NONPROFIT TECHNOLOGY POLICY WORKBOOK

UPDATED FOR AUGUST 2020

TECHIMPACT®
IDEALWARE℠

CommunityIT Innovators®
where technology meets mission

IT Support for Nonprofits

Accomplish Your Mission with Better IT

Your technology shouldn't hold you back. It should drive you forward. We can help.

We're the only IT company that's exclusively served nonprofits for over 25 years.

We constantly research and evaluate nonprofit technology to ensure that you get cutting-edge solutions that are tailored to the needs of your organization. Our technicians are friendly IT experts who are passionate about serving nonprofits. Get a strategic IT partner. Reduce issues. Get peace of mind.

Services Include:

- Managed IT Support
- Workstation and Server Monitoring
- Managed Antivirus
- Managed Backup
- Email Filtering, Security, and Continuity
- Training and Technology Adaptation
- Managed Firewall
- Onsite Support
- Cybersecurity
- Server Hosting
- Network Management
- Cloud Management
- Endpoint Management
- Consulting and Strategy

Ready for Better IT? Let's Talk.

communityit.com • connect@communityit.com
1101 14th St NW #830, Washington, DC 20005

Want to be sure you're making the right IT decision?
Download our free Nonprofit Guide to Vetting a Managed Service Provider.

HOW WAS THIS REPORT FUNDED?

This report is funded by the visible ads paid for by our sponsors. Tech Impact Idealware was responsible for all of the research and editorial content of this report, which was created without the review of those who funded it. Vendors of any systems included in this report do not pay for inclusion nor does Idealware accept any funding from vendors at any time. Neither the funders nor vendors had any input over the editorial content of this report. We're grateful to our sponsors, Community IT and WizeHive.

Reprinting and Quoting

TABLE OF CONTENTS

Introduction 6
Worksheet 1: Acceptable Use Policy 7
Worksheet 2: Bring Your Own Device (BYOD) Policy 22
Worksheet 3: Data Security Policies for IT Workers 29
Worksheet 4: Incident Response Policy 40
Worksheet 5: Disaster Recovery Policy 41
Additional Reading 48
About This Report
- Authors 49
- Contributors 49
- About Our Sponsors 50
- About Tech Impact's Idealware 51
- About the Technology Learning Center 51

INTRODUCTION

Nonprofits face many of the same risks as businesses, and often additional funding and legal challenges, too. And, like all businesses, nonprofits also have to consider how to maintain high ethical standards and hold individuals and the organization accountable. Nonprofit leaders are familiar with ethics policies to protect their organizations from legal charges and Human Resources policies to protect staff members.

It's becoming painfully clear that nonprofits also face the growing security risks that come with our expanding online lives and mobile-friendly world. However, nonprofits generally have been slow to consider implementing similar policies for IT security issues.

Tech Impact Idealware created this workbook to help you identify the policies you need and get you started developing and implementing them. Through a series of five worksheets, we'll walk you through what to consider as you develop policies for your organization to define the expectations for staff members using company computers or other equipment, established precautions to take when staff use their personal smartphones or other devices for work, guidelines for protecting organization and constituent data from unauthorized access, and more.

> ***The world is full of risks. But with proper planning, you can minimize your damage if and when something goes wrong.***

This workbook will also help you develop a strategy for responding to security incidents or major disasters and provide a framework for how your organization can recover and get back to normal.

The world is full of risks. But with proper planning, you can minimize your damage if and when something goes wrong.

WORKSHEET 1:
Acceptable Use Policy ▶▶▶

The most difficult step of defining security policies for your organization is often identifying where to begin. Since many of the concerns your policies will need to address may be unfamiliar to you, and may require additional research, the easiest place to start is with your acceptable use policy, since it covers quantities you already know—your employees and the equipment you have on hand. In this worksheet, you'll build out a policy for acceptable use of your organization's computers, software, and other equipment that staff members use.

Policy Purpose and Scope

Start off your acceptable use policy with a general statement on the problem that the policy is intended to address or prevent (the "purpose" of your policy), what technology—hardware, software, or otherwise—it covers, and the people who are covered by the policy (the "scope"). In addition, your statement should also include your organization's name and a comment on the importance of having the policy in place. For example, you might mention that inappropriate use of technology exposes your organization to various risks such as virus or malware attacks, which then compromise network systems and data, putting your organization at risk of a lawsuit.

