NeighborWorks®
FLORIDA COLLABORATIVE

TECH & CYBER DISRUPTION ACTIVATION GUIDE

This guide provides organizations with the tools, decision points, and activation procedures needed to maintain mission-critical operations before, during, and after a technological and cyber disruption. For the purpose of this guide, these are the natural disasters we will be referring to.

A. Hazards Covered


Ransomware Attack


Data Breech


Network Outages


Cloud Service Failure


Email Compromise


Comms System Failures

NeighborWorks® FLORIDA COLLABORATIVE

B. Planning Focus

- Data backups
- Cybersecurity controls
- Multi-factor authentication
- Vendor continuity agreements
- Alternate communications channels

C. Activation Triggers

- Ransomware notification
- Unauthorized access detection
- Extended system outage
- Data corruption
- Loss of internet connectivity

D. Activation Priorities

1. Isolate affected systems
2. Notify IT leadership
3. Activate incident response team
4. Implement backup communications
5. Protect sensitive information
6. Inform stakeholders

E. Recovery Focus

- System restoration
- Data recovery
- Forensic review
- Regulatory reporting
- Staff retraining

Sample Scenario:

On Monday morning staff discover all organizational files have been encrypted by ransomware.

What happens in the first 30 minutes, 4 hours, and 24 hours?

Find more disaster resources on our website: