Disaster *Planning* Guide

An overview of the basic components anyone can plan with.

How to navigate

The side tabs take you to different sections in the document.

These icons help you navigate through:

- Previous page
- Table of contents
- Next page
- Click to learn more

Table of contents

Click numbers or sections to navigate

Disclaimer

This best practice guide focuses on helping advisors prepare for unforeseen events that disrupt their business. This is not a comprehensive planning guide. All insurance and financial transactional processes should be guided by your dealership or financial partners. Your IT partner should have a plan to assist you with recovery of IT assets and solutions for business continuity.

Nothing in this guide is a substitute for solutions provided by your IT vendor or business consultants. This guide is intended for educational and general awareness purposes only. Note also that it does not cover responsibilities related to compliance or industry regulations.

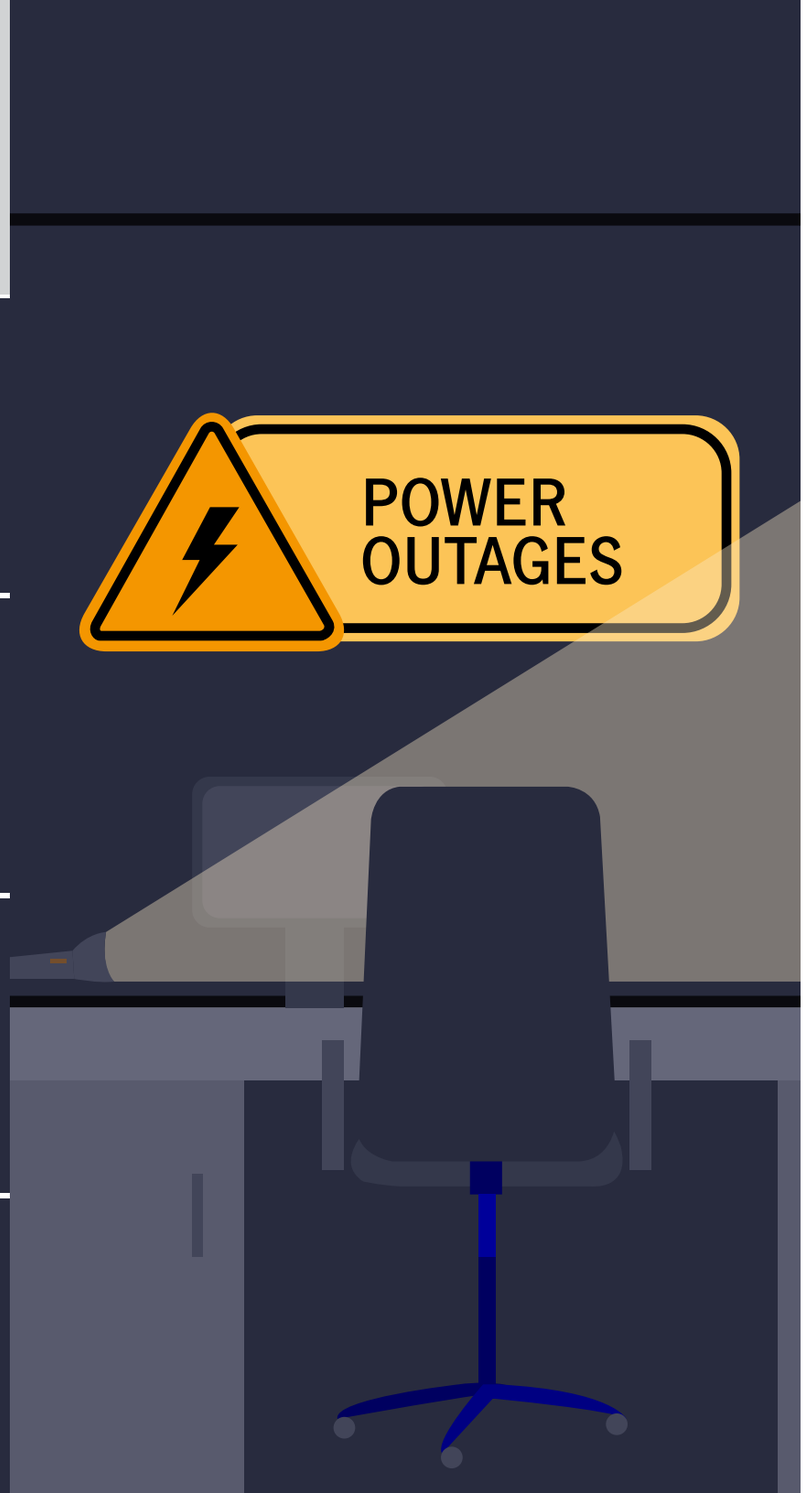
Goals and Objectives

You may be reading this guide and thinking, "My office is way too small to need all these preparations," but you would be wrong! Unforeseen events can happen anywhere, anytime and to anyone – even you.

