

Hurricane Season IT Preparedness Checklist

For Jamaican organizations. Prepared by Syxel Technologies Limited.

How to use this checklist

This checklist covers how to protect your IT systems, data and business operations during the Atlantic hurricane season, which runs from 1 June to 30 November. Delete this page before you adopt it.

- Replace everything in [square brackets] with your own details, and delete items that do not apply to your site.
- Name one person to coordinate IT preparations and a deputy who can act if they are unavailable (section 2).
- Complete the "before the season" items in section 4 by 1 June each year. Most of the work happens here, when there is time to buy equipment and test it.
- Fill in Appendix A (asset and photo inventory) and Appendix B (emergency IT contact sheet), print them, and store copies away from the office as well as in the cloud.
- Keep the backup status log in Appendix C up to date through the season.
- Print the post-storm restart checklist in Appendix D and keep it with your server or network equipment so it is at hand when the power comes back.
- Run a short test before the season: switch to backup power, fail over to the backup internet link, restore a file from backup, and log in remotely.

This checklist is about IT only. For personal safety, shelter, evacuation and storm information, follow the Office of Disaster Preparedness and Emergency Management (ODPEM) at odpem.gov.jm, bulletins from the Meteorological Service of Jamaica, and other official guidance. Staff safety always comes before equipment.

This checklist was prepared by Syxel Technologies Limited. For help with backup power, backup internet, data backups or a site assessment, contact sales@syxeltech.com.

[Organization] Hurricane Season IT Preparedness Checklist

Document owner	[Name, role, e.g. IT Coordinator or Operations Manager]
Approved by	[Name, role]
Site(s) covered	[Address of each site]
Version	[1.0]
Last tested	[Date of last backup power, failover and restore test]
Next review	[Date, before 1 June each year]

1. Purpose and scope

This checklist sets out how [Organization] prepares its IT systems for the hurricane season, protects them when a storm threatens Jamaica, and restores them safely afterwards. Its aim is to protect our data, limit damage to equipment, and get the business working again as quickly as conditions allow.

It covers:

- servers, network equipment, computers, laptops, phones and printers;
- data and backups, including cloud services;
- backup power: UPS units, inverters, batteries and generators;
- internet connections, including any Starlink or other backup link;
- CCTV, alarm and access control systems;
- remote working, key contacts, passwords and records needed for insurance.

It does not cover personal safety, building protection, evacuation or weather forecasting. For those, follow ODPEM (odpem.gov.jm), the Meteorological Service of Jamaica, your parish disaster coordinator and other official guidance. No one should put themselves at risk to protect equipment.

2. Roles and responsibilities

Role	Name	Responsibilities
IT coordinator	[Name]	Owns this checklist, makes sure each stage is completed, keeps Appendices A to D up to date, and decides when systems are shut down and restarted.

Role	Name	Responsibilities
Deputy IT coordinator	[Name]	Acts for the IT coordinator if they are unavailable, and holds a copy of the contact sheet and emergency access details.
Management	[Name, role]	Approves spending on backup power, backup internet and backups, decides when the office closes and reopens, and approves remote working arrangements.
IT support provider	[Company, contact]	Supports backups, failover, shutdown and restart, and checks equipment after the storm.
Department leads	[Names]	Make sure their teams have charged laptops, can work remotely if required, and have saved their work to approved storage.
All staff		Save work to approved storage, take home assigned equipment when told to, and report damaged or missing equipment.

3. Critical systems and recovery priorities

List the systems the business needs most, in the order they should be restored. This order guides the restart in Appendix D and tells everyone what to protect first.

Priority	System or service	Why it matters	Longest acceptable outage	How we recover it
1	[e.g. Internet and firewall]	[e.g. needed for email, cloud systems and payments]	[e.g. 4 hours]	[e.g. switch to Starlink backup link]
2	[e.g. Accounting or point-of-sale system]			[e.g. restore from cloud backup]
3	[e.g. File server]			
4	[e.g. CCTV and access control]			
5				
6				

4. Before the season (complete by 1 June)

Do this work early in the year. Equipment, generator servicing and installers are harder to get once a storm is forecast.

