AT&T Business

Prepare your business for the unexpected: a planning guide

No matter where your business is located around the world, disasters, emergencies, events, and pandemics can cause potential business disruptions. That's why you need two disaster plans. Your long-term plan helps ensure business continuity and faster recovery. Your short-term plan is what you need in place right before a disaster hits.

We created this planning guide to help you prepare for disasters and other events, with checklists for short and long-term business preparations.

AT&T is committed to delivering the highest levels of service quality and reliability for our customers under all circumstances. At any stage in an emergency or threatening situation, please focus on your safety first. We'll be there to help support your business recovery.

AT&T Business

Long-term planning

Develop a business continuity plan to help protect your business and your customers before an event strikes.

- **Plan for the impact of an unexpected or catastrophic event on your business** – Explain in detail how critical business communications and services will be offered during a period of outage.
- **Assess your data and technology needs in the event of a failure in operations** – Identify critical business processes, data, and technology needs on both the internal and external levels.
- **Communicate your plan to employees and vendors** – Train employees on their specific responsibilities during a disaster and educate your vendors on your disaster plan.
- **Coordinate with external organizations on how to help your community** – Reach out to local organizations to share disaster preparedness plans and find opportunities for cooperation.

Short-term planning

Make a plan you can activate quickly for evacuation, crisis management, and communication.

- **Set up a call-forwarding service to a predetermined backup location** – Set up a single or multiple hotline number(s) for employees, employees' families, customers, and vendors to call so that all parties know about the business situation and emergency plan.
- **Protect hardware/software/data records/employee records, etc.** – Routinely back up these files to an off-site location. Cloud services can remove the burden of offsite data storage and ensure faster recovery from temporary or remote locations.
- **Outline detailed plans for evacuation and shelter-in-place plans** – Establish a backup location for your business and a safe meeting place for all employees.
- **Create a remote access plan** – Equip business-critical staff with remote work access in advance, so they can access applications and databases from remote locations, when connectivity is restored.
- **Assemble a crisis-management team and coordinate efforts with neighboring businesses and building management** – Outline a plan for supply chain continuity for business essentials.

Resources

Links for preparedness and recovery.

It's important to identify reliable sources of information for disaster preparedness efforts. Here are some additional resources from AT&T and government agencies:

AT&T resources:

AT&T Web Site
AT&T Network Disaster Recovery
AT&T Business Continuity for Enterprise

Non-AT&T resources:

- BCI Standards and Guidelines *www.thebci.org*
- Federal Emergency Management Agency (FEMA) - Ready *ready.gov*
- Federal Emergency Management Agency (FEMA) *fema.gov*
- National Security Telecommunications Advisory Committee (NSTAC) *dhs.gov/nstac*
- NCS - TSP Program Office *https://www.fcc.gov/general/telecommunications-service-priority*
- NOAA National Oceanic and Atmospheric Administration *noaa.gov*
- U.S. Health and Human Services *pandemicflu.gov*
- World Health Organization *who.int*
- Centers for Disease Control and Prevention (CDC) *cdc.gov*

AT&T Business

Business Continuity Planning Checklist

When unexpected or even catastrophic events occur, businesses must protect their employees and continue critical operations that support their communities. To protect your business, planning is essential. As a business leader, you understand the strategic importance of a solid continuity plan. That's why Business Continuity Planning focuses on multiple aspects of your business, to help you make sure you can recover the technology and processes required to operate after an unforeseen disruption in normal operations.

To help in your disaster preparedness efforts, AT&T developed the following checklist. The checklist identifies important, specific activities that businesses can do now to prepare for an event.

