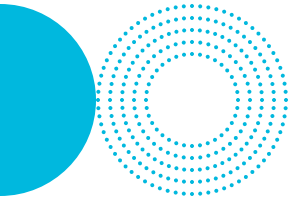
The Resilient Organization

A Guide to Nonprofit Disaster Preparedness

CDP Center for Disaster Philanthropy

techsoup

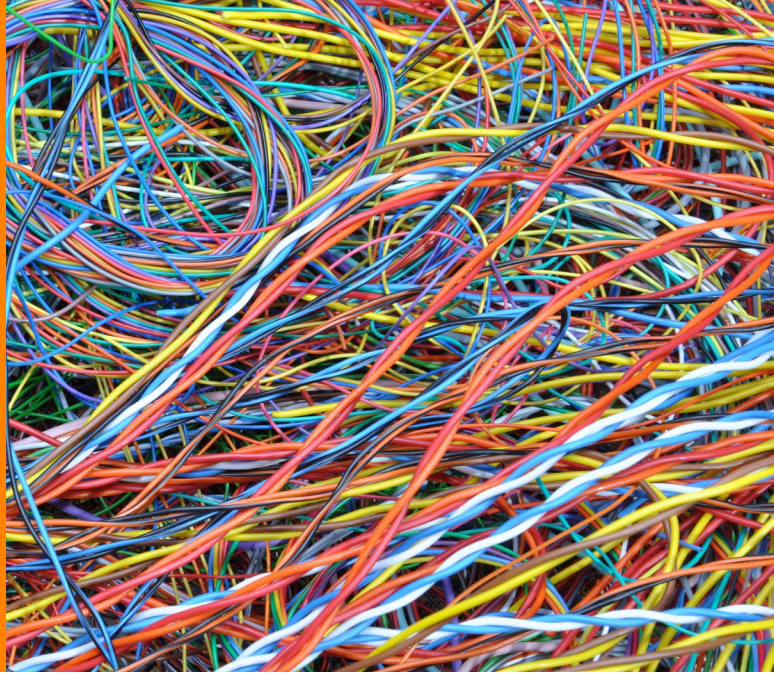


Published by TechSoup

The Resilient Organization: A Guide to Nonprofit Disaster Preparedness

Contents

About This Guide



TechSoup has written this guide to give nonprofits some tactical and actionable steps to make their organization better able to recover from a disaster quickly and participate in response efforts as needed.

We would like to acknowledge the valuable contributions from the Center for Disaster Philanthropy and the Louisiana Association of Nonprofit Organizations.

Why Prepare for Disasters

A disaster can create significant disruption to your nonprofit's operations by physically damaging property, displacing staff and volunteers, and creating a surge in demand for services.

Every event has a different personality and presents a unique set of challenges — for both nonprofits and the vulnerable populations they serve.

With a thoughtful plan, your organization can become more resilient and better able not only to withstand future disasters but also to help respond to them. And while disasters are generally regarded in a negative light, they can actually present opportunities for disaster-resilient nonprofits to grow and even expand their service offerings.

The Importance of Nonprofit Organizations in Their Communities

Nonprofit organizations already play a critical role in the social and economic health of a community, including these activities:

- Providing meals to needy citizens
- Caring for injured and stranded wildlife
- Counseling those suffering from addiction
- Providing job training skills
- Teaching standard K-12 school and university courses
- Recycling and repurposing a wide range of goods produced and discarded by society
- Caring for endangered wildlife habitat
- Showcasing the cultural legacy of their city

Nonprofits are also expected to participate in response and recovery after a disaster — regardless of whether that is part of their core mission or not. Therefore, it is even more important to be disaster resilient so that you will be ready to continue and expand your operations in the time of an emergency.

Financial Impact of Disasters on Nonprofits

Planning for business interruption can make the difference between resuming operations after a disaster or closing the doors. According to a 2018 report released by the National Institute of Building Sciences, every $1 invested in disaster mitigation saves $4 to $7 in recovery costs. While the report is not technology-centric, you can expect similar savings when dealing with a technical disaster.

A little preparation goes a long way to making it easier to return to operations, shift emphasis, and scale programs after a disaster. The recommendations in this guide can be applied to many types of disasters, including pandemic situations, and are meant to be used together with our other guides, *A Guide to Nonprofit Disaster Recovery and Disaster Preparedness for Your Staff and Volunteers*.

Step 1:
Figure Out What Has Already Been Done and What You Need to Do Next

This section will provide you with the basics you should have on hand and attend to in the face of a natural or human-made disaster. We will look at the necessary measures for the survival of you and your co-workers and the continuity of your organization's major functions, with an emphasis on technology planning.

To begin with, use the checklist below to assess how prepared you and your organization are and what to work on first.

Does your organization have all key organizational documents, contact information, and lists of your technology and other physical assets collected and saved both electronically and in hard copy?

Task: Collect and create repositories of critical documents

Does your organization have an emergency response/evacuation plan? Are there emergency supply kits for staff members?

Task: Draw up an emergency response plan and assemble supply kits

Does your organization have a plan for how to communicate internally and externally during and after a disaster/emergency?

Task: Create a disaster communications plan

Does your organization have a plan for the continuity of primary operations after a disaster/emergency?

Task: Create a continuity of operations plan (COOP)

Does your organization have a plan for data backup and the backup of equipment and devices?

Task: Review your data backup system or service to ensure that it meets your current needs or contact your IT provider to have one set up.

Are the staff members and key volunteers in your organization informed of all the disaster preparedness plans and trained accordingly?

Task: Conduct annual management, staff, and volunteer training on disaster response, communications, and COOP plans

---

Does anyone in your organization know the procedures to recover technologies after a disaster or emergency?

Task: Create a dedicated group (two or three people) who will be responsible for managing the recovery of hardware and other technologies after a disaster, including providing guidance to remote staff members with impacted equipment.

Is your organization prepared for post-disaster crowdfunding?

Task: Include fundraising and assistance outreach in your disaster communications plan and set up online donations capability now.

Does everyone in your organization have information on how to plan and prepare for the survival of themselves and their families in the face of a disaster or emergency?

Task: Provide your staff with the resources in the guide *Disaster Preparedness for Your Staff and Volunteers*

Don't worry if you can implement only some portions of this list right now. Pick the components that seem most important for your nonprofit and go with that. Every step is one step further in the right direction.

Step 2:
Create a Disaster Preparedness Plan for Your Organization

Maintaining or recovering the operation of your organization during disasters can be made much easier if planned ahead of time. Start with these four main steps:

Centralize and create backup copies

of all your organization's critical operational information and documentation for storage in a safe place.

Write an emergency communications plan

that will inform both internal staff and volunteers as well as the community you serve of your organization's operational status.

Create an emergency response plan

that provides clear instructions on roles and actions to be taken when an emergency occurs.

Create a continuity of operations plan (COOP),

which will include the three previous points plus additional preparations that will enable you to get back up and running as quickly as possible.

Centralize Your Information

The first step in preparing your organization is to ensure that you have all your important documents and information in a safe and accessible place. This is the centerpiece of your disaster planning and preparation. This information repository should contain all the business information that is at the core of your nonprofit's operations. In the event that your facilities are unreachable — by flooding, fires, or shelter-in-place orders — this is the information you will need to get your nonprofit running again.

Store all the crucial information you collect in all three of these places:

1 A go-bag
(also called a disaster box)

hard copies of your documents and information that are protected from natural disasters and theft in a transportable, fireproof, waterproof safe or safe deposit box

2 A master key
(also called a portable digital device)

encrypted, on a portable storage device

3 The cloud

encrypted, off-site, and online

The Go-Bag

The particular bag or box you use for your go-bag isn't terribly important, as long as it holds everything and is waterproof. In areas prone to hurricanes or floods, we suggest plastic bins with watertight lids since these have been proven very effective at keeping paper dry and intact. These containers are affordable and can be found at most office or hardware stores. If your organization is prone to experience earthquakes, where fire is a common aftermath, you may want to use fireproof safe boxes.

As a basic principle, your go-bag should be something someone can put in a car and drive away with quickly. You can store it in the office or at the home of the executive director or a board member.

The go-bag should contain contracts, grants, policies, and other documents (see the next section, Information to Include). These copies should NOT be originals: all documents should be copies. Keep the originals in your office's filing system. While you may have electronic copies of many of these documents, it is important to print them out. In a disaster scenario, you may not have regular computer access.

Master Key

Your portable digital device master key can be a USB flash drive or another type of external drive or portable device. Everything you put into your go-bag you also put on this master key in an electronic version.

These types of devices range in price, but you may want to invest in a "ruggedized" USB drive that will better withstand physical damage. There are numerous secure flash drives on the market that automatically encrypt and password-protect any data that's saved on the drive. Some include additional features such as fingerprint scanners or automatic deletion of files after a certain number of incorrect password attempts.

A less expensive alternative is to use a standard flash drive using the special encryption application with your operating system.[1] You can either encrypt an entire disk or create an encrypted virtual disk that can then be stored on the flash drive, shared with others, and accessed with the right credentials.

1. You can use the standard Windows BitLocker or Mac FileVault.

Create at least two copies of your master key:

The first copy should be added to your go-bag.

The second copy should be held by one other person and stored somewhere outside of your organization's office — in a board member's office, an executive team member's home, a safety deposit box, and so on.

The Cloud Repository

And finally, an electronic copy of all your critical files should also be stored in a secure cloud data storage account that is accessable to designated staff and board members, so that if the executive director is out of town or incapacitated, others in your organization can recover your data and files without delay. Good cloud-based document repositories include nonprofit options from Microsoft, Google, Box, and Dropbox and should be set up with encryption, password protection, and limited access rights.

When choosing those who will have access to or hold sensitive organizational data, consider these factors:

Who and how many people in your organization have the authority to make time-sensitive decisions about the operations and tech infrastructure?

Who is trustworthy and lives in a geographic area that's not subject to the type of disaster events that you most anticipate?

Information to Include

The information you need to collect for storage in your go-bag, master key, and cloud information repository should include

Organizational documents
Administrative documents (contracts, grants, policies, etc.)

Contact information for board members, employees, volunteers, funders, and other key stakeholders

An inventory of your computers, equipment, software, and more

Your COOP

Your emergency communications plan

As you read through the following lists, you may find that your organization has additional items that are not included due to the nature of your specific programs and services. Use the lists below and provided in Appendix 1 to create a customized go-bag checklist for your organization.

Organizational Documents

These items are the proof that your organization is a legal organization and your basic rules for operating. In a disaster situation, you are likely to need to consult your bylaws and policies and procedures to familiarize yourself with your organization's emergency plans.

- [ ] Charter
- [ ] Board bylaws
- [ ] Budget
- [ ] Your COOP
- [ ] Your recent Form 990
- [ ] Your 501(c)(3) determination letter

Administrative Documents

These items contain your nonprofit's financial, legal, and personnel information. You will need this information so you can get access to your money, file insurance claims, and get back in business.

- [ ] Insurance policies
- [ ] Memoranda of understanding (MOUs)
- [ ] Grants and contracts
- [ ] Leases and deeds
- [ ] Personnel policies
- [ ] Organizational process documents (accounting procedures, hiring papers, etc)
- [ ] Audit

Your accountant can print you a copy of your financial statements, including the following:

- [ ] Depreciation schedule
- [ ] Chart of accounts
- [ ] Bank accounts information
- [ ] Investment information
- [ ] General ledger
- [ ] Aged receivables
- [ ] 1099 vendor report
- [ ] Budget projections

Contact Information

Include all contact information you would need to get your organization back up and running after a disaster, including contact data for all groups included in your Emergency Communication Plan (discussed in a following section), such as

Employee contact information.

You might consider integrating the collection of this information into your hiring process. Also, it is a good idea to set the policy and let your employees know that their home contact information will only be used in the event of an actual emergency.

Board and volunteer contact information.

Add the collection of this information to board and volunteer onboarding activities.

Funder contact information

Facilities and business contacts

Client directory

Contact information for web hosting and backup services.

If there is an account representative devoted to your organization, include that name and contact information also.

Technology recovery contacts.

Keep track of contacts such as computer maintenance providers that you'll need during your recovery.

Supplier contact details.

Keep track of your suppliers and any information about them that could be relevant to restore continuity.

Technology and Facilities Information

Information you will need about the computers, machines and information in your office.

Alternate site data sheet:

This should detail any alternate operating locations for your organization if there is a disaster. This could be the offices of a fellow nonprofit or other organization that is located outside your direct geographic area.

Computer and network inventories:

These should include warranties and receipts for computers and peripherals. For your computers and network, one quick and easy (and free!) way to inventory is Spiceworks.com. Go to Spiceworks and create a free user account; then log in and go to the Inventory section. It has a network-aware program that you can install on your computer. The inventory tool will automatically look over your network and create a report of what it finds. It will record all the information you will need about your computer, including model, serial number, software, and hardware. Depending on your network, you may need to run the program from each computer, but it will still save you a ton of time. This is a great timesaver, but if you would prefer to inventory by hand, we have included a Technology and Facilities Information form in the appendix of this document.

Equipment inventories:

Take down the model number, serial number, and information about components and customizations for your copiers, scanners, fax machines, and any other equipment you have.

Photo or video inventory:

It is very important to have proof of all the items inside your office for insurance purposes. Take overlapping photos of your entire office to record all the furniture, computer equipment, and so on that you have. Be sure to open closets and cabinet drawers to capture any valuable items you have stored away. Update these photos at least once a year and whenever new valuable equipment is procured. Then add these images to your electronic disaster box. Photos can be taken with any smartphone camera or a digital camera.

Copies of software and licenses:

- Installed or on-premises software: Having a backup copy of all of your operating systems, office applications, database program, antivirus, and so on will make it much cheaper and easier to set up replacement computers.

- Cloud-based software: Many business tools and programs are now accessed through online applications or websites, so you will want to make sure that you have a list of all of these that are used by your staff and the login information.

IT continuity plan:

- *Technology priorities assessment*
  Identify the essential applications that are required to operate your organization. Begin with key business-critical applications; then work through each job role (examples below). Indicate whether applications will be needed within 24 hours, three days, and a week following a disaster.

  Examples of job roles:
  Accounting, Payroll, Timekeeping, Banking, Inventory, Access Management, CRM, Web Site, E-mail, Phone/VoIP, File Storage, Donation Processing, Volunteer Management, Desktop Publishing, Video Editing, Security Video/DVR, File Backup
- *Key recovery staff*
  List key staff members who will be responsible for recovering systems and services identified above. Historically, businesses find that up to 50 percent of staff may not be able to report to work immediately after a disaster, so it is imperative that all recovery processes be thoroughly documented (click by click), and multiple staff members trained on each task.
  Assuming all staff members are available to help, identify the personnel who are essential to recover your systems and where these systems will be recovered.
- *Report requirements*
  Keep track of all of the reports that you produce regularly, and note if a report is of a central or critical nature and its special requirements.
- *Phone system recovery*
  Use this chart (PDF) to identify what your phone requirements will be after a disaster.

Data backup overview:

- Information about where, how, and how frequently your data is stored and backed up
- Instructions for how to restore your data
- Passwords for encrypted data: Consider an online password storage application
- Login information for web hosting and backup service providers
- Login information for administrative accounts on all computers

Updating the Information

All the information must be current, or it's of no help. Update it regularly with personnel changes, twice a year at a minimum (e.g., in December and June). Much of the information will not change between updates, but some, like the contact sheets, grants, and contracts will have new information that would be important after a disaster.

When to update:

Schedule these updates according to known disaster seasons, if you have one. For example, do this update in June if your office is located in hurricane-impacted areas.

How to update:

We recommend gathering all the updated materials in a folder at the office and then uploading them to your master key and cloud storage and bringing them to an off-site location to add to your go-bag. While you are updating the electronic files, make sure to always save only the most recent versions of documents to your cloud storage and master key.

Security and Privacy

Remember that your disaster box and master key contain extremely sensitive and personally identifiable information. It is extremely important to keep this information secure. Make sure that you secure the electronic files with a password or restricted access. You might go so far as to put a lock on your physical go-bags to ensure the security and privacy of your data.

Do NOT leave the go-bag or master key at the office on the floor, in your car, or anywhere that the materials are at a higher risk of being destroyed or stolen. It may also be a good plan to ask your insurance provider if having this highly secure information located off-site requires an additional policy.

Emergency Response Plan

Emergency response plans are generally for situations when your organization needs to either evacuate or urgently respond to an emergency. According to the Occupational Safety and Health Administration (OSHA) minimum requirements, an emergency response or action plan should include

- Means of reporting fires and other emergencies in your area
- Evacuation procedures and emergency escape route assignments
- Procedures for employees who remain to operate critical on-site operations before they evacuate
- Accounting for all employees after an emergency evacuation has been completed
- Rescue and medical certifications and duties for employees performing them
- Names or job titles of persons who can be contacted

The FEMA emergency response plan template is a great resource for building your own emergency response plan. The template covers the planning for evacuation, shelter-in-place, lockdown, severe weather, natural and human-caused disasters, medical emergency, and fire emergency. It can be customized based on the needs of your organization.

Evacuation

For hurricanes or other predictable disasters, you will probably have a couple days' notice to evacuate. We have outlined a two-day task list, but you may have to compress the timeline to fit the time you've got. First and foremost, be safe. Do not work until the last minute and leave yourself no time to evacuate. As you prepare to leave, these are the most important things.

Communication:

Know where your people are going, how to get in touch with them, and how to coordinate with your stakeholders and response partners.

Data:

Make backups of anything not already in your go-bag and data that is updated daily or weekly and that is critical to your operations (for example, healthcare organizations need their most recent data on prescriptions issued). Make more backup copies than you need and distribute them to several people going in different directions. There is no telling who will be able to come back first. If possible, and your IT person approves, evacuate your physical servers. The pre-evacuation data sheet (see Appendix 1) is an important tool to manage your nonprofit's work after a disaster. While employees may be evacuated for days or weeks, you will be able to see where they were on what projects and what deadlines are approaching. And you will have contact information for their evacuation location.

Equipment preparation:

If you have an IT person, work with them to draft a prioritized list of equipment to evacuate. For equipment you leave behind, heavy-duty trash bags do a great job protecting electronics from water. Before evacuating, unplug your electronics and put a trash bag over them. If they are on the ground, move them onto a desk. Tuck the open end of the bag underneath. If your nonprofit staff uses laptops, evacuate them with employees.

Review the evacuation checklists below and in Appendix 1; they are a good starting point for most organizations, but of course, they may need some additions for your organization.

48 HOURS BEFORE EVACUATION

Remind your board, employees and volunteers of your communication plan and any check-in times, locations, email addresses, and phone numbers they will need.

Have employees and board leadership complete the pre-evacuation data sheet. Remind employees of disaster policies and procedures, especially any payroll changes.

Communicate with your property manager so that you know each other's plans. Get copies of keys and security codes if you need them.
Communicate with response collaboration partners to confirm gather points, times, and response functions.

If your nonprofit will be active in the disaster response efforts, buy the following:

- Water and food for all essential employees, volunteers, and clients for at least three days
- Spare batteries for flashlights, radios, portable TVs, and other electronics
- Other supplies that you've identified as necessary for your response activities
- Petty cash.

24 HOURS BEFORE EVACUATION

Have employees copy files for the projects they're currently working onto a CD or USB flash drive to take with them so they can work remotely.

Raise electronics off the floor and away from windows and cover with trash bags (for flooding danger).

File ALL papers and lock drawers.

Pack up equipment being evacuated — you should evacuate as much of your smaller, more expensive equipment as possible. Always evacuate your external hard drives.

Lock all windows.

Gather updates for your go-bag:

- Most recent digital backups
- Up-to-date client and funder lists
- Updated payroll information

AS YOU LEAVE THE OFFICE

Unplug ALL electronic equipment.

Leave a cheap answering machine plugged in with a message about your organization's response activities and alternative contact info.

Close all interior doors. This mitigates the damage if wind or water get into the building.

Post contact information in a waterproof cover conspicuously. Tape it to the inside of your main office door, for example.

Lock the exterior door.

Emergency Supply Kit for the Workplace

For situations where you need to be prepared to shelter at your office for at least 24 hours, make sure you have a workplace emergency kit prepared — refer to the Personal Workplace Emergency Preparedness Kit checklist from the American Red Cross for guidance. The checklist includes similar items you would put in your family emergency kit, such as food, water, medications, first aid supplies, flashlight, battery-powered or hand-cranked radio, and tools and supplies. Store all these supplies in a "grab and go" case. Additionally, staff members might want to store a pair of comfortable shoes in case they need to walk home.

Additional Workplace Safety Resources

The American Red Cross also offers workplace safety training and preparedness programs,[2] including these:

OSHA-compliant first aid/CPR/AED training

Corporate preparedness programs

A comprehensive AED program

A wide variety of safety and preparedness products

A suite of mobile apps that put lifesaving information at your fingertips (as discussed earlier in this module)

Corporate wellness offerings

Contact the closest American Red Cross office to your nonprofit to see if they can provide on-site workplace safety programs for your nonprofit, your employees, and your key volunteers.

Emergency Communication Plan

Gathering contact information for your staff, board, donors and business contacts (see the preceding section Centralize Your Information) is important, but it is only a part of a communications plan. Having a proper communications plan also includes

Internal communications plan for staff members

External communications and disaster public relations plan

Internal Communications

During and after a disaster, the main goal of your internal communication plan is to make sure everyone is safe and then to coordinate response and recovery activities. Be prepared to provide employees with information on when, if, and how to report to work following an emergency.

Consider setting up one or more dedicated communication methods, such a telephone calling tree, a password-protected page on the company website, an email alert, or a call-in voice recording to communicate with employees in an emergency. Also establish check-in procedures, so that employees can leave an "I'm Okay" message in a catastrophic disaster.

2. Check https://www.redcross.org/content/dam/redcross/atg/PDFs/Take_a_Class/PHSS_Workplace_Safety_Catalog.pdf

Check-In and Notification Procedures

After a disaster, you and your staff will want to know that you're all okay. Establish a check-in procedure, which should include

The HOW:

how people should communicate with each other (phone, text, email, etc.)

The WHO:

assignments of who contacts whom.

The WHAT:

what information should be communicated as part of this check-in (personal safety, location, ability to work, next check-in time, etc.)

For example, require those staff members with Internet access to email the disaster group email address within a certain time period (e.g., within 12 hours of the disaster striking). If they don't have Internet access, have them call or text message their supervisor, who can send a message to the group. Depending on the type of work you do and the type of disaster, a daily all-staff check-in call may be a good policy to consider: It will help you to stay abreast of any changes impacting your staff.

Phone/Text Tree

Phone/text trees use landline and cellphone numbers to contact all staff members and provide information to them, or direct them how to communicate back that they are safe. The phone or text tree generally follows your normal chain of management, which means that each manager will contact direct reports in case of emergency. The last people on the tree contact executive leadership and report any people who could not be contacted. This way everyone is accounted for, and the system is not reliant on any one individual. You should assign a specific person to be responsible for contacting new staff members. In a disaster, phone networks can become overwhelmed, whereas text messages often go through.

