

State of North Carolina

Department of Health and Human Services

Division of Child and Family Well-Being



Crossroads MIS

Maintenance and Enhancement Services

North Carolina WIC Program

Disaster Recovery and Contingency Plan

Contents

1. Document information.....	iii
2. Introduction.....	- 1 -
2.1 Integrated Project Plans	- 1 -
3. Voyatek Business Processes.....	2
3.1 Voyatek Disaster Recovery Plan.....	2
3.2 Physical Environment.....	3
3.3 Team Environment	3
3.4 Disaster Declaration.....	3
3.5 Voyatek Disaster Recovery Team	4
4. North Carolina Contacts & Notification.....	0
4.1 Notification	0
5. Mitigation Strategies	1
5.1 Voyatek Staff Availability	1
5.2 Zone Redundancy	1
5.3 System Data and Backup Strategy	2
5.3.1 Backup and Recovery Overview	2
5.3.2 High Availability.....	2
5.3.3 Virtual Machine Backup Policy.....	3
5.3.4 Database Backup Schedule	3
5.4 Offsite Backup Storage.....	5
5.4.1 Storage Account Backup	5
5.4.2 Backup Validation and Testing	5
5.4.3 Backup Security	6
6. Disaster Recovery	7
6.1 Recovery Objectives	7
6.2 Compute (Application, Batch, Reporting Servers).....	7
6.3 Azure SQL Managed Instance (MI).....	8
6.4 Storage (Azure File Shares & SFTP Containers)	8
6.5 Public Access and DNS Failover	8
6.6 Azure Site Recovery Failover Procedure	8
6.7 Application Availability During Failover	9
6.8 Disaster Recovery Playbook.....	9
7. Disaster Recovery Testing	0

8. Disaster History	1
9. Disaster Impacting North Carolina.....	2
10. Appendix A Disaster Recovery Playbook.....	3

Figures

Figure 1 - Geo-zone-redundant storage data replication.	3
--	---

Tables

Table 1 Document Identification	iii
Table 2: Document Edit History	iii
Table 3: Document Approvals.....	iv
Table 4: Definition of a Disaster	3
Table 5: Voyatek's disaster recovery plan contacts	5
Table 6: North Carolina's Contacts for Disaster Recovery.....	0
Table 7: Backup frequency and retention schedule for NC Crossroads.....	3
Table 8: Draft DR Playbook Tasks for NC Crossroads.....	3

1. Document information

Table 1 Document Identification

Identification		Description
Document Name	Disaster Recovery and Contingency Plan	
Project Name:	Crossroads	
Project Sponsor(s) Name	Krushanu Majmundar	
Project Manager	Jennifer Saunders	
Document Version	1.7	
Document Status	Revisions for RFP 30-25002	
Data Submitted	2/09/2026	
SharePoint Location		

Table 2: Document Edit History

Date	Version	Section Changed/Description	Prepared by
12/18/2018	0.1	Jay Saunders, Three Sigma Software	Draft version (Contract 30-36820_18 DHHS_DPH)
3/6/2025	1.0	Jennifer Saunders, Voyatek	Revisions for RFP 30-25002
12/1/2025	1.1	Jennifer Saunders, Voyatek	Revisions per BAFO #1 30-25002
12/5/2025	1.2	Jennifer Saunders, Voyatek	Incorporate internal feedback.
12/16/2025	1.3	Jennifer Saunders, Voyatek	Add list of integrated project plans and final edits for submission to NC
1/20/2026	1.4	Molly Jones, NC WIC	NC review comments
1/23/2026	1.5	Jennifer Saunders, Voyatek	Incorporate NC's feedback into the document.
2/4/2026	1.6	Molly Jones, NC WIC	NC final feedback
2/5/2026	1.7	Jennifer Saunders, Voyatek	Accept revisions from v1.5 and incorporate NC's final feedback. Update Draft DR playbook in Appendix A

Table 3: Document Approvals

Name/Role	Signature	Date
Voyatek		
Jennifer Saunders Project Director		
North Carolina		
Molly Jones Crossroads Release Manager		
Kim Lovenduski Deputy Director, Community Nutrition Services Section		

2. Introduction

This plan outlines the disaster and recovery procedures for the North Carolina Women, Infants and Children program's Crossroads system in case of a disaster that impacts NC Crossroads operations. This plan specifically speaks to a disaster that affects the use of the production NC Crossroads system hosted in the Azure Cloud, which affects the ability of clinic staff to perform activities for North Carolina WIC and requires support personnel to enable the users to resume operations at the clinics.

This plan covers the procedures for declaring a disaster and communicating with North Carolina staff, interim business operations, and the steps to resume full operational capacity.

2.1 Integrated Project Plans

The Disaster Recovery Plan is the primary document for information on NC Crossroads disaster recovery and business continuity. The plans documented below are integrated plans and rather than duplicating information, this plan references and or builds upon the following project documentation:

- *Appendix A: Transition-In Plan* – DR testing milestones, environment setup schedule during Transition-In phase
- *Appendix B: Product Management Plan* – Overall project governance, RACI matrix, roles and responsibilities for disaster recovery activities
- *Appendix D: Quality Assurance Management Plan* – Testing standards, acceptance criteria, and test documentation requirements for DR testing
- *Appendix E: Rehosting Implementation and Rollout Plan* – Azure infrastructure architecture, high availability configuration, network architecture, FortiSIEM monitoring
- *Appendix G: Security and Vulnerability Plan* – Encryption standards, access controls, RBAC policies, and data protection requirements for backup security
- *Appendix H: Risks and Issues Management Plan* – Risk identification, tracking, and mitigation strategies for disaster scenarios
- *Appendix J: Configuration Management and Release Management Plan* – Configuration baseline management, version control, and source code availability during disasters
- *Appendix N: Help Desk Plan -- Appendix N: Help Desk Plan -- Support availability, escalation procedures, alternate contact methods during disaster events, and service level agreements, including Vendor-Hosted System Availability and Statewide Production Down*
- *Appendix P: Communications and Coordination Plan* – Stakeholder notification procedures, escalation priorities, contact directory, and communication methods during disasters
- *Appendix R: Production Deployment Plan* – Deployment-specific and infrastructure-level details including protected resources, RTO/RPO targets, rollback procedures, and monitoring thresholds

This plan will be maintained as a living document throughout the contract, with updates made as processes documented in this plan are refined and as disaster recovery requirements evolve based on State needs and hosting needs. Where processes are already documented in other project management plans that are also living documents, those plans will be updated as needed.

3. Voyatek Business Processes

3.1 Voyatek Disaster Recovery Plan

A disaster is a sudden or non-predicted event that jeopardizes the ability of Voyatek to deliver services to North Carolina. A disaster can include both natural and man-made events as defined later within this document. Short of a disaster is a disruptive event that is anything that puts operations at risk and can range from a cyberattack to a natural disaster. The Voyatek disaster recovery (DR) plan has processes for preparing for disaster recovery, including planning, testing, and steps for executing the plan.

The Voyatek DR plan is intended to address the availability of the production Crossroads environments. These Crossroads environments are maintained and hosted by Voyatek.

During transition-in and annually thereafter, Voyatek staff will conduct DR planning, and collaborate with the project stakeholders to develop and implement a feasible plan considering different variables of the project and organization. The plan delineates the activities, resources, and responsibilities for all involved parties when a disaster occurs. *Appendix H: Risk and Issues Management Plan* will be updated during DR planning and annual testing at a minimum.

Voyatek takes steps to mitigate failure and risks by using modern and secure techniques in architecture design, monitoring, and protecting infrastructure and data. Those techniques include encryption, vulnerability scanning, behavior analysis, network segmentation, frequent backups/snapshots, and geographic backup systems.

For the NC WIC project, all essential tools will reside within Microsoft's Azure Cloud. Source control and issue management will reside in Azure DevOps Services. Azure DevOps Service has regional redundancy and is designed to be highly available. This capability will enable Voyatek and NC WIC to continue accessing key project resources throughout almost any potential disaster event.

Voyatek will also utilize the Microsoft Azure-hosted SharePoint service to provide high availability of project archives and documentation.

Creating a well-designed DR plan supports end users so they are able to focus on operations and not systems availability and stability. The typical steps in our DR planning include:

- Inventory of IT resources—Collecting data on all relevant IT resources (e.g., data hardware, software, etc.) supporting the project.
- Inventory of operations—Gathering the input from key stakeholders to identify operations that are potentially at higher risk, incident scenarios, and responsible parties for resolving the issues.
- Recovery timeline—Working with stakeholder(s) to set recovery goals and timeframes by which certain systems need to be back in operation including Recovery Point Objective (i.e., time since last backup) and Recovery Time Objective (i.e., time to recovery).
- Data backups—Safeguarding a recent copy of all data assets for mission-critical applications.
- Human risk—Mitigating the possibility of humans being a source of disaster, intentional or not.
- DR plan testing—Confirms the plan is drafted, tested, and complete so it is actionable and effective in case of a disaster.
- Business Continuity — The organization-wide strategy to maintain essential operations during and after a disaster. The business continuity plan should incorporate the DR plan to complete preparation to meet any unexpected circumstances.

3.2 Physical Environment

Voyatek will not be hosting any instances of the system (UAT or production) at company-owned facilities. All hosting will be in the Microsoft Azure cloud. Physical environment security is the responsibility of the cloud hosting provider.

3.3 Team Environment

The team operates from facilities located in Overland Park, KS, Columbia, MD, and Richmond, VA. Team members in these locations are equipped to work from other locations if necessary. Additional team members work from geographically dispersed locations within the United States.

3.4 Disaster Declaration

Definition of a Disaster: A disaster is a sudden or non-predicted event that jeopardizes the ability of Voyatek to deliver services to the state as defined within the contract. A disaster can include both natural and man-made events, examples are listed in Table 4:

Table 4: Definition of a Disaster

Disaster	
Arson	Pandemic
Azure System Failure	Riot
Bomb damage/hoax	Snowstorm

Disaster	
Break-in/theft	Strike
Cyber Attack	Sunspots
Earthquake	System failures at the local WIC agencies' sites
Explosion	Telecommunications Failure
Fire	Terrorism
Flooding	Thunderstorm
Hail	Tornado
Hurricane	Tsunami
Ice Storm	Vandalism
Lightning	Water leak

A disaster will be declared if the production environment is non-operational or expected to be non-operational for 24-hours. This duration does not imply that no action will be taken for shorter outages. Members of the Voyatek management team will initiate the disaster management protocol in the event of a qualifying disaster.