Being prepared for a disaster isn't just for large advisor offices or branches; it is necessary for businesses of all sizes. Please review this guide and use the parts that could apply to you and your clients during unforeseen events.

Our goals are:

- To understand the types of disasters or disruptions that could affect your business.
- To ensure that the disaster plan is communicated to all staff, clearly identifying all essential roles and responsibilities.
- To ensure the business operates while recovering from the disaster or on an interim basis during disruptions.
- To maintain communication and service to your clients.



Defining Disaster

Your plan should identify the most probable events that could happen in the next 50 years. Floods, fires, storms, pandemics are all considerations. Also keep in mind that simple building closures can cause significant disruptions.

Classify The Threats

We can structure disasters into 3 classes to help guide how we prepare and respond. Your own situation and location may change how you classify potential disasters. Here are some examples:

Class 1 - Infrastructure

A Class 1 disaster will cause you to activate your disaster plan. The response will involve continuing business operations remotely.

Scenarios

1. **Permanent building closure:** Building is closed due to a disaster such as fire, explosion, or flood.
2. **Power Outage:** Electrical outage that could affect a community, city, or Province and last hours to days.
3. **Server Room Outage:** Servers, desktops, and all equipment cannot be used.
4. **Stay at Home Government Orders:** Pandemic or other disaster related event.

Class 2 - Natural Disaster or Pandemic

A Class 2 disaster will lead to a reduction in available staff to work in the office and building access will be reduced or temporarily blocked.

Scenarios

1. **Pandemic:** Mandatory reduced office staff but still able to access the office.
2. **Weather disruptions:** Major seasonal storms or flooding events affecting ability to attend the office.
3. **Temporary building closure:** Longer than 30 days.

Class 3 - Service Outages, Failures and Cybersecurity Breaches

A Class 3 disaster includes business partner(s) service outage where they are experiencing their own Class 1 or Class 2 disaster.

Class 3 can include:

- Cybersecurity breach
- Ransomware
- Services strikes
- Internet service outage
- Email service outage
- Cloud service outage

Scenarios

1. Report of stolen funds or information from fraudulent email attack — business email compromise, loss of login credentials or unauthorized access to systems.
2. Loss of a device — laptop, desktop, smartphone, USB storage device containing confidential data or system login capabilities or credentials.
3. Physical break-in or insider theft of paper records.
4. Inadvertent transfer or transmission of client information.

Class Evaluation

Take the time to evaluate the impact to your business and probability of it happening in the next 10 years. Focus on events most likely to happen and with the highest impact. Example:

CLA		IMP	PRB	
1	Server Room Outage	Med	Low	Azure cloud server
1	Flood	Med	Med	On river plain and ground floor
2	Pandemic Lockdowns	Med	High	Ongoing concerns
3	Ransomware	Med	High	Ensure offsite backup
3	Canada Post Outage	Low	Low	Substitute couriers

Plan Activation Criteria

- The business owner must evaluate the disaster, determine the class and instruct the office manager to activate the disaster plan or a part of it.
- Using a checklist to summarize tasks will make the process much easier to start.

The first step in creating a **disaster plan** is to clearly assign the responsibility for emergency preparedness to an individual or a team depending on the size of your operations. Always assign one person to lead the planning process and ensure they have sufficient authority to get things done.

- Establish what determines activation of the plan.
- Identify key business partners, such as IT or infrastructure vendors, and determine if they have a disaster plan. How will it affect you?
- Assess potential financial impact or resource requirements of an emergency on the business.
- Ensure adequate supplies, such as personal protective equipment, hygiene supplies like hand sanitizers, cleaning products, masks, protective barriers, etc.
- Perform trial runs of the plan and update accordingly.
- Documents should be stored in a secure external location including cloud storage.

Sample list of contacts to maintain:

- Service vendors contact list
- Staff contact list
- Key client contact list
- Business partners contacts
- Key suppliers
- Utility contacts
- Activation checklist

Planning Pillars

As part of your disaster planning process, there are four key areas you will need to keep in mind: people, buildings and service vendors, equipment and data.

People

- Contact information in the form of home, cell phone and emails for employees and details for customers, vendors, suppliers, etc.
- Maintain a separate key cient contact list. Being proactive in contacting important clients can go a long way in mitigating losses and managing client expectations.
- With a comprehensive list of contacts, you can utilize phone calls, texts, websites and even social media to provide updates on your recovery or operational processes and let everyone know you're still in business.

Building and Service Vendors

- Document addresses of physical locations, home addresses, storage units and deposit boxes, as well as copies of leases. Make a list of the people who have access or keys for each resource.
- Maintain contact information for building maintenance or management.
- Document core service providers or regular service deliveries. Include account numbers, phone PIN for support, passwords.