Email Group

An email group, like an all-staff emergency email alias, or those provided by Yahoo Groups or Google Groups, also works well in an emergency communication situation. Be sure your staff's personal and work email addresses are added to whichever channel you use. Make sure your staff knows about the group and how to access it.

Calendaring System

Your organization should have an integrated calendaring system in place (such as Outlook or G Suite) so that, if needed, anyone on staff can look up anyone else and see if they are out of the office, in a meeting, or on vacation. This will go a long way toward helping you determine your staff's whereabouts in a disaster.

Volunteer Management Platforms

Many nonprofits operate with volunteers, and in this case, the internal communication should include key volunteers as well.

Additionally, volunteers often become available after a disaster, but problems can arise without proper management. The following volunteer management platforms may help prevent or reduce such problems.

GivePulse:

An all-in-one system to manage, communicate, register, and schedule your one-time and ongoing volunteers with shifts, a calendar, and a database.

4Bells:

A mobile application to deploy known volunteers to complete urgent, time-sensitive tasks, like delivering important documents, picking up a dog from the pound, or deploying volunteers after a disaster.

G Suite for Nonprofits:

You can use Google products to connect with, survey, train, and engage with volunteers. Capture volunteer information with Google Forms, streamline communication with Groups, engage and inform with Google Sites, and host trainings with Google Meet. Learn more from this Google video.

Office 365 F1:

This licensing is specifically for nonprofit volunteers and provides a lightweight way to quickly deploy the tools you use for internal staff to manage volunteers.

External Communications

Once you've triggered your internal communications plan, the next priority during and immediately after a disaster is to reestablish communication with those outside your organization — your community, including neighbors and government officials, those you serve, and those who support you.

Prioritizing Your Audiences

If the disaster is widespread, communication systems are likely to be overwhelmed, so prioritize who needs to be reached first.

Consider your constituents. Focus on services, functions, programs, and audiences first, before you consider machines, networks, and applications. Your Continuity of Operations Plan (see next module) will help you better identify this information.

- Who supports you?
- Whom do you support?
- Who relies on you the most?
- Who might be suffering as a result of the disaster and be in need?
- Which programs must continue through the time when you will rebuild? And which ones can be postponed?

Those who support you. Reach out to those who have provided or currently provide funding and other support to your organization, whether that be individual donors, foundations, or government entities.

Contact your insurance providers, if needed, to begin the claims process and to deploy their agents, adjusters, and restoration service providers to your site.

The demand for your services may increase after a disaster, so you need to be realistic about your resources and how many constituents you can serve if your organization or members of the staff have suffered damages.

Public Relations

You should also spend some time planning what your communication to the media will look like after a disaster. First and most importantly, you should decide *who* will be your organization's spokesperson during a disaster. This is important for two reasons:

1. It will ensure that the rest of your staff can focus on response work, not commenting to the media.
2. It prevents inconsistent, incomplete, and inaccurate information from getting out and confusing your message.

Make sure your spokesperson is kept in the loop as the disaster and response efforts unfold so they can accurately relay information to the media.

Pick someone who is calm under pressure, speaks well, and knows your organization — this does not necessarily have to be your executive director. Remember that the goal of public relations is to communicate effectively and get your organization's message across.

You might consider having digital templates for media packets ready ahead of time that include basic information about your organization, its mission and program, the last annual report, a one-page biography of the executive director, and prepared statements regarding disaster events and your organization's role in recovery, including how to support you. These can help the media quickly become familiar with your organization.

Additionally, it is important that your organization's information is accurately listed in public resources. Update your information in the local phone books, search engine listings, the Secretary of State's office, and any nonprofit association listing every year and anytime something changes.

Including Communications Plans in Your Information Backups

Don't forget to include a copy of your text/phone tree, check-in procedure, disaster group email address and website URL, disaster response activities, and other important contact information in your disaster box, master key, and cloud storage. Depending on how often you experience turnover on your staff, you may want to update it and distribute new copies to your staff a few times a year. The staff member you assigned to contact new employees not yet added to the text tree should write in new employees' alternate contact information on their copy of the text tree.

Continuity of Operations Plan (COOP)

The first step in creating a plan for operational continuity is to get key people from each of the main programs and services in your organization to help you. Do not forget to include someone familiar with your administrative operations. Together, you should address four major topics:

1. Identify business functions: What are the essential functions of your organization?
2. Conduct risk assessment and impact analysis: What sort of event could disrupt each of the business functions you identified?
3. Develop a continuity of operations plan: How will your organization continue its essential functions under a broad range of circumstances?
4. Identify policy considerations for disaster situations.

Part 1: Identify Your Organization's Business Functions

Identify essential functions that your organization cannot survive without; and then prioritize the other functions by their importance — taking into consideration funding, personnel, client needs, relevance to your mission, if there are other providers of the same service in your community, and other characteristics you find are appropriate. This establishes the order in which you will resume operations.

Part 2: Conduct a Risk Assessment and Impact Analysis

Before developing an action plan for what to prepare and how to recover, it's best to know what scenarios or risks you are preparing for. Your planning should start from identifying the potential disasters for your organization and what could happen if a disaster occurs.

A risk assessment considers the following factors:

Potential hazards and probabilities threatening these functions. What sort of event could disrupt each of the business functions you identified?

The likelihood of harm and its severity.

Steps to take to mitigate those risks and how you can implement them.

After identifying the possible hazard scenarios, determine how your organization and the services it provides will be impacted by the disruption during and after a disaster. This provides the basis for the investment in mitigation and recovery strategies.

Template

Use the templates below from Ready.gov to conduct risk assessment and impact analysis for your organization.

1 Risk assessment
(instructions included on the second page of the document)

Start from listing the important assets of your organization. Identify all the potential hazards that could cause an impact to your assets and the opportunities for prevention or risk mitigation. Then rate the probability of each type of hazard scenario and how it would impact each of your assets under the condition of existing mitigations. Higher hazard rating indicates a higher priority to create a mitigation strategy.

2 Impact analysis

The impact analysis should consider the operational and financial impacts resulting from the disruption, as well as timing and duration of a disruption. Use the Business Impact Analysis Worksheet from Ready.gov to gather information from managers and others within your organization who have detailed knowledge of the organization functions.

Part 3:
Develop a Continuity of Operations Plan (COOP)

The risk assessment and impact analysis act as the foundation of the continuity plan. Once that is complete, you need to document all the components of your COOP, which will identify resources and services you will need after a disaster to continue essential functions and other operations, and determine who will provide and how you will procure them in a disaster situation.

The plan should develop procedures for

Alerting, notifying, activating, and deploying employees

Identifying critical business functions

Establishing an alternate facility

Fostering personnel with authority and knowledge of functions

The COOP is important as a good business practice because the planning fosters recovery and survival in and after emergency situations, including localized acts of nature, accidents, and technological or attack-related emergencies. We recommend that nonprofit organizations develop and update a continuity of operations plan that includes attending to your IT systems See "Disaster Preparedness Plan for Your Organization's Technology" below.

Template

Use the COOP worksheet template in Appendix 1 to develop your own continuity plan.

Identify Alternate Operating Location or Facility

If you are not part of a larger organization or are unable to operate with staff working remotely, seek out organizations with a similar mission in other regions to develop a relationship with and where you can relocate your operations to in case of a disaster.

It is a good idea to develop plans for alternate locations for your offices in the event of a site-closing disaster, like a fire. If your organization has multiple sites, you may simply decide what operations would move to the other office. If you are a single-site organization, consider drafting a memorandum of understanding (MOU) with another nonprofit to establish a reciprocal arrangement that lets one nonprofit share office space with the other for a certain amount of time if a disaster should occur.

