## BUSINESS CONTINUITY POLICY

[Organization Name] recognizes the need to be prepared for emergencies that may disrupt business operations. This policy aims to guarantee that [Organization Name] creates objectives, plans, and procedures that limit significant disruption of the organization's critical business operations.

This policy applies to all management, employees, and suppliers who are involved in decisions and processes that influence the business continuity of [Organization Name].

DEFINITIONS

The following definitions apply to this document:

**Business Impact Analysis/Assessment (BIA)** - an exercise that determines the impact of losing any resource's support to an enterprise, establishes the escalation of that loss over time, identifies the bare minimum resources required to resume normal operations, and prioritizes process and supporting system recovery.

**Disaster Recovery Plan (DRP)** - a collection of human, physical, technical, and procedural resources that enable an activity to resume normal operation within a specified time and cost frame following an interruption caused by an emergency or disaster.

**Recovery Time Objective (RTO)** - the time allocated for the restoration of a business function or resource to its pre-disaster state following a disaster or disruption.

**Recovery Point Objective (RPO)** - established in accordance with the acceptable level of data loss in the event of an interruption of activities.

POLICY

In the event of an emergency, the Emergency Management Team is responsible for announcing emergencies, evacuating or closing down facilities as necessary, and communicating with staff. The Emergency Management Team will be led by an Incident Commander. Emergencies are not limited to natural calamities but may include cybersecurity.

The Emergency Management Team has the power to identify important business functions that have been impacted by the emergency and to commence the process for resuming operations in the sequence specified in this policy.

This policy is in place to ensure that business operations continue in the event of an emergency and to ensure the safety of all personnel. Failure to adhere to this policy or any directives given by the Emergency Management Team may result in verbal reprimands, formal write-ups, and termination, as judged necessary.

Emergency Management Team

The Emergency Management Team is responsible for the emergency response's technological aspects. The Incident Commander will lead the team. Members of this group (and only these designated members) have the authority to:

* Direct the closure of a facility
* Initiate employee and customer evacuations
* Announce the end of an incident
* Communicate with the media
* Establish the emergency response phone tree

Incident Commander

In the event of an emergency, the Incident Commander is responsible for interacting with internal and external resources. This individual is authorized to declare a state of emergency, shut down company facilities, and contact the media.

*Workflow*

The Incident Commander must take the following procedures immediately following an emergency to resume operations:

* Form a recovery team and work from top business priorities down for resuming operations.
* Ensure the safety of all personnel on the premises by assessing any residual hazards and securing the incident scene.
* Conduct a briefing for employees.
* Keep meticulous records; note that all decision-making should be documented, as should the damage, which should be videotaped or photographed.
* Establish charge codes for purchases and repair work to account for all damage-related expenditures.
* Adhere to your notification policies. Notify families of on-duty people, inform off-duty personnel of their job status, and notify insurance carriers and necessary government organizations.
* Preserve intact property by closing entrances and exits, repairing sprinkler systems, reestablishing electricity, protecting property from dampness, and removing smoke, water, and general debris.
* Work with appropriate government entities to coordinate your restoration efforts.
* Maintain control over salvage operations by separating damaged from undamaged property and holding damaged commodities until an insurance adjuster can inspect them. However, you should shift material outside if it obstructs traffic and is weather-resistant.
* With the assistance of an adjuster or the adjuster's salvor, conduct an inventory count of damaged goods. If you release any goods to the salvor, obtain a signed inventory stating the number and type of assets.
* Restore property and equipment. Consult the insurance adjuster and appropriate government bodies prior to doing any major repair work.
* Determine the replacement cost of damaged property and the financial impact of business interruption.
* Maintain ongoing communication with customers and suppliers to foster trust.

Business Risk Assessment

The [Insert Person] is required to perform yearly Business Risk Assessments and Business Impact Analyses for key business systems in their areas of responsibility.

The risk assessment must identify and describe the criticality of essential business systems and data repositories. At the very least, in doing the assessment, especially for cybersecurity, the following must be considered:

* Operations at physical sites that are critical to the business
* Number of staff in each location and how many are prepared to work remotely
* Number of people who need to relocate or move to work from home to continue operations
* Any technology gap
	+ How long it takes data or systems to recover
	+ Which systems could impede the operation
	+ Vetting of technology suppliers to learn how they can secure data and respond to disasters or cyber attacks
* Availability of reliable IT providers for necessary added services
	+ Inform IT of core systems involved, data that must be recovered, and the ratio of staff that must be operational in a given time (i.e., in 24 hrs)
	+ Require IT to do simulations

[Insert Person] must subsequently define and document a DRP, which will include.

