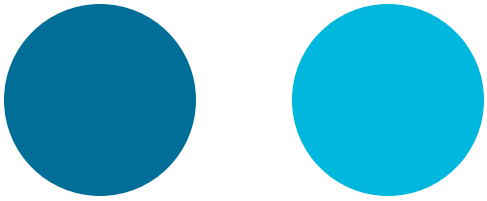
The Resilient Organization

A Guide to **Nonprofit Disaster Recovery**

What to do after a disaster has occurred

CDP Center for Disaster Philanthropy

techsoup



Published by TechSoup

The Resilient Organization: A Guide to Nonprofit Disaster Recovery (What to do after a disaster has occurred)

Contents

Rebuilding Your Organization After a Disaster

Until you have official confirmation from emergency management personnel that it is safe to move away from shelter and resume normal operations, 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, 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 that provide regular updates on domestic and international disasters and offer helpful tips and support for disaster recovery funding.

Your next steps to recovery are to address the following main areas as needed, according to the type of disaster you have experienced.

Activate Your Recovery Plan

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.

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.

Develop the Technology Triage List

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:

Communication is very important. In most cases, the first priority during and immediately after a disaster is to reestablish communication internally and with the outside world. To do this, you need to verify that your communications technologies are all working.

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.

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, and so on).

Support Your Staff

Again, people are the most important assets of an organization, whether paid or volunteer staff. One of the best methods of assuring your company's recovery is to provide for your co-workers' well-being.[1] Consider providing necessary health and financial support to help your staff recover after a disaster.

Supporting employee health after a disaster:[2]

Encourage your staff to have adequate food, rest, and recreation and allow time for them to stay at home and care for family needs. Have an open-door policy that facilitates seeking care when needed.

According to FEMA, getting back to work is important to the personal recovery of people who have experienced disasters. Workplace routines facilitate recovery by providing an opportunity to be active and to restore social contact. Encourage staff to reestablish routines when possible.

Sharing with others can speed personal recovery as well. Create opportunities for breaks where staff members can talk openly about their fears and hopes. Consider offering professional counselors to help staff members address their fears and anxieties.

Paying employees during and after disaster:

It's important that your organization have a detailed (strictly confidential) plan to pay employees. Checks may not be helpful, particularly after a widespread, catastrophic event if employees evacuate or the mail can't get through. The organization can pay employees with direct deposit as long as the backup payroll system and the bank computers keep running. Cash should also be considered as an option.

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

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

Reestablish Internal and External Communications

Reestablishing reliable communication — both external and internal — will be essential to rebuilding your infrastructure and continuing your core programs.

Reestablishing Internal Communication

Forwarding Phone Calls

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.

Do not assume in our technological era that landlines are not useful during an emergency. One of the most important aspects of owning a landline phone is the ability to remain connected to the grid. Signals sent and received by your landline phone are tied to your home or business location and can be used to find you in case of an emergency.

Using Personal Mobile Phones

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.

Email and Other Internet Services

If you have Internet access, cloud-hosted email should function correctly, as would any online messaging applications such as Teams, Slack, Google Meet (all of which have free consumer versions and nonprofit pricing for the more secure business versions). There are also other consumer tools such as Skype or WhatsApp, but be careful about the security and privacy of any free tools.

If your email service has been disrupted, and you need to find a new provider to switch to, that process will require that you update what is called your mail exchange (MX) record, which is similar to an update of your website's domain address. Typically, your email hosts (previous and new) will give you information about what your MX record should be (usually it's an address like mail.mydomain.com or an IP address). If you have a service provider doing the migration, then they should handle this work.

Reestablishing External Communication

Forwarding Phone Calls

Your website is the digital "front door" of your organization. Update your website with the latest information first, including any changes in your organization's services and instructions on how to stay informed (see the section below on website recovery).

You might also consider whether it would be advisable to set up an emergency website or landing page that is activated in a disaster for external communication and regularly updated to keep followers aware of changing conditions on the ground and responses to the community's needs.

You should also post updates about your organization's recovery efforts on Facebook, Twitter, or whichever social media channels you use most frequently. For nonprofits working to help others during a disaster situation, use social media and remember that Twitter is one of the most-used platforms in those instances, due to its quick and fast posting abilities.

Change all of your outgoing voicemail and email messages to include basic information about your organization's efforts to rebuild as well.

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

Tell officials what your organization is prepared to do to help in the disaster relief effort. Also communicate with local, state and federal authorities what emergency assistance is needed for you to continue essential business activity. You should also be prepared to give neighboring nonprofit organizations a prompt briefing on the nature of the emergency so they may be able to assess their own threat levels.

Recover Data

If you have already documented your data backup processes as part of your disaster preparedness, you should activate the data recovery protocols you have established. And of course those applications and data that you have hosted in the cloud should continue to be accessible via an Internet or mobile phone connection.

For data that has not been backed up, is haphazard, or where your backup protocols are not well documented (or documentation is out of date), unfortunately there is no "one size fits all" data recovery approach. Backing up and restoring data is more of an art than a science, and it may require extensive systems knowledge to restore some domain services and components.

PRO TIP

For physical documents that have sustained water damage (such as during a flood or hurricane), you can freeze them to prevent further damage, such as mold, until you are able to dry them out properly. Check out more ways to dry wet paper from wikiHow.

Each application and file type may have a different recovery method from the next. For example, documents and spreadsheets can be copied freely from disk to disk, disk to cloud, or disk to tape. Files such as accounting and email databases have accompanying log files that keep track of each transaction. They require a database-aware backup program in order to keep the files synchronized and together.

Most server operating systems include basic backup capabilities, which typically have fewerfeatures than third-party packages. Some older operating systems will only restore data to an identical, or at least similar type of hardware, which may be difficult to source after a disaster. If you are able to overcome this limitation, you may find the built-in backup program will allow you to restore an entire database, whereas a full-featured backup program may allow you to perform single-object-level recovery.

Image-based backups are quite popular, and backup files should be stored both locally and in the cloud. This will allow administrators the flexibility of restoring the file system locally or turning the backup file into a fully functional virtual server in the cloud. While this type of operation is intended to be used as a temporary measure, it is extremely helpful when server hardware has been damaged or you are unable to access your offices.

If You Have On-Site Backup Storage

Your data recovery method depends on the backup strategy you've put into place. For example, if you perform a weekly server backup, and nightly incrementals, you will first need to restore files from your weekly backup and then restore each nightly backup.

You should only attempt recovery if you have a stable power source and appropriate environmental control. A portable generator rarely provides clean power for expensive electronics, and may cause damage to the replacement hardware. Similarly, hardware that reaches an ambient temperature of 85 or 90 degrees may automatically shut down to protect the internal components from damage. Make sure you have adequate cooling available wherever you choose to recover your hardware.

If you have a network attached storage (NAS) or removable hard drive, verify that it powers on and that you do not hear any abnormal sounds. A repetitive clicking sound usually means the disk drive is physically damaged and should be powered down immediately if you hope to recover any data from it.

If you are unable to recover data from your backup files, 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 physical printouts of the data exist that you can reenter

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, but they generally run in the thousands of dollars — it depends on the level of damage and the amount of reconstruction that is necessary. It's possible your insurance policy may help cover some of this expense. If the lost information is extremely important to your mission, such as your donor list, you might want to pay for data recovery.

If Your Backups Are in the Cloud

Here are some items 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 data from the cloud back to an on-premises system, how long will the file copy take?

Can your backup provider ship your backup on physical media?

Lost Passwords

Even though a system is functional, you may have lost the password 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 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, you may want to leave this process to an IT professional.

Apple computers — You can reset the Mac login password using the associated Apple ID, using the recovery key in FileVault, or using the administrator account.[3]

Routers, firewalls, and other network equipment — Some manufacturers provide a mechanism to reset a lost or forgotten password, but not all. If your device does not have this functionality, you can usually reset the device to the factory default settings through a manual process.

Your Website

Your website is a convenient way to inform the public about your organization's recovery efforts and any changes to your operating hours or services that you provide. If power and Internet access is consistent enough, you should be able to update your website normally.

3. Learn more at: https://support.apple.com/guide/mac-help/reset-your-mac-login-password-mh35902/mac

If You Need to Move Your Website or Email

If you host your own website or email system on-premises, you may need to relocate these services to a cloud provider in the event your building is destroyed or otherwise inaccessible.

While this process is not impossible, it does require access to your domain registrar, DNS records, or both to redirect web traffic to your new site.

Website Migration Procedures

A website usually consists of three components, all or any of which may have been affected.

Domain registrar:

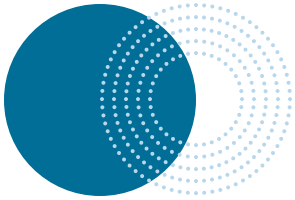
This company registers your website's domain name (www.mywebsite.org, for example). This is different from your site's content, which is stored by a web hosting provider. Although your domain name can be registered with a separate domain registrar, it is often registered by a web hosting provider.

Web hosting provider:

A web hosting provider supplies the disk space and network for your website. You might also have hosted your own website. If so, you may want to move this hosting to another provider after a disaster in order to restore your website as quickly as possible.

Web content:

You might have backups of your website. However, if you lack these, you may want to publish a simple page quickly with contact information and status updates for your supporters. If you are unable to do that, you may want to post a blog temporarily separate from your usual hosting provider. If you use social networking and microblogging sites, you should post frequent status updates.



If your web hosting company is down and you need to get some sort of presence on the web as soon as you can, take the following steps.

1 Choose a new web host.

If you do need to pick a new web host, remember that picking the right platform is important if you have backups of your site, which may have been built on a specific platform (for example, WordPress, Drupal, or Joomla!). It's also important if you hope that your original web host will return and you want to maintain the same platform in case you switch back. Your website may have included a database on the web host's servers. If so, the availability of the correct database platform (for instance MySQL or MS SQL Server) is also essential.

2 Update your domain registration.

Once you have selected and paid for a web hosting service, you have to update the information at your domain registrar. This will "point" the address of your domain to the new web host (as opposed to the old one). Often you can do this if you log in to your domain registrar's control panel and update the information yourself.

A registrar's website will usually provide contact information in case you have lost your login information and password or you can't prove your identity to the registrar's satisfaction. See the following section Proving Your Identity for more help in these situations.

3 Upload your website content.

Once you have set up the web host and domain registrar to point to the right address, you can begin to upload your web pages. This is true for simple contact pages (if you don't have any backups). It's also true for the original website if you do have backups and have access to them.

If Records Are Inaccessible

If you are missing login or password information, you will need to contact your web hosting company to change your login and password information. A WHOIS lookup may be able to provide relevant information to help you prove your identity to the company you need to contact or help you identify individuals who have this information.

Proving Your Identity

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

https://tools.DNSstuff.com (use the WHOIS Lookup feature)

https://whois.icann.org/

Enter your domain name in the site's WHOIS lookup box. The resulting WHOIS information page will tell you

The registrar ("Registrant")

The contact person for the domain ("AdministrativeContact")

The name server and IP addresses ("Discovered NameServers")

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.

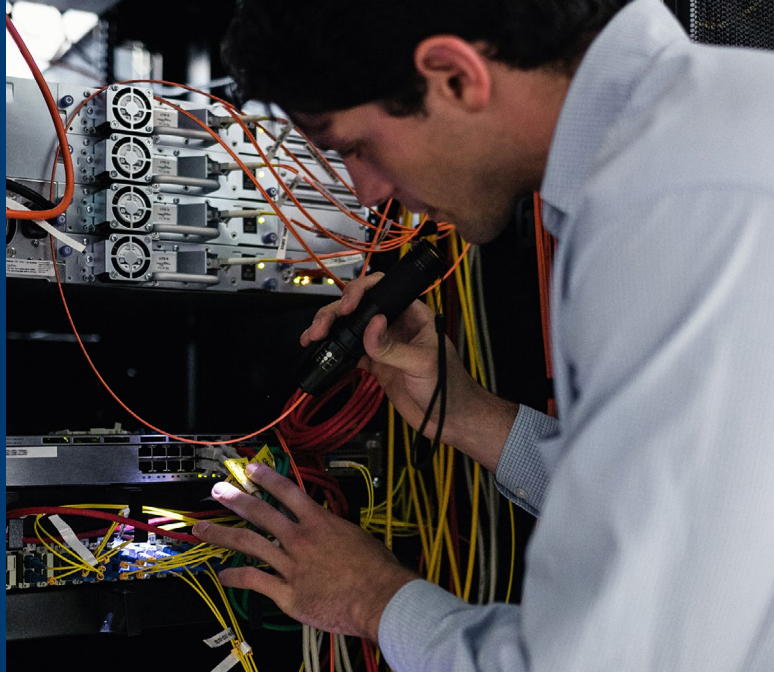
If You Are Uncertain Who Your Current Web Host Is