Replacement Equipment

Be sure to think about other office logistics and what you'll need to operate in an alternate location. This could be general equipment like furniture, computers, equipment, phone lines, and office supplies, or it could be specialized equipment that is unique to the work you do, such as medical supplies or logistics management equipment.

Memoranda of Understanding (MOU)

Having an MOU for an alternate site means you can have your office open and operating at some level within days, instead of weeks. A MOU is a signed agreement between two organizations that describes how they plan to work together. It should state the terms of the agreement, including goods and services being exchanged, time limits, compensation, and the scope of the agreement.

The MOU will not provide for every detail of the arrangement, but it does document the agreement and would be important in case of legal proceedings (see Appendix 1 for a sample agreement).

Part 4:
Identify Policy Considerations

You will need to establish board-approved policies for disaster situations:

How to activate the COOP:

Who has the authority to "declare" a disaster?

Succession of authority:

If the executive director is unavailable in a disaster, who is next in line? Do they have fiscal authority? Establish lines of succession based on position title, not individual, and extend the line of succession several steps deep. Communicate to staff members their position within the success plan.

Alternate decision-making:

Is your board's executive committee empowered to make major decisions without calling a full board meeting in a disaster?

Personnel:

Do your policies draw a distinction between essential and nonessential employees, and if so, what does that mean in terms of their compensation, responsibility, etc. Is that distinction included in their job description?

Payroll:

Who gets paid how much in a disaster situation? How long can employees expect to receive full compensation? Half compensation? Are employees required to have direct deposit? If not, how will they receive their check in a disaster?

Clients:

Depending on the nature of your organization's mission, you may need to develop policies about the type, scope, and availability of services in a disaster.

Additional Resources for Creating a COOP

Using a Business Impact Analysis and Risk Assessment to Prepare for Business Disruptions

Emergency Preparedness Resources for Businesses

Every Business Should Have a Plan, a 12-page booklet from FEMA

Risk assessment:

- From Ready.gov
- From the Canadian Centre for Occupational Health and Safety

Additional risk assessment template from CCOHS

Sample risk assessment (PDF)

Business impact analysis

Business continuity plan from FEMA

Business continuity resource worksheet

Read more about COOP:

- Continuity of Operations Planning (COOP), Boston University
- COOP Brochure (PDF), FEMA
- Continuity of Operations Guidebook and Template for Nonprofit Service Providers, San Jose State University

Step 3:
Disaster Preparedness Plan for Your Organization's Technology

Basic Principles of Technology Disaster Planning

What does it take for technology disaster planning? The good news is that technology preparedness can be achieved in varying measures (every little bit counts), and there are a lot simple preparedness measures that are in reach of even the not-so-technical people.

Let's take a brief look at those building blocks that can help minimize the impact to your infrastructure in the event your organization is impacted by a physical or virtual disaster:

Keep clear documentation of the key components of your IT infrastructure.

Put data loss prevention protections in place.

Enable remote access to your on-premises data and systems
or (better yet)
move those systems to the cloud.

Increase the access security of your important data.

Set up a unified communications system for your organization.

Documentation

The Challenge

Your technology infrastructure has likely evolved over time. Chances are you've had a dozen different "tech" people working on your computers over the years, without leaving a single page of documentation. You've probably added new hardware and software applications or upgraded older ones since they were initially installed. And you may very well be maintaining a historical dataset on a 12-year old-computer because it wouldn't import into your new CRM system.

This is pretty typical for most small organizations, and it may hinder your ability to recover from a disaster quickly.

The Solution

In order to improve your organization's IT resiliency, you must first identify and understand every component of your technology infrastructure. This includes components located on premise, as well as equipment and data stored in remote locations, or managed by others, including contractors and "cloud" platforms.

Before you say "We have an IT department for this," or "We contract our IT services to ____," just know the executive director of the organization is ultimately responsible for the success or failure of the business. They can (and probably should) fire the IT team if they can't recover your systems after a disaster. But that won't necessarily save the organization or avoid a significant finding during your next audit. That said, it's essential for nonprofit leaders to understand their technology infrastructure as it relates to their operations.

It's important to note that many technologies are dependent on other systems or components in order to function properly. For example, a VoIP telephone system may require user account authentication from an Active Directory server. If the server is unavailable, users may not be able to access voicemail.

Some installed versions of software are sensitive to the environment and may need to be returned to their exact state or version before they will work after recovery. A common example would be an accounting system that receives regular software updates. If it was purchased three years ago, you may have installation files for version 12, but with the updates, you may now be running version 14.10. Reinstalling version 12 from CD on a new computer may work, but the program may not be able to read your company data in the database since it's a much newer version.

Maintaining comprehensive documentation of your environment, and a physical inventory of all hardware and software assets, will enable you to identify and prioritize your recovery objectives.

Data Loss Prevention

The Challenge

Although we typically associate "disaster" with physical damage and destruction, most technology disasters are caused by hardware failures, computer viruses and malware, or careless users. A failed hard disk will generally lose all files stored on the disk, with slim chances for recovery. Similarly, a crypto-virus will encrypt every data file it can find on the affected user's machine, as well as any network-connected drives, rendering them unusable. This type of event can cripple an entire organization and can only be reversed by paying an extremely large ransom to the hackers.

The Solution

There are simple things that nonprofits and small organizations with fewer resources for a comprehensive technical solution can do to protect important data.

Protect against viruses and malware:

Protect computers against viruses and malware by installing a reputable antivirus product.

Reduce spam by utilizing your email system's built-in filtering settings.

Educate users to recognize suspicious emails and websites through cybersecurity training.

Password-protect AND implement multi-factor authentication (MFA) for any constituent relationship management and donor database applications and log out each time you finish using them.

Back up your data:

Save data frequently and ensure that you are backing up important documents and databases, preferably in the cloud (e.g., online storage, near-line storage, and offsite/offline storage).

Create and securely store recovery discs (for installed software applications) to restore your nonprofit's computers to a working state. If discs are not available, check online to find procedures and solutions applicable to you.

Back up data from cloud-based applications — even the cloud software providers can lose your data. Implement a separate backup service. File storage and sharing services like Google Drive, OneDrive, or Dropbox should be considered as another data repository that needs to be backed up to prevent service and access interruption.

Remote Access

The Challenge

Moving to remote work, a.k.a working from home, the cafe, or the public library, can be triggered by a desire to reduce the size of your office or an employee who moves for family reasons. In the situation of a disaster, there may be an even more urgent need for remote access when the office facilities are destroyed and access to important data is restricted. It can be the factor that determines how quickly your organization can get up and running.

The Solution

There are two solutions to accessing operational information and systems remotely:

1. Ensure that your systems and data are digitized and moved to the cloud. Move to cloud-based software and infrastructure systems that are hosted in the cloud. This is the single best way to maintain continuity of operations when physical access to your office is not possible.

2. Set up remote access software and tools using a VPN and remote desktop software. You will need a security appliance that offers firewall protection and VPN capability (Cisco Meraki offers several) to give encrypted and secure access to systems located in the office. For software that is installed on a specific computer or server in the office, you can use a remote desktop client (RDC) that will allow you to access that machine from anywhere. Do NOT use any free versions of RDCs: They may be giving hackers free access to your systems.

Information Security

The Challenge

Information security is undoubtedly one of those terrifying and intimidating ideas, not because we don't see the value in it, but because we don't know how to go about "becoming" secure or knowing if we're "secure enough."

To really understand the importance of overcoming our hesitance in taking that leap, it's important to understand the consequences of not taking on that battle.

