



Executive Summary

Overview

Heartland Ambulance Service, LLC is a leading provider of medical transportation services in Indiana, known for its commitment to delivering high-quality, reliable, and timely emergency and non-emergency medical care. Founded in 2010 by Kenneth W. Jackson, the company has grown to encompass a comprehensive range of services, including 911 emergency response, non-emergent medical transportation, and fixed-wing air ambulance services.

Mission & Values

Heartland Ambulance's mission is to provide the highest quality of care, recognizing each patient's individual needs and ensuring a positive work environment for its team members. The company's vision is to be the premier private ambulance provider in Indiana, setting industry standards through exceptional patient care and innovative service delivery.

Services Offered

- 911 Emergency Services: Fast and efficient emergency medical response.
- Non-Emergency Transportation: Safe and comfortable transport for patients needing routine medical transfers.
- Advanced Life Support (ALS) and Basic Life Support (BLS): Skilled medical care during transit.
- Fixed-Wing Air Ambulance: Rapid long-distance medical transport.

Technological Integration

The company utilizes a state-of-the-art multilingual AI dispatch center, which enhances the efficiency of routing and staging ambulances. This technology ensures optimal resource allocation and real-time data tracking of vehicle locations, crew information, and job statuses, thereby improving overall operational effectiveness.

Commitment to Excellence

Heartland Ambulance prides itself on maintaining a state-of-the-art fleet and specialized service programs, allowing it to navigate financial challenges and continue providing top-notch services. The company is also actively involved in local, state, and national EMS associations, reflecting its dedication to staying at the forefront of industry standards and best practices.

Leadership & Experience

With over 80 years of combined experience in emergency medical services, the leadership team at Heartland Ambulance brings a wealth of knowledge and expertise to the company. This experience is instrumental in maintaining high standards of care and operational excellence.

Heartland Ambulance Service, LLC remains dedicated to enhancing patient care, fostering strong community relationships, and leading the medical transportation industry with innovation and integrity.

**Point of Contact**

Joshua Keywood
President of Government Contracting
Heartland Ambulance Service, LLC
4180 Elmhurst Drive, Indianapolis, IN 46226
Phone: 260-444-6212
Email: jkeywood@heartlandambulance.com

Signature of Authorized Representative

I, Kenneth Jackson, Managing Member of Heartland Ambulance Service, LLC hereby certify that the information offered in the proposal meets all general conditions.

Kenneth Jackson
kjackson@heartlandambulance.com
Phone: (765) 863-5150

Secretary of State

Heartland Ambulance Service is currently active with the Indiana Secretary of State.

Contract Terms/Clauses

Heartland Ambulance Service will accept the sample contract as written, without change.

Company Information

Company Bidder ID #
FEIN: 27-2430695
Type of Business: LLC
NAICS Code: 621910

General Information



Disaster Recovery Plan

Introduction

Purpose: The purpose of this Disaster Recovery Plan (DRP) is to outline the procedures and processes Heartland Ambulance Service LLC will follow in the event of a disaster to ensure the safety of patients, staff, and continuity of operations.

Scope: This DRP covers all aspects of the company's operations, including communication, IT systems, medical equipment, personnel, and facilities.

Objectives

1. Ensure the safety and well-being of all patients and staff.
2. Maintain continuity of critical ambulance services.
3. Minimize disruption to operations.
4. Ensure timely and effective communication.
5. Protect and restore IT and medical systems.
6. Meet regulatory compliance and reporting requirements.

Risk Assessment

- Natural Disasters (tornadoes, floods, earthquakes)
- Fire
- Cyber Attacks
- Power Outages
- Pandemic Outbreaks
- Terrorist Attacks

Emergency Response Team

Disaster Recovery Coordinator:

Operations Manager:

IT Manager:

Medical Director:

HR Manager:

Responsibilities

Disaster Recovery Coordinator: Oversees the entire disaster recovery process.

Operations Manager: Manages the continuity of ambulance services.

IT Manager: Ensures the recovery and functionality of IT systems.

Medical Director: Oversees patient care and medical protocols.

HR Manager: Manages staff welfare and communication.



Emergency Communication Plan

INTERNAL

- Establish a communication tree for quick dissemination of information.
- Use multiple channels (SMS, emails, internal messaging systems).

EXTERNAL

- Designate a spokesperson for media and public communication.
- Utilize social media and the company website for updates.

Data Backup & Recovery

Data Backup: Ensure daily backups of all critical data, stored securely off-site.

Recovery: Implement a recovery protocol for quick restoration of IT systems and data. Test backups regularly.

Facility & Equipment

Alternative Facilities:

- Identify and arrange for alternative facilities if the primary site is unusable.
- Ensure all necessary equipment and supplies are available at these sites.

Equipment Maintenance:

- Regularly maintain and test all medical and IT equipment.
- Keep an inventory of spare parts and essential tools.

Staff Preparedness

Training:

- Conduct regular training sessions on disaster response and recovery procedures.
- Perform annual drills to ensure staff readiness.

