The Resilient Organization

A Guide to IT Disaster Planning and Recovery
<table>
<thead>
<tr>
<th>07</th>
<th>11</th>
<th>15</th>
<th>16</th>
<th>19</th>
<th>22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Understanding Basic Principles of IT Resiliency</td>
<td>Preparing for the Worst and Planning for the Best</td>
<td>Assessing Your Organization</td>
<td>Centralizing Information</td>
<td>Technology Priorities Assessment</td>
</tr>
<tr>
<td>23</td>
<td>25</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>Key Recovery Staff</td>
<td>Project Planning and Rollout</td>
<td>Technology Recovery Contacts</td>
<td>Report Requirements</td>
<td>Supplier Contact Details</td>
<td>Phone System Recovery</td>
</tr>
<tr>
<td>36</td>
<td>38</td>
<td>39</td>
<td>43</td>
<td>47</td>
<td>50</td>
</tr>
<tr>
<td>Files and Databases</td>
<td>Types of Backups</td>
<td>Types of Approaches</td>
<td>Our Best Advice</td>
<td>Guidelines for Choosing On-Premises Backup Hardware</td>
<td>Backup Software</td>
</tr>
<tr>
<td>32</td>
<td>33</td>
<td>36</td>
<td>51</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Master Key</td>
<td>Staff Members and Training</td>
<td>Files and Databases</td>
<td>Email</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Page</td>
<td>Section</td>
<td>Page</td>
<td>Section</td>
<td>Page</td>
<td>Section</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------</td>
<td>------</td>
<td>-------------------------------</td>
<td>------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>52</td>
<td>Website</td>
<td>64</td>
<td>Rebuilding Your Organization</td>
<td>80</td>
<td>If Records Are Inaccessible</td>
</tr>
<tr>
<td>54</td>
<td>Equipment and Devices</td>
<td>67</td>
<td>Files and Databases</td>
<td>82</td>
<td>Equipment and Devices</td>
</tr>
<tr>
<td>56</td>
<td>Power Supply</td>
<td>69</td>
<td>If You Have On-Site Backup Storage</td>
<td>84</td>
<td>General Safety Tips</td>
</tr>
<tr>
<td>57</td>
<td>Servers</td>
<td>71</td>
<td>If Your Backups Are in the Cloud</td>
<td>86</td>
<td>Hardware Recovery Tips</td>
</tr>
<tr>
<td>58</td>
<td>Personal Computers</td>
<td>72</td>
<td>Lost Passwords</td>
<td>88</td>
<td>Network Recovery Tips</td>
</tr>
<tr>
<td>59</td>
<td>Mobile Devices</td>
<td>74</td>
<td>Email and Phone</td>
<td>90</td>
<td>Mobile Internet connectivity</td>
</tr>
<tr>
<td>60</td>
<td>Networking Equipment</td>
<td>77</td>
<td>Your Website</td>
<td>92</td>
<td>About the Guide</td>
</tr>
<tr>
<td>62</td>
<td>Recovering from Disaster</td>
<td>79</td>
<td>Proving Your Identity</td>
<td>93</td>
<td>Partners</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introduction
This e-book is designed for those of you who have been tasked with securing the technical future of your organization.

We’ll walk you through some of the basics for IT resiliency and how to prepare your organization and IT systems to bounce back more quickly from a disruptive event. We’ll also show you how best to move through the recovery process.

A nonprofit has many stakeholders who rely on its security and program delivery: people who receive services, grantees, donors, volunteers, and personnel. You may or may not have any educational or professional background that pertains to information technology, but you’ve found yourself with the responsibility for this aspect of your organization’s work.

You might have advance warning of a disaster that allows you time to prepare, or you might unexpectedly find yourself in the middle of a disaster.

Don’t despair. This guide will provide you with the basics you need to have at hand and attend to in the face of a human-made or natural disaster.

This guide isn’t intended for organizations whose early rescue or relief operations may put staff members in danger. For those in dangerous situations, please refer to the local Red Cross at http://www.redcross.org/get-help or Red Crescent at http://www.ifrc.org/en/news-and-media/current-operations/.
A disaster is a disaster. Some of you may have already experienced significant disruption from wildfires, earthquakes, and hurricanes; others, sabotage from former employees, damage during civil unrest, or criminal activity. All of these events can result in damaged computers, lost data, or both. In a survey TechSoup undertook, 86 percent of organizations backed up their records regularly, but only 69 percent had clear documentation of how and where critical data was stored.

This is the third major revision of *The Resilient Organization: A Guide to IT Disaster Planning and Recovery*. The initial version of this guide was written shortly after Hurricane Katrina struck the southern United States in 2006.

In this latest version, we’ve divided the e-book into three sections so that you can jump in at the stage appropriate to your interests and your organization’s need:

1. Understanding Basic Principles of IT Resiliency
2. Preparing for the Worst and Planning for the Best
3. Recovering from Disaster

Following the advice in this document will increase your organization's resiliency.

*You’ll increase your capacity to survive a disaster and to rebuild your IT infrastructure so that you can resume your primary activities.*
To improve your organization’s IT resiliency, start with preventing data loss, encrypting your data, and unifying your communications.

Data loss prevention refers to preventing the loss of any data by taking appropriate security and disaster preparedness measures. There are simple things that nonprofits and small organizations with fewer resources for a comprehensive technical solution can do to protect important data.

Protect computers against viruses and malware.

Maximize spam prevention.

Educate users to recognize suspicious emails and websites.

Open email from known senders only.
Be suspicious of odd subject lines and "social engineering" designed to trick users into taking actions that would compromise your security, such as clicking a link or providing personal information.

Password-protect any constituent relationship management and donor database applications and log out each time you finish using them.¹

Save data frequently and ensure redundancy of important documents and databases.

Save recovery discs to restore computers to a working state.

If discs are not available, check online to find solutions applicable to you.²

Consider cloud-based solutions and specify how they and you will safeguard online data by ensuring that the service is specifically designated "online backup" or "remote backup."³

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.⁴

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.⁵ 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.⁶

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" (UC) refers to technologies and organizational practices that simplify and integrate multiple forms of communications. These communications can include phone, email, video and web conferences, SMS, voicemail, social networking, and document transmission.

This effort often involves centralizing services via Internet Protocol (IP), rather than disparate service providers. The main advantage is that employees have the capacity to access and reply to messages with the use of whatever device is available at the moment. That feature reduces lag time and facilitates internal and external communication.

Analyzing patterns of communication (see section on preparedness) will aid your decisions about communications.

---

1. Periodically download data of this type using the Export as CSV ("comma separated values") function to save to a server or a backup location.

2. In Windows, recovery disc creation differs by version. In macOS, press Command-R to initiate the macOS recovery process. You can also download a separate "Recovery Disk Assistant" on a USB drive.

3. A file-sharing service like Google Docs, OneDrive, or Dropbox should be considered as another location that needs to be backed up to prevent service and access interruption.

4. For example, HIPAA in the United States requires encryption; see [https://www.hhs.gov/hipaa/for-professionals/privacy/](https://www.hhs.gov/hipaa/for-professionals/privacy/).

5. Microsoft Word, for example, allows for password protection and encryption under the "Protect Document" settings.

6. For Windows, BitLocker technology can encrypt the entire drive or a data folder. For macOS, FileVault is available for macOS Panther and up, with levels of implementation that vary. This feature is available for Android or iOS mobile devices as well.
Preparing for the Worst and Planning for the Best

A disaster may never hit your office, but if you adopt certain technologies and strategies, you can deepen your work and its impact. You can also make your organization faster and more efficient in responding to challenges and opportunities. Smart preparation is one of the ways in which you fulfill your organizational mission and lessen any disruption in your day-to-day operations.

Any organization-wide project requires administrative leadership, subject-area knowledge, and a commitment of staff time. The same is true for increasing your organization’s capacity to withstand a disruption to its IT system. You’ll need the support of the organization, as well as a basic familiarity with the terms and processes described in this document. You’ll also need work assignments dedicated to completing and regularly updating the protection of your IT infrastructure, files, and databases.

Ensuring the health of your IT services may be a part of a larger organizational plan to prepare for major changes such as leadership succession, economic downturns, or personnel shifts. As you read through this e-book, please note that we have recommended the development or updating of a Continuity of Operations Plan (COOP) that includes attending to your IT systems. And, at a minimum, we encourage you to consider migrating your files and database storage to the cloud.

As you read through the e-book, you'll find questions for discussion and charts for recording your IT materials and processes. We’ve also included descriptions of specific steps you can take to protect your workplace, and resources and products to guide your deliberations and actions.

This section on preparedness has three goals:

- To document essential processes and reduce downtime during an emergency;
- To devise a sound backup plan;
- To protect your systems, equipment, and devices.
Assessing Your Organization

Here are some questions you can use to guide the development of a responsive IT disaster plan.

1. How do employees most regularly communicate with each other: by phone or by email?
2. Do employees use personal phones and email addresses for work?
3. Do volunteers, contractors, and other people who aren’t staff members use the office telephones, email accounts, and computers?
4. What steps would be necessary to re-establish communication in a disaster situation?
5. Where is data held: remotely or on-premises?
6. Where is the data that needs to be backed up?
7. Do you have hard-copy data (government forms, contracts, leases, financial information, or personnel information) that requires backup? Are these documents stored in a waterproof safe or file cabinet, as well as scanned or computer-generated?
8 Is there an inventory of all information hardware (personal computers, laptops, phones, mobile phones, servers, files, and networking equipment)? Warranties and receipts?

9 Are staff members adequately and regularly trained for emergencies?

10 Consider the physical and utility outcomes of various scenarios (flood, tornado, power outage, fire, and so forth). What is the likely damage that will affect IT infrastructure and functions? Do any of these impacts alter your preparedness plans?

11 Investigate your insurance policies to determine what sort of coverage you may have for loss of work, location rental, recovery services, and equipment and device replacement. Your coverage, and any support from the government and disaster service organizations, will determine much of the restoration of your facilities and IT infrastructure.

