periodic and ongoing basis, or at the direction of the Agency.

<Add more information as needed.>

8.2 Maintenance Trigger

<Instructions: Verify and provide information on the maintenance trigger.>

Revisions to the <Vendor's> Contingency Plan should be considered for inclusion any time significant changes occur within the <Vendor's> Production environment. Types of changes that could affect the plan include:

- Equipment changes
- Software conversions/additions/modifications
- Module integrations
- Staff changes
- Network changes
- Support service changes

<Add more information as needed.>

APPENDIX A – CONTACT LIST

<Instructions: Verify and provide information on the contact list.>

Appendix A is the Recovery Team Contact List that lists the contact information of the key <Vendor> Team members.

The file included is the <provide name> and located at <provide location/breadcrumb path to the file>

<Add more information as needed.>