

Policy

DEPARTMENT: Information Technology (IT)	POLICY #: IT.01.006
TITLE: Disaster Recovery	VERSION: 5
APPROVED BY: Brenden Soos	ORIGINAL EFFECTIVE DATE: 11/02/2022
APPROVAL DATE: 10/25/2024	LAST REVIEW DATE: 02/21/2026
APPLICABILITY/SCOPE: ☒ Curana Health – All divisions ☐ AllyAlign Health ☐ Curana Health Medical Group ☐ Curana Health ACO	

Contents

1	Scope	3
2	Purpose.....	3
2.1	Objectives	3
2.2	Inventory of IT Assets	3
3	Definitions, Abbreviations, and Acronyms.....	4
4	Policy	5
4.1	Damage Assessment	5
4.2	Disaster Recovery Declaration.....	5
4.3	Communication Plan.....	5
4.4	Notification Procedures	6
4.5	Recovery Time Objective	6
4.6	Recovery Point Objective.....	7
4.7	Process.....	7
4.8	Data Backup.....	7
4.9	Disaster Recovery Testing.....	8
4.9.1	<i>Step-by-Step Recovery Process</i>	<i>8</i>

4.9.2	<i>Compliance, Monitoring, Approval, and Maintenance</i>	8
4.9.3	<i>Record Keeping</i>	8
4.10	Business Function Recovery Levels	8
4.11	Roles and Responsibilities.....	9
4.11.1	Internal Contacts	9
4.11.2	Disaster Recovery Team	9
4.12	Threat Matrix.....	10
4.13	Disaster Recovery Procedures	10
4.13.1	DR Plan for Damage to Servers	11
4.13.2	Alternate Work Locations	11
4.14	Access to Care.....	11
4.15	Call Centers	11
4.16	Transaction Process	12
5	References	13
6	CMS/Regulatory Citation	13
7	Accreditation Citation	13
8	Change Log	13
9	Compliance Approval	13

1 Scope

This policy applies to Curana Health – All Divisions. The following disaster recovery policies apply to managed services governed by Curana Health’s Business Continuity Model for Short & Long-Term Business Interruptions.

Curana Health has geographically separated operations with specific functions to that location per office and data center.

2 Purpose

The purpose of this procedure is to detail the policies and procedures for Curana Health in the event of a disruption to critical Information Technology (IT) services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

2.1 Objectives

- Minimize downtime and data loss.
- Ensure quick recovery of IT services.
- Protect organizational assets.

2.2 Inventory of IT Assets

- Business Critical Applications
 - GehriMed
 - Microsoft Azure
 - Microsoft 365 Suite
 - GoTo Call Center
 - PayCom HRIS

3 Definitions, Abbreviations, and Acronyms

Acronym / Definition	Meaning
BCP	Business Continuity Plan
CC	Compliance Committee
CCPO	Chief Compliance and Privacy Officer or delegate
CH	Curana Health
CIO	Chief Information Officer
CEO	Chief Executive Officer
CISO	Chief Information Security Officer
VP	Vice President
DR	Disaster Recovery
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITECH	Health Information Technology for Economic and Clinical Health
RPO	Recovery Point Objective (amount of data that can be lost within a period most relevant to a business before significant harm)
RTO	Recovery Time Objective (target time set for recovery of IT and business activities after a disaster)
VoIP	Voice Over Internet Protocol
IT	Information Technology
HRIS	Human Resources Information System
DBA	Database Administration
DNS	Domain Name Service
ITSM	IT System Management
SaaS	System as a Service
UM	Utilization Management
PCP	Primary Care Provider
PBM	Pharmacy Benefit Management

4 Policy

All production systems and software are hosted at offsite hosting facilities including cloud hosting. In the event of any failure or inaccessibility of this location, immediate troubleshooting will begin, and an initial triage of the situation will be provided to the CIO.