12 Is there a Continuity of Operations Plan (COOP) that is automatically reviewed and updated? Does this COOP include an information technology backup plan? Does it define who will be responsible for or oversee backups and how often these will be performed?

7 Any COOP template will need to be adapted to serve the needs of your organization. Here’s one designed specifically for the nonprofit community: [http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1384&context=etd_projects](http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1384&context=etd_projects).
We’ve mentioned the organizational importance of developing a detailed and nuanced Continuity of Operations Plan (COOP) for disaster recovery.

A piece of that plan will be preparing to restore the organization’s IT infrastructure and function after a disaster happens. Necessary details might currently be scattered throughout your organization or known by too few people.

Here is a list of informational tidbits to gather as part of your preparation.

- Instructions for how to restore your data
- Passwords for encrypted data
- Contact information for any employees, volunteers, or consultants who maintain your organization’s tech infrastructure
- A phone tree that includes landline and cellphone numbers for all staff members. The phone tree should follow your normal chain of management, which means that each manager will contact direct reports in case of emergency
Login information for administrative accounts on all computers

Login information for web hosting and backup service providers

Contact information for web hosting and backup services. If there is an account representative devoted to your organization, include that name and contact information

Software registration information, including keys

As the IT contact person in your organization, you will be an important contributor to building a comprehensive and effective COOP.

Following are some schematics that will help to organize and direct your work.
This chart may be helpful in identifying the essential applications that are required to operate your organization.

You can map which applications may be needed over the 24 hours, three days, and week following a disaster.

<table>
<thead>
<tr>
<th>Department</th>
<th>Location</th>
<th>Application</th>
<th>Workstation/server ID</th>
<th>Needed within 1 day?</th>
<th>Needed within 3 days?</th>
<th>Needed within 7 days?</th>
</tr>
</thead>
</table>
Here we assume that all staff members are available to help.

If that’s true, the table below helps you to identify the personnel who are essential to recover your systems and where these systems will be recovered.

<table>
<thead>
<tr>
<th>Service type</th>
<th>Assigned personnel</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Transport requirements — List the transportation you will need (cars, taxis, or public transit) during the recovery phase. Remember to include parking and any special requirements.

Expense codes — Keep track of expenses so that you can inform insurers, funders, and the community about the impact of recovery on your finances. As an example, consider whether you should track all time spent on recovery with an expense code (a special one for disaster recovery) when your accounting systems are operational again.

Accommodation — List all accommodations that you need during your recovery by both type (office, staff lodging) and duration. Remember to include additional items like food and other supplies.

Maps and directions — List maps and directions that you might need during recovery. For example, you could use an online mapping service to save maps and directions to the nearest hospital, fire station, or community center.

Construct your COOP carefully and consider whether you should conduct a disaster practice session.

A day’s worth of planning can save you massive future investments of time and energy and reduce stress on your organization.

Project Planning and Rollout
Use the form below to keep track of contacts such as computer maintenance providers that you’ll need during your recovery.

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(such as network, database, systems)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of vendor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(such as consultant, company, corporation)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred contact method</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(email/mobile/IM)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact info</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Use this chart**

to keep track of all of the reports that you have and need. Note if a report is of a central or critical nature and its special requirements.

<table>
<thead>
<tr>
<th>Report/file name</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last modified by</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last known location</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority (high/mid/low)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovered?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checked out by</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Use this chart to keep track of your suppliers and any information about them that could be relevant to restore continuity.

<table>
<thead>
<tr>
<th>Supplier name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract type</td>
<td></td>
</tr>
<tr>
<td>Reference number</td>
<td></td>
</tr>
<tr>
<td>Contact details</td>
<td></td>
</tr>
</tbody>
</table>
**Phone System Recovery**

*Use this chart* to identify what your phone requirements will be after a disaster.

<table>
<thead>
<tr>
<th>Number at primary site</th>
<th>Replacement available?</th>
<th>Necessary at recovery site?</th>
<th>Single line?</th>
<th>Two lines?</th>
<th>Speaker phone</th>
<th>Recording</th>
<th>Private line?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Store all this crucial information mentioned in this section

1. In hard copy sheltered from natural disasters and theft, as in a waterproof safe or safe deposit box;

2. Encrypted, on personal storage devices;

3. Encrypted, off-site and online.

PRO TIP:
This information must be current, or it’s of no help. Update it regularly with personnel changes, and annually at a minimum, perhaps as you review your organization’s insurance policies for the year.
Your master key is a portable USB flash drive.

Here you’ll keep all information that you’ll need to restore your technology infrastructure after a disaster or to respond to any other unforeseen incidents. It’s a place where you can compile all of your important documentation and other crucial information safely and conveniently.

Flash drives range in prices, 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. 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.

The master key should, at the very least, be held by the executive director of your organization and one other person. For distribution to others, consider

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

Who is trustworthy and lives in a geographic area that’s not subject to repeated disaster events?

8 You can use the standard Windows BitLocker or Mac FileVault.
It’s useless to have a disaster plan if your staff members don’t know about it or if 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. Here are some guidelines to raise awareness within the organization.