Once a disaster has been declared, Voyatek staff will utilize this plan to initiate communications with state staff, coordinate with Voyatek staff, and to execute plans to restore hosting services. Systems used to support the project will be brought back up (possibly in a different hosting region) within 24 hours. Once the disaster has been resolved, Voyatek will coordinate with state staff to schedule the return of services to the primary hosting region with a minimum of project disruption.

3.5 Voyatek Disaster Recovery Team

The following key staff included in Table 5 below will be responsible for leading the Voyatek response to disaster recovery events. Contact information will be provided in the final version of this plan.

Table 5: Voyatek's disaster recovery plan contacts

Staff Name	Role	Phone	E-Mail
Jennifer Saunders	Product Manager	913-461-8585	Jennifer.Saunders@voyatek.com
Krushanu Majmundar	Project Director/Systems Recovery Coordinator	410-258-1144	Krushanu.Majmundar@voyatek.com
Cindy Kochersperger	Business Analyst	(913) 269-3773	Cindy.Kochersperger@voyatek.com
Rob Shaw-Fuller	Network Engineer		Rob.ShawFuller@voyatek.com
Gezahegn Gute	Database Administrator		Gezahegn.Gute@voyatek.com

4. North Carolina Contacts & Notification

In case of a disaster or a smaller service disruption, Voyatek will contact the primary point of contact and or all state contacts identified in Table 6 to communicate with North Carolina state staff and to coordinate services during the disaster event.

Table 6: North Carolina's Contacts for Disaster Recovery

Staff Name	Role	Phone	E-Mail
Molly Jones	Crossroads Release Manager	919.850.6608	molly.jones@dhhs.nc.gov
Sharon McDougal	Customer Service Desk Manager	919.622.0556	sharon.mcdougal@dhhs.nc.gov
Kim Lovenduski	Deputy Director, Community Nutrition Services Section	919.218.3654	kim.lovenduski@dhhs.nc.gov

4.1 Notification

Short-term Event: The most common short-term event is the loss of power or telecommunications for one or more team members. In case of a short-term event, it will be the responsibility of the Voyatek product manager to notify either the Crossroads Release Manager or an identified distribution list based on the state of the nature of the disruption and the affected team members. The goal will be to provide alternate contacts or workaround communication methods for the impacted individuals. This communication will be provided as soon as possible and will be within 60 minutes of the event being identified.

Disaster Event: If Voyatek has determined that a disaster will impact routine operations for more than 24 hours, the decision to execute the disaster recovery plan to relocate Crossroads hosting operations to a secondary facility will be made. Once this determination has been made, the Voyatek Product Manager or a company executive will contact state staff (as identified in Table 3) within one hour to notify them of the initiation of the disaster recovery plan. This communication will include:

- Guidance on effective/available communication methods during the disaster event.
- Assignment of non-affected staff providing support during the disaster event.
- Establishing the communication mechanism for regular status updates regarding the disaster.

Regular updates regarding the status of a disaster recovery event will be provided during the move from the primary environment to the disaster recovery environment. Following the disaster event, the Voyatek Product Manager will coordinate the orderly return to normal business operations in a manner that minimizes disruption to Crossroads operations.

5. Mitigation Strategies

5.1 Voyatek Staff Availability

The primary objective in response to either short- or long-term disruptions to operations will be the ability to provide the state with help desk and technical support as required within the contract. The Voyatek team includes project management, quality assurance, and technical resources that reside in geographically disparate locations. This aspect of the team allows Voyatek to continue to provide each of those service elements even in the event of regional disruption without investing in redundant staffing capacity.

The primary determination needed in the event of a disaster will be assessing telecommunication capabilities and responding to any outages. The primary communication method for NC support is MS Outlook email and secondary is MS Teams chats and meetings. If either of these communication methods are down, the Voyatek Production Manager and Crossroads Release Manager will communicate the issue and confirm the other communication method will be used until the outage is resolved. However, if both MS Outlook and MS Teams are down, the Voyatek Product Manager will contact the Crossroads Release Manager to provide secondary phone numbers for support services. These will likely be cell phone numbers for staff.

Most Voyatek staff members are equipped with laptop computers. In the event of a facility disruption, they can continue to provide services from home or other office locations. Every attempt will be made to continue operations using laptop equipment, cellular communications, and organizational procedures in the event of a disaster.

5.2 Zone Redundancy

The first tier of protection for business continuity and system availability is Azure zone redundancy. The second tier of protection is Azure Site Recovery described in Section 6 Disaster Recovery. The production environment is deployed with zone redundancy within the Azure East US region. Availability zones are physically separate datacenter locations within a region, each with independent power, cooling, and networking infrastructure. Zones are typically separated by several kilometers to reduce the likelihood that multiple zones would be affected by local outages, weather events, or infrastructure failures, while remaining close enough to support low-latency synchronous data replication.

Zone-redundant resources are automatically replicated or distributed across multiple availability zones by Azure. If an outage occurs in one availability zone, Azure manages failover to another zone automatically, allowing regional services and high availability to be maintained by the remaining zones. During zone redundancy failover, the entire NC Crossroads system remains available, including all external interfaces and portals. Azure automatically manages failover to healthy availability zones, so no manual intervention is required.