Tips:

People:

Maintain spreadsheets with your contact details and use secure cloud storage to share with other employees.

Buildings and Service Vendors:

Maintain details on your insurance and document what resources may be available to your business in the event of a disaster.

Planning Pillars

Equipment

- Computer hardware — including model, serial number, purchase date and cost. Include network equipment and printers.
- Software — including version, serial/key, purchase date and cost.
- Tools, office supplies and equipment, office furniture, etc.

Data

- Important documents, payroll information, accounting files, records, login/passwords and data backup locations should be identified and documented in the plan with their location and method to access.
- Backup processes and method of access for your business should be documented, preferably in detail by your IT vendor.
- Data stored at an alternate physical or cloud location must be encrypted. If any decryption keys are generated, ensure they are documented. Consult with your IT vendor.
- If data are stored in a cloud service, they must also use two-factor authentication.

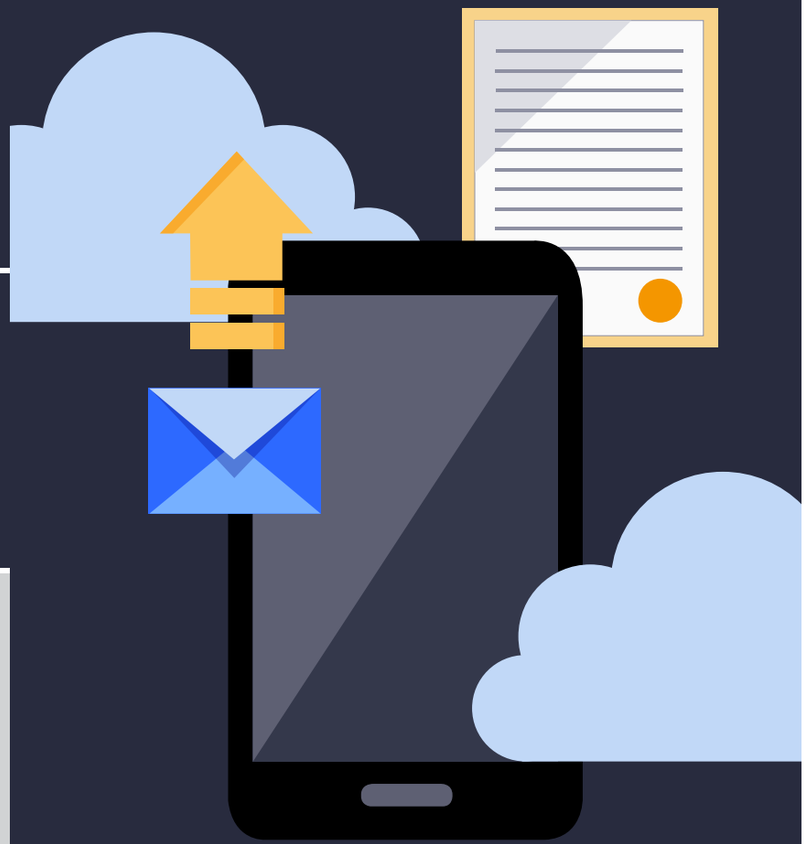
Tips:

Equipment:

This could be necessary for insurance purposes. Your IT vendor should be engaged to provide you these details.

Data:

Consult your IT vendor to ensure you are taking advantage of cloud-based solutions or remote access tools for your alternative operating procedures during a disaster.



Business Continuity

Roles and Office Functions

As the business owner, you may be occupied making key business decisions or communicating with clients or partners during a disaster or emergency. Having roles assigned in advance will keep confusion and stress to a minimum while ensuring that high-priority items are completed efficiently.

The **Emergency Preparedness team,** in consultation with the rest of your staff, should start by documenting the following:

- List the daily and weekly functions of each employee/role.
- Categorize functions for client-facing or internal business.
- Identify what the crucial business functions are.
- Recognize time-sensitive tasks.
- Determine how each task can be completed remotely and what is needed if the office and associated resources are not available.
- Compile a list of supplies required to continue business operations.

Once all tasks and business functions have been identified and documented, you can begin preparing a schedule for each essential service/function and assign the responsibilities to the appropriate employees.

Communications

Make sure you can access your business website and social media accounts so you can post your operating status and alternative contact details.

- Maintain good communications and manage relationships with all staff levels
- Liaise with local government agencies such as Health Canada and Public Safety Canada.
- Prepare and disseminate timely and accurate information.
- Educate staff about possible emergencies. For example, in the event of a pandemic, give information on signs and symptoms of influenza, modes of transmission, personal and family protection, and response strategies.