The moment a new staffer joins your organization, update your backup plan. New staff members will create more data. They may need to travel or work from home part of the time. They may use their own mobile devices in the office or be assigned one. All of the above factors are reasons to review your backup plan and revise it if necessary.

All new staff members should be required to read your backup plan, especially any organization-specific information, at orientation. This ensures that they are informed of your organization’s setup. They may also make suggestions to improve the plan that are based on their experience in their previous jobs.
Staff members should meet regularly to review the disaster plan, particularly in locations or regions subject to repeated disaster events, and to verify documentation. In any case, the plan should be reviewed annually, perhaps tied to the season of employee reviews.

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 your 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 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.

Likewise, when staff members leave the organization, your plan and documentation need to be updated. Also take care of these tasks.

Archive the former employee’s email (don’t delete it). Forward the emails that are sent to that address to the former employee’s manager.

Change any passwords that the employee had access to, including passwords for the organization’s presence on any social networking sites. If applicable, have the employee make a list of any accounts and passwords that he or she set up on behalf of the organization.

If the employee had a master key, or passwords that decrypted files, be sure to change those as well. If fingerprint identification was used for access, be sure that you are able to access the data prior to the employee’s departure.

Back up the former employee’s computer. Reformat it before you give it to another employee.

Keep a list of up-to-date email addresses for former employees. This is useful for two reasons. First, it allows you to forward any personal messages that an employee might receive at the old email address. Second, you might discover in a disaster that the employee forgot to document a crucial piece of information.
Remember that regular backups and clean, clear documentation go hand in hand.

So in addition to choosing the appropriate backup to use, make sure to document what is being backed up and to where.
Types 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 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.

Don’t neglect to back up Windows files and folders that are stored on the desktop, or the bookmarks in your browser.9

Some programs will also allow you to back up configurations or settings — find out if your programs support this functionality.

9 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.
There are three broadly defined approaches to backup: on-premises backup, remote backup, and cloud-based options.

Whatever method you choose will use software that schedules backups at regular intervals. The approach you choose will depend on

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?

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

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

Security — Is the data encrypted by you or by a provider? Who has access to the machines, networks, or processes that store data?
Here is a chart comparing the approaches to backup.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premises</td>
<td>Data is backed up to media located on-site, such as USB flash drives, an external hard drive, or a shared drive on the network.</td>
<td>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.</td>
<td>Backed-up data is vulnerable to loss through theft or damage. Operating systems have only rudimentary backup applications; you must acquire specialized backup software. It is still essential that you store copies of backup data off-site.</td>
</tr>
<tr>
<td>Remote</td>
<td>Data is backed up to a remote location, but managed by your organization.</td>
<td>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.</td>
<td>Internet access is required to back up your data. Data recovery takes time if done via the Internet. Your provider may be able to mail you your data, but you may incur extra costs. You also have to entrust critical data to a third party.</td>
</tr>
<tr>
<td>Cloud ¹¹</td>
<td>Data is backed up to a third-party website, with redundancy and availability of the provider’s choosing.</td>
<td>This option is considered safe from hardware failures and therefore from lost files or databases. It means lower costs, regardless of the size of your organization’s technological infrastructure.</td>
<td>You may need to download important information if you need to ensure immediate accessibility, or use a mail client as a backup (if those mail services are also backed up).</td>
</tr>
</tbody>
</table>
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.

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

10 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.

11 An example would be Google Apps for Nonprofits. See https://www.google.com/nonprofits/products/
If you can choose only one strategy to increase your organization’s IT resiliency, it would be to move as much of your organization’s files and database material to the cloud as is possible.

At the very minimum, you can shift a copy of all your data to the cloud. You can either store your files in the cloud while continuing to use desktop apps, or you can replace current applications with cloud-based software as a service (SaaS) applications.

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 move to the cloud, consider these factors:

- Your connection
- Data scale
- Satellite or affiliate locations of your nonprofit
- Data types
- Relative costs of hosted services per user
- Data access controls, security, and scalability
- Whether you have more than one method to protect a variety of applications and data
All the information we have supplied here about traditional backups might be unnecessary if you migrate information to the cloud.

And remember: some companies donate or discount cloud solutions for nonprofits!


TechSoup also hosts workshops and webinars to assist nonprofits with cloud migration.
Here is a chart comparing approaches to cloud backup. 12

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Description</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed applications and managed disaster recovery</td>
<td>Particular products or email in the cloud</td>
<td>Less complicated for the user, because the product or provider will conduct the full recovery; based solely on usage</td>
<td>Be sure to review your service agreements carefully for particulars about disaster recovery</td>
</tr>
<tr>
<td>Backup to and restore from the cloud</td>
<td>Transfers on-premises information into the cloud</td>
<td>Requires cloud storage only using backup applications and appliances; less complicated than replication</td>
<td>Slower recovery times</td>
</tr>
<tr>
<td>Replication to virtual machines in the cloud</td>
<td>Either on-premises to cloud or cloud-to-cloud</td>
<td>Best recovery times and data loss recovery points</td>
<td>More complicated</td>
</tr>
</tbody>
</table>

12 This table was drawn from [http://searchdisaster-recovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained](http://searchdisaster-recovery.techtarget.com/feature/Disaster-recovery-in-the-cloud-explained).
Guidelines for Choosing On-Premises Backup Hardware

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.