The following NC Crossroads components are configured for zone redundancy:

- **Virtual Machines (Application, Batch, and Reporting Servers)** – Production servers distributed across availability zones to maintain application availability during zone outages

- **Azure SQL Managed Instance (Business Critical tier)** – Zone-redundant high availability with synchronous data replication across availability zones
- **Azure Storage (GZRS)** – Zone-redundant storage with data replicated across three availability zones within the primary region

Recovery objectives for zone redundancy are:

- **Recovery Time Objective (RTO): Less than 1 hour** – Azure automatically manages failover to healthy availability zones, typically completing within minutes.
- **Recovery Point Objective (RPO): Near-zero** – Synchronous data replication across availability zones ensures minimal to no data loss during zone failover.

5.3 System Data and Backup Strategy

5.3.1 Backup and Recovery Overview

North Carolina Crossroads will leverage Azure Backup Center to centrally manage and monitor backup and recovery operations across all virtual machines, databases, and Azure storage workloads. Azure Backup Center provides a single pane of control for policy management, protection status, recovery points, audit history, and compliance reporting. Azure Backup Center provides consistent backup governance.

All North Carolina Crossroads servers will be protected using Azure Recovery Services Vaults, managed through Backup Center. Backup policies are standardized to preserve data integrity, support operational recovery, and meet North Carolina's long-term retention requirements.

5.3.2 High Availability

Crossroads production will be using Microsoft's Azure SQL Server Managed Instance (MI) with premium processing and in the business-critical tier. This service provides the highest reliability and fast database performance. The Production database will be in the Azure East US Region and will be actively synchronized with the disaster recovery database in the Azure West US 3 Region.

In the final version of this plan, Voyatek will add a diagram showing the high availability architecture as implemented in Azure for NC Crossroads.

In addition to the highly available environment, backups of the database managed in Azure are stored in a geographically redundant location. The entire server can be restored from these backups to a secondary paired region.

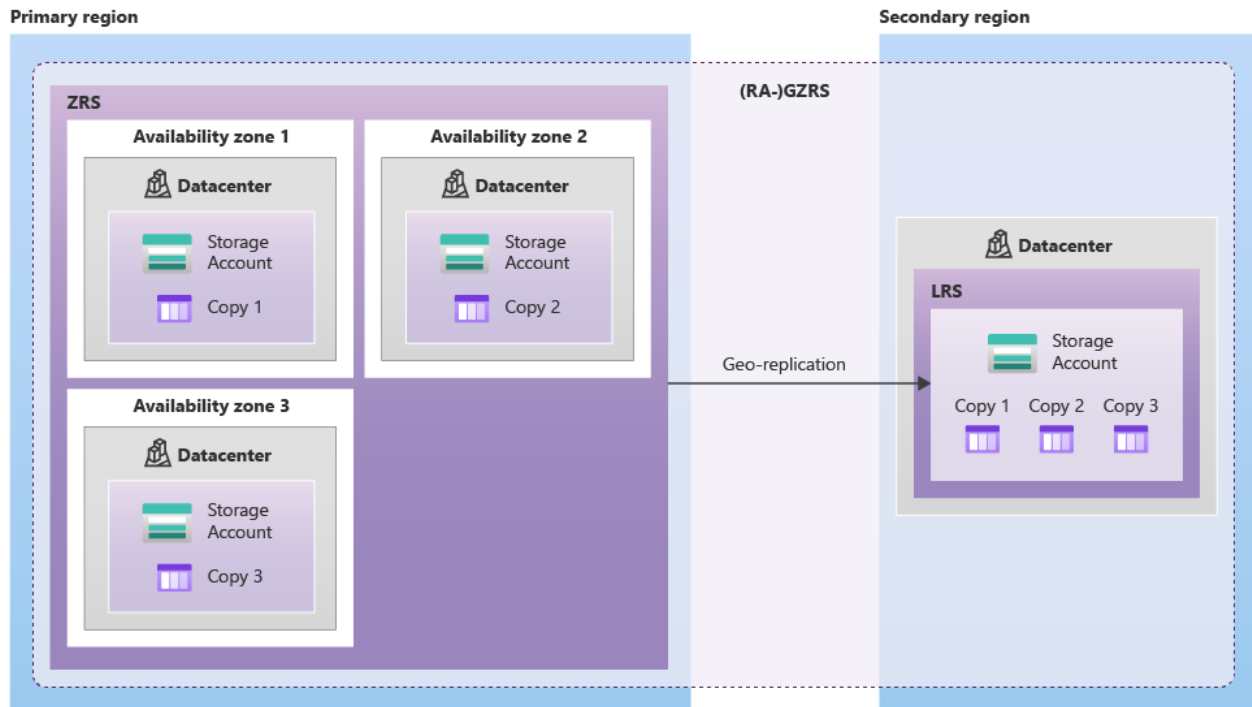


Figure 1 - Geo-zone-redundant storage data replication.

5.3.3 Virtual Machine Backup Policy

The standard backup policy for all North Carolina Crossroads virtual machines is configured for:

- Daily backups at 1:00 AM Eastern Time
- Instant recovery snapshots maintained for seven (7) days
- Daily backups are maintained for thirty (30) days
- Monthly backups maintained for six (6) months
- Yearly backups are maintained for seven (7) years

This retention schedule aligns with North Carolina's requirement to maintain participant and benefit data for six (6) years after the last participant activity and complies with state data retention policies.