1 Planning for the impact of an unexpected or catastrophic event on your business

	Completed	In progress	Not Started
Identify a coordinator and/or team with defined roles for preparedness and response planning. Potential team members may include: Information Security, Operations, Systems, Police/Security, Physical Plant, Insurance, Legal Affairs, Public Affairs, Human Resources, Comptroller, Audit Division, Safety Office, and/or Emergency Response Team.			
Conduct a business process and services inventory to understand which processes are mission-critical to the survivability of the business.			
Determine acceptable levels of service during the recovery period and what processes need to be maintained or restored first to keep the business running.			
Identify essential employees and other critical inputs (sub-contractors, services, logistics, etc.) required to maintain business operations by location and function during the event.			
Conduct a technology asset inventory to determine and document the mission-critical technology components, their locations, how they're configured, and who is responsible for management.			
Once key components are identified, determine what measures should be taken to protect and recover them.			
Understand the rules or regulations governing your business operations. If you had a business disruption (either a complete disruption or one that changes how you operate for the short-or long-term), would you be able to maintain compliance? (Sarbanes-Oxley, HIPAA, GDPR, privacy, etc.).			
Understand customer or business partner performance metrics/service level agreements to assess risk for breach of contract or to put in place performance remedies for your customers.			
Identify a budget: Quantify the potential costs of downtime or total business failure. Develop a business case to optimally invest in risk mitigation.			

2 Assessing your data and technology needs in the event of a failure in operations

	Completed	In Progress	Not Started
Determine the status of your existing disaster recovery plan. Do you have one and is it maintained? Have you tested the plan?			
Determine vulnerability of your organization's technology infrastructure to natural disasters, including floods, fires, earthquakes, pandemics, etc.			
Set clear recovery time objectives for each of your business/technology areas.			
Determine the need for off-site data storage and backup.			

AT&T Business

2	Assessing your data and technology needs in the event of a failure in operations	Completed	In Progress	Not Started
	Develop a technology plan that includes hardware, software, facilities, and service vendors.			
	Secure clear understanding and commitment from vendors on your plan.			
	Secure a backup vendor, if necessary, to perform that critical function if your primary vendor is impacted by a business failure.			
	Perform security risk assessments around specific threats where possible. Examples of data security include: virus protection, intrusion detection, hacker prevention, network events, component failures, and systems crashes.			
	Assess, if possible and based on prior events, how quickly and accurately your business and technology were restored by existing staff. What were the lessons learned so they can be addressed in future planning?			
	Determine the effectiveness of your data backup and recovery policies and procedures. Are the procedures fully documented and is an appropriate staff member responsible for the maintenance of that documentation?			
	Perform a data recovery test. Was the test successful?			
	Prepare an incident plan for mitigating a security breach. Audit annually, as security threats can change. If not assess why and update the Business Continuity plan accordingly.			

3 Communicating your plan to employees and vendors

		Completed	In Progress	Not Started
	Determine who needs to be contacted with critical information. Build distribution lists and maintain for accuracy.			
	Develop a contact plan to reach employees: SMS text, home, email, etc.			
	Ensure employees know where to receive information and updates about whether they can return to work or if they are to report to a different location (internet, conference bridges, etc.).			
	Ensure mission-critical employees know their roles in the plan and that they have access from remote locations (i.e., home Wi-Fi, phone, VPN for security).			
	Make sure the plan can be executed by alternate employees who are not necessarily the “experts” in cases where those employees cannot be reached.			
	Determine the need for a designated recovery site for your people to resume work. Plan for communications, data connectivity, desktops, and workspaces at that site.			
	If you require support from vendors, ensure they also have a documented plan that complements your needs. Review periodically to keep the plan current.			

4 Coordinating with external organizations and helping your community

		Completed	In Progress	Not Started
	Collaborate with your local government agency to share your plans and understanding of their capabilities in the event of a business-impacting catastrophe.			
	Share your plan with your building management, so they have a clear understanding of their role in safely securing the building and your employees.			
	Share best practices with other business leaders in your community, chambers of commerce, and business associations to improve community response efforts.			

Please visit us at www.business.att.com, or contact your account executive to discuss how AT&T can help you with your business continuity plans.