700 Disaster Recovery Policy v2

700 DISASTER RECOVERY POLICY

700.1 Purpose:

The purpose of this Disaster Recovery Policy is to establish a framework for the timely recovery and restoration of critical systems, data, and services in the event of a disaster or major disruption at the Archdiocese of Baltimore. The policy aims to ensure the organization's ability to resume essential operations and minimize the impact of disruptions on its mission and stakeholders.

700.2 Scope:

This policy applies to all employees, volunteers, contractors, and any individuals who have access to the Archdiocese of Baltimore's systems, data, and network resources.

700.3 Disaster Recovery Framework:

3.1. Business Impact Analysis (BIA)

a. A comprehensive business impact analysis will be conducted to identify critical systems, applications, and data assets, and determine the maximum allowable downtime and recovery time objectives.

b. The BIA will help prioritize recovery efforts and allocate resources accordingly.

3.2. Disaster Recovery Plan (DRP)

a. A disaster recovery plan will be developed. maintained, and regularly tested to provide guidelines, procedures, and responsibilities for recovering critical systems and services.

b. The DRP will include step-by-step instructions for data backup and restoration, system recovery, communication, and post-recovery activities.

3.3. Data Backup and Recovery

a. Regular backups of critical data and systems will be performed and stored in a secure and off-site location.

b. Backup procedures will be documented and tested to ensure the integrity and availability of backups for recovery purposes.

3.4. Alternative Facilities and Infrastructure

a. Alternative facilities, such as a secondary data center or cloud infrastructure, will be identified and prepared to facilitate the recovery of critical systems and services.

b. Redundant hardware, networking, and power systems will be implemented to minimize single points of failure.

700.4 Disaster Recovery Procedures:

4. 1. Disaster Declaration and Activation

a. The authority and process for declaring a disaster and activating the disaster recovery plan will be established.

b. Designated personnel will be responsible for initiating the recovery process and coordinating the efforts of the recovery team.

4.2. Recovery Team Roles and Responsibilities

a. A recovery team comprising representatives from relevant depa1tments will be formed and trained to execute the recovery plan.

b. Roles and responsibilities of recovery team members will be clearly defined to ensure an organized and coordinated response.

4.3 Recovery Process and Testing

a. Recovery procedures, including system restoration. data recovery, and post-recovery validation, will be documented and tested periodically.

b. Regular testing and drills will be conducted to evaluate the effectiveness of the disaster recovery plan and identify areas for improvement.

700.5 Communication and Notification:

a. Clear communication channels will be established to notify relevant stakeholders, including senior management, employees. and external parties. about the disaster and recovery progress.

b. Communication plans will be developed to ensure timely and accurate

updates are provided during the recovery process.

700.6 Policy Review:

This Disaster Recovery Policy will be reviewed on a periodic basis to ensure its effectiveness, relevance, and alignment with evolving business needs and industry best practices.

Please note that this is a general example and should be customized to fit the specific needs and requirements of the Catholic organization. It is recommended to seek legal advice and consult with relevant stakeholders when drafting or implementing a Disaster Recovery Policy.