BUSINESS HURRICANE PREPAREDNESS

GUIDE & CHECKLIST

Protect Your Employees, Technology, Data & Operations Before, During & After The Storm

Hurricanes don't just threaten buildings. They threaten business continuity. Use this guide to help your organization prepare for severe weather, minimize downtime, and recover faster.

BEFORE
Hurricane Season

- [ ] Review Business Continuity Plan
- [ ] Review Disaster Recovery Procedures
- [ ] Verify Backups Are Running Successfully
- [ ] Test Backup Restorations
- [ ] Confirm Cyber Insurance Coverage
- [ ] Update Employee Contact Lists
- [ ] Review Emergency Vendor Contacts
- [ ] Verify UPS and Battery Backup Systems
- [ ] Confirm Remote Work Capabilities
- [ ] Document Critical Systems
- [ ] Conduct a hurricane preparedness review with department leaders
- [ ] Verify emergency communication procedures with employees
- [ ] Review cybersecurity awareness training with all staff

72 HOURS BEFORE
Expected Impact

- [ ] Verify Latest Backups
- [ ] Secure Outdoor Equipment
- [ ] Charge Laptops & Mobile Devices
- [ ] Notify Employees Of Procedures
- [ ] Test VPN Connectivity
- [ ] Confirm Emergency Communications Plan
- [ ] Verify Generator Fuel Levels
- [ ] Protect Critical Hardware

24 HOURS BEFORE
Expected Impact

- [ ] Perform Final Data Backup & Store Additional Copies Offsite
- [ ] Shut Down Non-Essential Systems
- [ ] Elevate Equipment If Flooding Is Possible
- [ ] Secure Network Equipment
- [ ] Verify Offline Access To Contacts
- [ ] Confirm Recovery Team Availability

DURING
The Storm

- [ ] Prioritize Employee Safety
- [ ] Monitor Emergency Alerts
- [ ] Document Outages
- [ ] Maintain Emergency Communications
- [ ] Avoid Unnecessary Travel

AFTER
The Storm

- [ ] Assess Facility Safety
- [ ] Inspect IT Equipment For Damage
- [ ] Verify Internet Connectivity
- [ ] Restore Systems According To Plan
- [ ] Document Losses For Insurance Claims
- [ ] Review Recovery Performance
- [ ] Update Disaster Recovery Documentation

CYBERSECURITY
Considerations

- [ ] Watch for phishing emails related to storm recovery, aid, insurance claims, and emergency repairs
- [ ] Require multi-factor authentication (MFA) on critical systems
- [ ] Monitor for unusual login activity during and after the event
- [ ] Verify software updates and recovery tools come only from trusted sources
- [ ] Maintain endpoint protection and monitoring during remote operations
- [ ] Verify all wire transfer and payment requests through a secondary communication method
- [ ] Be cautious of disaster-relief scams and fraudulent vendor communications
- [ ] Monitor for suspicious remote access attempts during recovery efforts
- [ ] Provide cybersecurity awareness training so employees can identify phishing emails, social engineering attempts, impersonation scams, and other hurricane-related cyber threats
- [ ] Review incident response procedures with key staff members
- [ ] Confirm critical vendor contact information is up to date and verified

enitech
IT support and consulting

Emergency Planning Worksheet

Key Business Contacts

Primary Contact: _____

Secondary Contact: _____

Building Management: _____

Insurance Provider: _____

Utility Company: _____

Internet Provider: _____

Critical Technology Vendors

Managed IT Provider: _____

Cloud Provider: _____

Backup Solution: _____

Phone System Provider: _____

Cybersecurity Provider: _____

Critical Business Systems

Accounting Software: _____

ERP / Line of Business Apps: _____

Email Platform: _____

File Storage Platform: _____

Customer Database: _____

Recovery Notes: