Disaster Recovery Plan for IT Risk

1. Introduction

 - Purpose: The purpose of this Disaster Recovery Plan is to outline the steps and procedures to be followed by the non-profit housing organization in the event of any IT-related disasters or risks.

 - Scope: This plan covers a range of potential IT disasters, including system failures, cybersecurity breaches, natural disasters, and human errors.

 - Objectives: The objectives of the plan are to minimize downtime, restore critical IT systems, protect sensitive data, and ensure business continuity.

2. Risk Assessment

 - Identify potential IT risks and their impact on the organization.

 - Prioritize risks based on their likelihood and severity.

 - Regularly review and update risk assessment to address new threats.

3. Backup and Recovery Procedures

 - Regularly backup all critical IT systems and data, with multiple copies stored in secure off-site locations.

 - Test backups periodically to verify their integrity and ensure recoverability.

 - Maintain a current inventory of all critical hardware and software.

 - Document and regularly update step-by-step procedures for system recovery.

4. Incident Response Team

 - Establish an incident response team responsible for coordinating disaster recovery efforts.

 - Identify individuals with specific roles and responsibilities, including a team leader, IT experts, communication coordinators, and decision-makers.

 - Provide appropriate training and resources to the incident response team.

5. Communication Plan

 - Establish a clear communication plan to ensure timely and effective communication during and after an IT disaster.

 - Define communication channels, including emails, phone calls, text messages, and social media platforms.

 - Identify internal and external stakeholders needing updates during a disruption.

 - Appoint spokesperson(s) to provide consistent messaging to stakeholders.

6. Recovery Protocols

 - Evaluate the impact and severity of the IT disaster and implement the appropriate recovery protocols.

 - Document a step-by-step recovery plan for each IT system, including hardware, software, networking components, and data.

 - Clearly define recovery time objectives (RTO) and recovery point objectives (RPO) for each system.

 - Implement redundant systems and alternative solutions to minimize downtime during recovery.

7. Cybersecurity Measures

 - Deploy robust cybersecurity measures to protect sensitive data from theft, unauthorized access, and breaches.

 - Regularly update antivirus software, firewalls, and intrusion detection systems.

 - Educate employees on cybersecurity best practices to minimize the risk of social engineering attacks and other security threats.

8. Testing and Drills

 - Regularly test the disaster recovery plan and conduct drills to ensure its effectiveness.

 - Document test results, identify areas for improvement, and update the plan accordingly.

 - Involve all relevant stakeholders in the testing process.

9. Plan Maintenance and Documentation

 - Regularly review and update the plan to reflect changes in IT infrastructure, systems, or risks.

 - Store copies of the plan in secure off-site locations and provide access to all key personnel.

 - Train new employees on the disaster recovery plan and ensure their understanding.

10. Plan Activation and Post-Recovery Measures

 - Activate the plan promptly in the event of an IT disaster.

 - Continuously monitor the recovery process and adjust strategies as necessary.

 - Conduct a post-recovery review to evaluate the effectiveness of the plan and update it accordingly.

 - Communicate with stakeholders about the recovery process and provide any necessary reassurances.

11. Plan Review and Update

 - Schedule regular reviews of the Disaster Recovery Plan to ensure it remains up-to-date and effective.

 - Assign responsibility for reviewing and updating the plan to a designated individual or team.

 - Keep all relevant documentation and contacts up-to-date.

12. Plan Activation Checklist

 - Develop a checklist that outlines the specific steps to be taken when the disaster recovery plan is activated.

 - Include contact information, key system recovery priorities, and a timeline for recovery.

Remember, disaster recovery is an ongoing process, and it is essential to regularly review and update the plan to address emerging risks and changes in technology.