

## How to create an Emergency Response plan using the Frank online tool:

Before you start you need to appoint an **Emergency Coordinator** for the company. Having one person responsible for all things emergency related will ensure that response planning is placed at the preferential level and not overlooked or neglected. When deciding on the right person, it's important to consider their role in the organisation, their level of experience, whether they have a broad understanding of the business and where they live.

This Emergency Response plan has been designed so that you can create it with minimal effort, however time will still need to be allocated to collect organisational specific information and consider contingency scenarios. The content has been compartmentalised into sections so that you can create your emergency response plan over time if needed.

Planning for a worst-case scenario – when creating your emergency response plan a practical approach is to assume a worst case scenario including:

- Loss of access to the organisational facilities, loss of equipment and loss of supplies
- Loss of IT and communications
- Loss of skilled or key staff who perform critical functions

Your contingency plans will focus on restoring critical functions and may include:

- Moving staff or operations to an alternative location
- Moving to back up or manual systems
- Using alternative resources
- Replacing equipment and repairing the organisation
- Returning to the organisation as soon as practicable

Who has access to your Emergency Response Plan – Your emergency plan is only accessible to the person/s with the access to the secure login. (Your Risk Manager at Frank will have access to the plan).

# `How to guide' for emergency response planning using ResilienceTec



# ResilienceTec

## How to Create your Online Emergency Response Plan

### Contents

The Planning Process .....	3
General Instructions for Using the Online Tool .....	5
Logging in .....	5
Forgotten Password.....	5
Creating or Editing your Emergency Response Plan.....	5
Entering Information .....	5
To Include a Section in your Plan .....	6
Printing a <b>Draft</b> Section of your Emergency Response Plan .....	6
Publishing and Printing your Emergency Response Plan.....	6
Duplicating your Plan.....	7
Uploading other Planning Documents .....	7
Section Guide.....	8
Section 1: Information about the Organisation, Staff and Activating the Response Plan.....	8
Section 2: Premises information .....	9
Section 3: Key contact information– Support Agencies & Services Providers .....	9
Section 4: Risk Identification and Reduction.....	9
Section 5: Specific Planning Activities .....	9
Section 6: Loss of Power Supply to the Organisation.....	9
Section 7: Disruption of Water or Gas Supply to the Organisation .....	10
Section 8: Disruption to Telecommunications Systems .....	11
Section 9: Loss of IT Systems or Data.....	11
Section 10: Loss of Business Records .....	13
Section 11: Complete or Partial Loss of the Organisation Premises.....	14
Section 12: Medical Supplies, Equipment and Furniture .....	14
Section 13: Unique Identifier and Contract Numbers.....	14
Section 14: Communication during an Emergency Response.....	14
Section 15: Insurance .....	15
Section 16: Loss of or Non-availability of Key Staff .....	15
Section 17: Business Continuity Plan .....	16
Section 18: Impact on Business of an Infectious Event .....	16

## Contents The Planning Process

[ResilienceTec](#) will lead you through a process of all hazard planning. This means that the planning concentrates, mainly, on the effects of events rather than the event itself.

Your organisation will need to assess what areas of the plan that they need to complete. Generally speaking the more sophisticated the business the more sections of the plan you will need to complete, over and above the basics (loss of power, water, IT buildings etc.). After completing section one, which is compulsory, you should complete section two, this section deals with risk treatment. By establishing what your risks are you will be able to determine what sections you need to complete over and above the basics.

### *Appointing an Emergency Coordinator*

It is recommended that you appoint a staff member as the 'emergency management coordinator', and if possible undertake some training. Having one person responsible for all things emergency related will ensure that response planning is placed at a preferential level and not overlooked or neglected.

When deciding on an appropriate staff member, it is important to consider their role in the organisation, their level of experience, whether they have a broad understanding of the organisation and where they live.

Depending on the size of the organisation, it would be worth considering appointing a deputy emergency management coordinator, in the event that the primary emergency management coordinator is on extended leave or becomes ill during an emergency.

### **Role of the emergency management coordinator(s)**

It is vital that the emergency management coordinator(s):

- ensure that they, and all staff have up-to-date knowledge and skills relating to emergency response planning and management (which is specific to the location of the organisation)
- draft and finalise an emergency response plan for the organisation
- be responsible for training and educating the entire organisation team about the plan
- be responsible for reviewing and updating the plan on a quarterly basis
- test or exercise the plan (or components of the plan) annually
- ensure staff can access the printed plan at any time
- make decisions as to whether/when the emergency response plan needs to be activated
- be responsible for building and maintaining relationships with other nearby organisations to discuss strategies of working together in the event of an emergency
- be responsible for connecting with local council and local emergency services.