Backups and data

- ☐ List every system that holds business data, including servers, computers, cloud services, CCTV recorders and phones (Appendix C).
- ☐ Back up all business data to at least one location away from the office, such as a cloud backup service or an encrypted drive kept at another site.
- ☐ Keep at least one backup copy that ransomware or an accidental deletion cannot change, for example a backup with version history or an offline copy.
- ☐ Make sure backups run automatically and someone checks that they succeed. Record the checks in Appendix C.
- ☐ Test a restore: recover a sample of files and, for important systems, a full system or database. A backup that has not been restored is not proven.
- ☐ Write down how long a full restore takes, and compare it with the longest acceptable outage in section 3.
- ☐ Confirm that laptops and staff files are saved to approved cloud or server storage, not only on the local drive.
- ☐ Back up firewall, router, switch, Wi-Fi and phone system configurations, and store copies off-site.

Power

- ☐ Put servers, network equipment, the firewall, Wi-Fi, the CCTV recorder and the access control panel on a UPS (uninterruptible power supply) or inverter.
- ☐ Check UPS and inverter batteries. Replace any that fail a load test or are past the manufacturer's replacement period.
- ☐ Work out how long your backup power will run the critical equipment, and whether that is long enough to shut down cleanly or keep working.
- ☐ Set up automatic, safe shutdown: install the UPS management software or network card so servers and storage shut down cleanly before the battery runs out.
- ☐ Fit surge protection on every powered device, and on network and coaxial cables that enter the building from outside.
- ☐ If you have a generator, have it serviced, test it under load, and confirm it can supply the critical IT equipment. Keep the UPS between the generator and sensitive equipment.
- ☐ Have any generator connection or transfer switch installed by a qualified electrician. Never connect a generator to building wiring without one.

- ☐ Record the fuel arrangements for the generator (supplier, storage, expected running time) in Appendix B.
- ☐ Label each UPS, inverter and power circuit so anyone can see what it feeds.
- ☐ Write a shutdown order for the site (the reverse of Appendix D) and post it beside the server or network cabinet.

Internet and backup connectivity

- ☐ Arrange a second internet link from a different provider or technology, such as Starlink, fixed wireless or a cellular router, so one outage does not cut you off.
- ☐ Configure the firewall or router to fail over to the backup link automatically, and test the failover.
- ☐ Remember that by default Starlink blocks inbound connections, and a public IP address is only offered on certain plans. Check that VPNs, remote access and CCTV viewing still work over the backup link.
- ☐ Put the Starlink router and any backup link equipment on the UPS. The Starlink Standard kit draws an average of 75 to 100 W, so include it when sizing backup power.
- ☐ Starlink says its equipment is not designed to withstand hurricanes. Plan now how the dish will be secured or taken down before a storm: who will do it, how long it takes, and where the dish and cables will be stored indoors.
- ☐ Check that every outdoor dish, antenna and camera mount is fixed firmly, and photograph the installation for insurance.
- ☐ Keep a mobile data plan or hotspot available for key staff in case both links fail.
- ☐ Write down account numbers and support contacts for each provider in Appendix B.

Protecting equipment from water and wind

- ☐ Identify where equipment sits near windows, doors, skylights, roof leaks or ground-floor areas that could flood.
- ☐ Raise servers, network cabinets, UPS units and computers off the floor, on shelves, racks or stands, where you can do so safely.
- ☐ Plan where equipment will be moved to before a storm: an interior room away from windows and outside walls, and off the floor.
- ☐ Keep heavy-duty plastic sheeting, bin bags, tape and waterproof containers on hand to cover equipment.
- ☐ Keep a few watertight containers for laptops, backup drives, documents and the items listed in Appendix B.
- ☐ Make sure the server or network room door can be locked and its keys are listed in Appendix B.