Your purpose and scope statement should be direct and straightforward. Many such statements may follow this simple format:

The purpose of this policy is to outline the acceptable use of _____ at [Your Organization]. These rules are in place to protect the employee and [Your Organization]. Inappropriate use exposes [Your Organization] to risks including virus attacks, compromise of network systems and services, and legal issues.

Use the lines below to draft a purpose statement for your acceptable use policy:

Who Does This Policy Affect?

An important part of your Acceptable Use Policy is who the policy affects. Below, we've provided some sample text to include in your written policy and a list of roles typically covered by acceptable use policies. On the next page, go through the list and check off each person or role that you wish to include in your organization's policy. Are there any other roles or types of employees at your organization not listed? Use the extra lines at the bottom to record anyone else this policy should cover.

"This policy applies to the following:"

- ☐ Full-time employees
- ☐ Part-time employees
- ☐ Contractors
- ☐ Consultants
- ☐ Temporaries
- ☐ Volunteers
- ☐ Interns
- ☐ Board members
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Exceptions: (fill this section out after you've completed the brainstorming exercise at the end of this worksheet.)

What Does This Policy Cover?

In addition to the people your policy applies to, you need to define the equipment or other resources that are covered by the policy. Do you want to specify individual devices or types of technology, or make a blanket statement that the policy applies to all equipment that is owned or leased by your organization? Go through the list below and check off each that you wish to include in your organization's policy. Use the extra lines at the bottom of the list to list any additional technology or equipment at your organization this policy should cover.

"This policy applies to all of the following that is owned or leased by our organization:"

- ☐ Computer equipment
- ☐ Other electronic devices
- ☐ Software
- ☐ Operating systems
- ☐ Storage media
- ☐ Network accounts providing email
- ☐ WWW browsing
- ☐ FTP
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Repercussions and Consequences of Policy Violation

What are the consequences of noncompliance? Many organizations make a broad statement that ends with "including termination." How specific do you want to be about this? Use the lines below to draft the consequences you feel would be appropriate for violating your organization's Acceptable Use Policy.

Use and Ownership

A good way to start your acceptable use policy is by defining some general guidelines around the rights and ownership of affected equipment or data. The equipment may be owned by your organization, but who is responsible for regular maintenance—IT staff or the person using that computer on a day-to-day basis? Depending on the nature of your work, staff members may be responsible for creating public documents, reports, multimedia files, etc. Who owns those files? Go through the following prompts to identify guidelines around use and ownership rights for organization equipment and information.

Who owns the data stored on your organization's devices? Does this proprietary information belong solely to the organization? Are there exceptions where a staff member, contractor, or other employee may retain rights to files or data they create or use as part of their duties?

Who has access to what kinds of data? Can data be shared? In what circumstances?

If staff members are uncertain about who owns data or whether they have permission to share it with outside parties, whom do they ask?

All electronic devices, such as computers, printers, and smartphones, require regular maintenance to operate correctly. Even data—such as files stored on the network or records in a database—need periodic maintenance to ensure information is recorded properly and to optimize storage space. Who is responsible for equipment maintenance? Does each staff member take responsibility for maintaining the equipment they use or are only certain individuals permitted to conduct maintenance?

When should equipment maintenance take place? Do you want to define a schedule for how often maintenance takes place?

Especially for organizations with more staff members, or those that rely heavily on contract or temporary employees, it may be essential to monitor your organization's equipment, systems, or network traffic to ensure that staff members are following these policies. On the other hand, especially for organizations with a small group of trusted employees, actively monitoring usage may be unnecessary. Will you monitor traffic and/or activities on your networks? Who will do this? How? How often?

General Security Guidelines

While much attention around security is focused on technology, the greatest threat to your organization's security is staff members. Part of your Acceptable Use Policy should cover basic expectations for security practices.

Do you wish to restrict staffers to the minimum data they need to do their job? How do you define minimum and how will this be adjudicated?

Do you require all devices to have passwords?

No one likes to have to restart or log back into their computer after a break—it slows us down and is inconvenient. But leaving a computer unlocked and unattended can invite the risk of unauthorized access to confidential records or sensitive information. It's important to balance these two concerns to find a reasonable length of time a workstation can remain unlocked while employees are away from their desk—longer than a bathroom break but shorter than a lunch break, for example. Do you want every computer or device to hibernate or logout if not in use? How much time should pass before they have to log in again?