### *Structure of ResilienceTec*

[ResilienceTec](#) contains planning information that is likely to be common to all organisations and prompts you to edit or fill in information that is specific to your organisation. The plan is divided into 18 sections.

When you log in the first two pages that you see are your 'business home page', and then your 'facility home page'.

#### **Business home page**

- this page is where you create the individual response plans for your different areas or facilities
- you can change your password here.
- You will find a video tutorial in the left side bar.

#### **Area or Facility home page**

- you access the planning pages from here
- you can upload documents specific to the facility for safekeeping here. They are then stored for easy access should you need to.
- you can duplicate your plans here to create multiple area/facility plans
- you can archive a plan should you need to
- You will find a video tutorial in the left side bar.

After these initial sections you will access the detailed planning sections where you will enter the information for your actual plan.

## **Workload**

[ResilienceTec](#) has been designed so organisations can create an emergency response plan with minimal effort, however time will still need to be allocated to collect organisation specific information and consider contingency scenarios. The content has been compartmentalised into sections so organisations can incrementally create their emergency response plans over time.

### *Planning for a worst-case scenario*

When creating your contingency plans a practical approach is to assume the worst case scenario, including:

- loss of access to the organisational facilities, loss of equipment and loss of supplies
- loss of IT and communications
- loss of skilled or key staff who perform critical functions.

Your contingency plans will focus on restoring critical functions and may include:

- moving staff or operations to an alternate location
- moving to back up or manual systems
- using alternative resources
- replacing equipment and repairing the organisation
- returning to the organisation as soon as practicable.

### *Who has Access to Your Emergency Response Plan*

Your emergency response plan is only accessible to the person/s with access to the secure login. Once you have been issued with a username and chosen a password, you become responsible for their security and for any use of [ResilienceTec](#) conducted through them.

Your emergency response plan is protected by [ResilienceTec's](#) secure network. If you contact [ResilienceTec](#) requesting assistance, they will be able to access your plan to assist.

# General Instructions for Using the Online Tool

## Logging in

1. Go to <https://www.frank.resiliencetec.com/sign-in> and click sign in.
2. Enter your username and password.

## Forgotten Password

1. Go to <https://www.frank.resiliencetec.com> and click "Forgot your password".
2. Enter your email address or username and you will be sent an email to reset your password.

## Creating or Editing your Emergency Response Plan

1. If you are creating your emergency response plan for the first time:
  - i. Click on [add plan](#), in your business home page, to create a plan for your organisation
  - ii. Enter your organisation name, ensure correct spelling and capitalisation as this name will autofill throughout your plan.
  - iii. Accept the terms and conditions. Otherwise you will be unable to use the tool. To see detailed information click on the blue "Emergency Response Planning Website terms and conditions"
  - iv. You will then navigate to your area home page. To begin entering information click on the [Start your response plan](#) button. After your first visit this will read, [Edit your response plan](#).
2. You can take as many sessions as you like to complete your plan, you need not do it in one sitting.
3. You must complete Section 1. The completion of other sections and subsections within your plan are optional. Select the sections and subsections that reflect the size and need of your organisation.

## Entering Information

**You must complete Section 1 first as this contains essential information about your organisation.** This information will populate other fields throughout your plan.

You are able to edit and publish the content in your emergency response plan at any time. Try to be consistent with the names and titles of staff members so they are easily identified.

- Each section is presented with various numbered sub sections.
- Text that is unable to be altered or deleted is black.
- Tan coloured boxes are for contacts and will auto fill into other parts of your plan.

- Computer Hardware Maintenance Providers:

Infomatrix
Phone 09 570 2400

Input text in the pale grey boxes.

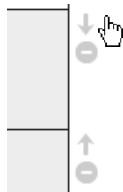
- Some of the pale grey boxes contain template examples that can be edited.
- When you click on this text it will turn dark grey to indicate that it will appear in your PUBLISHED PLAN.
- If the information is not relevant to your organisation, delete it and enter your organisation information.