Imagine that you just had your annual gala. It was a grand event with outstanding attendance, 70 percenf first-time guests (a lot of whom made generous gifts afterwards). It set the stage for another great annual gala for the next year. Now imagine that due to a "security incident" caused by your development director, who cannot tell his iPhone from TV remote, all the spreadsheets and files containing data from your annual gala, including event attendances, ticket purchases and gifts made afterwards, are now information publicly available on the Internet. How many of those first-time guests are going to translate into repeat donors or loyal advocates?

Yes, information security is very important, no matter the size or scale of your organization. So how do you secure your information?

The Solution

Although it's hard to achieve 100 percent security, you can take incremental steps to make your information more secure than it may be now.

Data encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption doesn't prevent information from being intercepted, but it denies access to the content of the message. Encryption can be tied to biometrics of authorized individuals.

The use of encryption might not be a strategy that most organizations consider. However, in some instances, state and federal laws may dictate a certain level of encryption for sensitive data. This is particularly true for health information.

In all cases, however, people who trust you with their personal information deserve your protection. They include donors, constituents, grantees, and volunteers. Consider activating three levels of encryption:

File encryption

allows for individual encryption of files so that they can only be unlocked with a password. (Beware: If you rely solely on a software program's password protection, the file itself may not be encrypted.)

File system encryption

allows for an entire directory of files or even an entire operating system to be encrypted. This feature is available for certain operating systems and through third-party programs. It's also available for mobile phones and tablets.

Full-disk encryption

encrypts the entire drive, using a combination of hardware and software. This is the most secure level of protection against physical loss caused by a disaster.

Unified Communications

The Challenge

Every nonprofit communicates with its staff and the public in unique ways. In the case of a disaster, the office facilities may be damaged, restraining your access to phone systems, computers, or other important devices that you rely on to communicate with your employees, volunteers, donors, constituents, and other personnel.

The Solution

Unified communications (UC) refers to a collection of technologies and organizational practices that simplify and integrate multiple forms of communication. UC is not necessarily a single product, but a set of products that provides a consistent unified user interface and user experience across multiple devices and media types. These communications can include phone, email, video and web conferencing, texting, voicemail, social networking, and document transmission. The devices, or endpoints, of your UC system can be a computer or any mobile device (cellphones, tablets, etc.).

For example, one can receive a voicemail message and choose to access it through email or a cellphone. If the sender is online according to the presence information and currently accepts calls, the response can be sent immediately through text chat or a video call. Otherwise, it may be sent as a non-real-time message that can be accessed through a variety of media.

The main advantage of UC is that staff members have the ability to receive calls or access and reply to messages through whatever device is available at the moment. That feature reduces lag time and facilitates internal and external communication.

There are complete UC systems available such as those available from Microsoft's Office 365 and Microsoft 365 cloud solutions. And UC systems can be created through the integration of a variety of excellent telephone, email, online chat, group collaboration, and video conferencing tools.

Analyzing patterns of communication for your organization can aid your decisions on which communications solutions to choose (see "Emergency Communication Plan" above).

Summary

A good indicator of whether your organization is well equipped to give your employees ready access to essential business systems and enable them to track data consistently in the aftermath of a disaster is if your organization is well equipped to do that on any ordinary day.

Data Backup Solutions

There was a time when all information was kept in paper files and your key information was but one step from disappearing in a fire, flood, or hurricane. Today the widespread use of digital files means you can more easily make copies and backups, reducing (but not eliminating) the likelihood of data loss.

Fires, floods, hacks, and viruses can still destroy your data, so having redundant data storage is important to prevent the loss of important information and documents. Consider the following when deciding how to manage your data storage and backup:

Scope and frequency of the backups — how much data to back up and how often?

Strategies to back up the data — what devices and applications do you plan to use?

Security of backups — how to ensure the security of the private and sensitive information?

Documentation of backups — how to keep track of the backup records?

Scope and Frequency of Backups

A full backup

is the most complete and also the most time-consuming. It also requires more storage space than other options.

An incremental backup

only backs up files that have been changed or created since the most recent incremental backup. This is faster and requires less storage space. However, in order to restore your files completely, you will need to have all incremental backups available. And in order to find a specific file, you may need to search through several incremental backups.

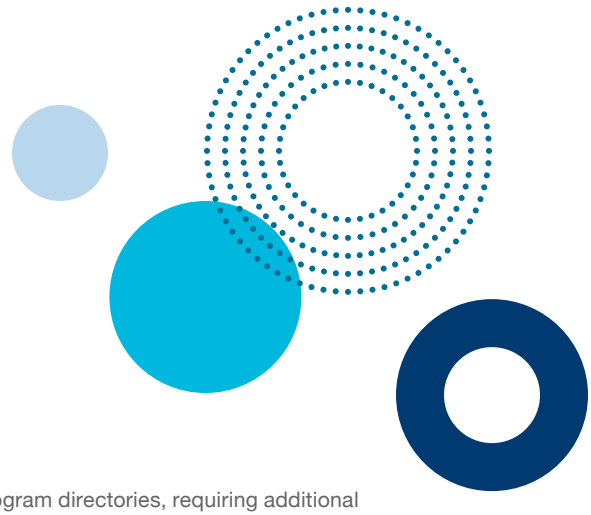
A differential backup

also backs up a subset of your data, but only backs up the files that have been changed or created since the last *full* backup.

A bare-metal backup,

also known as a "snapshot," is a full-system image backup. If you have the expertise and storage space, choose this option. It minimizes the time to reinstall and reconfigure your operating system in the event of a disaster.

In addition to backing up critical data, don't neglect to back up Windows files and folders that are stored on the desktop, or the bookmarks in your browser.[3] Some programs will also allow you to back up configurations or settings. Find out if your programs support this functionality.



3. Special database- or financial-software packages may store files in their program directories, requiring additional backup. Some browsers such as Chrome allow you to sync your bookmarks online.

Data Backup Strategies

There are three broadly defined strategies to backing up:

1. Remote backup
2. Cloud-based backup
3. On-premises backup

Whatever methods you choose will use software that schedules backups at regular intervals.

PRO TIP

Due diligence is required in making a selection from among these options. Three key considerations are support, redundancy, and security.

Support

Staff expertise — Who has the time, knowledge, and trust of the organization to accomplish these chores or oversee their successful outsourcing?

IT budget — What are the base and additional storage charges?

Reliability and speed of Internet service — How fast is its service both downstream and upstream?

Security

Is the data encrypted by you or by a provider? Who has access to the machines, networks, or processes that store data?

Redundancy and recovery needs

Amount of organizational data generated, and what data would be most essential in the event of a disaster — Is there a guarantee or an insurance of a successful recovery?

Need for rapid restoration of data — Where is the data held, in a dedicated data center or a co-located third-party provider? Do you or the provider have disaster experience?

Here is a chart comparing the different backup strategies.

Type	Description	Pros	Cons
Cloud	Data is backed up to a third-party site, with redundancy and availability of the provider's choosing.	• This option is considered safe from hardware failures, and therefore from lost files or databases. • It is generally lower in cost, regardless of the size of your organization's technological infrastructure.	• Since data is offsite, it may take time to download files and folders. • Large image files may take hours to days to fully synchronize, depending on connection type and speed.
Remote Backup	Data is backed up to a remote location but managed by your organization.	• You pay for storage and traffic, not for the equipment. • In the event of a localized disaster, your data is still viable. Software for regularly scheduled backups is included in your subscription. • This option is good for organizations with multiple workstations and large amounts of data.	• Internet access is required to back up your data. Data recovery takes time if done via the Internet. • Your provider may be able to ship your data on a USB drive, but you may incur extra costs. • You have to entrust critical data to a third party.
On-Premises (Least Secure: Recommended only for specific situations)	Data is backed up to a device or media located on-site **Example:** USB flash drives, an external hard drive, or a shared drive on the network.	• All the data is within your reach and is available for immediate retrieval. • This option is manageable for a small organization with fewer workstations and devices.	• TData backed up to portable media is vulnerable to loss, theft, or damage. • Most operating systems have only rudimentary backup features, so you should consider specialized backup software. • It is still essential that you store copies of backup data off-site.[4]

4. Ideally, backups are stored in a fireproof safe deposit box and rotated in and out once a week. Another method is to follow the 2x2x2 rule: two sets of backups that are held by two different people in two different locations. Frequency and redundancy may be determined by your organization's resources.