Assign communication tasks to each member of the office

Example

User	Accountability
Advisor A	Contact business partners (dealer, banks, suppliers).
Advisor B	Contact key clients (see appendix).
Assistant A	Contact (IT vendor) to begin server restore.
Assistant A	Outbound email notification to clients.
Assistant B	Inbound point person for client calls and emails.
Assistant B	Emergency management updates to office team.
Admin	Contact clients with appointments to re-schedule or cancel until further notice.

Technical requirements

Example

Resource	
Internal staff	Ability to access contact list for personal phone and email.
Inbound phone calls from clients	• If phones are down, sign up for temporary soft phone service OR internet VOIP service: This can be a 1-800 and is active immediately. • Update website with this number or a cell number of primary contact person for all inbound calls. • Establish someone to direct all inbound client communications.
Voicemail	• Ensure voicemail of all active numbers is checked regularly. • VOIP service can email voicemail recordings.
Email	Access email directly through web browser.
Website	Have a note placed on your home page on how clients can reach you, Manulife Securities, or post status.
Fax	Forward fax number to VOIP fax service.

Policies, Procedures, Organization

Establish policies such as compensation and absences, return to work procedures, Remote Office Setup, flexible work hours and travel restrictions.

- Define chain of command for plan activation.
- Establish emergency safety policies for the workplace. For example, in the event of a pandemic, establish policies that will help prevent the spread of influenza, such as promoting respiratory/hygiene/cough etiquette and prompt exclusion of people with influenza symptoms.
- Establish policies for employees who are directly affected by the emergency. For example, in the event of a pandemic, set policies for employees who have been exposed.

Test Your Disaster Plan

Testing your disaster plan is key to making sure your business is prepared to meet any challenges an unforeseen event may pose.

1. Use a "real-life" scenario to test your plan.
2. Make sure all office staff are involved, know their roles and understand how to access the plan information independently.
3. Document what went smoothly and what did not. Create a task list for improvements to be worked out before the next test.
4. Have a meeting to discuss your disaster plan test. Schedule on a semiannual or quarterly basis.
5. Make the necessary adjustments to improve and streamline your disaster plan, especially as things change in your office — for example, new hires or changes in technology.
6. Engage other resources for ideas and best practices.

For Smaller Offices

Testing your plan is key — and as a small office you have the advantage over large offices!

An advisor and marketing assistant(s) should be able to walk through the disaster plan quickly and easily, as there are fewer "moving parts" to consider.

Tips:

Test Your Disaster Plan:

Remember, this plan is a living document that needs to be continuously updated as your business changes and threats evolve.

For Smaller Offices:

Involve your IT vendor to confirm that backups are configured properly and can be restored easily.

Sample Activation Checklist

Administration and Communication

- [ ] Contact phone company, forward main line to voicemail, cell number or alternative service. (Utility Contact List)
- [ ] Update voicemail message with new contact info, reassure clients and advise there could be delay in reply.
- [ ] If business phone line cannot be accessed, sign up with alternative service.
- [ ] Ensure voicemail includes cell number for alternative contacts, including email.
- [ ] Create VOIP fax account and have fax number forwarded to new number.
- [ ] Call anyone with appointment scheduled in next 15 days to re-schedule or resolve.
- [ ] Contact IT vendor to begin alternative IT access plans. (Supplier Contact List)
- [ ] Emergency management updates to office team, if required, twice a day. (Staff Contact List)
- [ ] Outbound email notification to clients. (Key Client Contacts List)
- [ ] Ask phone company for conference number for staff or set up Zoom or Teams account. (Utility Contact List)

Advisor

- [ ] Contact business partners (dealer, banks, lawyers). (Partners Contact List)
- [ ] Contact key clients that you are in touch with on regular basis. Supply alternative contact. (Key Client Contacts)
- [ ] Confirm payroll for staff will continue without any manual workflow or approvals.
- [ ] Confirm access to company cheques, online banking, other passwords to transactional systems.

Logistics

- [ ] Advise courier companies of alternative pickup/ delivery point. (Suppliers List)
- [ ] Advise Canada Post to arrange mail forward to alternative address. May be available online. (Suppliers List)
- [ ] Contact business partners (MGA, Dealer, bank) and provide alternative contact details. (Partners Contact List)

Business Continuity

- [ ] Team conference call to review roles and responsibilities as outlined in plan by role.
- [ ] Ensure staff have home PC, access to Web email, and phone number known to everyone.
- [ ] Prioritize tasks based on client impact and time of year.
- [ ] Staff to contact DTSC – 1- 800-667-4266 for Manulife software support.
- [ ] Ensure payroll functions are not affected.
- [ ] Assign priority to any tasks, applications or money flow that was in process during disaster event.
- [ ] Confirm login details to important cloud-based storage, software applications or portals.