CCTV and access control

- ☐ Put the CCTV recorder (NVR or DVR), its network switch and any cameras powered from that switch on a UPS.
- ☐ Back up important footage to the cloud or another site, or set up cloud recording for key cameras, so footage survives if the recorder is damaged or stolen.
- ☐ Check that you can view cameras remotely, including over the backup internet link.
- ☐ Find out how each access-controlled door behaves when power fails: whether it unlocks (fail-safe) or stays locked (fail-secure). Record this in Appendix B.
- ☐ Check the battery backup on access control panels and locks, and replace weak batteries.
- ☐ Make sure mechanical override keys for controlled doors exist, work, and are stored securely with a named keyholder.
- ☐ Export or print the list of access cards and users, and back up the access control system configuration.
- ☐ Confirm who your alarm or monitoring company will call, and that the call list is current.

Remote work readiness

- ☐ Decide which roles can work from home, which cannot, and what they need to do so.
- ☐ Test that remote staff can reach email, files, business systems and the VPN, if you use one, from outside the office.
- ☐ Make sure every remote worker uses multi-factor authentication and can still sign in if they lose their phone, for example with backup codes.
- ☐ Confirm that laptops are encrypted, patched and have current security software.
- ☐ Arrange call forwarding or a cloud phone system so the main business number can be answered elsewhere.
- ☐ Prepare a short message for customers and staff that can be sent if the office closes, and decide who sends it.

Key contacts and passwords

- ☐ Complete the emergency IT contact sheet in Appendix B, print it, and give copies to the IT coordinator, deputy and management.
- ☐ Store emergency administrator passwords, recovery codes and encryption keys securely offline: for example in a sealed envelope in a locked, fire and water resistant safe, or on an encrypted drive, with a second copy at another secure location.
- ☐ Make sure at least two trusted people can reach the offline credentials, and record who they are, not the credentials, in Appendix B.
- ☐ If you use a password manager, set up its emergency access or recovery options.
- ☐ Never write passwords on the contact sheet, on equipment or in unencrypted files.

Insurance records and asset list

- ☐ Complete the asset and photo inventory in Appendix A, including serial numbers and where each item is kept.
- ☐ Photograph or video every room, rack and major item of equipment, showing labels and serial numbers. Store the files in the cloud as well as on site.
- ☐ Keep purchase receipts and invoices, or copies, with the inventory.
- ☐ Check with your insurer or broker what your policy covers for electronic equipment, data recovery and business interruption, and what evidence they need for a claim.
- ☐ Record the policy number and claims contact in Appendix B.

Test and train

- ☐ Run a backup power test: switch off mains power to the IT equipment and confirm the UPS, inverter or generator takes over and safe shutdown works.
- ☐ Run a failover test: disconnect the main internet link and confirm the backup link takes over.
- ☐ Run a restore test and a remote login test, and record the results.
- ☐ Walk the IT coordinator, deputy and anyone else involved through this checklist.
- ☐ Record the test date in the document control table and fix anything that failed.

5. When a hurricane watch is issued

A watch means hurricane conditions are possible. Follow official bulletins from the Meteorological Service of Jamaica and ODPEM. Use this time to finish preparations while power and internet are still working.

- ☐ Tell management and staff that hurricane IT preparations have started, and who to contact.
- ☐ Run a full backup of every critical system and confirm that it completed. Record it in Appendix C.
- ☐ Confirm the latest cloud or off-site backup copy is complete and up to date.
- ☐ Ask staff to save all work to approved cloud or server storage, not the local drive.
- ☐ Charge every laptop, phone, tablet, power bank and spare battery.
- ☐ Check UPS and inverter battery levels, and top up generator fuel through your normal supplier.
- ☐ Test the backup internet link and confirm remote access works over it.
- ☐ Confirm who will secure or take down the Starlink dish and other outdoor equipment if a warning is issued, and that they have what they need.
- ☐ Take fresh photos or video of equipment and rooms for insurance, and upload them to the cloud.
- ☐ Print current copies of Appendix B and Appendix D, and check that the offline credentials are where they should be.
- ☐ Confirm which staff will work remotely if the office closes, and that they can take their equipment home.

- ☐ Check that remote CCTV viewing works and the alarm company has the current call list.
- ☐ Move spare equipment, backup drives and important documents into watertight containers.

6. When a hurricane warning is issued

A warning means hurricane conditions are expected. Finish IT tasks early so that everyone can leave in good time and follow official safety guidance. Do not stay behind to protect equipment.

