Data Security Pre-Disaster

This playbook provides a detailed sequence of steps designed to secure electronic data and records before the occurrence of a natural disaster. It focuses on precautions and recommendations to prevent data loss and ensure business continuity.

Step 1: **Risk Assessment**

Conduct a thorough risk assessment to identify the types of natural disasters that could impact your area and the potential risks to electronic data and systems. This could include floods, earthquakes, hurricanes, etc. Determine which data is critical for operations and needs prioritization.

Step 2: **Backup Data**

Regularly backup critical data using a 3-2-1 strategy: maintain at least three copies of your data, with two available locally on different devices and one stored offsite. Ensure backups are encrypted if they contain sensitive information.

Step 3: **Secure Offsite**

Choose an offsite backup location that is geographically distant enough to be unaffected by local natural disasters. Use cloud storage services that offer robust security and reliability or a physical offsite facility.

Step 4: **Data Redundancy**

Implement data redundancy solutions such as RAID systems or distributed databases to minimize the risk of data loss due to hardware failures that might occur during a natural disaster.

Step 5: **Disaster Recovery Plan**

Develop and maintain a comprehensive disaster recovery plan (DRP) that includes procedures for securing and restoring electronic data. The DRP should be regularly reviewed and updated.

Step 6: **Testing**

Periodically test your disaster recovery measures and data backup systems to ensure they work as expected. This includes simulating disaster scenarios and practicing data recovery procedures.

Step 7: **Secure Physical Devices**

Safeguard physical devices that store sensitive data in secure locations less likely to be affected by natural disasters. Consider using waterproof, fireproof safes or data storage containers.

Step 8: **Access Control**

Ensure that only authorized personnel have access to sensitive data and backup systems. Implement strong access controls and authentication mechanisms.

Step 9: **Employee Training**

Regularly train employees on best practices for data security and the specific steps to take in the event of an impending natural disaster. Ensure they are familiar with the disaster recovery plan.

General Notes

Insurance

Verify that your business insurance policy includes coverage for electronic data loss due to natural disasters. This step can provide financial protection against potential recovery costs.

Compliance

Ensure all disaster recovery and data security practices are in compliance with relevant industry regulations and data protection laws.