Cloud Backup Solutions

If you could choose only one backup strategy to increase your organization's IT resiliency, it would be to move as much of your organization's files and data to cloud-based applications and systems as possible.[5]

As we've discussed before, in the event of a disaster, quick access to your office computers, network, and resources is hardly a guarantee. Moving files from desktop-based applications to web-based apps will allow personnel to work easily from off-site locations with advantages for your ongoing work. It also increases the ease of restoration following a disaster.

In assessing your organization's ability to back up files to the cloud, consider these factors:

- Your Internet connection
- Satellite or affiliate locations of your nonprofit
- Data scale
- Data types
- Relative costs of hosted services per user
- Data access controls, security, and scalability
- If you have more than one method to protect a variety of applications and data

Choosing Remote Backup Solutions

There are a wide variety of remote backup solutions (meaning storage plus service fees) available on the market, and new players are coming on the market all the time — IDrive, Backblaze, Acronis True Image, and Carbonite. Additionally there are many independent providers that can tailor services to your organization's needs. TechSoup has a service that is specific to nonprofits.

5. You can read a summary of the pros and cons of cloud migration at http://www.techsoup.org/support/articles-and-how-tos/what-are-the-benefits-and-drawbacks-of-cloud-computing

Choosing On-Premises Backup Hardware

All the following information about on-premises backups might be unnecessary if you migrate to the cloud.

Determine how much data you need to back up.

Survey the machines on your network or at least a representative sample.

- How large is each user's documents folder?
- How large is the email file?
- How much data is in your organization's primary shared folder?

Add up the totals for all your machines, or multiply the average by the number of machines in your organization. Be sure to leave room to add a few new staffers and to plan for growth — additional bytes of data per person will add up in a year.

Double that number.

Choose a backup solution that allows you to store at least double the amount that you think you will need to back up every three months. This will give you room for growth and will also allow you to store incremental backups on the same media as full backups.

Consider the device's speed and how it interfaces with your computer.

When you have a large amount of data to back up, a big storage device is less useful if it writes data slowly. Make sure your hardware can support reasonably fast data transfer rates.

Network Attached Storage (NAS)

NAS is a great solution for nonprofits that want to back up a lot of data easily. Disk-based technologies such as backup and file-storage servers, as well as external hard drives, are the backup media of choice. NAS devices offer disk-based storage like a dedicated file server or backup server, however, it's small and portable. Depending on the model, NAS devices may offer specific features such as scheduled backup or FTP access. You can also back up data from NAS via an external drive to store off-site.

Storage Area Network (SAN)

For larger networks and disk space requirements, a SAN is a network of storage devices that are accessed and shared via standard network communications. If you want to use NAS or a SAN, you must have a robust network that can properly support fast data transfers within the network.

Portable Storage Devices

CDs, DVDs, and portable flash drives are convenient and cost-effective, but they are inappropriate as your organization's primary local backup solution. They are less secure than other backup solutions, and they discourage best backup practices, such as completion of incremental backups.

Backup Software

Dedicated backup software allows for more detailed refinement of the backup options as well as more sophisticated management of multiple computers. It also allows for a wider view of all the data that is backed up, for example, and less intervention on the actual computer itself.

PRO TIP

Make sure your backup software has full read-back verification and test the backups BEFORE you need them. Simulate a disaster scenario and try to restore a few files to a different computer at a different location.

Email

It's important to understand your organization's email system, where your messages, calendar appointments (if applicable), and contacts are stored, and whether email attachments are automatically stored locally, or by your email service provider.

If your organization uses an in-house email server (e.g., Exchange server), you must include it in your backup plan. Email servers require special backup utilities.

If you use a webmail service (Google G Suite, Office 365), check with your email service provider about its backup and restore policies.

If you use a webmail service offered through your Internet service provider (ISP), find out whether the ISP backs up your email messages and document the process to recover lost or deleted messages.

If your organization doesn't use an in-house email server, and doesn't use a cloud service, then mail is stored locally on users' computers. The mail folder on each computer must be backed up.

- As an example, a Microsoft Outlook data file (.pst) contains your email messages, calendars, contacts, tasks, and notes. It may be stored in one of the following default locations:

  drive:\Users\<username>\AppData\Local\Microsoft\Outlook

  drive:\Users\<username>\Roaming\Local\Microsoft\Outlook

  drive:\Users\<username>\Documents\Outlook Files

  drive:\Users\<username>\My Documents\Outlook Files

  drive:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Outlook

Website

If you host your website on-site on an in-house server, then it should be backed up like any other server. If it's hosted off-site, make sure your web hosting provider is backing up the data (be sure to review the provider's data backup policy). As with other services that are managed by a third party, it's a good idea to maintain a copy of your website, preferably on a cloud-hosted server.

Security of Backups

The physical security of your backup media and data is just as important as your production network. Backups must never be stored in an unsecured location, particularly if the data contains private and sensitive information about your organization, employees, and donors. Backups should be password protected at a minimum and encrypted if possible.

For online and network drive backups, use a user account separate from your local administrative account. Most servers and domains have a designated backup account with restricted permissions for this purpose. The permissions will usually allow files to be copied during a backup operation but restricted from being opened or executed. Embracing this strategy will provide an extra measure of protection in the event your user account is compromised.

Keeping Clear Documentation of Backups

Remember that regular backups and clean, clear documentation go hand in hand. In a TechSoup survey, 86 percent of organizations backed up their records regularly, but only 69 percent had clear documentation of how and where critical data was stored. In addition to choosing the appropriate backup to use, make sure to document what is being backed up and to where.

Securing Your Equipment and Devices

In every office environment, there are multiple systems that will need to be physically protected and backed up regularly. In addition to each user's desktop or notebook computer, you must include local servers, network attached storage drives, telephone systems, and networking equipment in your planning.

Physical Security

Your computers, data files, and network infrastructure should be secured as tightly as your HR file cabinet and company checkbook. Servers, routers, and backup media should always be located in a locked room, with access restricted to essential employees or authorized contractors.

In addition, you should never allow anyone to access your physical or wireless production network. If your organization would like to provide wireless access to clients or customers, a separate guest network should be created with appropriate security measures in place to isolate each network from the other.

Power Supply

Power for your on-premises equipment is critical to the preparedness of your organization. Ideally, mission-critical facilities will have a standby generator permanently installed to provide temporary power to the building during extended power outages. These backup power systems use an automatic transfer switch that can sense the loss of power from the grid, start the generator, and provide power to prewired circuits.

Although portable gasoline generators are relatively inexpensive and convenient, they can burn up to a gallon of fuel per hour and will need to be refueled often. Unless you have a steady supply of fuel, and staff to refuel regularly, portable generators are usually not a tenable strategy.

For brief power outages or unpredictable power surges, an uninterruptible power supply (UPS) is an effective way to protect your equipment. Although laptops and mobile devices have batteries, desktop computers, networking equipment, and servers do not. It is beneficial to connect all networking equipment, servers, and desktop computers to UPS units. Compared to a basic power strip or surge protector, a UPS has a built-in battery that will enable the user to initiate a graceful system shutdown. Some UPS models have the ability to connect to computers via a serial or USB port and can automatically initiate a shutdown.

You should budget to replace UPS batteries every two years. A good strategy may be to replace half of your UPS batteries each year.