Data and people

- ☐ Run a final backup and confirm the off-site or cloud copy is complete.
- ☐ Send remote workers home with laptops, chargers and power banks, and confirm they can sign in.
- ☐ Send the agreed message to customers and staff about opening hours and how to reach the business.
- ☐ Turn on call forwarding or switch the main number to the cloud phone system, if planned.
- ☐ Take any portable backup drive off site with the IT coordinator or deputy, in a watertight container.

Equipment

- ☐ Secure or take down the Starlink dish and any other removable outdoor antennas, following the provider's instructions, and only if it can be done safely before conditions worsen. Bring the dish and cables indoors and keep exposed cable ends dry.
- ☐ Move computers, printers and portable equipment away from windows and outside walls into the interior room you identified, and raise them off the floor.
- ☐ Unplug equipment that will not be needed, including computers, printers, monitors and chargers, to protect it from surges when power fails and returns.
- ☐ Cover equipment that cannot be moved with plastic sheeting. Do not wrap anything that will keep running, as it needs airflow to stay cool.
- ☐ Decide whether servers and network equipment will run on backup power through the storm or be shut down. If the site will be empty, a controlled shutdown is usually safer.
- ☐ If shutting down, follow the shutdown order posted at the cabinet: user computers first, then applications and servers, then storage, then network equipment, then the UPS.
- ☐ Leave CCTV, alarm and access control running on backup power if they are protected and you want to monitor the site remotely.
- ☐ Lock the server or network room and confirm the keyholder.
- ☐ Record what was shut down, moved or covered, and where it is, so the restart team knows the state of the site.

7. During the storm

During the storm the priority is everyone's safety. Follow ODPEM and official guidance. IT work waits until officials say it is safe.

- ☐ Do not go outside, onto a roof or up a ladder to adjust a dish, camera or antenna.
- ☐ Do not go into the office to check or move equipment.
- ☐ Do not switch equipment back on if power flickers or returns briefly. Wait for the restart in section 8.
- ☐ If you can view CCTV or monitoring remotely, note any damage, water or intrusion with the time, but do not act on it in person until it is safe.
- ☐ Keep phones and power banks charged and conserve battery where you can.
- ☐ Remote workers: save work often to cloud storage, and expect connections to drop.
- ☐ The IT coordinator keeps a simple log of what is known about the site and systems, with times.

8. After the storm and recovery

Return to the site only when officials say it is safe to do so. Building, electrical and flood hazards must be cleared by the right people before IT work starts.

Assess

- ☐ Wait for confirmation that the building is safe to enter and the electrical supply has been checked where there was water or structural damage.
- ☐ Photograph and video all damage before moving or cleaning anything, for the insurance claim.
- ☐ Check every item in Appendix A against the inventory and record what is damaged, wet or missing.
- ☐ Do not power on any equipment that got wet, sat in standing water or shows signs of moisture. Set it aside for inspection by a technician.
- ☐ Inspect the Starlink dish, cables and mounts for impact damage or water before reconnecting. Let any wet cable dry out fully first.
- ☐ Check outdoor cameras, antennas and cabling for damage, loose mounts and water in connectors.

Restore

- ☐ Wait until mains power is stable before restarting equipment. Power often drops and returns several times after a storm.
- ☐ Restart systems in the order set out in Appendix D, and tick each step off.
- ☐ If the main internet link is down, confirm the backup link has taken over, or reinstall the Starlink dish once it is safe to do so.

- ☐ Check that each system on the priority list in section 3 is working before declaring it restored.
- ☐ Restore any lost or damaged data from the latest good backup, and record what was restored in Appendix C.
- ☐ Check CCTV recording, the alarm and access control, including that doors lock and unlock correctly and the system clock is correct.
- ☐ Change any passwords or access codes that had to be shared during the emergency.
- ☐ Tell staff and customers when normal service resumes.

Claim and learn

- ☐ Send your insurer or broker the photos, inventory and damage list as soon as you can.
- ☐ Keep receipts for emergency repairs, rentals, fuel and replacement equipment.
- ☐ Replace UPS batteries, surge protectors and any equipment that took a surge, even if it still seems to work.
- ☐ Hold a short review: what worked, what failed, and what to fix before the next storm. Update this checklist and record the date.