Disk-based technologies such as backup and file-storage servers, as well as external hard drives, are the backup media of choice. For example, network attached storage (NAS) is a type of device that offers disk-based storage like a dedicated file server or backup server would. However, it’s in a small and efficient chassis. NAS may offer specific features such as scheduled backup or FTP access; it depends on the model. NAS is a great solution for nonprofits that want to back up a lot of data easily. You can also back up data from NAS via an external drive to store off-site.

For larger networks and disk space requirements, consider a storage area network (SAN). A SAN is a network of storage devices that is 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.
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. However, they can be great if you need to

Create quick copies of critical files. If you store critical files on a CD, DVD, or flash drive, you’ll be able to easily access your files without specialized backup hardware or software and without an Internet connection. USB flash drives are highly cost-effective in terms of price per storage and offer good transfer rates. They also do not require an external power supply to be functional.

Transfer files from one computer to another.

Archive old data that you don’t need to access or restore. DVDs are appropriate for the storage of data that you won’t need to modify, such as photos and finished printed materials. Plus, discs make your archives portable, which makes it easy to store a copy off-site. They are also nonvolatile, and, depending on the specific media type, not erasable.
Backup Software

For individual users, Windows and macOS operating systems both have built-in backup tools.

These built-in tools for backup are adequate for individual computers. However, a dedicated program is preferable if you have the resources to pursue an organization-wide strategy. A dedicated backup program allows for more detailed refinement of the backup options, as well as more sophisticated management of multiple computers. It 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**

Be sure you understand how your email is set up.

You’ll need to know where your messages (sent and received), calendar (if your email application has one), and contact information are stored. Determine if attachments to email are automatically stored in a backup or by your service provider.

If your organization uses an in-house email server, you must include it in your backup plan. Email servers have their own backup utilities; check the user manual for more information.

If you use a webmail service, check with your email service provider about its backup and restore policies. If the webmail service is offered through your Internet service provider (ISP), find out whether the ISP backs up your email.

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 backed-up email messages, calendars, contacts, tasks, and notes, and can 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 a server, then it should be backed up like any other server.

If it’s hosted off-site, your web hosting provider would back up the data according to that provider’s data backup policy.

Be sure to check with your provider to determine if its backup and restore policy is sufficient for your organization’s needs. As with other services that are managed by a third party, there are many reasons to keep a copy of your website on an office computer. Most content management systems allow you to back up your own content on a local computer, which you should include in your regular backups.

As a part of your preparedness work, you might also consider whether it would be advisable to set up an emergency website. The website would be launched in the event of a disaster and regularly updated to keep followers aware of changing conditions on the ground and responses to the community’s needs.

Another way to update your website is by linking its users to your Twitter and Facebook feeds. You can also update it through online blogging sites that can be accessed through any sort of Internet connection using mobile phones or other devices. Internet services are typically provided at emergency shelters and in disaster recovery centers, if conditions allow.
In any office environment, there may be multiple devices to back up.

In addition to the computers you use regularly, consider your power supply, servers, personal computers, mobile devices, and networking equipment.
Your power supply for your on-premises equipment is very important to the resiliency of your organization.

If you have on-premises backup equipment, it needs to be able to continue to run during minor outages or the unpredictable surges that may happen day to day. Although laptops and mobile devices have batteries, desktop computers, networking equipment, and servers do not. An uninterruptible power supply (UPS) is an effective way to protect yourself from small, power-related disasters. It is best to have multiple UPSes, depending on your setup, to offer redundancy. Compared to your basic power strip or surge protector, a UPS has a battery built in to enable a graceful shutdown via a data connection to a server.
You should have regularly scheduled backups for your servers.

In addition, it’s good practice to conduct a full backup of your server before every major update. Then you will have a way to restore your server’s entire hard drive if anything goes wrong during the update.  

13 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.)
If your employees, contractors, or volunteers work with their personal computers, their data should be part of a regular backup strategy. For all remote backup services, you can install a backup program on any computer, even for one that is not on the work network.

**PRO TIP:**
As a simpler alternative, you could require that work that’s performed at home is saved to a work computer or shared storage solution.
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

The setup and configuration that the networking equipment has is important information that takes time to reconstruct.

Information such as ISP details, reserved IP addresses, special routes, and wireless settings should be backed up as well. Both retail- and enterprise-level networking equipment allows you to back up configuration information if you access the device via a workstation. Ask an IT professional to map your configuration in a hard copy and save it to a file.
Recovering from Disaster

Disaster has struck.

You might not have had any warning; you might be unprepared to move forward. Take a deep breath. Recovery is a process, not an event, and nurturing your stamina for the long term will be one of the ways you support your organization.

Or, if you’ve had the good fortune to prepare for disaster, your prior activities will support your recovery and rebuilding efforts. The careful collection of information and decision making that went into designing your Continuity of Operations Plan (COOP) will launch your organizational triage, and restart your systems and services.

In either case, this section will guide you in rebooting the IT infrastructure of your organization.