You can try a WHOIS lookup (see Proving Your Identity 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 as well (see Proving Your Identity above for how to do this).

Recover Equipment and Devices



It may be advisable to maximize your insurance coverage and call in the professionals to repair or replace 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, follow the guidance below.

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 be connected to 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.

Hardware Recovery Tips

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.

Clean and dry hardware that you intend to revive yourself. 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. Desiccant packs can be used to help remove moisture from inside electronics, and can be purchased at most major home improvement stores. 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.

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.

Check 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.

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, 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 your modem in 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 adding a network switch.

Once you have a working switch 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, can break connectors and jacks and pull equipment to the floor. If you need to run a cable across a traffic path, tape the cables to the floor to keep them from becoming a trip hazard.

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 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 device. If possible, refer to the documentation that you have set aside, or the master key of information.

Mobile Internet Connectivity

In times of disaster, there will be a greater demand on mobile networks for both personal and official business. Cell towers may be down as in the case of a tornado or hurricane, or the data circuits that provide connectivity may be damaged. If the towers are functional, Mobile broadband providers may limit data speeds or reallocate cellular bandwidth to handle more voice calls initially, but they will generally add network capacity within 24 to 48 hours.

Text messaging is generally a reliable means of communications, even when the networks are congested.

Post-Disaster Fundraising

Your nonprofit may be looking forward to the regular donations for post-disaster recovery, but unfortunately, you might discover that the disaster has had a negative impact on your longtime donors as well. It becomes necessary to look for other funding sources. Where should you start?

Establishing Your Credibility

Well before disaster strikes, every nonprofit organization should establish the strongest possible credibility by creating a profile at reputable platforms and obtaining necessary certificates. This can help you to more quickly access funding and other support post-disaster.

GuideStar

We recommend nonprofits get onto GuideStar now and create a profile, filling it out at least to the gold seal level. Your nonprofit's profile can be updated anytime after its creation and should be updated annually. GuideStar will automatically upload your Form 990 tax returns. When you get your GuideStar seal, the seal should be placed on the front page of your website with a link back to the profile. GuideStar will provide you with the seal for the appropriate level of your profile's completion (Bronze, Silver, Gold, or Platinum).

If needed, nonprofits can push disaster relief donors to GuideStar if the donation "button" has been activated for your profile. The option to have a "donate" button affixed to your GuideStar profile is provided.

Charity scams are legion during disasters. The Federal Trade Commission (FTC) shares information about how to donate wisely and avoid charity scams. They note, "when you decide to support a cause you care about, you want your donation to count. Doing some research and planning your giving can help ensure your donations get where they'll do good." In this sense, having a reputable profile on GuideStar already in place will make a world of difference when disasters strike and donors seek to help their favorite nonprofits.

Verified Facebook Page

Facebook is increasingly used for communications during and after disasters and for fundraising campaigns.

Does your nonprofit have an updated Facebook page?

Have you secured verification for your page (by uploading a copy of your IRS letter or other key organizational documents to Facebook)?

This is another way to ensure public confidence in your nonprofit organization, which is increasingly key to successful fundraising and community building.

State-Specific Requirements

Some states may have their own certification requirements. Protect your nonprofit and its reputation by securing one before disaster strikes and ensure that you can demonstrate complete transparency.