Incoming calls will be transferred to alternative fixed line/mobile connections as follows: ↓

- To add additional rows of information click:



- To reorder rows of information, use the up or down arrows:



- To delete entire rows click on the minus button at the end of the row and the text will grey out and a grey line will appear through the text. To undelete entire rows, click on the minus and the text will reappear.

Check availability of mobile phone chargers -

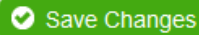
Check availability of mobile phone chargers

- To switch on paragraphs that are relevant to your organisation, select the tick box next to the heading. If you do not tick the box, they will not appear in the printed version of your plan. To switch them off again, un-tick the box

Our Practice has a Back up Power Generator Installed

The following actions are required to start the generator and switch over to alternative supply lines:

- Click the “Save Changes” button at the bottom of the page to save your plan as you create it:



## To Include a Section in your Plan

- When you have completed a section, tick “Section is complete”



- Completed sections will appear in the menu on the left with a green tick next to them, as you can see below.

## Emergency Response Plan

2. Key Contact Information ✓
3. Loss of Power Supply to the Practice ✓

- Only sections marked as complete will appear in your published emergency response plan.

## Printing a Draft Section of your Emergency Response Plan

If you wish to review a section you have completed in your emergency response plan you can click on “Print Section”.



However, this is not how you create your completed response plan, to do this follow the instructions below.



## Publishing and Printing your Emergency Response Plan

- You may publish your plan at any time, irrespective of how many sections you have completed or partially completed. Only sections where you have ticked “Section is complete” will appear in your published plan.
- The yellow boxes prompting you to enter information will not appear in your printed plan.
- Click on “Publish” follow the instructions.



- Click “Download & Print” and a PDF copy of your plan will open. Your most recently published plan will appear at the top of your list of Published Response Plans on your homepage. Each version is given a number.

## Published Response Plans

Version	Date Published	
8	Wednesday, January 30th 2019, 7:11:20 pm	
7	Wednesday, January 16th 2019, 12:08:27 pm	

- You may republish your plan as often as you wish.

## Duplicating your Plan

If your business has multiple organisations, many of the details are likely to be the same. To save time you can create an emergency response plan for one of the organisations and duplicate it. You can then edit this new duplicated plan.

### Duplicate

Click "Create duplicate plan" to create a new plan for another facility but containing the same information as an existing plan that you have already set up. You can then edit this new plan with information specific for that facility.

Create duplicate plan

## Uploading other Planning Documents

Any existing documents such as fire evacuation plans, pre-planned ordering lists or other documents related to emergency response planning can be uploaded into the Documents Section on the first page when you login.

### Documents

Upload a new document for this plan:

Upload

## Reviewing the plan

### Review

Review and monitor your plan on a quarterly basis. Information sourced in the preliminary research will change regularly, so it is crucial that the information in the plan remain current and up to date. Emergency response plans should be fluid and revised when needed to reflect changes in emergency management processes and incorporate learning from past events.



## Section Guide

### Section 1: Information about the Organisation, Staff and Activating the Response Plan

#### *Single Point of Contact*

It is important to have a single point of contact in which all communications are routed. This ensures consistency of messages to external organisations and that all incoming messages are received and shared with the correct people. Communications via this contact can be monitored and logged during an emergency event.

The use of a mobile phone for the single point of contact offers greater flexibility during an event, as they can remain with the emergency coordinator and can easily be handed over to a deputy. The person minding the single point of contact phone should also have access to email, landline phone and fax. The single point of access email address should be generic e.g. SPOC@....

#### *Location of the Emergency Response Plans*

Your emergency coordinator will need access to your emergency response plan at work and at home. Keep the latest version of your plan in an easily accessible place. All staff should be familiar with your emergency response plan and response process.

#### *Emergency Instructions*

On page 2 of your emergency response plan there are basic “What to do” instructions for staff to first consider, and then contact the emergency coordinator or to raise the alarm.

#### *Information about Staff*

The tool prompts you to enter information that will assist in managing staff during an event. These entries will print as a table and staff will be grouped by professional role.

- The travel time to work will assist in choosing staff who can respond most promptly.
- Record home suburb to assist with carpooling.
- Use the ordering arrows to determine the order of staff in the call-in tree.