5.3.4 Database Backup Schedule

Voyatek performs regular backups following North Carolina's retention and recovery policies:

Table 7: Backup frequency and retention schedule for NC Crossroads

Backup Type	Frequency	Retention
Daily (Differential, Transaction Log)	Daily	30 days
Full	Weekly	30 days

Backup Type	Frequency	Retention
Monthly Full	With EOM processing on the last day of the Month	Six months
Bi-Annual PC Report	With EOM processing on April 30 th every two years starting in 2026	Until NC confirms PC reporting is complete
Yearly Full – Calendar Year	Backup taken on December 31 st each year	Seven years
Yearly Full – State Fiscal Year	Backup taken on June 30 th of each year	Seven years
Yearly Full – Federal Fiscal Year	Backup taken on September 30 th of each year	Seven years

Backups are encrypted, stored in redundant cloud locations, and validated through automated and manual verification checks.

Daily & Weekly Backups (Azure SQL Managed Instance)

Azure SQL Managed Instance performs automated full, differential, and transaction log backups. All backups are retained as part of the Point-in-Time Restore (PITR) chain for a configurable retention period of 7–35 days. Differential backups are taken automatically at platform-managed intervals, typically every 12–24 hours. Transaction Log backups are every 5-10 minutes.

The retention window applies to the overall PITR backup chain, not to individual backup types. Full, differential, and transaction log backups are maintained together as part of the PITR chain for the configured retention period. This automated backup strategy enables point-in-time recovery to any moment within the retention window.

Month-End Full Backup

The full database backup that is performed after production End of Month (EOM) processing finishes on the last day of the month is the monthly full backup. This backup captures the complete state of the system following all monthly processing activities.

Yearly Full Backups

Three full database backups will be retained as “yearly full backups”. A full backup will be taken after completion of End of Month Processing on June 30th, September 30th and on December 31st each year. All three backup files will be retained to support long-term data retention and compliance requirements.

Bi-Annual PC Report Backup

Voyatek will review North Carolina’s process for the Participant Characteristics (PC) report submission. A full database backup will be performed after business hours on April 30th according to FNS guidance for the Participant Characteristics (PC) report submission that occurs bi-annually. This backup is retained onsite until USDA completes their review of the report.

5.4 Offsite Backup Storage¹

All backup data is stored using Azure's geo-zone-redundant storage (GZRS) capabilities, which provide comprehensive protection through multiple layers of redundancy. GZRS combines high availability across availability zones with geo-replication for regional disaster protection. Data is copied across three or more Azure availability zones within the primary region (Azure East US) and simultaneously replicated to a secondary geographic region (Azure West US 3 Region). This provides:

- Geographic separation of backup data from the primary site
- Protection against regional disasters affecting the primary data center
- Automated replication without manual intervention
- Compliance with North Carolina's offsite storage requirements

This architecture allows backup data to remain accessible even if an availability zone becomes unavailable or unrecoverable. Additionally, the data remains durable during a complete regional outage or disaster affecting the primary region. GZRS is designed to provide at least 99.99999999999999% (16 9s) durability of objects over a given year.

The automated replication occurs without manual intervention, providing geographic separation of backup data from the primary site while confirming compliance with North Carolina's offsite storage requirements. This eliminates the need for manual backup transfers or coordination while maintaining protection against regional disasters affecting the primary data center.

Additionally, Voyatek can provide North Carolina WIC access to an Azure storage location, allowing the State to take possession of backups on any schedule desired for additional offsite retention if required. This provides the State with direct control over backup retention policies while leveraging Azure's robust storage infrastructure.

5.4.1 Storage Account Backup

Files (user-uploaded documents, signature captures) are stored in an Azure storage account. In production, this account is configured with geo-zone-redundant storage (GZRS), which means storage is redundant across three availability zones in the deployed region (Azure East US Region) as well as to a secondary region (Azure West US 3 Region), where it is also stored across three availability zones.

GZRS is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year. This configuration provides that for the critical application data remains available and recoverable in the event of hardware failures, zone outages, or regional disasters.

5.4.2 Backup Validation and Testing

Backup integrity is validated through:

- Automated verification checks performed by Azure Backup Center after each backup job
- Manual test restores performed quarterly to verify backup recoverability
- Annual disaster recovery exercises that include full system restoration

¹ Information on Azure storage redundancy: [Data redundancy - Azure Storage | Microsoft Learn](#)

- Monitoring and alerting for backup job failures through Azure Monitor and FortiSIEM

Any backup failures or issues are escalated to the Voyatek disaster recovery team and North Carolina WIC disaster recovery contacts for resolution.

5.4.3 Backup Security

All backup data is protected through:

- Encryption at rest using Azure Storage Service Encryption with Microsoft-managed keys
- Encryption in transit using TLS 1.2 or higher
- Role-based access control (RBAC) limiting backup access to authorized personnel only
- Soft delete capabilities providing protection against accidental or malicious deletion

6. Disaster Recovery

Azure Site Recovery is a disaster recovery as a service (DRaaS) that provides business continuity by orchestrating replication, failover, and recovery for workloads in Azure and on-premises environments. It protects against planned and unplanned outages by replicating virtual machines (VMs) and physical servers to a secondary location, such as another Azure region, and allows for testing the recovery plan without impacting production. In the event of a disaster that disables the primary Azure region for NC WIC MIS, Voyatek will use Azure Site Recovery Failover services.