4.1 Damage Assessment

Initial triage of the situation will begin following notification of a system outage. A preliminary damage assessment shall address:

- Cause of outage or disruption
- Potential for additional disruptions or damage
- Areas or systems affected
- Physical infrastructure location
- Status of system / applications
- Users affected
- Impact to business
- Estimated time to restore

4.2 Disaster Recovery Declaration

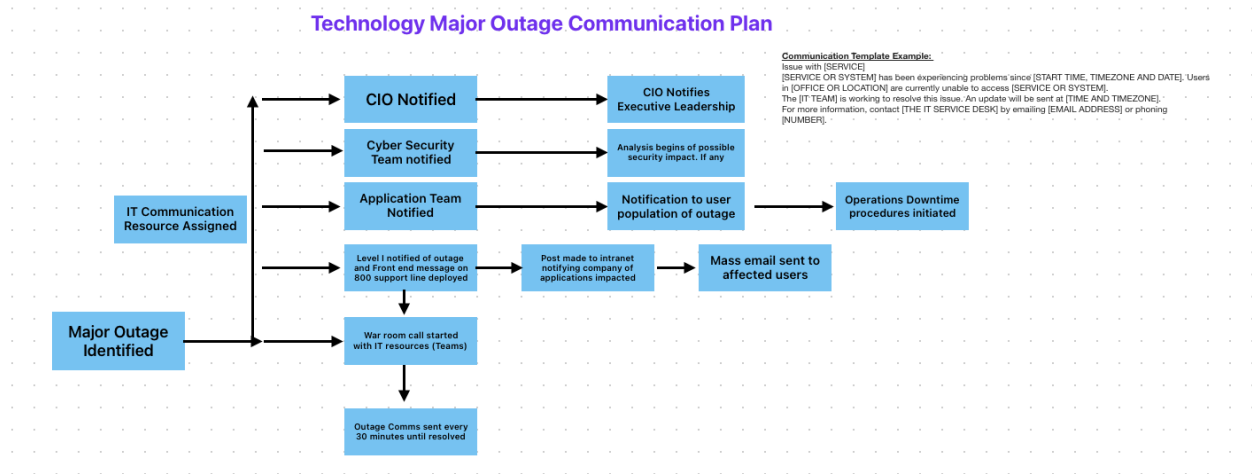
Troubleshooting efforts will continue for up to four (4) hours or until the CIO or designee declares a disaster and implements Curana Health's DR plan. The CIO or the CCPO will implement the DR plan.

4.3 Communication Plan

A communication bulletin will be sent out to all application users and external partners to notify them of the outage. Updates and restoration bulletins will be sent out in accordance with the applicable Curana Health corporate communication policy and as required by contractual obligations. BCP Manager and/or Business Continuity & Disaster Recovery Committee members will be notified to initiate a broader enterprise wide BCP process if needed.

- List key stakeholders and their contact information. Located on SharePoint in DR plan folder.
- Establish communication methods (emails, messaging apps). Located on SharePoint in DR plan folder.

4.4 Notification Procedures



We are committed to ensuring that our beneficiaries experience no adverse effects or disruption of service due to the storm threat or any other potential outage events. Below is a summary of the steps we are taking to mitigate or eliminate the risk of disruption to our members.

4.5 Recovery Time Objective

Curana Health's BCP is designed to reduce the risk to an acceptable level by ensuring the below noted recovery timeframes by recovery level. Recovery levels are defined by Curana Health business functions and the resources required to support them:

Recovery Level	Recovery Level Definition	Recovery Time from Outage*
1	Business Critical (BC)	< 15 hours
2	Support Critical (SC)	< 24 hours
3	Production Operations (PO)	< 72 hours
4	Non-Critical Operations (NCO)	< 2 weeks

*Recovery Time after Curana Health has declared a disaster.

4.6 Recovery Point Objective

Recovery Level	Recovery Level Definition	Recovery Point from Outage
1	Business Critical (BC)	< 4 hours
2	Support Critical (SC)	< 12 hours

It is the responsibility of the Technology Operations Department to enforce this policy.

4.7 Process

The process below is a high-level description of procedures for recovery operations. Detailed procedures are addressed in Curana Health's BCP.