We’ll walk you through

Questions to guide your work plan
How to reconnect with service providers
How to retrieve data and files
How to assess damage to your equipment
Initially, your organization will identify what needs to be done and in what order. Then, you can work to obtain the resources, funds, advice, and technology that you will need to begin the recovery process.

Until you have official confirmation from emergency management personnel that it is safe to move away from shelter, do not do so.

If you have access to a phone or electricity and can use the Internet, check for updated safety information with local city or county officials, fire and safety responders and utility providers, FEMA at [www.fema.gov](http://www.fema.gov), or with early relief providers, such as the Red Cross.

Make sure that you rely on dependable outlets, such as those listed above and others such as [disasterphilanthropy.org](http://disasterphilanthropy.org) that provide regular updates on domestic and international disasters and offer helpful tips and support for disaster recovery funding.

Activate your COOP if you have one. Regardless, set up your project teams, and schedule regular meetings (in-person and otherwise) of key decision makers.

Every organization will have different technology priorities after a disaster. However, there are some general guidelines that can help you to develop a good technology triage list:

1. **Communication is very important.**
   In most cases, the first priority during and immediately after a disaster is to reestablish communication with the outside world. If the disaster is widespread, communication systems are likely to be overwhelmed, so prioritize who needs to be reached first.

   Contact your insurance providers to begin the claims process and to deploy their agents, adjusters, and restoration service providers to your site.
Consider your constituents. Focus on services, functions, programs, and audiences first, before you consider machines, networks, and applications. Refer back to your COOP, if you have one.

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?

Which ones can be postponed?

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

2 Identify any equipment that's been damaged or lost. Insurers may provide temporary equipment while yours is being restored or replaced. Use this information to decide what to do first. Restoration and repair of systems can take a significant amount of time. In order to succeed at triage, you will need to focus your efforts where they will have the most impact.

3 If there will be a delay in restoring Internet service in your office or in the homes of staff members, consider collaborating with another organization whose services may be intact, or working with organizations and businesses that might have large phone or computer banks (public libraries, schools and universities, etc.).
Files and Databases
Think about your servers. Recovery of your servers may be a high priority, since it is essential in order to recover your data and to restore your network. Attempt to recover the servers only if the power and network are in good enough condition to warrant their revival.

If you have data that is stored in a remote system, you might not have the consistent power and bandwidth to restore your system sufficiently. Again, focus on the data and systems that will have an immediate impact post-disaster.

If you have a backup, try to restore it only if your equipment is stable enough for recovery. If you have a network attached storage (NAS) or removable hard drive, verify that its status lights come on. Also check that you do not hear any abnormal sounds when you plug it in. However, if there is even a remote chance that your power is unstable, then you should abandon the attempt to restore.

If You Have On-Site Backup Storage
If you have lost data during a disaster and your backup plan lacks a strategy to address this sort of catastrophe, there’s still hope.

The information that follows can help in your data recovery efforts.

Look for other places where you might have inadvertently stored your data. Perhaps you emailed copies of your files and what you need is an attachment to an email. Perhaps printouts of the data exist that you can re-enter (data entry is often less expensive than hired help from technology experts).

If you do find a copy of your data, back it up and make a copy before you do anything else. Use this copy only and save the original in case something goes wrong with the duplicate backup.

Look for the name, type, and model number of your computer anywhere on the case. Try to find the recovery discs for the operating system. Remember to consider warranties and manufacturer support. Call the manufacturer to see if it can help fix your computer.

In the event that backup media and hardware are unreachable or unusable, you’ll need outside help to recover the data. There are many companies that recover data. Costs vary — it depends on the level of damage and the amount of reconstruction that is necessary. Go back to your insurance review to determine if this type of service is covered. If the lost information is extremely important to your mission, such as your donor list, you might want to pay for data recovery.
Here are some questions to consider as you plan your recovery.

Do you have the bandwidth and network capacity to restore from cloud backups?

If you plan to restore from the cloud to on-premises infrastructure, how long will that restoration take?

Can your backup provider mail you physical media, in the event that you cannot fully restore via the Internet?
Even though a system is functional or revived, you still may have lost the passwords to access it.

Here are some ways to restore access.

**Windows computers**
There are many ways to restore a lost Windows password. Methods vary by Windows version. Generally, you’ll need to download an image (ISO) file to create a boot disk, or download a piece of software to overwrite an existing password. This can be a complicated process, so unless the recovery is extremely urgent, it is advised that you leave this process to your IT consultant or other IT professional.

**Apple computers**
You can use a macOS installation CD to reset the passwords on a computer.

**Routers, firewalls, and other network equipment**
If you still have it, check the instruction manual that came with the equipment. Most network equipment comes with default passwords. All equipment can be hard-reset to the factory settings — usually you push down the reset button during startup or in a set pattern. If the manual that you need is lost, you might be able to find it online.
Reestablishing reliable communication — both external and internal — will be essential to rebuilding your infrastructure and continuing your core programs.

Your staff may need to work at home or use mobile phones. If so, you can have your office numbers temporarily forwarded to the appropriate landline or mobile numbers. Most hosted Voice over Internet Protocol (VoIP) services allow you to redirect lines to outside numbers.