> The Texas secretary of state asks businesses and nonprofits to secure Certificates of Account Status before conducting any business transactions. These Certificates of Account Status, previously called Certificates of Good Standing, provide the status of an entity's right to transact business in Texas.

Often funders will require a copy of state certification to be provided along with a nonprofit's application for a grant, particularly after a disaster when funding requests increase, as do incidents of fraud.

Check with your state government about whether and what specific certification or licensing is necessary to obtain in order to collect donations or certify legitimacy.

IRS Letter of Nonprofit Status

In addition, double-check your IRS letter of nonprofit status regularly. Read the IRS website page Exempt Organizations — Affirmation Letter.

Has that key IRS document been updated in recent years?

If you filed several years ago, are you still operating under the same name that appears on the IRS affirmation letter?

These kinds of documents are critical items that you do not want to be questioned about during or after a disaster. Routine checking and maintaining an updated GuideStar profile, Certificate of Account Status, or other credentials will make a big difference in donors feeling comfortable supporting your organization.

Raising Relief and Recovery Funds

Many local community foundations set up disaster relief funds after emergencies occur. One should look to the local community foundation for help.

Disaster recovery funds from the Center for Disaster Philanthropy (CDP) allow donors to give now to support recovery needs that will continue to surface long after our attention has turned away from these disasters.

The Disaster Assistance Improvement Program (DAIP) of the federal government aims at improving survivor access to disaster information and making applying for disaster assistance easier. The Federal Emergency Management Agency (FEMA) acts as the managing partner of DAIP.

As was mentioned earlier, GuideStar allows nonprofits to collect donations on its platform. If you have a GuideStar profile in place before the disaster, consider activating the "donate" button. This allows donors to give directly online via their favorite nonprofit's GuideStar profile. The GuideStar "donate" button is managed by Network for Good. The direct deposit option can also be activated with Network for Good if you do not want to wait for a check to arrive in the postal mail.

GlobalGiving has a disaster division as well. But as with GuideStar profiles, one must set up a profile well in advance, then activate it once crowdfunding is needed after a disaster. Hence, nonprofits wanting to use this platform need to be proactive.

Last but certainly not least, consider activating your own online giving processing platform for disaster fundraising. For instance, you can set up direct donation "pages" in advance via your own processor, but keep them hidden on your platform of choice until you need to make them public.

Be proactive! Post a link to donate securely online on the front page of your website. Most platforms today have sophisticated apps for mobile giving. Activate those by making finding and downloading them easy: post an easy "app" link on your website's front page and on relevant social media. For instance, Qgiv has the mobile app Givi. Others to consider are PayPal and Blackbaud (RE Mobile App).

PRO TIPS

- Using reputable crowdfunding platforms could help your nonprofit broaden its audience and raise more money. But beware of platform fees (in addition to gift processing fees). You may want to consider the cost-efficiency when making choices. Sometimes the best answer might be "in house."

- Direct donors to your website first, and on the website, provide a prominent link to the direct donation page. On the donation page, put your organization's name prominently on it (perhaps in multiple locations). More information is a good thing. Make sure donors know it is "you."

  Oftentimes, nonprofits and their constituents will "share" direct donation links on social networks to encourage donations by family members and professional colleagues. But sometimes, once someone clicks on the link, it can be unclear if the link is legitimate. Make sure that the donation page and link contains information that instills confidence in donating to your nonprofit. Be absolutely sure donors are being directed to the right place in one or more of these ways: (1) to your official website; (2) via a secure link and directly to your nonprofit's bank account; (3) via your GuideStar profile and the approved donation link found there.

References

- **Survey of Hospital Employees' Personal Preparedness and Willingness to Work Following a Disaster**

- **How Do You Pay Employees When Disaster Strikes?**,
the ADP SPARK newsletter

- **How to Pay Employees During a Disaster**,
Chron

- **Employers Helping Employees — Disaster Relief**,
KPMG (PDF)

- **BBB Tip: Charitable Giving After a Tragedy or Natural Disaster**,
Better Business Bureau

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.