Small business disaster hub

Prevent - Prepare - Respond - Recover - Communicate

All small businesses' checklists

Australian Government

This initiative is jointly funded by the Commonwealth and Queensland Governments under the Disaster Recovery Funding Arrangements (DRFA).

Queensland Government

Contents

All small businesses checklists

In a disaster or emergency it can be difficult to know what to do first and where to turn to for help. The Small business disaster hub can help you manage a range of disasters and emergencies and get back to business sooner.

Use these resources to learn how to prevent, prepare, respond, recover and communicate when disaster strikes. Remember that no one can do it alone and help is always available.

We've outlined 4 stages to help your business manage a disaster or emergency:

- prevent and prepare
- respond
- recover
- communicate

The Small business disaster hub includes checklists for several small business sectors. This document includes checklists that can apply to all small businesses.

How to use this document

1. Save this document on your computer desktop so you can access it if the internet is offline.
2. Select the links on the contents page or use the prevent, prepare, respond, recover and communicate links above to learn how to manage a disaster.
3. For a quick outline of how to manage a disaster see the top 10 tips. Select any of the numbered tips for more detail.

More information

For more information on the tips outlined in this document, visit the Small business disaster hub at business.qld.gov.au/disasterhub

Download the Small business disaster hub app for Apple or Android, or use the QR codes below, to access this information offline and receive relevant alerts.

Download from App Store

Download from Google Play

Return to contents page

Types of disasters and emergencies

Natural disasters

- Cyclone and storm surge
- Severe storm
- Flood
- Bushfire
- Drought

Major health event

- Pandemics (e.g. coronavirus (COVID-19), human influenza)
- Epidemics (e.g. mosquito borne diseases such as dengue virus, malaria)
- Localised outbreaks (e.g. Legionnaires' disease, diseases from animal contact)
- Food poisoning or contamination (e.g. Campylobacter, Salmonella)
- Medical event or serious injury (e.g. serious injury, death).

Emergency

- Biosecurity threats (pest and animal disease outbreaks)
- Workplace accidents or deaths
- Dangerous material spills, leaks or explosions
- Loss of power or infrastructure
- Major transport disasters
- Terrorist or major criminal incidents
- Climate change risks

Information technology (IT) threat

- Cyber-attack
- Data hacking
- IT failure

Reputational incident

- Highly negative media or social media coverage
- Rumour-driven crisis
- Inappropriate workplace behaviour (e.g. bullying, harassment)
- Organisational misdeeds and legal action (e.g. fraud, theft)

Return to contents page

Top 10 tips

How to manage a disaster or emergency

1 Make a plan
Identify your risks and plan what you will do, including evacuation plans

2 Review insurances, policies and finances
Check your insurance and finances are adequate to cover your business

3 Prepare your business
Prepare your premises – clear vegetation and loose items, back up data and pack emergency kit

4 Plan for alternatives
Plan for power outages, loss of deliveries, access and alternate ways to operate

5 Monitor the incident
Listen to emergency alerts, know where to shelter or evacuate and follow advice

6 Assess impact on your business
When safe to return, assess and photograph the damage and contact your insurer and bank

7 Connect
Connect and communicate with staff, customers, guests and community

8 Financial recovery
Apply for financial assistance and other business support

9 Communicate and promote
Develop marketing strategies to communicate with customers and promote positive news or deals

10 Recovery planning
Consider what you've learned and update policies, plans and staff training

Return to contents page

Prevent and prepare

Consider what actions you can take to prevent or reduce the likely effects of an incident and prepare steps to plan for, respond to and recover from unavoidable events.

Make a plan

☐ **Prepare a business continuity plan**

Develop a business continuity plan to help you prevent risks, prepare for potential impacts, respond to and recover from a disaster or emergency.

Steps to include in your plan:

- identify key events, emergencies and risks most likely and that would have the most negative impact on your business
- prepare a risk management plan for how to respond to key risks and incidents
- create or review business policies, procedures and standards
- check you are meeting your workplace health and safety obligations including laws, regulations and codes of practice
- identify staff roles and responsibilities in an emergency and share team contact details
- identify and record customer, supplier, insurer and emergency contacts
- identify and record local emergency alerts and warnings and update channels
- create an emergency evacuation plan and procedures (e.g. identify assembly points, assign roles such as first aid officers, shutting down operations)
- conduct regular emergency drills with staff/visitors/customers/guests and document in your emergency plan
- create an event log to record information, decisions, actions, and before and after damage photos for insurance purposes
- create a recovery plan to document what steps to take after an incident.

☐ **Develop a communication plan**

Prepare a communication plan or marketing plan to help you know what to say and when, include:

- who is responsible for speaking to the media and managing social media
- social media and media guidelines
- messaging to handle disasters and emergencies.
- consider developing a digital strategy (website, social media and advertising) to promote your business after an event.

Return to contents page

Prepare your business

☐ Review insurances, policies and finances

- Check insurances are up to date and adequately cover your business, assets and any rebuilds or repairs that may be required.
- Photograph equipment or assets to show pre-event condition.
- Review and document how you will manage orders and cancellations.
- Check you have financial reserves and emergency cash on hand.

☐ Plan alternatives for loss of power, access, communication and operations

- Plan for extended power outages – get a generator and fuel.
- Plan and document how to prepare for supply chain disruptions.
- Ensure you have enough stock, supplies or spare parts in case you're cut off.
- Identify alternative off-site locations to operate from.
- Plan for flexible staffing arrangements (e.g. work from home, online meetings)
- Review ordering, booking and cancellation policies, including goodwill measures such as refunds.