9. Review

[Role] reviews this checklist before 1 June each year, after any storm that affects our sites, and whenever we change our main systems, internet providers, backup power or office location. The review includes the tests in section 4 and updates to Appendices A to D.

Appendix A: IT Asset and Photo Inventory

List every item of IT equipment. Photograph each item showing its label and serial number, and record the photo file name. Keep this list in the cloud and keep a printed copy off site.

[illegible]

Item and description	Make and model	Serial number	Location	Assigned to	Purchase date and value	Photo file	Storm plan (move, cover, take home)

Appendix B: Emergency IT Contact Sheet

Print this sheet and keep copies with the IT coordinator, the deputy and management, and at another location. Do not write passwords on this sheet.

Role or organization	Name	Phone	Email	Account or customer number
IT coordinator				
Deputy IT coordinator				
Managing director or owner				
IT support provider				
Main internet provider				
Backup internet provider (e.g. Starlink account holder)				
Electricity provider				
Generator service and fuel supplier				
UPS and inverter supplier				
Alarm and CCTV monitoring company				
Access control supplier				
Insurance broker or insurer (policy number)				
Landlord or building manager				
Key software and cloud vendors				

Role or organization	Name	Phone	Email	Account or customer number

Where things are kept

Item	Location	Who has access
Offline administrator passwords and recovery codes	[e.g. sealed envelope in safe, location]	[Two named people]
Second copy of offline credentials		
Server or network room keys		
Access control override keys		
Off-site backup drive		
Printed copy of this checklist and Appendices A to D		
Generator keys and fuel		

Access-controlled doors on power failure

Door	Fails unlocked or locked	Override method and keyholder
[e.g. Main entrance]	[Fail-safe (unlocks) or fail-secure (stays locked)]	

Official sources for storm and safety information: Office of Disaster Preparedness and Emergency Management (ODPEM), odpem.gov.jm; Meteorological Service of Jamaica, metservice.gov.jm.

Appendix C: Backup Status Log

Record each backup check and restore test during the season, and every backup taken when a watch or warning is issued.

[illegible]

Date	System or data	Backup type and location	Completed	Restore tested (what and result)	Checked by	Notes

Appendix D: Post-Storm Restart Checklist

Use this when officials say it is safe and the site has been checked. Restart in this order, and do not move to the next step until the previous one is working. Adjust the order to match your systems.

Before switching anything on

- ☐ The building has been confirmed safe to enter and the electrical supply checked where there was water or structural damage.
- ☐ Damage has been photographed before anything was moved or cleaned.
- ☐ Mains power has been stable for [at least 30 minutes], or the generator is running steadily.
- ☐ Equipment that got wet or sat in water has been set aside and will not be powered on until a technician inspects it.
- ☐ Cables and connectors are dry, and surge protectors are in place.

Restart order

- ☐ Power: UPS units and inverters on, batteries charging, no fault lights.
- ☐ Internet: modem, fiber terminal or Starlink router. Reinstall the dish only when it is safe to work outside.
- ☐ Firewall and router, then confirm internet access and failover.
- ☐ Core network switches, then other switches.
- ☐ Wi-Fi access points.
- ☐ Storage (NAS or SAN), then wait until it is fully ready.
- ☐ Servers that provide sign-in and directory services, then application and database servers.
- ☐ Business applications, in the priority order from section 3.
- ☐ CCTV recorder and cameras: confirm recording and correct date and time.
- ☐ Access control and alarm: test each door and check the clock and user list.
- ☐ Phone system and call forwarding: return to normal routing.
- ☐ Staff computers and printers.

Before declaring systems restored

- ☐ Each critical system has been tested by a person who uses it.
- ☐ Backups have run successfully since the restart, and Appendix C is updated.
- ☐ Any data restored from backup has been checked.
- ☐ Damaged and missing equipment is recorded for the insurer in Appendix A.
- ☐ Staff and customers have been told normal service has resumed.

Restart completed by	
Date and time	
Problems found and actions taken	
Approved by	