## Activating the Response Plan

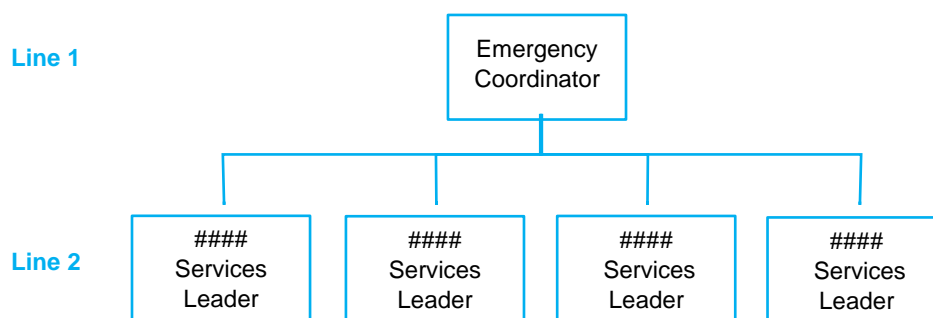
Your emergency coordinator will activate your emergency response plan during an event, if required.

#### *The Telephone Call-in Tree*

The telephone call-in tree determines the order in which you call in staff to restore business processes and service provision if an event occurs.

When setting up your telephone call-in tree:

- the second line of your tree should include senior staff, particularly leaders in business or service provision
- ensure that your emergency coordinator has a documented deputy
- the call-in tree is to bring key staff into work during an event, if you have a very large organisation you may not wish to list all staff. However, you are not limited to two rows, the below diagram is just an example of layout.



## Section 2: Premises information

This section gives you the opportunity to upload site and evacuation maps, list your evacuation plan, outline your greater responsibilities in an emergency for example some organisations are host welfare centres in a declared emergency. Lastly you need to detail your post emergency checklists (re-entering buildings and auditing response against the policies).

When uploading your maps please use a jpeg or PDF format.

## Section 3: Key contact information– Support Agencies & Services Providers

### *Emergency Support Agencies*

Enter the contact details of your local emergency support agencies.

- Police / Fire / Ambulance
- Council
- Hospital
- Coastguard

### *Service Providers*

List of all your service providers, contact details and account numbers. During an event being able to quickly access this list will enable you to communicate your situation quickly to the appropriate organisation and set the recovery process in motion. When you fill in these providers information will pre populate through into other areas of your plan so you do not have to re-enter information.

## Section 4: Risk Identification and Reduction

Use this section to formally identify your risks. Ask different groups/departments within the organisation to identify their specific risks.

For each identified risk a likelihood and consequence value needs to be identified from the drop down menu.

You will also need to identify activities around,

- Preparedness
- Response and
- Recovery

This identification is crucial as the rest of you planning will flow from it.

## Section 5: Specific Planning Activities

In this section you can plan specific response actions for your organisation against specific risks, such as,

- Fire
- Earthquake
- Tsunami
- Flooding/Storm/Severe Weather/Tornado
- Hazardous Substances
- Suspicious Letter or Package
- Bomb Threat
- Violent or Armed Intruder
- Serious Injury or Death on Site

None of these sections are compulsory and can be included or not, using the check box.

## Section 6: Loss of Power Supply to the Organisation

Power supplies to organisations may be disrupted in the event of a disaster. Some may even have a total loss of power for some time. Disruption to the power supply will affect many of the organisation's appliances and systems. Consideration of how computer systems, telephone systems, automatic doors, heating and cooling systems and lighting will be affected is key to disaster planning.

### *Lighting*

Battery-powered emergency lighting to highlight exit routes is a mandatory requirement for facilities accessed by the public. However, this lighting will likely not be sufficient for all rooms and parts of the organisation if there is a disruption

to the power supply. Therefore, for safety purposes, ensure that staff have easy access to the emergency kit and additional torches, including a well-stocked supply of batteries.

Organisations may also wish to consider purchasing wind-up or solar dynamo torches that can also be used to charge mobile phones.

### *Uninterruptable Power Supply (UPS)*

The majority of organisations will have an uninterruptable power supply (UPS) installed, which is designed to protect the computer server for a short period of time in the event of a power outage. UPS are usually not intended to be used for long periods of operation. However, if this is a significant concern, it may be worth considering increasing the capacity of the power supply during emergency preparations. Refer to the use of power generators.

### *Computer Systems*

If computer servers are not shut down properly during a power outage, they can incur significant damage. Most organisations should have a UPS, which continues to deliver power to the organisation's main server to allow time for computers to be shut down correctly and/or initiate a forced shutdown of the system.