☐ Back up data and secure documents

- Back up your data and store off-site or use cloud storage.
- Save digital copies of key business documents (e.g. insurance, business registration, property deeds, key contracts, licences, certificates, awards).

Pack an emergency kit

☐ Equipment

- First aid kit – check contents are current and complete
- Personal protective equipment (PPE) e.g. masks, gloves, safety glasses, hand antiseptic, disinfectant
- Radio – portable battery powered
- Torches and batteries
- Spare batteries, power boards and power banks
- USB memory sticks/flash drives
- Computer storage (portable hard drives/data storage, back-up tapes, discs)
- Digital and printed business documents
- Spare keys and security codes
- Mobile phone and chargers (portable and car)
- Marker pens (for temporary signs) and general stationery
- Hazard tape
- Plastic sheeting and waterproof bags for valuables
- Utility knife
- Tie down straps and rope

☐ On the day

- Cash
- Keys for buildings, vehicles and equipment
- Important or valuable equipment that is easily moved
- List of visitors or customers (on premises or expected) and contact details

Prevent and prepare for specific risks

Natural disaster prevention and preparation

☐ **Cyclone, severe storms and floods**

- Search the coastal hazard property map for business property risks.
- Check emergency alerts and contacts for Queensland businesses.
- Check with your local council to access:
  - flood plans or records to see if your business could be affected and what the impact might be
  - local flood arrangements for your area
  - local disaster updates.
- Check if your building meets cyclone standards (properties built after mid-1980s should withstand cyclonic winds).
  - If not up to standard, consider how to protect or temporarily relocate your business.
- Clear gutters, check wiring, smoke and fire alarms etc.
- Clear loose equipment and vegetation around your premises. Learn how to clear vegetation before and after a natural disaster.
- Plan for any staff, customers or others remaining on your premises so they are fully informed and have access to first aid and emergency supplies.
- Identify where to relocate stock, equipment and vehicles.
- Store hazardous materials safely above ground level or off-site in case of flooding.
- Sandbag your premises for flooding (if applicable).
- Secure doors and windows (e.g. use shutters, metal screens, tape on glass).
- Check Queensland weather warnings and current tropical cyclone updates from the Bureau of Meteorology (BOM).
- Visit your local council for local disaster updates.

☐ Bushfires

To prepare for a fire:

- install fire protection equipment appropriate for your workplace (e.g. foam or dry powder extinguishers for flammable liquids)
- maintain fire equipment, including regular checks and tests by the supplier, with maintenance contracts in place
- train staff to use fire extinguishers and fire hoses (if required)
- have a written emergency evacuation plan in place and ensure staff know their roles and responsibilities.

To prepare for a bushfire:

- clear gutters, loose equipment and vegetation around buildings and access points
- form a firebreak around your buildings (cut grass, trim vegetation clear of building and clear gutters)
- fit wire screens to doors, windows and vents, and enclose all gaps (if applicable)
- store flammable materials such as wood, gas, petrol and paint well clear of buildings
- keep ladders available for roof access (inside and out)
- fit hoses to reach all parts of the building and gardens (if mains pressure water not connected, get a high-pressure pump)
- read bushfire alerts and information from Queensland Fire and Emergency Services
- visit the Rural Fire Service to:
  - subscribe to bushfire map and warnings
  - learn how to prepare for bushfire season
- learn how to clear vegetation before and after a natural disaster for fire management
- visit your local council website for local disaster updates
- find state disaster, emergency alerts and contacts for Queensland businesses.

☐ Drought

Include specific drought preparation steps in your response plans:

- devise an action plan for maintaining, using and reviewing all water resource supplies
- check with local industry networks and authorities for drought planning guidelines or requirements when developing your plan
- contact local authorities to obtain specific information to help develop drought management strategies for your business
- assemble facts about rainfall records (you can use a combination of official records and local experience)
- identify alternate water supplies, consider using non-potable water
- regularly maintain your water consumption sources (e.g. install water-efficient nozzles on taps, check for leaks)
- regularly maintain equipment that uses water
- introduce water saving measures in your workplace.

Plan for heatwaves:

- Advise workers, guests and customers on how to prepare for a heatwave and how to avoid heat stress.
- Visit WorkSafe Queensland for more information on how to protect workers from heat stress and use the heat stress calculator to predict the risk of heat-induced illness and find out how to prevent it.

If water restrictions are declared impacting your business:

- check with your local council to learn about current water restrictions, guidelines and compliance requirements
- use the water restrictions preparation checklist
- install water-efficient appliances or fittings and check for leaks
- introduce water-efficient procedures for your business operations and staff
- educate and train staff about the importance of water efficiency and its benefits to the business.

Go to respond to natural disasters ›

Major health event prevention and preparation

☐ **Coronavirus (COVID-19)**

- Read about COVID-19 plans to find out what kind of plan or checklist you need.
- Keep up to date by checking the current business restrictions for COVID-19.

☐ **Pandemic or influenza**

Pandemic prevention and preparation

- Read about pandemic risk management for business.

Influenza prevention and preparation

- Find flu prevention resources to help prevent influenza spreading.
- Read more about human influenza and influenza pandemics.

☐ **Mosquito borne disease**

- To prevent or reduce the risk of mosquito borne diseases in your premises or property:
  - regularly check for potential breeding sites (PDF, 1.5MB) and empty outside containers capable of storing water
  - provide insect repellent and long-sleeved clothing for staff and customers
  - advise staff and customers about how to avoid mosquito bites.
- Find out about preventing the spread of mosquito borne diseases.