Azure Site Recovery Key functions

- Data Replication - Replicates physical and virtual machines, Azure VMs, and machines from other cloud providers to Azure, or replicates Azure VMs to another Azure region.
- Failover - Supports both planned and unplanned failovers to a secondary location, which can minimize data loss and downtime.
- Recovery - Orchestrates the failover process, which can include multi-tier applications with customized recovery plans that specify the order in which servers are brought online.
- Testing - Enables non-disruptive testing of the disaster recovery plan in an isolated environment, confirming the process works as expected before a real outage occurs.
- Failback - Allows you to return your workloads from the secondary location back to your primary site after an outage is resolved.

6.1 Recovery Objectives

For catastrophic events affecting the entire Azure East US region, geo-restore capabilities enable failover to the West US 3 disaster recovery region. This secondary site provides an additional layer of protection beyond the zone redundancy described in Section 5.2 Zone Redundancy for secondary site failover using geo-restore are:

- Recovery Time Objective (RTO): 12 hours – The maximum acceptable time to restore system operations at the secondary site following a regional disaster.
- Recovery Point Objective (RPO): 1 hour – The maximum acceptable data loss, based on asynchronous replication to the disaster recovery region.

Detailed recovery procedures for secondary site failover are documented in the DR Playbook (Appendix A).

6.2 Compute (Application, Batch, Reporting Servers)

All virtual machines are protected using Azure Site Recovery.

- Azure Site Recovery continuously replicates Production VMs from the primary region to the DR region (Azure West US 3 Region).
- Replicated VMs are pre-staged in DR with reserved static IP addresses, VNET assignments, and NSG/firewall rules aligned to the Production configuration.

- Failover and failback procedures are defined in the DR playbooks and tested during scheduled DR exercises.

6.3 Azure SQL Managed Instance (MI)

Databases are protected using SQL MI Failover Groups.

- The Production SQL Managed Instance (MI) is paired with a secondary SQL MI in Azure West US 3 Region
- Data is replicated continuously from the primary SQL MI to the secondary SQL MI using Azure's native Always On availability technology.
- Automatic or manual failover modes are selectable; Crossroads environments use customer-managed failover to coordinate across applications, batch workflows, and external integrations.

6.4 Storage (Azure File Shares & SFTP Containers)

All shared application storage is configured with Geo zone redundant storage (GZRS).

- GZRS asynchronously replicates data to a secondary Azure region, confirming that application file shares and SFTP-delivered data remain recoverable in a regional outage.
- Storage access in the DR environment is re-bound to private endpoints during failover.

6.5 Public Access and DNS Failover

External access is managed using Azure Traffic Manager, which provides DNS-based global failover.

- Each application endpoint is registered as a Traffic Manager endpoint in both Production and DR.
- State or agency DNS records point to the Traffic Manager FQDN via CNAME records.
- When a failover is initiated, Traffic Manager routes clients to the DR endpoint without requiring the agency to modify DNS directly.

6.6 Azure Site Recovery Failover Procedure

The following high-level steps outline the Azure Site Recovery failover and failback procedure. Detailed steps and timing are documented in the DR Playbook described in Section 6.8.

1. **Initiate Failover.** From the Recovery Services vault, select the replicated items (VMs) to fail over.
2. **Verify and Access Failed Over VMs.** Once failover completes, confirm that the VMs in the secondary site are running and properly sized. Confirm network connectivity (RDP/SSH) is configured by checking NSG rules, public IP assignments, and firewall settings.
3. **Smoke Test Secondary Site.** Perform smoke testing of the Crossroads system in the secondary site to confirm the application is operational and interfaces are working. Resolve any network, environment, or interface issues before proceeding.

4. **Commit the Failover.** After validating workloads, commit the failover.
5. **Reprotect in Secondary Site.** With workloads now running in the secondary site, reprotect them so they replicate back to the primary site setting the replication direction from secondary to primary in preparation for failback to the primary site.

Voyatek will coordinate and plan failback timing with North Carolina staff to return to the primary hosting site in a manner that minimizes disruption to Crossroads operations.

6. **Fail Back to Primary Site.** When the primary site is operational, initiate a planned failover from the secondary site back to the primary.
7. **Smoke Test Primary Site.** Perform smoke testing of the Crossroads system in the primary site to confirm the application is operational and interfaces are working. Resolve any network, environment, or interface issues before proceeding.
8. **Re-protect in Primary Site.** Enable replication from the primary site back to the secondary site to restore the original disaster recovery posture.

6.7 Application Availability During Failover

Azure Site Recovery Failover is set up for full system recovery to the secondary Azure region. When failover is initiated, the entire application is unavailable during the actual failover process while VMs, databases, storage, and DNS are transitioned. Once failover completes, the following are fully available:

Core Application Components:

- All NC Crossroads application functionality including portalsk
- Azure SQL Managed Instance database
- All virtual machines (Application, Batch, and Reporting Servers)
- Azure file shares and user-uploaded documents (GZRS replication)
- External access routes via Azure Traffic Manager DNS failover
- External interfaces - interface endpoints are pre-configured in the disaster recovery environment and restored as part of the failover process

6.8 Disaster Recovery Playbook

The Disaster Recovery Playbook is a detailed operational document that provides step-by-step instructions for executing failover and failback procedures. The playbook includes specific tasks, timing estimates, responsible parties, and status tracking to coordinate execution during both DR tests and actual disaster events.

The playbook documents:

- Pre-exercise preparation tasks and coordination activities
- Infrastructure failover sequence for VMs, databases, and storage
- DNS and network configuration updates

- Application smoke testing procedures
- Reverse replication and synchronization steps
- Failback procedures to restore primary site operations
- Post-failback tasks including documentation and corrective actions

The playbook is maintained and updated based on lessons learned from annual DR testing exercises. The NC Crossroads playbook is provided in Appendix A.

