idealware

Helping Nonprofits Make Smart Software Decisions

LEGAL SERVICES NTAP
NATIONAL TECHNOLOGY ASSISTANCE PROJECT

# DISASTER PLANNING AND RECOVERY: PREPARING FOR YOUR RESPONSE CHECKLIST

**Stop and think about how many disasters can strike your office. There are the natural disasters—streets could flood, a tornado or an earthquake could wipe out your block—but there are also person-made disasters. Fire can engulf your building, an inept staff member can erase files, or hackers can hold your data for ransom. And then there are the predictable disasters—a server malfunctions or a computer crashes and can't be recovered.**

No one disaster is all that likely, but there's a good chance that some kind of disaster—natural, self-inflicted, or malicious—will occur during the life of an organization. To protect yourself and your clients, you need to plan ahead.

## Consider the Scenarios

Understanding what can happen is the first step toward developing a plan that's flexible enough to guide you through any disaster. Here are four scenarios that cover nearly every disaster recovery situation.

**1. Your office technology is gone.**

Imagine that every computer, printer, server, router—everything in your office suddenly disappeared. What information or software would be lost forever?

**2. The office power is out for two weeks.**

What will be inaccessible during that time? Is there anything you can't go without for that long?

**3. Key staff members are suddenly gone.**

What information do they have that no one else has? Are there passwords or credentials that can only be accessed by one person? What organizational functions will struggle the most without that person?

**4. Sensitive information gets breached.**

How will you stop the breach? How will you manage the response to clients, volunteers, or donors?

*Source: Joshua Peskay, Round Table Technology*

Below are questions to ask as you assess your organization and develop a plan to make sure your office makes a speedy recovery in the event of any disaster.

| |
|---|
| **1.** Do you have personal contact information for every staff member? |
| **2.** Do volunteers or other people who are not staff members use your organization's technology infrastructure, including phones or email addresses? How will an outage affect them? |
| **3.** In the event of a natural disaster, what is the process for contacting and accounting for each staff member to verify that they are safe and able to help with the recovery process? |
| **4.** Do you have a safe meeting place where everyone can go if your office is damaged or remains dangerous? |
| **5.** In the event of a natural disaster, will you provide food, transportation, or lodging for staff members or clients? If so, detail how you will carry this out. |
| **6.** What are staff roles in a disaster? Make sure to include secondary people to step in if the primary person is not available. |
| **7.** What functions or services are essential to your organization or your clients? List them in priority order. |
| **8.** What activities can you not afford to let stop? |
| **9.** What will it take to make sure there is no interruption of service for those essential activities? |
| **10.** How quickly do you need to get back to work on your essential activities? |
| **11.** Are there ways to get work done without technology? |
| **12.** What equipment do you have in your office? List and prioritize them based on their importance in helping you carry out essential functions or services. |
| **13.** Where will you purchase or acquire new hardware? |
| **14.** Is data held remotely, in the Cloud, or in the office? If data is in multiple locations, specify what is where. |
| **15.** Where are your data backups held? |
| **16.** Are you confident in the steps needed to restore a backup? If not, you should practice a few times. |
| **17.** Whose role is it to restore the backups? |
| **18.** What's your plan for contacting clients, volunteers, or donors about the incident? |
| **19.** How will you determine what information each group needs? |
| **20.** Do you have paper data that needs to be backed up digitally? Are the paper records stored in a cool, dry place that is less susceptible to a natural disaster or fire? |
| **21.** If there's an online attack or malicious software on your network, how will you contain it? |
| **22.** Do you have both paper and digital copies of all of your hardware warranties and receipts? |
| **23.** Do you provide training for staff members to help them stay safe in the event of an emergency? |
| **24.** What are the most likely disasters in your area? For example, earthquakes for West Coast offices, floods or tornadoes for the Midwest. List your location's top disaster threats. Does seeing this list change any of your plans? |
| **25.** Review your insurance policies. Do they cover lost time, location rental, recovery services, and equipment and device replacement? Knowing what money you will have to support your recovery will help you determine what to recover and how quickly you can get it running again. |
| **26.** Where will you store your plans? It won't do you any good to have a plan if it burns up in a fire. Keep everything in Cloud storage or on a flash drive (maybe more than one) and in a secure location away from your office. |

## ABOUT IDEALWARE

**Idealware, a 501(c)(3) nonprofit, is the authoritative source for independent, thoroughly-researched technology resources for the social sector. Find more free resources about software selection and dozens of other areas of nonprofit technology at www.idealware.org. This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.**