Do you require individual staff members to include disclaimers when posting on message boards or social media? If so, what do you want that disclaimer to say?

USB drives and external hard drives are easily lost or stolen. Will you allow work-related data to be stored on these devices? Is so, how will you manage these devices, including encryption?

Unacceptable Use

Below we've provided a sample set of statements about unacceptable or inappropriate uses of organization-issued devices and accounts that you might consider including in your written acceptable use policies. Go through the list and check off each that you wish to include in your organization's policy. Remember that these are only a sample of what an acceptable use policy might prohibit, and your organization's needs may differ. Is there anything not listed below that you would want to address as part of your policy? Use the extra lines to write down any other uses of technology you want to prohibit.

The following activities are strictly prohibited:

- ☐ The violation of copyright, trademark, or other intellectual property rights of individuals or organizations including, but not limited to, pirated software and the unauthorized use of photography.
- ☐ Accessing organization data for purposes not related to work duties.
- ☐ Illegally exporting technology in violation of international or regional export control laws.
- ☐ Introducing malware or other malicious software to organization devices or the devices owned by staff members.
- ☐ Using technology to violate HR or ethics policies.
- ☐ Using organization computers or other technology for personal commercial use.
- ☐ Using organization-issued equipment for games or other entertainment purposes during or outside of work hours.
- ☐ Viewing or transmitting pornography on the organization's network or devices.
- ☐ Using organization technology to promote fraudulent offers.
- ☐ Making guarantees or "statements about warranty."
- ☐ Knowingly causing or enabling a breach of organization security procedures.
- ☐ Disrupting network communication.
- ☐ Unauthorized attempts to intercept data.
- ☐ Circumventing user authentication or security procedures.
- ☐ Any attempt to interfere with the regular operations or duties of the organization—locally or virtually.
- ☐ Sharing personal information about other staff members with unauthorized parties outside of the organization.

- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Password Policies

Your most basic tool for keeping your organization secure is often the easiest to exploit: your passwords. People are lazy, and while we know that we should use more secure passwords, and to keep them safe, we still end up using the same password for multiple different accounts.
Go through the following prompts to identify guidelines around secure password usage as part of your policy.

What are the minimum security standards for a password? How many characters (numbers and letters) are required? Do passwords need to include special characters (e.g. %, !, &)? Do passwords need to be case-sensitive with a certain number of capitalized letters?

Are staffers required to change passwords periodically? How often? Can they repeat passwords?

What specifically constitutes a weak password for your organization? Simple patterns (e.g., “121212”), common passwords (e.g., “password1”), personally identifiable information such as a birthday, and public information about the organization such as its street address are all examples of password mistakes that organizations should avoid.

What are your guidelines for handling passwords at the user level? No writing them down? Making sure they're encrypted if stored on a device?

Will you require Multi-Factor Authentication (MFA)? If so, on what additional factors will be used?

The past few years have seen a growth in software to manage passwords, allowing users to follow guidelines without needing to remember dozens of individual passwords. A password management program, such as LastPass, Dashlane, or 1Password, can be a useful tool to ensure staff members comply with your password policies. Do you want to use a password management program? If so:

Is use of a password management program required by staff members, or only recommended?

Will your organization manage permission levels and access to accounts centrally, or is it the responsibility of each individual to manage their own passwords and account access?

Will you periodically audit passwords by attempting to crack them?

Do you allow multiple staffers to share any accounts? Which accounts can and cannot be shared?

Email and text messages are not as secure as many people think. Some staff members might try to share passwords via email, text, or chat. Even when the password is for an account that you've defined as OK to share, how the password is shared can potentially compromise your software or system. Below, write a simple statement clarifying how passwords can be transmitted to other authorized users.

In the event that a user's password(s) are compromised or otherwise exposed, how soon does the staff member need to report that breach to the organization? Will you measure that timeframe in days or hours?

Email Use and Guidelines

Email is an essential part of how work happens. Some of your staff members may have never known a world without email, while for others, their organization email may be the only account they use. In either case, it's important to include in your acceptable use policy proper use of the medium and expectations for how to communicate as a representative of the organization.

Go through the following prompts to identify guidelines around email use and decorum.

To an extent, it's understood that staff members may use their organization email account to communicate with colleagues both inside and outside the organization. But there should be limits to reasonable use of email for non-work purposes. How will you define reasonable use for email? What limits on personal versus business use?