☐ **Legionnaires' disease**

- Learn about Legionnaires' disease – caused by the Legionella bacteria and can be found in equipment with water (e.g. air conditioning, pools and spas, misting systems).
- Read the Legionella guidelines and resources from Queensland Health to help you minimise the risk.

☐ **Diseases passed from animals**

- Read the disease prevention in animal contact areas guidelines and resources from Queensland Health.
- Read how to prevent illness in animal contact areas.

☐ **Food poisoning or contamination**

- If you handle or sell food, you must comply with food and beverage industry regulations.
- Read Queensland Health's:
  - Know your food business booklet (PDF, 1MB) to assess your food safety practices and requirements
  - food safety resources for information about safe food storage, preparation and regulations.
- Visit Safe Food Queensland for mandatory food safety accreditation, advice and notification requirements.

☐ **Serious injury or illness, death or dangerous incident**

- For more information, go to workplace accidents or deaths in this document.

Go to respond for major health events ›

Emergency prevention and preparation

☐ **Biosecurity threats (pest and animal disease outbreaks)**

- Learn how to protect your business from Biosecurity Queensland.
- Develop a biosecurity management plan using the template from Animal Health Australia.
- Read how to upgrade your biosecurity management plan checklist.
- Read more about what to do during a pest or disease outbreak.

☐ Workplace accidents or deaths

- Visit WorkSafe Queensland for information and resources to keep your workplace safe, including:
  - first aid and emergency plans
  - what to do in an emergency
  - incidents and notifications
  - hazard identification checklist (PDF, 32KB)
  - safety and prevention tools and templates
  - mental health and wellbeing
  - business and employer responsibilities for the health and safety of yourself, workers, visitors, clients, and volunteers.
- Learn about personal safety in the workplace.
- Read more about your workplace health and safety obligations.

☐ Dangerous materials spills, leaks or explosions

- Learn how to manage hazardous chemicals in the workplace.
- Read health and safety resources from Workplace Health and Safety Queensland (WorkSafe):
  - hazardous chemicals
  - managing risks of hazardous chemicals in the workplace – code of practice 2021
  - controlling fire and explosion risks
  - risk management plan template.

☐ Loss of power or infrastructure or transport disaster

- Plan for loss of power, for example buy/lease a generator, relocate your business to other premises or find alternative storage for goods requiring electricity.
- Check your ABC local radio, local council or see disasters and alerts for any transport disaster updates and road, airstrip or port closures.
- Plan alternate suppliers or delivery routes if major infrastructure or transport routes are disrupted.
- Read more about supply chain disruptions.

☐ Terrorist or major criminal incident

- Learn more about premises security and crime prevention.
- See the Queensland Police Service's business security assessment checklist (PDF, 1.9MB).
- Visit Safeguarding Queensland for counter-terrorism information.

☐ **Climate change risks**

- Learn how to manage environmental risks and other climate risks to your business.
- Find out about the drought and climate adaption program from the Queensland Government.

Go to respond for emergencies ›

IT threat prevention and preparation

☐ **Develop an IT or cyber security plan**

Steps to include in your plan:

- Learn about the legal IT requirements as part of the Spam Act 2003 (Cwlth), the *Electronic Transactions (Qld) Act 2001* and privacy laws.
- Identify key events and risks that are most likely to occur and would have the most negative impact on your business, including:
  - cyber-attack or data hacking where hardware, data or information is illegally accessed or stolen
  - phishing – scam emails, texts, messages or phone calls designed to trick you out of money or information
  - malicious software (or malware) which is used to access bank details, credit card numbers or passwords
  - denial-of-service attacks – disrupts websites or emails.
- Read the small and medium business information and resources from the Australian Cyber Security Centre, including:
  - small business cyber security guide
  - step-by-step guides to protecting your software, applications and devices
  - protecting your business online
  - register to receive alerts about current online threats.
- Learn about the latest scams by visiting Scamwatch from the Australian Competition and Consumer Commission.
- Plan and respond to key risks and incidents by developing IT policies and procedures, including:
  - hiring an IT expert to improve IT security
  - backing up your data regularly to external or cloud storage
  - auditing and automatically updating your IT systems and software
  - providing a secure site through Transport Layer Security (TLS), which provides encryption
  - introducing multi-factor authentication
  - strengthening passwords by using at least 10 characters (including letters, numbers and special characters) or a passphrase and issue alerts to change passwords regularly
  - using password protected encrypted links rather than attachments
  - using zero knowledge encryption cloud storage.
- Investigate buying cyber risk or liability insurance.
- Install anti-virus and anti-spyware software, spam filters and ransomware protections to secure your computers against threats.
- Develop procedures or training so staff recognise, avoid and report a cybercrime to the Australian Cyber Security Centre.

- Control access to your computer system by:
  - limiting who has access (i.e. restricting administrator privileges)
  - not sharing passwords
  - closing accounts when staff leave.
- Plan how to recover from an incident.
- Conduct regular training with staff and update your plan.

Also consider...

- reading preparing for and responding to cyber security incidents by the Australian Cyber Security Centre.
- visiting the Australian Cyber Security Centre for more resources.
- learning more about data breach preparation and response (PDF, 1.MB) by the Australian Information Commissioner.

Go to respond for IT threats ›

Reputation incident prevention and preparation

☐ **Social media and media policies**

Use this sample social media guidelines template and adapt to your business's needs.