Servers

On-premises servers not only store your organization's files and application data, but may also control the security of your network. The loss of a domain controller can prevent users from accessing data or other resources on your network, so it is essential that these systems be backed up regularly.

Today's technologies allow administrators to take "snapshots" of server data several times a day, which is helpful in quickly restoring files in the event they are overwritten or accidentally deleted. There are different types of backup strategies that can be employed to protect your equipment, which vary by vendor and objective. It's good practice to conduct a full backup of your server before installing monthly updates, as well as major line-of-business application updates. This will ensure you have a way to "roll back" or restore your server's hard drive if anything goes wrong during the update.[6]

Personal Computers

Regardless of whether your employees, contractors, or volunteers work with their personal computers, your organization's data should always be part of a regular backup strategy. Remote backup services are available that will back up file- and folder-level data from remote users even when they are away from the office network. Alternatively, you could provide remote users with VPN access to your work network to save files, or you could use a shared storage location through the Microsoft Office 365 or Google Apps platforms.

6. A proper file server should also have a server-class operating system, with hot-swappable hardware RAID. (RAID stands for "redundant array of independent disks." A RAID system divides and replicates data among multiple physical drives, which protects the data from loss in the event of a disk error.)

Mobile Devices

If you store critical data on your mobile devices, such as contact lists or other documents, this data needs to be backed up as well. It's generally not recommended that you store sensitive data on a mobile device. However, if you must keep that data on a mobile device, those files must be encrypted. For instructions on how to encrypt your files, see the device's manual or find instructions online.

For phone backup, you can choose which apps you wish to back up to the cloud, or you can link to a personal Microsoft account or file- and photo-sharing apps. Check your owner's manual or find instructions online.

For tablets or music devices, check for internal storage capacity and for backup frequency using the owner's manual or through online instructions, just as you would for your organization's computers. Also, check out which cloud-based options are available to you.

Networking Equipment

Network and infrastructure equipment requires configuration that takes time to reconstruct. Information such as ISP connection details, reserved IP addresses, special routes, and wireless settings should be backed up as well. Both retail and enterprise-level networking equipment allow you to back up configuration information if you access the device via a workstation. Ask an IT professional to document your network configuration and save it to a file.

Redundant Internet Connection

Almost every organization has experienced an Internet outage, regardless of whether the service is provided by the phone company, cable company, or wireless provider. Each technology has vulnerabilities — cable cuts, power outages, and so on. If your organization relies on Internet connectivity to access cloud applications or communicate externally, you should strongly consider installing a secondary connection through a different provider. Provider diversity is a key strategy for resiliency, and the additional expense is negligible compared to lost productivity.

Phone Service

Voice over Internet Protocol, or VoIP, is a modern and convenient way for organizations to connect telephones over computer networks. What once meant waiting for weeks for traditional phone lines to be installed can now be accomplished by administrators in minutes. Workers no longer need to be inside the office to make and receive phone calls over company phone lines.

While most VoIP PBX systems are hosted in the cloud, many offices have hybrid systems where the phone lines are physically terminated at the main office location, but remote users are able to connect via an Internet connection.

These systems require special consideration during planning, as they require special network configuration. Your facility may be inaccessible during a disaster, and you may not be able to access your phone system to forward calls during a power or Internet outage. Check with your telephone provider to see if disaster routing services or remote call forwarding are available to allow you to redirect phone calls to an alternate phone number or branch office remotely.

Step 4:
Train Your Staff Members

It's useless to have a disaster plan if the staff members don't know about it or they forget about its existence. For many organizations, even those that regularly work in disaster zones or with the needy on a daily basis, staff training on disaster preparedness is inadequate. To prepare all the members in your organization for responding to future disasters, it's necessary to inform them about the plan, provide necessary training, practice regularly, and keep the plan updated.

Inform and Train Your Co-Workers

Use newsletters, intranets, staff meetings, and other internal communications tools to communicate emergency plans and procedures. Conduct regularly scheduled education and training seminars to provide co-workers with information, identify needs, and develop preparedness skills. Include disaster training in new employee orientation programs.[7]

7. Source: https://www.fema.gov/media-library-data/1389022685845-7cdf7d7dad7638a19477d01fdbfa820f/Business_booklet_12pg_2014.pdf

Practice and Revise the Disaster Plan Regularly

Just like a fire drill, you might simulate disasters that affect the regular operations of the organization. It can be as minor as an Internet outage. How will the staff respond? Did the backup last run properly? Did the restoration work as expected?

You can then do a post-simulation analysis to fill in any gaps in the plan or to work with staff members who need additional training.

Your community may have regular disaster emergency drills that are a part of its community preparedness programs. Capitalize on these occasions to do your own internal preparedness review and updates. If you rent, lease, or share office space, coordinate and practice evacuation and other emergency plans with other businesses in your building or facility.

Backup Staff Planning

It is estimated that 30 to 50 percent of employees will not show up for work during and after a disaster for a variety of reasons. They may be impacted personally, or have other family members to take care of. Schools will likely be closed for several weeks, so they may have issues with childcare. This means all employees should be cross-trained to handle other duties during a disaster.

Follow the rule of three[8] — at least three people should know how to perform the essential backup and recovery tasks.

Identify the top 10 crucial IT duties and cross-train staff regularly so they are easily able to execute those crucial duties during transitions, vacations, illnesses, and other absences.

7. Source: https://johnkenyon.org/nonprofit-technology-planning-for-turnover-and-disasters/

Employee Transition

Employee transition offers a good time to raise awareness within the organization and make necessary revisions to the disaster plans. Here are some guidelines when employees transition in and out of your organization.

When a new staffer joins your organization:

Update your backup plan. Add new staff member data and take the opportunity to review your backup plan and revise it if necessary.

Include the plan in the routine onboarding process. All new staff members should be required to read your backup plan, especially any organization-specific information. This ensures that they are informed of your organization's setup.

When staff members leave the organization:

Your plan and documentation should be updated.

Additional tasks:

Keep a list of up-to-date email addresses for former employees in case the employee forgot to document crucial information.

Change any passwords that a departing employee had access to, including passwords for the organization's presence on any social networking sites.

If the employee had a master key, or passwords that decrypted files, be sure to change those as well.

Appendix 1: Checklists

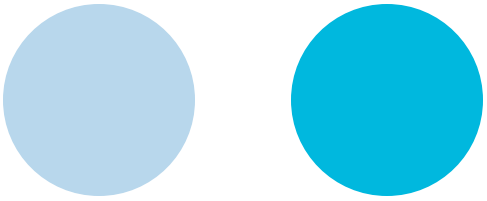
You can download these checklists for use in your organization.

All are PDF files.

- **Disaster Box Content Checklist**
- **Employees Contact Record**
- **Technology and Facilities Information**
- **Pre-Evacuation Report**
- **24 Hours Prior to Evacuation**
- **Continuity Worksheet**
- **Memo of Understanding Sample Template**

Appendix 2: Other References

- **Survey of Hospital Employees' Personal Preparedness and Willingness to Work Following a Disaster**
- **Nonprofit Technology Planning for Disasters (and Turnover)**, John Kenyon
- **Continuity of Operations: an Overview**, FEMA (PDF)
- **Continuity of Operations Planning**, Boston University Department of Emergency Management
- **Every Business Should Have a Plan**, FEMA (PDF)
- **What Are the Benefits and Drawbacks of Cloud Computing?**, TechSoup



techsoup

Main Office

TechSoup
435 Brannan Street, Suite 100
San Francisco, CA 94107
(415) 633-9300
Email Customer Service

Press Contact

Email PR at TechSoup
(415) 633-9403

Affiliate Accounts

Organizations with multiple members or affiliates, and those looking to place donation requests for 20+ organizations, please contact us here.

Business Development

For information about donating products, see Become a Donor Partner.