Your staff members might need to use personal mobile phones for work during the recovery effort. If so, find out whether their mobile plans include enough minutes and data per month to cover the increased usage.
If you have Internet access, consider using Skype or a similar service.

Change all of your outgoing voicemail and email messages to include basic information about your organization’s efforts to rebuild. The message should briefly outline any changes in your organization's services and instructions on how to stay informed.

Consider establishing a "help desk" if you anticipate that there will be high demand for information from your organization, screening calls to avoid overwhelming switchboards and personnel.

If your email service has been disrupted, and you need to find a new provider, consider the following. You will need to update what is called your mail exchange (MX) record, which is similar to an update of your website's domain address. Typically, your email host will give you information about what your MX record should be (usually it's an address like mail.mydomain.com or an IP address).
Your website is a central way to inform the public about your organization's recovery efforts and any changes to the services that you provide.

You should also take the opportunity to communicate with your allies to coordinate and potentially pool resources.

If power and Internet access is consistent enough, you should be able to update your website normally.

You should also post updates about your organization's recovery efforts on Facebook, Twitter, or whichever social media channels you use most frequently.
Proving Your Identity

If you have lost login and password information for updating your website or you need to make more substantive changes (such as changing web hosting companies), you may need to contact your domain registrar or hosting company to have your login information reset.

Some companies, given the circumstances, may be flexible around identity verification. However, times of disaster are often ripe for fraud. So it’s likely you will still be required to convincingly prove who you are before you can make changes, such as having your login information updated.

You can find information to help you more easily prove your identity by performing a WHOIS lookup. These lookups provide information about your website, such as the admin contact, domain registrar, and more. This information is available via different websites, including

http://DNSstuff.com
(use the “WHOIS Lookup” feature)

https://whois.icann.org

In the best scenario, the person (or entity) listed as the admin contact will match your current contact information. For example, if the "admin email" is an email address you have access to, you should use that email address to communicate with your domain registrar or hosting company.

Sometimes the email address is masked, which makes it harder for you to find out which email address to use to contact the registrar or hosting company. If the street address is correct (and matches your letterhead), you can send written requests.

Details regarding payments made to the company you are contacting can also help prove your identity. If you have access to the date, amount paid, and credit card number used to pay for services, this may help prove your identity.
If Records Are Inaccessible

If you are missing login or password information
You may be able to identify individuals who have this information by performing a WHOIS lookup (see the "Proving Your Identity" section above for how to do this).

If you can’t find login or password information, you will need to contact your web hosting company to change your login and password information. A WHOIS lookup can also provide relevant information to help you prove your identity to the company you need to contact (see the "Proving your identity" section above for how to do this).

If you aren’t sure who your current web host is
You can try a WHOIS lookup (see the "Proving Your Identity" section above for how to do this). Sometimes, it’s obvious (you’ll see something like dns.webhostcompany.com), whereas other times, all you’ll see is just an IP address.

If you don’t know who your domain registrar is
You can try a WHOIS lookup (see the "Proving Your Identity" section above for how to do this).
It may be advisable to maximize your insurance coverage and call in the professionals to repair your damaged equipment and devices. You might be adept at quantifying your IT inventory and having good records in place to confirm your purchases and warranties. But actually taking apart a machine may be the appropriate moment to end your personal IT recovery services. If, however, you have no choice but to attempt repair and restoration yourself, or you are asked to supervise the process, here are some dos and don’ts as to how to proceed.
General Safety Tips

Ensure that you have a safe environment before you begin the hardware recovery process. For your own safety, observe these precautions.

If the floor, any electrical wiring, or computer equipment is wet, make sure the power is off before you enter the room or touch any metal, wet surfaces, or equipment. If you’re certain that the power is off and that it is safe to move the equipment, move it to a safe, dry environment with reliable electrical power.

If you need to use temporary extension cords and cables, make sure that you follow safe procedures. Cords and cables should either be placed where they won’t be walked on or taped to the floor to provide protection in high-traffic areas. Be sure that the cables are rated for the device and appliance that they are connected to.

Make sure that tables are sturdy enough to support the equipment placed on them, and that if you stack equipment, it will remain upright and stable, especially when it is connected to cables or other peripherals. Allocate a little extra time to make sure everything is stable, neat, and orderly.

Once you have a safe, dry environment, it’s important to make sure that you have good, reliable electrical power before you connect or turn on any computer equipment. A good first step is to plug in an electric light to make sure it shines steadily and provides the same amount of illumination that it normally would. You can also try to plug in things you can afford to lose and test them out. An example of something you can afford to lose might be a radio or any other device that requires only a small amount of power. You may need to purchase or rent power-generating equipment to clean up, charge devices, or verify equipment — it depends on the urgency and situation, and what is being supplied through insurance or volunteer-based services.
To avoid power surges and brownouts, turn off and unplug computers when they will be unused for an extended period. If a lightning storm is expected or the power goes out, turn off and disconnect computers and other sensitive equipment. Keep them off until the power is back on and stable. Power surges often occur when the power returns. Computers should have a backup system for short-term power or an uninterruptible power supply (UPS), which also provides isolation. Laptops are isolated by their power supplies and batteries, but reliable power is still important to avoid damage. Your UPS may have exhausted its battery power during an outage, but its surge protection capabilities may be unaffected.