Develop media guidelines:

- appoint a media spokesperson for your business
- outline how to respond to media phone calls and messages:
  - get the journalist's name, organisation, contact details and deadline
  - ask what questions they have
  - let them know the appropriate person will respond shortly
- provide comments to the journalist only if it's directly relates to your area of expertise and you have approval
- before responding to the media:
  - review or draft key messages
  - plan and practice your response
- during an interview:
  - don't feel you need to answer every question, just stick to what you want to say
  - avoid saying 'no comment', instead say; "I can't confirm right now," or "I don't have those details," and "what I can tell you is...".

☐ Customer complaint management process

Develop processes for customer complaints and managing negative online comments and reviews. These can include:

- responding to genuine concerns and negative reviews
- listening and responding to customer feedback professionally and politely
- responding privately to resolve issues raised online, but later posting how you have resolved it
- removing offensive online posts
- correcting or removing any misleading or false online content as soon as possible.

☐ Workplace and staff policies

To avoid inappropriate behaviour ensure you have appropriate workplace health and safety and staff policies in place, including:

- ensuring all staff have required qualifications and appropriate training and supervision for their role
- developing a checklist of key policies or staff induction processes for new staff members:
  - employee behaviour policy or staff code of conduct
  - workplace health and safety policy and procedures including:
    - » safe work
    - » bullying and harassment
    - » anti-discrimination and equal opportunity
    - » stress
    - » fatigue
    - » violence
  - customer service policies
  - handling of money processes.
- Read the cash in transit code of practice 2011 and cash in hand guidance material from Safe Work Australia.
- Read about preventing and responding to occupational violence.
- Use the mental health and wellbeing resources for businesses.

Go to respond for reputation incidents ›

Respond

Know where to get the most up-to-date information and where to get help if you need it. Always call ooo in a life-threatening emergency.

Monitoring, responding and reporting incidents and emergencies

☐ **Monitor the incident, initial response and reporting**

Natural disasters

- Monitor all emergency alerts and contacts.
- Check Queensland weather warnings and current tropical cyclone updates from the Bureau of Meteorology (BOM).
- Monitor the Rural Fire Service's bushfire map and warnings and the Queensland Fire and Emergency Service's bushfire alerts and information.
- Check your ABC local radio and local council for alerts, updates and evacuation centre locations.
- Activate your business continuity plan.
- Follow emergency services advice to shelter or evacuate.
- Communicate with staff, customers and suppliers to advise them about your business operations.

Major health events

- If a staff member or customer contracts a contagious disease and has potentially exposed others at your workplace notify your local public health unit or call 13 HEALTH (13 43 25 84).
- Monitor and follow any public health directions (e.g. for COVID-19) or other alerts (e.g. Queensland Health alerts).

Food poisoning incident

- If you suspect a food product has been intentionally contaminated, report it to 13 HEALTH (13 43 25 84).
- If a food poisoning incident occurs:
  - advise the customer to see a doctor
  - record customer contact and complaint details (see customer complaint form template)
  - remove any suspect food from sale, label it as 'suspected unsafe food' and refrigerate it for testing
  - report it to your local Public Health Unit or call 13 HEALTH (13 43 25 84).

Workplace emergency (medical, fire, police):

- Immediately phone ooo and follow emergency services' advice.
- Keep staff, visitors and customers safe.
- Activate your business continuity plan (includes emergency plan)
  - collect your emergency kit
  - unplug electrical equipment, shut down master electrical board and gas supply
  - secure business premises, vehicles, stock and equipment, information, records and data if there's time
  - evacuate premises if you need to leave.

Workplace or visitor accident

- Immediately phone 000 and follow emergency services' advice.
- Give first aid if it's safe to do so.
- Don't touch or move anything unless you are giving first aid, to stop further injury to the injured person(s) or to prevent serious property damage.
- Notify Workplace Health and Safety Queensland or the Electrical Safety Office if the incident is a death, serious injury or illness, or a dangerous accident.
- Notify WorkCover Queensland or your workers' compensation insurer.

Biosecurity incident

- Report all biosecurity incidents immediately to the Department of Agriculture and Fisheries (Biosecurity Queensland) on 13 25 23:
  - animal health and diseases (including emergency diseases, reportable diseases and zoonoses) – includes livestock, birds, bees and aquatic animals
  - plant pests and diseases (including weeds that may be new to Australia)
  - pest ants including fire ants – report to 13 25 23 or complete the online fire ant yard check form.

Suspicious behaviour or extremist activities

- Report immediately to the National Security Hotline on 1800 123 400. Suspicious behaviour can include:
  - unusual purchases of large quantities of fertiliser, chemicals or explosives
  - unusual filming or photography of official buildings or critical infrastructure
  - suspicious vehicles near significant buildings or busy public places
  - unattended bags.

☐ **Communicate**

- Communicate regularly with staff, customers, suppliers and distributors to let them know if your business is open/closed and if there is any impact on your stock, operators or deliveries. Go to communicate.

Go to recover ›

IT threat response and reporting

☐ **IT threat response**

Contain and assess the threat

- Check for any suspicious activity, unauthorised bank withdrawals or unauthorised access to customer information.
- Assess what information has been breached, the cause, extent of the breach and what you can do to fix the issue, including:
  - advising staff not to share or click on links in suspect emails
  - backing up your system
  - shutting down the breached system (if possible)
  - changing computer access privileges and passwords
  - appointing an external IT or cyber security expert.
- Assess if the data breach will result in serious harm to anyone whose information was involved.
- Report data breaches to the Australian Cyber Security Centre.