### *Telecommunications*

Switchboard telephone systems are generally reliant on electricity. See Section 8 for Disruption of Telecommunications.

### *Power Generators*

Diesel or petrol generators can provide the organisation with power if power supplies are disrupted. Generators can be used for back-up lighting, computer systems and other appliances in specific areas. Used in conjunction with a UPS, power generators can ensure that clean power is delivered to sensitive equipment such as computers and medical equipment.

Organisations may wish to consider the feasibility of hiring or purchasing back-up power generators as part of the emergency response planning process. Reserving a generator in the event of an emergency may involve an annual reservation fee to ensure that the organisation is given priority during significant demand.

Even if you do not reserve a generator you should do the following in preparation of ever needing to do so.

- Establish what critical equipment you will need to run during an extended power cut. This should include staff amenities, such as fridge, kettle and microwave.
- Contact an electrician/electrical engineer to calculate what size generator you will need. If you are running a server from this power source please ensure that you inform the person you are talking to as this will inform the type of generator you use.
- Contact your local supplier of generators and store their contact details in your emergency plan

### *Internal Faults*

If a loss of power occurs due to a fault within the facility, you will need to contact your electrician to repair the fault.

Electrical safety may be compromised by internal faults or damage. Contact your electrician quickly so you can switch off sensitive equipment manually and isolate affected areas of your switchboard.

## Section 7: Disruption of Water or Gas Supply to the Organisation

### *Disruption to Water Supply*

In a disaster, organisations may experience disruptions to their water supply. Disasters can damage water pipes; affect local water supplies, which may become contaminated; or even completely cut off.

It is crucial that staff know where the water mains is located and how to turn it off. The location of the water mains should be highlighted on the organisation map.

Organisations should consider keeping a well-stocked supply of bottled water and alcohol sanitizer in the event that the local water supply is contaminated. Bottled water can be stored in the emergency kit. Arrangements for boiling and storing water for additional supplies should also be considered during the disaster planning process.

If there is damage to the water pipes and flooding results, staff will need to shut off the mains water supply to the organisation.

### *Disruption to Gas Supply*

Faulty supply lines, valves or appliances are potentially hazardous and require an evacuation of premises. Contact emergency services and do not switch any electrical appliances on or off as this could create a spark and an explosion.

If you have a loss of gas supply and use gas for heating, consider keeping some electrical heaters in storage. If you use gas for water heating, put up notices for staff and patients to conserve hot water supplies.

## Section 8: Disruption to Telecommunications Systems

Communication systems such as telephone lines and the internet can be affected during a disaster. Disruptions to communication channels can have a significant impact on the organisation's overall business operations. Given this, a well-thought-out contingency plan is key to the organisation's overall emergency response and should involve as many different communication channels as possible.

### Telephones

Emergencies will affect phone systems in different ways, so it is important to ensure that there are multiple options available in the event of a disaster (e.g. a landline phone if mobile towers are affected). Mobile phones can be overwhelmed during an emergency and should not be solely relied upon.

In situations where mobile phone communication is down, it is recommended that analogue phones be used by the organisation. An analogue phone is one which draws power from the telephone lines and does not require a separate power source.

Purchase, or reserve if available, an analogue phone and store the unit in the emergency kit to ensure easy access for all staff. Training on how to divert phone calls, in the event of an emergency, should also be provided to relevant staff.

In the event that communication lines (landlines) are affected, it is likely that mobile phones will be utilised in an emergency. In this instance, the organisation's landline can be diverted to a mobile number to ensure business continuity. Ensure that this phone is used for essential calls only and text or sms messaging is used wherever possible.

### Internet

Communication via the internet may also be impacted during a disaster. Programs which rely on internet connection may go down.

By keeping a hard copy of this plan available both on and off site you may be able to make important communications via mobiles phones.

Organisations may consider investing in alternative internet connection to ensure ongoing access to the internet during a disaster. Alternative options include mobile data devices, dial-up modems and satellite dishes. Organisations need to also consider alternative ways for conducting business if there is a loss of internet access, such as having cash transactions and manual swipe machines (for credit cards) stored in the emergency kit.

Depending on the emergency, the organisation should be able to employ a range of strategies (as listed above, including both alternative electronic devices and manual hard copies) to continue functioning in some capacity.