7. Disaster Recovery Testing

NC Crossroads production environment is required to undergo an annual Disaster Recovery (DR) test. The exercise is performed according to the documented DR Playbook and validates all critical failover components. This includes confirming VM failover and application service startup in the DR region, verifying SQL MI failover group readiness and client connectivity, and confirms both Network Service and Local System service contexts can access shared storage after failover. The test also validates that Azure Traffic Manager correctly redirects external traffic to the DR endpoint. After the exercise, a Corrective Action Report (CAR) is generated to document results, remediation needs, and any updates required to the DR procedures.

8. Disaster History

Voyatek hasn't experienced any disasters in the past three years.

9. Disaster Impacting North Carolina

Voyatek is not responsible for State, Local Agency, and Clinic computing infrastructure, Voyatek is responsible for the operation of AZURE Cloud-based Production and disaster recovery site. However, we understand the need to provide support to our clients during times of crisis including a disaster event. Voyatek has provided support to states on numerous occasions that go beyond any identified contract deliverable scope. An example of this commitment is when county local agency of one of our customers was forced to cease all computer operations due to malware impacting their entire network. Voyatek offered to overnight training laptops configured with project software and drivers to allow for uninterrupted operations within the agency. Support for these types of events is an important part of our service offering and an opportunity to demonstrate commitment to our clients.

Since working with North Carolina, Voyatek has provided support for a number of disaster and crises impacting the WIC program such as COVID-19, formula shortages, Hurricane Helene, and government shutdowns.

In the event of a disaster in North Carolina, the Voyatek project manager will coordinate support activities with designated North Carolina staff. This may result in a variety of support activities including but not limited to:

- Providing additional short-term staffing to meet the volume of client needs during the disaster.
- Sending team members to provide on-site support.
- Providing increased help desk support as part of disaster recovery operations.
- Assisting North Carolina with planning and alternatives analysis in response to the unique event.
- Participate in WIC meetings to identify interim procedures or strategies for serving participants in emergency scenarios using available Crossroads capabilities.
- Providing custom reporting, SQL query development, and other database support to provide access to business data, evaluate field activities or to resolve issues during the disaster event.

It is difficult to provide an exact protocol for supporting a North Carolina disaster recovery event. In most similar events, the primary need has been to provide experienced and skilled technical staff to support clients as they address the unique challenges presented by each event. This combined with the commitment to supporting states during a time of need are the primary drivers of success when overcoming disaster recovery challenges.

10. Appendix A Disaster Recovery Playbook

Table 8: Draft DR Playbook Tasks for NC Crossroads

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
DR PRE-EXERCISE PREPARATIONS												
	Kick-off (KO) DR Test Preparations for Production (PROD) DR Test	Feb 09, 2026	na							Planned	Voyatek NC Support & ITSS	
	Define scope of 2026 DR exercise (Failover; replication for failback)	Feb 09, 2026	na							Planned	Voyatek PM/ ITSS	
	Submit Change Request for DR Exercise (placeholder) CR: Tentative Date/Time: 2/13/2026 ##:## AM EDT	Feb 09, 2026	na							Planned	Voyatek PM	
	Voyatek Change Control Board (CCB) Review/Approve Voyatek ServiceNOW (or similar tracking tool) CR	Feb 12 or 19, 2026	na							Planned	Voyatek CCB	
	Initiate Review and Approve Playbook / Hour by Hour (HxH) Plan	Feb 13, 2026	na							Planned	Voyatek NC Support & ITSS	
	Review and Finalize all DR documentation	Feb 18, 2026	na							Planned	Voyatek PM/ ITSS	
		TBD-as needed										

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
DR EXERCISE PLATFORM PREP (NOT REQUIRED FOR ACTUAL DR)												
	Confirm SSL Certs are received, installed, and validated	Feb 13, 2026								Planned	Voyatek ITSS	
	Confirm DR Firewall has inbound rules for prod URL	Feb 13, 2026								Planned	Voyatek ITSS	
		TBD-as needed										
DISASTER RECOVERY (DR) FAILOVER PROCEDURES												
	Enter data into Production and capture screen shots - just prior to and during failover	Fri, Feb 20, 2026	9:00 AM	0:15	9:15 AM					Planned	Voyatek NC Support Team	
	Failover DR VMs in proper sequence as outlined in DR plan	Fri, Feb 20, 2026	9:15 AM	0:30	9:45 AM					Planned	Voyatek ITSS	
	Failover SQL Managed Instance (failover group)	Fri, Feb 20, 2026	9:45 AM	0:10	9:55 AM					Planned	Voyatek ITSS	
	Failover Storage Account to DR	Fri, Feb 20, 2026	9:55 AM	0:10	10:05 AM					Planned	Voyatek ITSS	
	Update Traffic Manager DNS to point to DR env; confirm DNS change propagation	Fri, Feb 20, 2026	10:05 AM	0:10	10:15 AM					Planned	Voyatek ITSS	
	Update DB connection strings if necessary	Fri, Feb 20, 2026	10:15 AM	0:05	10:20 AM					Planned	Voyatek ITSS	

