BARRETT

INFORMATION TECHNOLOGY, LLC

BUSINESS PREPAREDNESS GUIDE

Business IT Hurricane Season Checklist

A practical checklist to help reduce downtime, protect data, support remote work, and recover safely after severe weather.

Use this checklist before, during, and after a storm.

Print it, save a copy offline, and review it with your management team and key employees.

For help reviewing your readiness, open a ticket at barrettit.com/support.

Barrett Information Technology, LLC | barrettit.com | 1-888-374-4632 | sales@barrettit.com

How to Use This Checklist

This checklist is designed for small and midsize businesses preparing for hurricane season or other severe weather events. Review it before a storm is in the forecast, update the blank fields, and keep both printed and digital copies available outside the office.

Recommended review schedule

Review this checklist at the start of hurricane season, before any named storm affecting your area, after major technology changes, and after any real incident or outage.

Business Information

Business name _____

Primary office location _____

Main contact _____

Backup contact _____

Date reviewed _____

Priority Systems

List the systems that must be restored first. Keep the list short and realistic. During an outage, everything cannot be priority one.

System / Service	Why it matters	Owner	Recovery priority
Email / Microsoft 365 / Google Workspace			1 / 2 / 3
Phones / VoIP / Call forwarding			1 / 2 / 3
Line-of-business application			1 / 2 / 3
File shares / cloud storage			1 / 2 / 3
Accounting / payroll			1 / 2 / 3

Before the Storm: Core IT Readiness

1. Backup & Data Protection

[ ] Confirm all critical business files, databases, and server data are included in backup jobs.

[ ] Verify cloud services such as Microsoft 365, Google Workspace, SharePoint, OneDrive, and Google Drive have appropriate retention or backup protection.

[ ] Confirm backups are stored offsite or in a secure cloud location, not only on equipment inside the office.

[ ] Check the most recent successful backup date for servers, key workstations, and critical applications.

[ ] Confirm backups are protected from ransomware, accidental deletion, and unauthorized access.

[ ] Document who is authorized to request a restore and how to contact IT during an emergency.

[ ] Test restoring at least one file or confirm a recent restore test has been completed.

2. Servers, Workstations & Equipment

[ ] Move computers, servers, external drives, and network equipment away from floors, windows, and leak-prone areas.

[ ] Shut down non-essential workstations before an expected extended power outage.

[ ] Label critical equipment such as firewall, modem, switches, wireless access points, and servers.

[ ] Take photos of equipment, serial numbers, racks, cabling, and office technology areas for insurance records.

[ ] Confirm laptops, chargers, docking stations, and mobile devices are assigned to employees who may need remote access.

[ ] Do not leave external backup drives connected to systems unless that is part of the approved backup design.

3. Power Protection

[ ] Confirm servers, firewalls, switches, internet modems, and phone equipment are connected to UPS battery backup units.

[ ] Inspect UPS units for battery warnings, overload alerts, or failed self-tests.

[ ] Avoid plugging printers, heaters, coffee makers, or non-critical devices into UPS battery outlets.

[ ] Document how long your UPS units are expected to keep critical systems online.

[ ] Decide what equipment should be shut down if the power outage is expected to last longer than the battery runtime.

[ ] If using a generator, confirm safe power procedures and avoid unstable power reaching sensitive equipment.

Before the Storm: Connectivity & People

4. Internet, Firewall & Network

[ ] Save internet provider account numbers, support phone numbers, and circuit details somewhere accessible offline.

[ ] Confirm the firewall, modem, and network gear are documented and labeled.

[ ] Review whether a backup internet option is available, such as cellular hotspot, secondary ISP, or failover connection.

[ ] Confirm remote access methods are secure and do not rely on unsafe open ports.

[ ] Avoid last-minute firewall or network changes unless required for business continuity.

[ ] Keep a copy of key network information available to authorized management or IT contacts.

5. Phones, Email & Customer Communication

- [ ] Confirm how calls will be handled if the office is closed or phones are offline.
- [ ] Test call forwarding, voicemail-to-email, emergency greetings, or cloud phone access where applicable.
- [ ] Prepare a customer notice for closures, delayed responses, or temporary service changes.
- [ ] Confirm key staff can access email away from the office using multi-factor authentication.
- [ ] Keep employee, vendor, insurance, utility, ISP, and IT support contact lists available offline.
- [ ] Confirm who is responsible for sending customer updates and where those updates will be posted.

6. Remote Work Readiness

- [ ] Identify which employees are approved to work remotely during an office closure.
- [ ] Test VPN, remote desktop, cloud app access, and file access before severe weather arrives.
- [ ] Confirm remote users have laptops, chargers, MFA methods, headsets, and required applications.
- [ ] Verify employees know how to submit support requests when working remotely.
- [ ] Discourage use of personal devices unless approved and secured.
- [ ] Remind employees not to save business data only on personal desktops or local folders.

Cybersecurity During Hurricane Season

Cybercriminals often use urgent events to pressure employees into clicking links, opening attachments, approving payments, or sharing passwords. Storm season is a common time for fake alerts, insurance scams, delivery notices, charity scams, and banking fraud attempts.

7. Employee Cybersecurity Reminders

[ ] Be cautious of urgent storm-related emails, texts, invoices, insurance claims, donation requests, and password prompts.