### Radio

Where all other communication lines are down, a battery-powered radio can be used as a reliable means of receiving important information regarding an emergency. Organisations should purchase a battery-powered radio, with a supply of batteries, and place it in the emergency kit. Staff can tune it to a local station for up-to-date information regarding emergencies affecting their area.

## Section 9: Loss of IT Systems or Data

Organisations are becoming increasingly reliant on computer software and IT systems. When affected by disasters the risk of having computer hardware, software programs and IT systems damaged, including organisation management software increases dramatically.

### Hardware

During the disaster planning process, it is important to take a stock of all hardware and equipment. In the event that all of the hardware is destroyed or completely damaged, staff will be able to access a comprehensive list of what needs to be replaced. This list can be used as part of the organisation's asset register.

For those leasing computers and hardware, it is important to get in contact with the leasing company as soon as practicable to discuss the damage and the process involved in replacing items.

If equipment/computers in the organisation have been damaged as a result of a disaster, first determine the operational status of equipment (for safety purposes, organisations may need to seek advice from a professional) and then transfer any equipment and computers that have not been damaged to a safe operational area within the organisation so they are protected.

After an emergency, access to computers may be limited to those not damaged (if any). However, if the server is damaged or corrupted, other desktop computers will not be able to access information and/or programs from the network.

Organisations should consider having at least one laptop with a long battery life with current organisation data stored on it, or at least ensure access to the previous day's back-up (whether physical or on a secure cloud). With the correct connections, laptops can also be charged from cars.

It is important that organisations have suitable media reading devices to effectively restore data when IT systems are affected.

### Software and Applications

Software and access codes should be stored in a safe place (such as a fireproof box or secure online storage) so they can be easily accessed in the event they need to be reinstalled. It is also recommended that a list of all software and access codes be created and maintained, including software support phone numbers. This list can be used to become part of the organisation's asset register.

If software and applications do not work due to server damage, the organisation will need to seek assistance from an experienced IT technician, who will need to reinstall them. Software is generally stored on a disk or is downloadable from the vendor's website. When first purchased, software is either registered to the organisation or to an individual working within the organisation.

### Loss of data

In the general organisation setting, data protection is key to effective business continuity. While the majority of organisations have back-up procedures in place to protect data in the event of computer damage and data corruption, information management and information technology should always be considered as a high priority in emergency response planning.

Quality standards may well require storing critical and current information off site as part of high-quality back-up systems for information technology. As a minimum, organisations should be performing daily back-ups of all data (including email, shared documents, network file and databases and clinical and organisation software). It is also important to ensure that the daily back-ups are verified. When a threat of a disaster is imminent, organisations should keep a hard copy list of appointments (patients seen) to enable records to be recreated.

Advanced planning of IT will make the recovery phase significantly easier and faster. Organisations are advised to test their restore procedures regularly. Organisations should consider contacting software vendors for product-specific recommendations regarding restoration processes and checking data integrity.

Organisations should also perform a recovery on a regular basis (dependant on the risk assessed by the individual organisation) to ensure that recovery methods are working and appropriate for the organisation. This can be coupled with a test plan to verify data integrity (e.g. searching for patient X to confirm their history and demographics are correct as documented in the test plan).

When implementing data protection measures in the organisation, consider the data stored on desktop computers, as not all applications are connected to the server and therefore are not necessarily backed up daily. It is important to conduct regular audits on desktop computers/workstations to ascertain what data is being stored on local drives.

### New - Section 9a. Cyber Security Policy

Sections 9.a and 9.b are brand new sections. These sections deal with the growing threat of cyber attacks both malicious and accidental or human error.

Section 9.a enables an organisation to develop their own cyber security policy. This section is self explanatory and has similar functionality to the rest of ResilienceTec. It includes:

Incident response policy

Password policy

Network security policy

Network access policy

Back-up policy

Wireless access policy

Email policy

Payment policy

Confidential data policy

Mobile device policy

Data break policy with links to the respective agencies in NZ and Australia

Cyber insurance policy

Cyber staff training

Staff exit policy

Don't forget to turn on each applicable section by ticking the box at the top and then any additional boxes required.

9a.2

Network and Computer Security

Restricted Admin Privileges

This includes users who have accounts to configure systems or access sensitive information, across the entire organisation... [More](#)

• Our organisation has restricted admin privileges and we review access every 6 months.
• They are only used to perform admin tasks.
• All privileged admin accounts have an audit history.

