Fidesic

www.fidesic.com

FIDESIC DISASTER RECOVERY PLAN

Table Of Contents

Introduction

This Disaster Recovery Plan (DRP) outlines the processes and procedures for recovering from disasters and maintaining business continuity for Fidesic. The plan covers all data hosted on Azure SQL Server, IIS servers, and background services hosted on Azure VMs.

Objectives

- Ensure the safety of all personnel and assets.
- Minimize disruption to business operations.
- Ensure timely recovery of critical services and data.
- Maintain communication with stakeholders during and after an incident.

Scope

This plan applies to all systems, applications, and data hosted on Azure, including:

- Azure SQL Server
- Azure VMs hosting IIS servers
- Azure VMs hosting background services
- DNS hosted through GoDaddy

Disaster Recovery Team

Roles and Responsibilities

- **Disaster Recovery Manager**: Oversees the DRP implementation and coordination.
- **Database Administrator (DBA)**: Responsible for Azure SQL Server backup and recovery.
- **Infrastructure Engineer**: Manages Azure VM restoration and network configurations.
- **Application Support Team**: Ensures application and IIS server recovery.
- **Communication Lead**: Handles internal and external communications during a disaster.

Risk Assessment

Identify potential risks that could impact your infrastructure, including:

- Natural disasters (e.g., floods, earthquakes)
- Cyber-attacks (e.g., ransomware, DDoS attacks)
- Hardware failures
- Human errors

Business Impact Analysis

Identify critical services and their recovery priorities:

- **Priority 1**: Azure SQL Server (critical data storage)
- **Priority 2**: IIS Servers (customer-facing applications)
- **Priority 3**: Background Services (supporting applications)
- **Priority 4**: DNS services (hosted through GoDaddy)

Risk Reduction Strategies

Azure SQL Server

1. **Backup**: Perform regular automated backups using Azure SQL Database's automated backup features.
2. **Recovery**: Use Azure's point-in-time restore to recover the database to a specific time before the incident.

Azure VMs (IIS Servers and Background Services)

- **Backup**: Implement Azure Backup to perform regular VM snapshots.
- **Recovery**: Use Azure Site Recovery to replicate and failover VMs to another Azure region if needed.

Webapp Utilization (Future Strategy)

- Migrating the Fidesic website and all associated services to webapps will make backups and recovery as a specific process unnecessary. They can be redeployed as needed.

Automated Failover for Application Gateways (Future Strategy)

- Automated failover for application gateways ensures uninterrupted service delivery by quickly redirecting traffic to healthy gateways during failures.

Recovery Procedures

Initial Response

1. **Assess the Situation**: Determine the nature and extent of the incident.
2. **Activate DRP**: The Disaster Recovery Manager activates the DRP and notifies the team.

Data Recovery (Azure SQL Server)

1. **Access Backup**: Retrieve the latest backup from Azure SQL Database.
2. **Restore Database**: Use point-in-time restore to recover the database.
3. **Validate Data**: Ensure data integrity and consistency post-recovery.

Server Recovery (Azure VMs)

1. **Initiate Failover**: Use Azure Site Recovery to failover to the replicated VMs.
2. **Restore VMs**: If failover is not possible, restore VMs from Azure Backup snapshots.
3. **Reconfigure Network**: Ensure VMs are correctly networked and accessible.
4. **Validate Applications**: Ensure IIS servers and background services are functioning correctly.

DNS Recovery (GoDaddy)

1. **Access GoDaddy**: Log into the GoDaddy account to manage DNS settings.
2. **Restore DNS Settings**: Ensure DNS records are pointing to the correct IP addresses.
3. **Validate DNS**: Confirm that domain resolution is working correctly.

Communication Plan

- **Internal Communication**: Regular updates to all team members using Slack
- **External Communication**: Inform clients and stakeholders about the incident and recovery status via email and your company's status page.

Testing and Maintenance

- **Regular Testing**: Conduct quarterly DRP tests to ensure all team members are familiar with the procedures and to identify any gaps.
- **Plan Updates**: Review and update the DRP annually or after significant infrastructure changes.

Documentation

Maintain detailed records of all incidents, responses, and recoveries in Gitlab issues to improve future DRP efforts. If any big restore events are attempted, most recent steps should be recorded in a Gitlab wiki and linked appropriately above, if appropriate.

Appendices

Appendix A: Contact List

- **Disaster Recovery Manager**: Mike Skinner, 989-992-9753, mike@fidesic.com
- **Database Administrator (DBA)**: Mike Skinner, 989-992-9753, mike@fidesic.com
- **Infrastructure Engineer**: Mike Skinner, 989-992-9753, mike@fidesic.com
- **Application Support Team Lead**: Mike Skinner, 989-992-9753, mike@fidesic.com
- **Communication Lead**: Kevin Pritchard, 810-333-2307, kevin.pritchard@fidesic.com

Appendix B: Azure Resources and Configurations

- **Azure SQL Server**:
  - Hardware Configuration: Standard-series (Gen5), up to 80 vCores, up to 240 GB memory
  - vCores: 16
  - Min vCores: 2
  - Max Storage: 1807 GB
  - Auto-pause Delay: Disabled
  - Backup Storage Redundancy: Geo-redundant
- **Azure VMs**:
  - 4 IIS VMs (2 for API integrations, 2 for general traffic)
  - Behind application gateways

Appendix C: Testing Schedule

- **Quarterly Test Dates**: [Dates]
- **Annual Review Date**: 6/13/2025

By following this DRP, Fidesic aims to ensure the resilience and continuity of its services in the face of potential disasters.