Emergency Contacts:

- Maintain an updated list of emergency contacts for all staff members.
- Provide staff with emergency contact cards.

Recovery Procedures

Initial Response

1. Assess the situation and determine the extent of the disaster.
2. Activate the Emergency Response Team.
3. Ensure safety of all personnel and patients.



Operational Continuity

1. Implement alternative operational procedures.
2. Utilize backup facilities and equipment.
3. Maintain critical services while non-essential operations are suspended.

IT Recovery

1. Restore data from backups.
2. Ensure IT systems are secure and functional.
3. Monitor for any residual cyber threats.

Post-Disaster Review

- Conduct a thorough review of the response and recovery efforts.
- Identify areas of improvement and update the DRP accordingly.
- Document lessons learned and share with all staff.

Regulatory Compliance

- Ensure all recovery efforts comply with local, state, and federal regulations.
- Maintain detailed records of the disaster and recovery processes for auditing and compliance purposes.

Plan Maintenance

- Review and update the DRP annually.
- Incorporate feedback from drills and actual disaster responses.
- Ensure all staff are familiar with the updated DRP.

Approved by:

Kenneth Jackson
Heartland Ambulance Service
Date: 06/10/2024



Technology and Process for Securing State Information

Introduction

The purpose of this document is to outline the technology and processes Heartland Ambulance Service LLC utilizes to secure any state information maintained within our company. This includes details about our hosted IT infrastructure provided by VLI Tech, which plays a crucial role in ensuring data security and integrity.

IT Infrastructure

Hosted IT Infrastructure:

As our IT provider, VLI Tech supplies all necessary IT servers and software for our hosted implementation. Our IT infrastructure is hosted in highly secure, compliant, and redundant facilities to ensure data security and operational continuity.

The Cloud:

- Primary Data Center: Data Foundry Texas 1 Facility in Austin, TX.
- Mirror Site: Data Foundry Houston 2 Facility.
- Compliance: Both facilities are SOC2/SSAE16 and HIPAA compliant.
- Redundancy: All customer VMs and physical equipment are fully redundant, ensuring no single point of failure from public internet connections to cabling paths. VMware hosts run in an N+2 high availability configuration to ensure customer workloads remain operational even during a system failure.

Security

Network Security:

- Network Segmentation: Customer networks are built using the entire VMware virtualization stack. Each customer is assigned a subnet with no east/west communication allowed unless explicitly required.
- Traffic Control: Internal and external network access is restricted via an explicit allow method, ensuring only designated traffic traverses the networks.
- Micro-Segmentation: VMware NSX is deployed to control endpoints with firewall rules at the hypervisor layer, allowing control of traffic to and from each endpoint. This configuration is implemented using a strict deny-all, explicitly allow method.

Data Security:

- Encryption: All data at rest and in transit is encrypted using industry-standard encryption protocols.
- Access Controls: Access to sensitive data is controlled through role-based access controls (RBAC), ensuring that only authorized personnel have access to specific information.
- Monitoring and Auditing: Continuous monitoring of network traffic and regular audits are conducted to detect and respond to any unauthorized access or anomalies.



Backup & Recovery

RPO and RTO for Databases:

- RPO (Recovery Point Objective): 15 minutes for all dispatch and billing-related databases.
- RTO (Recovery Time Objective): Approximately 1 hour per 50 GB of database size, assuming a total server failure and the entire database server must be restored.

File Share Backups:

- RPO: 3 hours.
- RTO: Approximately 1 hour per 200 GB of data, primarily affected by the size of the attachment directory.

Service Machines Backups:

- RPO: 1 week due to minimal data storage and infrequent configuration changes.
- RTO: 1 hour per VM, typically 1-2 VMs.

Backup Testing:

- Quarterly Testing: All data-containing backups are tested quarterly to ensure consistency and viability of recovery.
- Annual Testing: Backups containing installed software are tested annually.
- Replication: Backups are replicated to three other storage repositories besides the Rubrik appliance, including an internal storage array in another VLI data center and two separate AWS regions. Internal copies are performed in real-time, AWS copies are performed in real-time to one region and daily to the second region.

Compliance

- Regulatory Compliance: Ensure all recovery efforts comply with local, state, and federal regulations. Maintain detailed records of disaster and recovery processes for auditing and compliance purposes.
- HIPAA Compliance: Adherence to HIPAA regulations to protect the privacy and security of patient information.
- SOC2/SSAE16 Compliance: Ensure that all data handling practices are compliant with SOC2/SSAE16 standards.

Conclusion

Heartland Ambulance Service LLC is committed to ensuring the highest level of security for state information maintained within our company. Through our partnership with VLI Tech, we leverage state-of-the-art technology and robust processes to protect sensitive data, ensure operational continuity, and comply with all relevant regulations.



Approved by:


Kenneth Jackson
Heartland Ambulance Service
Date: 06/10/2024