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
	Verify connectivity between App Tiers... App --> DBs	Fri, Feb 20, 2026	10:20 AM	0:10	10:30 AM					Planned	Voyatek ITSS	
	Test access to the application via the public URL in DR	Fri, Feb 20, 2026	10:30 AM	0:10	10:40 AM					Planned	Voyatek ITSS	
	ITSS notifies NC Support team recovery completed	Fri, Feb 20, 2026	10:40 AM	0:10	10:50 AM					Planned	Voyatek ITSS	
	Voyatek NC Support team completes subset of NC Crossroads Smoke Test: perform tests to confirm that core systems function as expected in Primary site. This includes validating database integrity and application functionality and confirming that all components are up and running. (does not include EBT interface testing)	Fri, Feb 20, 2026	10:50 AM	0:30	11:20 AM					Planned	Voyatek NC Support Team	
	Voyatek NC Support team notifies NC WIC testers that DR is ready for NC WIC to validate. (does not include EBT)	Fri, Feb 20, 2026	11:20 AM	:05	11:25 AM						Voyatek Test Manager	
	NC Testers conduct smoke test (not including EBT)	Fri, Feb 20, 2026	11:25 AM	:30	11:55 AM						NC WIC Testers	

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
	NC WIC Testers notify Voyatek NC Support Team that validation test is complete.	Fri, Feb 20, 2026	11:55 AM	:05	12:00 PM						NC WIC Testers	
	Voyatek NC Support team confirms for Voyatek ITSS that test is complete	Fri, Feb 20, 2026	12:00 PM	0:05	12:05 PM					Planned	Voyatek Test Manager	
	Testers complete documentation of test results	Fri, Feb 20, 2026	12:05 PM	0:10	12:15 PM					Planned	Voyatek NC Support Team & NC WIC Testers	
	ITSS Acknowledges Test in DR environment Completion	Fri, Feb 20, 2026	12:15 PM	0:05	12:20 PM					Planned	Voyatek ITSS	
REVERSE REPLICATION AND SYNCHRONIZATION - SQL												
	Enable/Confirm Resynchronization of SQL Managed Instance DBs to Primary site	Fri, Feb 20, 2026	12:20 PM	0:10	12:30 PM					Planned	Voyatek ITSS	
DR SITE FALLBACK PROCEDURE												
	Failback SQL Managed Instance DBs to Primary site	Fri, Feb 20, 2026	12:30 PM	0:10	12:40 PM					Planned	Voyatek ITSS	
	Failback Storage Account to Primary site	Fri, Feb 20, 2026	12:40 PM	0:10	12:50 PM					Planned	Voyatek ITSS	

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
	Failback to Primary - all VMs in Prod Env according to documented sequence	Fri, Feb 20, 2026	12:50 PM	1:00	1:50 PM					Planned	Voyatek ITSS	
	Update Traffic Manager DNS to point URL back to production IP; confirm DNS change propagation	Fri, Feb 20, 2026	1:50 PM	0:10	2:00 PM					Planned	Voyatek ITSS	
	Test access to application via public URL	Fri, Feb 20, 2026	2:00 PM	0:05	2:05 PM					Planned	Voyatek ITSS	
	ITSS notifies NC Support Team that system is failed back to primary and ready for smoke test	Fri, Feb 20, 2026	2:05 PM	0:05	2:10 PM						Voyatek ITSS	
	Voyatek NC Support team completes subtest of NC Crossroads Smoke Test: perform tests to confirm that core systems function as expected in Primary site. . (with the exception of EBT)	Fri, Feb 20, 2026	2:10 PM	0:30	2:40 PM					Planned	Voyatek NC Support	
	Voyatek NC Support team notifies NC WIC testers that Primary is ready for NC WIC to validate. (with the exception of EBT)	Fri, Feb 20, 2026	2:40 PM	:30	3:10 PM						Voyatek Test Manager	

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
	NC Testers conduct smoke test (not including EBT)	Fri, Feb 20, 2026	3:10 PM	:30	3:40 PM						NC WIC Testers	
	NC WIC notifies Voyatek NC Support and ITSS teams that NC validation complete.	Fri, Feb 20, 2026	3:40 PM	05	3:45 PM						NC WIC Testers	
	Voyatek NC Support team notifies Voyatek ITSS test completed	Fri, Feb 20, 2026	3:45 PM	0:05	3:50 PM					Planned	Voyatek App Team	
	Testers complete documentation of test results	Fri, Feb 20, 2026	3:50 PM	:30	4:20 PM					Planned	Voyatek NC Support & NC WIC Testers	
	Voyatek ITSS Acknowledges Test in Primary Completion	Fri, Feb 20, 2026	3:50 PM	0:05	3:55 PM					Planned	Voyatek ITSS	
		TBD-as needed										
POST-EXERCISE TASKS												
	Re-enable Database replication from Prod to DR	Fri, Feb 20, 2026	3:55 PM	0:10	4:05 PM					Planned	Voyatek ITSS	

LN #	Task Description	Start Date	Start Time (EDT)	Duration (Min)	End Time (EDT)	Actual Date	EDT Time	CDT Time	Comment	Status	Responsible Team	Individuals Assigned
	Create After Action Report (AAR) for DR Exercise	Feb 25, 2026		5 days	12:00 PM					Planned	Voyatek ITSS	Voyatek ITSS/PM
	Update Disaster Recovery Plan (DRP) and supporting artifacts	As needed								Planned	Voyatek	Voyatek ITSS/PM