Notify financial institution and those impacted

- Take action if financial details or credit cards have been fraudulently accessed:
  - notify your bank or other financial institution immediately
  - suspend accounts or take other action.
- Consult with law enforcement agencies who are investigating the breach before making details public of any fraudulent activity.
- When serious harm has occurred, you must:
  - notify suppliers/clients/customers impacted
  - tell them how to protect themselves and what you're doing to fix it.
- Offer support to staff if they have been affected – use wellbeing and mental health resources available.

Report cyber-crimes and data breaches to the following agencies:

- computer or online crimes (e.g. fraud, online image abuse, identity theft or threats and intimidation) – must be reported to police using ReportCyber
- data breaches – report online or phone 1300 363 992 – you have a legal requirement to report unauthorised access of personal information held by your business if it could result in serious harm
- cyberbullying, image based abuse or illegal and harmful content – report online to Australia's eSafety Commissioner.

Go to recover ›

Reputation incident response

☐ **Reputational incident response**

Key steps to take in the first hour following an incident:

- check and confirm the facts
- contact authorities (if required)
- brief relevant staff
- decide if you should respond
- prepare messaging
- decide who to contact, when to contact them, and the best communication channels (e.g. social media, radio, TV, newspapers)
- if appropriate, contact key stakeholders or those directly affected
- monitor social media and media coverage
- suspend scheduled social media posts or advertising campaigns until the incident is resolved.

Negative media or social media

First decide if responding to the issue will help or make the situation worse.

Social media response:

- review your social media guidelines (if you have them)
- for highly contentious issues, provide a social media response as soon as possible before it goes viral
- when responding, remain professional, respectful and polite.

Media response:

- review your media guidelines (if you have them)
- prepare your media response
- ensure the tone of your message is not defensive
- emphasise the wellbeing and safety of your staff, customers and the community come first
- explain relevant circumstances that may have led to the incident, policies in place to address it and steps taken to resolve it and prevent it from happening again
- put the incident into context – if appropriate, highlight how long your business has successfully operated without having a similar issue or has managed similar issues
- provide written responses to journalists.

Return to contents page

Rumour-driven crisis

Social media rumours:

- always be quick to correct or remove false or misleading information posted on your social media site(s)
- consider if responding to certain social media posts will help or escalate the issue
- when responding, always remain and professional, respectful and polite.

Media rumours:

- before responding to false media reports, consider if your comments will help or whether it will result in additional negative media attention
- when responding, clearly state how information or claims being made are incorrect, provide evidence where possible and ask the media outlet to remove the information or provide a retraction on the same or next day.

If the rumour has received wide coverage, send out communications to the media, staff, customers, suppliers and other stakeholders.

Inappropriate workplace behaviour or organisational misdeed

- Investigate all complaints of inappropriate workplace behaviour – using an external investigator can prevent claims of bias.
- Suspend the person responsible if there's a serious breach of your behaviour policy or code of conduct.
- Notify the police if required.
- Seek advice if needed from:
  - Workplace Advice Service offers free legal assistance on dismissals, workplace bullying and general protections
  - Heads up offers advice on bullying and mental health advice in the workplace advice.
- Identify how policies were breached and update procedures to stop it happening again.
- Let staff know how you're handling the incident and advise them of any new policies.

Go to recover ›

Recover

It can take months or years for businesses to fully recover from some disasters and emergencies. Having a plan to respond and recover can help speed recovery, but consider deferring any big decisions about your business's future immediately after a disaster.

Learning from what didn't work or what worked well when responding to or recovering from a disaster or emergency can help improve your future response or prevent issues from occurring again.

Initial recovery (hours and days after incident)

☐ Wellbeing and safety

- Protect yourself, your family and staff.
- Monitor emergency broadcasts for updates.
- Return to your premises only when safe.

☐ Assess impact on your business

- Return to premises when safe and secure dangerous debris.
- Assess damage to buildings, assets, vehicles and equipment.
- Record decisions and photos and/or videos of damage in an event log for insurance claims.
- Learn how to clear vegetation after a natural disaster and disaster clean-up tips.
- Estimate repair, replacement or relocation costs.

☐ Contact insurer and bank

- Contact your landlord and insurer before cleaning up – they may fund clean-up and require authorisation before repairs begin.
- Lodge your claim early – don't wait for a full damage assessment before lodging.
- Contact your insurer or bank for emergency funds or recovery activities.
- Contact your local council about kerbside pick-up.

☐ Communicate

- Update staff and customers.
- Stay in contact with other business owners, your local council and emergency services during recovery.

☐ **IT threat initial recovery**

- Fully investigate the data breach (or have an IT expert investigate).
- Monitor your systems for any ongoing suspicious activity.
- Update or enhance IT security systems to detect and prevent future breaches.

Early recovery (days and weeks after incident)

☐ **Wellbeing and safety**

- Take time out for your own wellbeing.
- Don't put yourself at risk when cleaning up, use qualified contractors for electrical or gas repairs or reconnections.

☐ **Staff**

- Update staff and offer support - see contact details for support services.
- Learn more about managing, paying or standing down your staff after an emergency and your obligations as an employer.

☐ **Assess business operations**

- Review your business continuity plan (includes recovery plan).
- Consider reopening options (e.g. alternate premises, hired equipment or contractors, reduced hours or services, online services).

☐ **Financial recovery**

- Assess how long you can operate with reduced or no revenue.
- Contact your bank, accountant, creditors and debtors to discuss options – use our suggested messages.
- Contact the Australian Taxation Office (ATO) to learn about dealing with disasters, how to fast-track your refund, delay lodgement obligations or more time to pay debts.
- Learn more about managing cash flow and debtors.
- Speak to a free financial counsellor on 1800 007 007 or rural financial counsellor on 1800 900 090.
- Add to your insurance claim as required.

☐ **IT and business records**

Disaster and emergency IT recovery

- Recover data and business records.
- Repair or replace damaged systems or equipment.

Data hacking or cyber-attack recovery

- Monitor ongoing suspicious activity and continue to update or enhance IT security systems.

☐ **Communicate**

- Continue to update customers and suppliers about your business operations. See suggested messages.
- Provide positive news to customers on your website and social media.
- Post photos and videos on social media to demonstrate when your business is back up and running.

☐ **Connect**

- Connect with other businesses in your industry and disaster recovery centres to find out how you can help your community, or they can help you.
- Accept community support – people want to help and you are not alone.

Long-term recovery (months or years after incident)

☐ **Wellbeing and safety**

- Look after your own, your staff and your family's wellbeing and mental health.
- Consider alternative roles or tasks for staff.
- Stay connected to your local community, industry and neighbouring businesses.
- Remember it's okay to accept assistance, even if you think others are worse off.

☐ **Business operations**

- Consider how to reduce the impact of future events on operations and buildings.
- Replace destroyed equipment, stock, records and documents.

☐ Financial recovery

- Assess your finances, cashflow and break-even point.
- Consider the viability of your business – is it better to rebuild or exit?
- Work with your accountant, lawyer or advisors on credit and repayment plans.
- Or speak to a free financial counsellor or rural financial counsellor.
- Learn about small business support services to get back on track:
  - Mentoring for Growth program

☐ Communicate and promote

- Answer emails promptly and thank people for support.
  - Develop a recovery marketing and promotion plan to promote your business.
  - Celebrate milestones and successes and let people know about your recovery steps.

☐ Avoid scams

- Protect yourself from scams.
  - Door-to-door repairs or fake tradespeople.
  - Profiteering and price gouging.
  - Charity scams – check if it is a registered charity.

☐ Recovery planning

- Record lessons learned from your business recovery (e.g. adequacy of insurance policies, and IT, accounting and record-keeping systems).
- Review and update your emergency plan and procedures.
- Update your business continuity plan, and business policies and procedures.
- Schedule regular emergency evacuation drills and provide appropriate training for staff.

Communicate

Communication is crucial before, during and after a disaster or crisis. Your staff and customers need to know if the event has impacted your business, if you will close and when you will reopen. They will also want to know what steps you are taking to prevent emergencies or other crises from occurring in the future.

Consider who your business might need to communicate with before, during and after a disaster or emergency. Key stakeholders may include:

- staff
- customers or guests
- clients
- suppliers and distributors
- banks and insurers
- industry body or association
- regulatory body or agency.

Use social media channels and your website to get the message out widely. We recommend you talk to staff face-to-face and call or email key customers, clients or suppliers who may be directly affected by the impact the disaster or emergency has on your business.

Use innovative ways such as videos, photos and promotions to get the message out when your business is back up and running.

Natural disaster suggested messaging

☐ **Before a severe weather event suggested messaging**

- We value all of our customers/clients and will keep you updated as best we can.
- We are well prepared for events like this and have activated our response plan.
- Our business will close from (provide details) until it is safe to return and resume operations.
- Please stay safe and follow emergency services advice.

For businesses responsible for staff, guests or customers during an event provide regular updates and advise them to prepare an emergency kit:

- We recommend you prepare an emergency kit including (water in sealed containers, canned food to last three days, can opener, medications, toiletry supplies, torch, mobile phone charger and portable power pack for charging phones and face masks).

☐ **During a severe weather event suggested messaging**

For businesses responsible for guests or customers during a disaster, advise them how to stay safe and where to go if evacuation is required.

- For more information and weather updates please visit (provide details).
- If you are in a life threatening or dangerous situation or require emergency assistance, please phone ooo.
- Please follow the advice of emergency authorities at all times.

Return to contents page

☐ **After a severe weather event**

If available, use your social media accounts, website or phone to advise customers and stakeholders about your business operations.

Initial recovery

- We have been following authorities' advice and plan to reopen our business as soon as it is safe to do so.
- Our doors may be temporarily closed, but you can still buy and order online. Visit our website at (provide website address).
- We wish all of our customers and clients a safe recovery.

Later recovery

- We are now open for business and ready to welcome all our customers back.
- Please be patient with us as we work to resume full operations.
- In the meantime, please visit our website to place an order.
- You can continue to contact us on (provide details).

Major health event suggested messaging

☐ **Public health event alert**

- The safety, health and wellbeing of our staff and customers is our first priority.
- In response to (add health event) we are following all directives issued by the Chief Health Officer and doing everything possible to ensure the safety of all staff and customers at our premises.
- We are continuing to monitor our policies in this changing environment and do our part to prevent the spread of (add health event).
- In line with guidance provided by Queensland Health we have updated our cleaning and hygiene measures in line with recommended guidelines. These include (list measures).
- To find out more about (add health event) visit (list appropriate websites and/or organisations).
- Thank you for your patience. We are receiving a high volume of phone calls and queries and will respond to your inquiry as soon as we can. In the meantime, please visit our website (or social media page) for more information.

☐ **Public health outbreak at business premises**

- The safety, health and wellbeing of our staff and customers is our first priority.
- We are working closely with authorities to identify the source of the outbreak and providing every assistance to help them with contact tracing of customers who may be affected.
- We have followed all directives issued by Queensland Health to protect our staff and customers and will continue to do so.
- On advice from Queensland Health we will be temporarily closing our business and doing a deep clean of all surfaces and areas on the premises.
- In the meantime, please visit our website to order online or for more information.