In the event of a declared failure Curana Health IT would begin failover procedures as follows:

1. Notify the BCP Manager and/or Business Continuity & Disaster Recovery Committee.
2. Inform clients of outage. (Curana Health Client Services team)
3. Failover to secondary data center and set servers to primary. (Curana Health IT Infrastructure team)
4. If there is a critical failure and failover to the secondary data center is not feasible, full restoration from backup will occur. (Curana Health IT Infrastructure team)
5. If required, restoration of databases on servers at the secondary site will occur using the last available database backup(s). (Curana Health DBA team)
6. Redirect DNS/domains to new location. (Curana Health IT Infrastructure team)
7. Inform clients once all applications and/or services are available. (Curana Health Client Services team)

4.8 Data Backup

- Each respective application vendor manages backups.
- Use offsite storage or cloud solutions for critical data.
- Curana also utilizes 2 offsite vendors for m365 backups of email and teams.
 - Backupify
 - ITSM

4.9 Disaster Recovery Testing

DR processes and procedures will be tested and validated annually. If Curana Health determines that a DR test is causing material interruptions to Curana Health business operations and/or those of Curana Health clients, the test will be suspended, and the production systems will be brought back online. The source of the failure(s) experienced will be identified and addressed.

Once the DR test plan has been revised and revised to mitigate business interruptions, a subsequent DR test will be performed at a later date, but in no event later than the following Curana Health fiscal year quarter. DR exercise results, lessons learned, and identification of mitigation tasks will occur prior to any following DR test exercise.

4.9.1 Step-by-Step Recovery Process

1. **Assess the Situation:** Evaluate the extent of the disaster.
2. **Notify the DR Team:** Activate the DR team.
3. **Vendor - Implement Backup Systems:** Start recovery from backups.
4. **Vendor - Restore Systems:** Follow recovery procedures for critical systems.
5. **Operations and IT - Test Systems:** Ensure all systems are operational.
6. **IT - Document the Incident:** Record what happened for future analysis.

4.9.2 Compliance, Monitoring, Approval, and Maintenance

Compliance with this policy may be monitored/audited periodically and reported to the IT Leadership & Security Compliance Committee (CC).

Approval and maintenance of this policy will be the responsibility of the Chief Information Officer (CIO).

4.9.3 Record Keeping

- Maintain logs of all backups, incidents, and recovery efforts.
- Store documentation securely and ensure easy access. Located on SharePoint in DR plan folder.

4.10 Business Function Recovery Levels

Curana Health's BCP identifies and classifies Curana Health business functions, and the resources required to support them into recovery levels. For each function, executive management has a role to evaluate, decide and take executive-level actions, if necessary:

Recovery Level	Recovery Level Definition	Functions
1	Business Critical (BC)	• Alternate Voice Communications • Executive Management (as required)
2	Support Critical (SC)	• Customer Support • Executive Management (as required)
3	Production Operations (PO)	• Core service applications, infrastructure and operations (including call center and fax solutions) • Executive Management (as required)
4	Non-Critical Operations (NCO)	• Non-critical, essential or required tools, services and operations • Executive Management (as required)

4.11 Roles and Responsibilities

4.11.1 Internal Contacts

The following individuals are to assume responsibility for restoring services when this policy is activated:

Name	Job Role	Contact Details	Disaster Recovery Process Owned
Todd Tyler	Chief Information Officer	1-XXX-XXX-XXXX todd.tyler@curanahealth.com	Accountable for all technology
Brenden Soos	Vice President, Technology Infrastructure & Operations	1-XXX-XXX-XXXX Brenden.soos@curanahealth.com	Accountable for all technology infrastructure and daily operations
Jacob Rubin	Chief Security Information Officer	1-XXX-XXX-XXXX Jacob.rubin@curanahealth.com	Responsible all Technology security

4.11.2 Disaster Recovery Team

Name	Job Role	Contact Details	Disaster Recovery Process Owned
Kevin Finkbiner	Manager of Infrastructure Operations	1-XXX-XXX-XXXX Kevin.Finbiner@curanahealth.com	IT Infrastructure Recovery
Denton Schraplau	Senior Infrastructure Engineer	1-XXX-XXX-XXXX Denton.Schraplau@curanahealth.com	Oversees DR Plan
Sam MacGregor	Director of Portfolio Management	1-XXX-XXX-XXXX samuel.macgregor@curanahealth.com	Internal and External Communications
Epting Enterprises	Support Staff		Assists with Technical Recovery