+ Add Row

Don't forget Under each section if you require more space to add additional parameters you can add a box by clicking



## Section 9.b Cyber Security Response

This includes:

- 1) Incident response plan with a detailed list of possible events and how to respond to these should they occur.
- 2) Cyber insurance response. If your organisation carries cyber insurance and an event occurs the first organisation to call is your cyber insurance provider, as typically they will work with you and guide you through what to do.

## Section 10: Loss of Business Records

A business record is any hard copy (printed) information required for preserving, continuing or reconstructing the organisation operations. In a loss situation, documents that only exist in hard copy format would need to be re-created or duplicates obtained. The ease with which you are able to retrieve copies can speed the process back to normal operations.

This section asks you to identify important print records/documents and identify arrangement for copies to be held offsite or scanned and stored electronically. Your electronic data however must be backed up (see Section 6)

Business records, however they are stored, must be kept current. Assign responsibility to a staff member for the currency and safe keeping of business records. In your storage and retrieval instructions, ensure security of those documents which are confidential to the business or are person sensitive, and include restricted access arrangements.

### Paper Records

While organisations can undertake a range of activities to minimise the overall damage caused to the organisation in the event of an emergency, paper records can be damaged irrespective of the protective measures employed.

During disaster planning and preparations, it is worth noting who the paper records recovery specialists in your area are, in the key contacts section.

## Section 11: Complete or Partial Loss of the Organisation Premises

Disasters can cause significant damage to a building's infrastructure, causing it to be uninhabitable and unsafe. If a organisation's infrastructure is damaged as a result of a disaster, it may be necessary for part or all of the operational activities of the organisation to be shifted to a temporary location.

Therefore, when preparing the organisation for a disaster, it is worth considering how the organisation will continue providing its essential services if it is affected. If it is determined that the organisation will continue to provide services, then an appropriate and safe location for the temporary organisation will need to be identified.

To facilitate this process, organisations are encouraged to enter discussions with other business owners who could allow your organisation to temporarily locate in their building. Other possible venues might include community halls, schools or vacant shops. These discussions will need to occur as part of the planning process and before an event. If an agreement is made, it should be documented and communicated to both parties.

Staff need to be made aware of any arrangements, so that if the organisation is affected and the emergency response plan is activated, staff can begin to make the appropriate arrangements to inform clients or others associated with the organisation of the temporary location.

While undertaking the preparations to set up a temporary organisation, it is important to have a printed copy of the organisation's emergency response plan including lists of key equipment and supplies that are required to run the organisation.

### *Re-entering a Building after a Disaster*

As part of planning preparations, staff should be made aware that re-entering a building after a disaster can be extremely hazardous.

Before anyone re-enters the organisation, the emergency management coordinator should seek professional advice from either a building engineer or a responsible member of the emergency response team about when it is safe to re-enter the building.

## Section 12: Medical Supplies, Equipment and Furniture

Any business regardless of its type will have equipment that is crucial to the delivery of its services. Disasters can have devastating effects on the organisation's infrastructure, including all of its contents.

As part of the emergency response planning process, organisations are advised to keep a log of all equipment and supplies in the organisation. In the event that some or all of the contents are destroyed, staff can quickly assess what equipment and supplies have been lost or damaged and what requires replacing. Both electronic and hard copies of this list should be created and maintained.

## Section 13: Unique Identifier and Contract Numbers

Authorisation codes to provide access to secure systems and processes need to be captured to enable appropriate access in an emergency or to re-establish business processes after an event.

**ResilienceTec** allows you to record unique identifiers, contract numbers and access codes for the organisation and members of staff.

### *Keeping Sensitive Information Private*

Any information that is business sensitive and that you DO NOT want to appear in your printed emergency response plan, you can enter into the table at the bottom of Section 13 "Secure Information". This information will remain online and will only be available to the staff you have given login access to your online emergency response plan.

In this area you may wish to store entry codes for safes, disarm codes for alarms or personal bank account details of business partners.

## Section 14: Communication during an Emergency Response

The majority of local councils now have well-developed messaging services to notify residents and individuals of potential and/or imminent disasters. It is recommended that the emergency management coordinator register for any service via their local council or local emergency service. This is also true of meteorological services.

The emergency coordinator should be responsible for activating the communication tree as described earlier, which will ensure that all staff are informed of a looming disaster.