☐ **Food poisoning or contamination incident**

- We are working closely with authorities to investigate this incident to determine the exact source and cause.
- The safety and security of our (staff, customers or guests) is our first priority.
- Our practices and standards are in line with the strictest health and safety regulations.
- We will continue making every effort to abide by these standards and will update our food handling processes if they are found to be responsible for the incident to prevent this from happening again.
- If anyone who has eaten (provide specific details of food source and timings) and is experiencing symptoms of (list symptoms), we advise you seek medical assistance.
- We sincerely apologise for any distress this incident has caused and our thoughts are with those who have been affected.

☐ **Medical event**

- For more information, read workplace accident or death suggested messaging.

Emergency suggested messaging

☐ **Dangerous materials, terrorist or major criminal incident suggested messaging**

- Our thoughts are with the individuals affected and their families.
- Our priority is allowing emergency services to do their job.
- We are working closely with the relevant authorities to ensure the safety of our staff, customers and/or guests.
- Authorities are well prepared to handle events like this, so please follow any directions they make.

☐ **Workplace accident or death suggested messaging**

- We are saddened to confirm that a (staff member/visitor/client/guest) was (injured or killed) in an incident today.
- Our thoughts are with them, their families and those who witnessed the incident.
- We are working closely with authorities and Workplace Health and Safety Queensland to assist in any way we can.
- We have suspended our operations/tours and will work with authorities to determine when we will re-open.
- We would like to thank emergency services for their immediate response.
- This has never happened before (or is very unusual) and we take the safety of our staff/guests very seriously.

IT threat suggested messaging

☐ **Notifying customers or clients of an IT failure**

- Our (telephone/online services/website) have been disrupted today due to unexpected technical issues.
- Our team is working hard to resolve the issue as soon as possible. We'll provide updates as soon as more information is available.
- We apologise for any inconvenience this may have caused. If you urgently need to contact us, please (phone/email/message or visit us at…).

☐ **Notifying customers or clients of a breach**

- We are contacting you to let you know a data breach has affected your personal data. On (date and time), we detected a breach of our organisation's IT security. As a result, some of your information has been accessed (provide type of data if appropriate – e.g. contact details).
- We've launched a full investigation to resolve the issue and we're working closely with authorities (the Australian Cyber Security Centre, the Australian Federal Police and/or the Australian Information Commissioner).
- We're taking the following steps to protect you by:
  - engaging an external cyber security agency to ensure we've taken all possible measures to minimise the impact of this security breach and reduce the risk of it happening again
  - continuing to monitor for suspicious activity and coordinating with relevant authorities and agencies
  - continuing to improve our systems to detect and prevent unauthorised access to user information.
- We take our obligations to safeguard your personal data very seriously. We recommend you consider taking the following steps to protect any further access to your (personal information or account details). As further safeguards:
  - update your password - use at least 12 characters, includes numbers, symbols, capital letters and lower-case letters (avoid using dates of birth or names)
  - review and update your contact methods for resetting passwords
  - review your account transactions and let us know if you notice anything suspicious
  - don't open attachments or click on links from unknown sources
  - ignore unsolicited communications that ask for your personal data or refer you to a web page asking for personal data
  - please also report anything out of the ordinary to (provide details).
- We sincerely apologise for any inconvenience this breach may have caused. If you have any questions or concerns please don't hesitate to contact us via (email or phone).
- We'll keep you informed if there is any further information about this breach.

Reputation incident suggested messaging

☐ **Suggested customer or guest negative post messaging**

- We're sorry to hear about your experience with (provide details). We take pride in our (services/products) and take feedback from customers seriously. Please message us directly so we can help resolve this issue.

☐ **Suggested rumour-driven incident messaging**

- Rumours that our business is experiencing (financial difficulties or other rumours) are completely unfounded and incorrect.
- We are open for business as usual.
- If customers or clients have any concerns, please feel free to contact us directly.

☐ **Suggested inappropriate workplace behaviour or organisational misdeed messaging**

- We take this matter very seriously and have a zero-tolerance policy towards workplace (bullying/harassment).
- The person involved has been suspended (or placed on leave) pending the outcome of the investigation.
- We are cooperating with authorities and have launched an independent investigation into the matter.
- Due to privacy considerations we cannot discuss the investigation publicly at this stage.
- As an initial step, we have put in place additional procedures for all staff members to (provide details) so this doesn't happen again.
- We will also review our policies and procedures to introduce mandatory ethics and workplace culture training as part of our staff inductions.

☐ **Suggested legal action messaging**

- We understand this is a distressing situation and an independent investigator is looking into the incident.
- We send our deepest sympathy to the family and friends of (use if an accident or death)
- The wellbeing of our staff, customers and the community always comes first.
- As this matter is before the court, we can't comment on the specific details of the incident, but will provide more information when we can.
- Thank you for your understanding at this stressful time.

Bank, utility provider and insurance claim tips – communicating post emergency

☐ Bank tips

Contact your bank

- Ask your bank about financial hardship options, for example:
  - changing loan terms
  - temporarily pausing or reducing repayments
  - deferring repayments and interest payments (all missed payments and interest will need to be repaid)
  - waiving fees and charges
  - consolidating your debt
  - finance to help cover cashflow shortages
  - deferring upcoming credit card payments
  - increasing emergency credit card limits
  - waiving early termination fees to access term deposits.
- Provide loan details (account name and number, payment amounts) and an overview of your financial situation.
- Request a hardship variation by using the sample letter generator from the Financial Rights Legal Centre to send to your bank.
- Your bank must advise you within 21 days about your hardship request. If you can't negotiate a variation, you can:
  - contact the bank's internal dispute resolution team
  - visit the Australian Financial Complaints Authority (AFCA) or phone 1800 931 678 to make a complaint, and get free advice and independent dispute resolution.

☐ Utility provider tips

Contact your utility providers hardship team.

- Ask about hardship payment options for your electricity, gas, phone or water bills following a disaster or emergency.

☐ Insurance claim tips

- Contact your insurer if you:
  - aren't sure the event is covered by insurance – you may be able to claim under your business interruption or income protection insurance
  - have lost your policy documents – your insurer will have a copy.
- Contact the Insurance Council of Australia (phone 1800 734 621) or read the insurance claims and disasters brochure if you have questions about your policy or don't know who you are insurer is.
- Check if your insurance policy:
  - funds clean-ups
  - requires authorisation before repairs begin
  - provides emergency or advance funds for wages or recovery activities.
- Gather all information about the claim:
  - complete an event log
  - items to claim and when purchased
  - equipment, furniture you've had to throw away
  - photo and/or video evidence.
- Make a claim and resolving issues:
  - lodge claim as soon as possible – don't wait for a full damage assessment before making a claim
    - » insurers must fast track a claim if you can demonstrate 'financial need' (read Item 64 of the General Insurance Code of Practice) – if the insurer agrees, an advance payment must be made within 5 days
    - » you must be informed of your insurer's decision within 10 business days of receiving your claim
  - contact the Australian Financial Complaints Authority on 1800 931 678 if you can't reach agreement with your insurer
  - phone Legal Aid Queensland on 1300 651 188 if you need information and advice on how to get a claim paid.

Useful links

☐ Financial assistance and other support

- See Queensland natural disaster assistance for information about grants, loans and other assistance.
- Find a mental health support service in Queensland.
- Complete Beyond Blue's anxiety and depression checklist to find out if you have been experiencing anxiety or depression.

☐ Natural disasters

- Visit the Bureau of Meteorology (BOM) for Queensland weather warnings and current tropical cyclones information.
- For bushfire alerts and information visit Queensland Fire and Emergency Services and Rural Fire Service for a current bushfire map and warnings.
- Check Queensland drought maps for drought declared areas.
- For local disaster updates find your local council.
- View Emergency alerts, warnings and contacts.

☐ Major health events

- Find out about Chief Health Officer public health directives.
- See COVID-19 business recovery resources.

☐ Emergencies

- Visit Biosecurity Queensland to learn how to protect your business.
- Visit Workplace Health and Safety Queensland to learn more about workplace health and safety obligations, tools and templates.
- Read Safeguarding Queensland for counter-terrorism information.

☐ IT threats

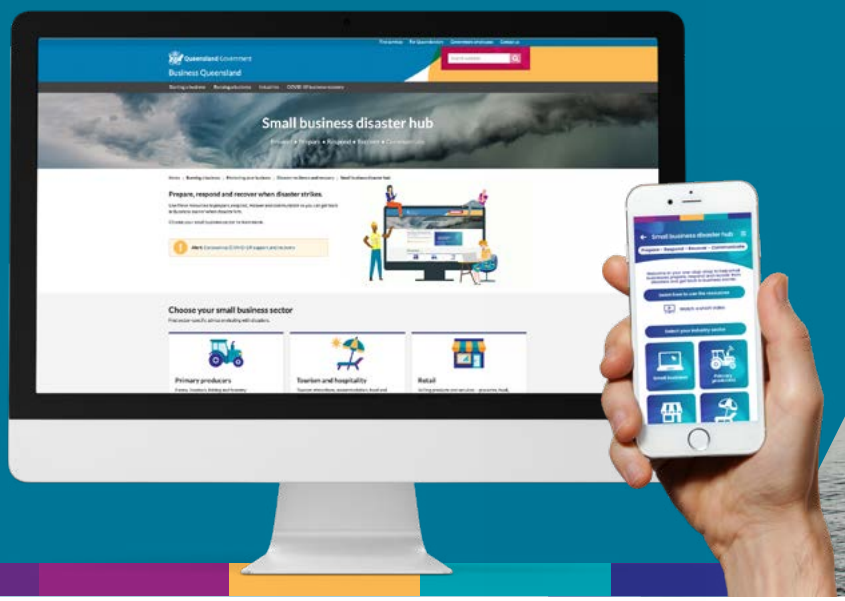
- Visit the Australian Cyber Security Centre for more resources and to use the Small Business Cyber Security Guide.
- Visit Scamwatch to avoid the latest online scams.

☐ Reputation incidents

- Visit Workplace Health and Safety Queensland to learn more about workplace health and safety obligations, tools and templates.
- Learn about putting business policies, procedures and standards in place.

Small business disaster hub

Prevent - Prepare - Respond - Recover - Communicate



More information

Visit business.qld.gov.au/disasterhub for more information and other resources, including:

- Emergency alerts and contacts
- Small business resilience case studies
- How to video animations

Download the Small business disaster hub app for Apple or Android, or use the QR codes below, to access this information offline and receive relevant alerts.

Download from App Store

Download from Google Play

Small Business Recovery Centre

Phone: 0459 873 781

Email: sbrc@desbt.qld.gov.au

Return to contents page

Australian Government

This initiative is jointly funded by the Commonwealth and Queensland Governments under the Disaster Recovery Funding Arrangements (DRFA).

Queensland Government