Ventilation is also very important. Make sure the vents on any equipment are unblocked. Computers can run in a warm environment as long as they have adequate ventilation. Avoid the tendency to put computers right next to each other or position the vents next to desks or cabinets. Use a fan to keep the air in motion in the room and around the computers if you think they might get too hot. Turn computers off if you leave the room and let them cool down before they’re turned on again. Consider whether you can work during the cooler part of the day and turn off computer equipment when it’s too hot to work comfortably.
Once you have verified the operating environment, assess the hardware situation independently or with professional guidance.

If you think you might require contingency suppliers who are third parties (such as salvage companies, or computer room suppliers who are mobile), notify them of your potential need.

1. Clean and dry hardware that you intend to revive yourself. Postpone or avoid any attempt to plug in or operate a computer until it’s completely dry and free of mud, dirt, or other debris. Your computer might work, but if you turn it on prematurely, you can destroy an otherwise healthy machine. It’s important to open up the chassis of your computers to make sure they are clean and dry inside and out. If there’s any debris, remove it carefully so that you protect the computer from the tendency to overheat from reduced airflow.

2. If you need to touch or put your hand or tools near any part inside the computer, wear a wrist strap with electrostatic discharge (ESD). Or, you can work on an antistatic mat. If you lack a wrist strap or mat, touch a grounded object (such as metal water pipes) before you touch the computer. Before you open the computer’s case, be sure all power sources are turned off, the computer is unplugged, and laptop batteries are removed.
3 Make sure devices such as routers, switches, and printers are completely dry before you power them up. If possible, wait to attach peripherals and cables to computers or avoid this entirely, unless you’re sure the equipment works properly.

4 Check your components twice. Even if a computer fails to start right away, put it aside to check later. Be sure to sort and label the equipment. These actions allow you to figure out what does work and what is broken. After that, you may be able to build computers that work from operational parts of different broken computers.

5 Once you get a computer to run, back it up if its data is more recent than your backups.
Network Recovery Tips

In the case of a flood or other inundation, a local area network (LAN) can be badly damaged. Network cables can become waterlogged and cease to function. Patch panels and jacks might also be damaged; switches, hubs, routers, and other electronic devices on your network might be shorted out by the water. Full restoration of your network to its original condition can take time and effort. It might be worthwhile to try to get a few devices back on first.

First, verify that the networking devices are safe to use. After this, try to plug in your modem to a reliable power source and see whether the lights come on as they normally would. Usually there would be a green light and a label such as "online" or "power." It’s possible that the settings were saved during the outage. If the modem has LAN ports, you can try to connect your computer in directly rather than use your regular networking devices. This is a good short-term solution until you or your IT consultants are ready to do more detailed reconfiguration. If it is safe to do so and there’s a need, expand the network by the addition of a hub or a switch.

Once you have a hub or switch that works in place, you can start to connect computers to the network via standard Ethernet cables. Try to run the cables along the base of walls and out of the way of foot traffic. Ethernet cables are easy to trip over, and when pulled abruptly, they can break connectors and jacks and pull equipment to the floor. If you need to run a cable across a traffic path, try to tape the cables to the floor to keep them out of the way.

**PRO TIP:**
When you pull up taped-down cables, try to pull the tape off the cable while it is still on the floor. If you pull up the tape and cable
together, it’s likely that the tape will wrap around the cable. Then the tape can be very difficult to remove.

If your organization had a wireless network, it may be more efficient to set up that network first to access the Internet, because it is easier to add additional users. A wireless network is also less reliant on a static location. However, you might not have access to certain servers — it depends on your network configuration — so do be aware of potential limitations. You might have had wireless access from your broadband modem previously, and your settings might have been retained. If so, then you should be able to use the same wireless settings as before. If wireless access has been lost, you’ll need to reconfigure the modem. If possible, refer to the documentation that you have set aside, or the master key of information.
In times of disaster recovery, there will be a greater reliance on mobile networks for both personal and official business. Numerous agencies, private citizens, and relief groups need to use the same networks to communicate with one another within the same region. Therefore, it would be ideal if the organization prioritized the use of this scarce resource.

If regular fixed broadband is currently nonoperational, but your work or personal mobile broadband is available, you should use it as needed.
This is the third major revision of

*The Resilient Organization: A Guide to IT Disaster Planning and Recovery*

The initial version of this guide was written shortly after Hurricane Katrina struck the southern United States in 2006.

In 2013, we made the information more concise and actionable, and added some key revisions pertaining to cloud and mobile adoption. We also translated the guide into certain languages for our global audience, and produced it in e-book form.

In this latest version, we have split the guide into several parts to better serve organizations who are recovering from a disaster and need support to rebuild their IT infrastructure to resume their primary activities.
This edition of the guide was created in partnership between TechSoup and the Center for Disaster Philanthropy with the generous support of Microsoft.

disasterphilanthropy.org
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.