4.12 Threat Matrix

This Disaster Recovery (DR) plan is to be activated when one or more of the following criteria are met:

- Fire
- Flood and water damage
- Earthquake
- Hurricane
- Bomb threat
- Terrorist attack
- Malicious intruder
- Social engineering attack
- Denial of service attack
- Pervasive malware attack
- Stolen confidential information
- Loss of key digital files and/or databases
- Server failure

The person discovering the incident must notify the following DR stakeholders, who collectively assume responsibility for deciding which – if any– aspects of the DR plan should be implemented, and for establishing communication with employees, management, partners and customers.

- First point of contact, Chief Executive Officer

- VP Infrastructure and Operations

4.13 Disaster Recovery Procedures

The CEO can invoke this DR Plan, and if not available, the CIO, CISO, or VP of Infrastructure and Operations.

Depending on the incident, and the number of and nature of the IT Services affected, one or more of the following DR procedures may be activated

4.13.1 DR Plan for Damage to Servers

Currently, there are no on-site servers. All data is stored on the production servers via SaaS relations with the respective vendor.

4.13.2 Alternate Work Locations

If access to the office is unavailable, key personnel should work from home. 90% of staff is remote workforce either at a Clinical site or home office.

4.14 Access to Care

- We have confirmed that all facilities have continuity plans in place in the event that the facility's operations are impacted.
- We have established a contingency Utilization Management policy in the event that the UM Call Center is disrupted. That policy establishes protocols for emergency authorization of service if the UM Call Center is unavailable.
- We will communicate the policy to each PCP in our network and all plan Nurse Practitioners as necessary
- We have established and communicated similar authorization protocols for pharmacy services and worked with our PBM to ensure that beneficiary access to medication is not disrupted and in case of loss of medication that it can be refilled timely

4.15 Call Centers

Our phone system and the systems that our call center agents are all hosted offsite in hardened data centers, so the integrity of the processing and system availability is protected. However, our call centers are at risk by

- Power or internet connectivity in our office
- Staff access to the office

To mitigate these risks, we have taken the following steps:

- Our phone systems operate using Voice Over Internet Protocol (VOIP). This allows us to connect to the phone system and queues from any internet connection. Similarly, our systems operate over internet via browsers, so our agents can access the required systems from any internet enabled location. If access to the office is disrupted, our first option will be for agents to work from home using the internet connection in their homes. Secondly, we have identified two alternate locations that we can use as alternate locations for our call center.
- Our Utilization Management support team operates from four locations, thereby mitigating the risk of internet connectivity loss.

By having multiple options to respond, we are lowering the risk that we are unable to respond in the case of service disruption.

4.16 Transaction Process

All transaction processing systems are hosted in hardened data centers, so the integrity of the processing and system availability is protected. As with the call center, the risk is ensuring staff access to the systems. We will employ the same strategies stated above to ensure that our claims processing, provider services, and other teams are able to continue to ensure timely processing for our members.

5 References

#	Reference Name	Resource Reference
1	IT.01.002	Contingency Plan
2	IT.01.012	Data Backup Plan
3	Business Continuity Model	For Short-Term and Long-Term Business Interruptions (TBC)
4	Run Book	Curana Health Disaster Recovery Run Book (TBC)

6 CMS/Regulatory Citation

#	Reference Name	Resource Reference
1	45 CFR §164.308(a)(7)(ii)(B)	Administrative Safeguards; Disaster Recovery Plan

7 Accreditation Citation

#	Reference Name	Resource Reference
	N/A	

8 Change Log

Document Version	Initial/Major / Minor Revision?	Date	Name	Comments
1	Initial	11/01/2022	Cybersecurity	Initial Creation
2	Minor	10/01/2023	Cybersecurity	Document format
3	Minor	11/01/2025	I/O	Process Update
4	Minor	02/21/2025	I/O	Document Update – Addition of Acronyms to section 3.
5		02/21/2026	Kate Cook	No Changes this refresh.

9 Compliance Approval

Date	Compliance SME Approval
	N/A