[ ] Do not click unexpected links related to FEMA, insurance, banking, shipping delays, payroll, or vendor payment changes.

[ ] Confirm multi-factor authentication is enabled for email, remote access, banking, accounting, and critical cloud services.

[ ] Report suspicious emails to IT before opening attachments or entering credentials.

[ ] Verify wire transfer, ACH, gift card, or vendor payment changes by phone using a known trusted number.

[ ] Do not forward phishing emails to others; use a screenshot or approved reporting method when possible.

8. Email Account Compromise Warning Signs

[ ] Check for hidden incoming or outgoing mailbox rules that forward, delete, or hide messages.

[ ] Review unfamiliar MFA prompts, impossible travel alerts, login alerts, or password reset emails.

[ ] Watch for customers reporting strange emails from your domain.

[ ] Confirm users did not approve unexpected sign-in prompts during an emergency.

[ ] Review suspicious forwarding addresses, unfamiliar delegates, or changes to recovery information.

[ ] Contact IT immediately if a mailbox may have been compromised.

When a Watch or Warning Is Issued

9. 72 to 24 Hours Before Impact

- [ ] Confirm recent backups completed successfully.
- [ ] Send internal instructions for office closure, remote work, and support procedures.
- [ ] Move exposed equipment away from flood-prone areas.
- [ ] Charge laptops, phones, battery packs, and mobile hotspots.
- [ ] Print this checklist and contact lists if needed.
- [ ] Confirm call forwarding or emergency voicemail greetings.
- [ ] Pause non-essential technology projects or changes until after the storm.

10. Final Office Shutdown Items

- [ ] Safely shut down non-essential computers and monitors.
- [ ] Leave only approved critical equipment powered on if required.
- [ ] Unplug non-critical equipment if safe and appropriate.
- [ ] Secure laptops, backup drives, paper records, and portable equipment.
- [ ] Confirm doors, windows, and technology rooms are protected from water intrusion.
- [ ] Notify IT if critical systems are being shut down so recovery expectations are clear.

Important safety note

Employee safety comes first. Do not ask staff to enter unsafe buildings, work around standing water, inspect electrical equipment, or power on damaged devices.

After the Storm: Recovery Checklist

11. Before Powering Equipment Back On

[ ] Inspect the office for water, visible damage, electrical hazards, and unsafe conditions.

[ ] Do not power on wet equipment, equipment exposed to water, or equipment in standing water.

[ ] Take photos of damaged equipment before moving or discarding anything.

[ ] Confirm power is stable before reconnecting critical systems.

[ ] Contact IT before reconnecting damaged firewalls, switches, servers, or storage devices.

12. Restore Business Operations

[ ] Confirm internet, phones, Wi-Fi, printers, servers, and shared files are functioning.

[ ] Check that backups resumed after power and internet were restored.

[ ] Review Microsoft 365, Google Workspace, accounting, payroll, and business application access.

[ ] Ask employees to report missing files, login issues, suspicious emails, or unusual account alerts.

[ ] Prioritize recovery based on the priority systems listed at the beginning of this checklist.

[ ] Document what worked, what failed, and what should be improved before the next storm.

Recovery Notes

Issue found	System affected	Owner	Status / next step

Emergency Contacts & Vendor Information

Keep this page printed and stored somewhere accessible. During an outage, your normal systems may not be available.

Contact type	Company / name	Phone	Account / notes
IT support	Barrett Information Technology	1-888-374-4632	barrettit.com/support
Internet provider			
Phone provider			
Power utility			
Insurance agent			
Building / landlord			
Banking contact			
Payroll provider			

Equipment Inventory Snapshot

Record the most important equipment. This is not a replacement for a full asset inventory, but it helps during insurance claims and emergency support.

Device	Location	Serial / asset tag	Notes
Firewall			
Internet modem / router			
Main network switch			
Server / NAS / backup appliance			
UPS battery backup			
Primary printer / copier			
Other critical device			

Final Quick Reference

Use this page as a fast reference during a storm or office closure. Keep a printed copy with management and a digital copy available outside the office.

Do This Before Leaving the Office

- [ ] Verify backups completed recently for critical systems.
- [ ] Forward phones or update voicemail if the office will be closed.
- [ ] Move equipment away from floors, windows, and possible leaks.
- [ ] Shut down non-essential systems safely.
- [ ] Take photos of important equipment and any existing damage.
- [ ] Confirm key employees know how to work remotely and contact support.

Do Not Do This

- [ ] Do not power on wet equipment or equipment exposed to water.
- [ ] Do not bypass multi-factor authentication or security controls for convenience.
- [ ] Do not click storm-related links, attachments, or payment requests without verification.
- [ ] Do not make unnecessary network or firewall changes during the emergency.
- [ ] Do not throw away damaged equipment before documenting it for insurance and support.

Call IT When

- [ ] The office has water damage near technology equipment.
- [ ] Internet, phones, email, or shared files are down after power returns.
- [ ] A backup, server, firewall, or network device shows an error.
- [ ] An employee receives suspicious login alerts, MFA prompts, or storm-related phishing emails.
- [ ] You need help restoring files, reconnecting equipment, or prioritizing recovery.