In the event of an emergency, the emergency coordinator should organise for phone calls to be diverted to an analogue, non-powered phone (or mobile if still operational) with a recorded message regarding the organisation's status and hours of operation, as well as any relevant advice to customers/ others associated with the organisation. If the organisation has a website or uses social media, information regarding its operation should also be updated by the emergency management coordinator and/or relevant IT support staff.

### *Clients*

Clients or others associated with the organisation with active appointments/orders/contracts will need to be urgently contacted. Alternative arrangements will need to be put in place for those needing urgent attention. If the organisation is likely to be disrupted for an extended period of time this will need to be communicated to ensure everyone knows how to access alternative services.

### *Media Policy*

Ensure your organisation has a media policy in place – who may or may not respond to media request for interviews and comments.

## Section 15: Insurance

Building, contents and business insurance are essential for any business.

During the disaster planning process, it is recommended that insurance policies for the organisation are reviewed regularly to ensure adequate coverage for the organisation.

To ensure adequate coverage, it is important that the policy covers:

- all natural and man-made disasters
- extensive damage and total loss of the building
- the entire contents of the building, including loss and damage to equipment and supplies
- costs associated with interruption to the business (may include staff pay and loss of revenue) – may trigger a higher premium
- costs associated with relocating to a temporary facility – may trigger a higher premium.

Information such as name of insurer, policy number, type of insurance, coverage and relevant claims telephone numbers should be included.

## Section 16: Loss of or Non-availability of Key Staff

In an emergency, many organisations may find that they have a significant reduction in staffing capacity and therefore cannot provide the same level of service. In a pandemic, there may be unexpected multiple staff absences: staff members may be sick, they may have to care for sick family members, they may be pregnant or they may have regular contact with someone who is terminally ill and cannot risk cross-infection. Staff affected by other disasters may also be absent for similar reasons.

Organisations are advised to consider how they will continue operating with a reduction in key staff. One way to help alleviate staffing issues is to provide staff with education and training in other roles (where a similar level of expertise is required) within the organisation.

Organisations may also wish to contact others nearby to ascertain if they have capacity to provide some staff for a short period of time. Organisations in close proximity may wish to consider pooling staff and resources in an emergency.

### *Accessing Computer Applications and Secure Data:*

Ensure that login details to access applications or data is either known by another person or recorded and stored in an accessible location (hard or soft copy). Ensure these details are kept updated.

### *Physical Access to Buildings, Secure Storage Areas:*

Unique keypad codes, security cards or key access to secure areas should be either held by 2 or more people or copies stored in an accessible location.

### *Virtual Working:*

Depending on a staff member's role, they may be able to work from home. This is easier done if your server and/or email and applications are hosted in the cloud (web based). Staff will need remote access to networks or a computer (laptop, desktop or tablet) loaded with appropriate data and applications.



## Section 17: Business Continuity Plan

A Business Continuity Plan (BCP) is a tool that your business uses to create a roadmap to recovery. While the above sections look at immediate response to an effect of an event, the BCP looks beyond the initial response.

Firstly any processes involved in your business (payroll, suppliers, IT, equipment) are listed and then set into order of priority. This means that the items at the top of the list are the critical processes that your business needs to get back up and running as soon as possible. Items at the bottom can wait longer. A Maximum Permissible Outage Time is established. This is the amount of time that you are able to have the function inactive, it also sets targets for the renewal of the function.

Having done this you will need to fill in the other rows which look at what is required to re-establish the function.

## Section 18: Impact on Business of an Infectious Event

Any large scale infectious event across a geographical area has the capacity to disrupt your business. This includes disease like measles (There have been outbreaks across New Zealand and Australia over the last few years) or pandemics (most recently 2009 H1N1).

Using this section you can look at how you will coordinate your business with a leadership position, it is also helpful to try to examine and record what the roles and responsibilities of this position will be.

Rostering during an event may be a problem as staff may be sick themselves, looking after sick family members or unable to get to work. Therefore a series of questions is developed to assess staff willingness and ability to work during an event.

In the case of pandemic influenza it may be worth offering the flu jab to your staff, free. In this instance record who has and who has not had the flu jab.

Due to their nature infectious events mean that infection prevention and control and cleaning become of critical importance. This section allows you to establish what are your risks and cleaning policies. In all probability you will need to complete this when the event is underway or in the lead up to the event as information about the infection becomes available. It may be possible to identify some areas now and this should be undertaken.