* Key business processes
* Available risks
* Recovery prioritization
* Recovery time goals
* Recovery point goals
* Budget

Once the BIA and DRP are done, the [Insert Person] will review them and sign.

Disaster Recovery Plan

Each [Insert Person] must have a signed DRP to guide them when hardware, software, or networks fail (short and long-term outages).

Each DRP must explain the amount of information or system unavailability and the process used to keep business running during an outage. The DRP must consider off-site computer operations wherever possible (cold, warm, hot sites).

Policies, legal, legislative, and regulatory obligations must be checked against each plan.

Each DRP must include:

• A backup plan in case of temporary hardware, software, or network failures.

• A plan for restoring business processes and services on-site.

• Procedures for testing, reviewing, and revising the DRP for all involved business systems.

*Data Backup and Restoration*

[Insert Person] is responsible for implementing a data backup and restoration strategy.

Each data backup and restoration strategy must identify the following:

* The system's data custodian.
* Each system's backup schedule.
* Where and how backup media should be stored and secured, as well as how access to backup media should be maintained.
* Who has the authority to delete backup media and store it.
* Appropriate restoration techniques for restoring critical business system data to the system from backup media.
* A restoration testing strategy and frequency of testing to confirm the plan's efficacy.

Communication

*Emergency Communication*

* In specific areas throughout the grounds, cellphones and computers equipped with wireless internet access will be available.
* A backup generator will ensure an Internet connection in the event of a power outage.

*Notification*

* Employees should notify [Insert Person] in the event of an emergency. Employees should call [Insert alternative Contact] if [Insert Original Person] is unavailable.
* The assigned staff are responsible for monitoring the local radio/weather report for indications of impending inclement weather.
* To assist employees regarding who to notify, emergency telephone numbers and a list of employees to call will be listed at [Location].
* In cases of evacuations, addresses to locations where employees should meet should be posted at [e.g., bulletin board, etc.]
* In the case of a facility-wide evacuation due to an emergency, the following announcement will be made to all employees:
	+ [Insert Message]

*Warning*

* The warning will have the following audio and visual components: [Insert Details].
* To assist those with particular disabilities who may have difficulties recognizing the warning, we have enhanced our warning system to include [Insert any Modified Alerts].
* Emergency exits will be identified with signs to draw attention to them and to assist evacuating staff.
* When customers or other visitors are present when a warning is issued, the Emergency Management Team should take the following steps to ensure that everyone safely evacuates: [Insert Evacuation Procedures].

Training

Employees will receive comprehensive training on evacuation and business restoration procedures. Specifically:

* All staff will meet with their department heads X times/year to review disaster preparedness and emergency action plan processes.
* During employee orientation, new employees will be presented with emergency action plans.
* Annual mock disaster training will be held in conjunction with local police and fire departments.
* Quarterly training sessions will include all of the following drills and will conclude with a full-scale simulated disaster.
	+ **Walkthrough drills:** Members of the business continuity planning team, department heads, and recovery teams will exercise their emergency response responsibilities.
	+ **Functional drills**: These drills will put specific functions such as medical response, emergency notification, warning, and communication procedures and equipment to the test, but not necessarily concurrently. Procedures for facility shutdown will be tested, reviewed, and updated as necessary. Personnel is tasked with the responsibility of evaluating the systems and identifying potential problems.
	+ **Evacuation drills**: Personnel walk the evacuation route to a designated spot to verify that all personnel are accounted for. Participants are required to take notes along the route on potential hazards that may arise during an emergency, such as cluttered stairwells and smoke in the hallways. Plans must be adjusted accordingly, and deficiencies must be addressed immediately.
	+ **Full-scale exercises**: A situation resembling a real-life emergency is replicated as nearly as feasible. These drills involve emergency response personnel from the corporation, as well as employees and management, as well as community response organizations.

Audit of the Policy

Annual audits will be undertaken on this business continuity plan, as well as evaluation and adjustment following each training exercise, emergency, change in staff duties, change in building layout or design, and change in policies or procedures. Personnel will be briefed if the plan is altered or modified.

The employee doing the plan audit will give the Incident Commander a signed and dated copy of the plan, along with any necessary adjustments. The strategy will be updated online upon evaluation. There will be X printed copies. One will be placed in [Insert Location], while the others will be placed [Insert locations].