The sending of unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material, is specifically prohibited by the CAN-SPAM Act. Violation of that act can result in your organization's entire domain being blacklisted as spam. With the importance of broadcast email to fundraising, that's a risk nonprofits can't take. Are there limits you want to set on who staff members can or can't email? Will you limit the number of people who can be included in an email?

Email messages are often forwarded to coworkers and colleagues who did not receive the original message but may need to weigh in on the discussion. However, it's important to understand the sensitivity or confidentiality of the message before doing so. What level of confidential detail can be included in a forwarded email? What guidelines do you wish to share?

While it's important to grow your organization's mailing list by asking supporters to subscribe, you might not want staff members to use their work email, or their position, to collect email addresses for non-work purposes. It might be fine, on occasion, to ask if a colleague would want to receive email about some personal cause or project, but it's not fine for staff members to sell lists of supporter email addresses to spammers. Where will your policy draw the line?

Can staffers send emails to people on your mailing list regarding information that's not related directly to the organization?

While we often want to trust our staff members to follow policies and guidelines on their own, for many organizations, the risk of confidential client records or financial information being shared by email is too great. Will you monitor staff email? How frequently and at what level?

Email Security

SUSPICIOUS EMAILS

Staff members are likely to get dozens of suspicious emails per week. Most of those emails will get caught by spam filters, but for those that don't, you need to provide guidance.

What steps should staff members take if they receive a suspicious email? Should they contact IT immediately or is there a checklist you'd like them to review first?

Will you provide training on how to detect suspicious emails?

If you provide suspicious email training, how often will you provide the training and will you use education and testing tools such as Knowbe4?

ATTACHMENTS

In business settings, one of the major uses of email is to share documents both with external parties (like funders, government agencies, partners) and internally. While attached documents are convenient for work, they are also a convenient method for unscrupulous parties to transmit viruses or other malicious software. It's best to not open attachments from unknown email addresses, or unsolicited attachments, but you may also consider defining the types of files that can and can't be opened when sent as an email attachment. For example, Microsoft Word documents (.doc or .docx), spreadsheets (.xls, .xlsx, .csv) and .PDF files are common file formats that are sent in work emails. However, you wouldn't normally email an executable file (.exe), which installs software when opened.

We've identified some commonly-encountered document types and their respective file extensions. For each, check off which files are safe to open as attachments, which should never be opened when sent in email, and which might be fine to open, under specific circumstances. For the latter, use the space provided to define under what conditions it's safe to open attachments of that type.

Document Type	Safe to Open	Never Open	Open under specific conditions
Microsoft Word (.doc, .docx)			
Microsoft Excel (.xls, .xlsx)			
Microsoft PowerPoint (.ppt, .pptx)			
Word Perfect (.wp)			
Text only (.txt)			
Comma-separated value (.csv)			
Rich text format (.rtf)			
Portable Document format (.pdf)			
Image files (.gif, .jpg, .png, .bmp)			
Video files (.mp4, .avi, .swf)			
HTML files (.htm, .html)			
Self-extracting Archive (.sea)			
Executable Files (.exe)			
Visual Basic Script (.vbs)			

Exceptions to this Policy

Finally, you should consider what exceptions may need to be made to this policy for certain roles or staff members. For example, if you wanted to prohibit staff members from installing new software on their workstations, or performing hardware maintenance themselves, you would need to make exceptions for IT staff—the people at your organization who are responsible for computer maintenance.

Use the lines below to brainstorm any exceptions to the policy. When are exceptions allowed? Who must approve any exceptions?

Once you've finished brainstorming, write down the conditions and proper protocol for exceptions to this policy in the Exceptions section at the beginning of this worksheet.

WORKSHEET 2:
Bring Your Own Device (BYOD) Policy

Many organizations now allow staff members to use their personal computers, smartphones, or other devices for work, a practice known as Bring Your Own Device, or BYOD. Some nonprofits choose to do so because it's more convenient or more efficient for staff members to use the devices they're already comfortable with. Others do so to cut costs—it's cheaper for staff members to use their own computers than for the organization to buy computers for everyone. Whatever the motivation, all organizations that allow staff members to bring their own devices should define a policy for what devices are and are not allowed, set rules for the appropriate use of personal devices, and take steps to ensure the security of all personal devices.

Who Does This Policy Affect?

An important part of your BYOD policy is who it affects. Below, we've provided some sample text to include in your written policy, and a list of roles typically covered by policies. Go through the list and check off each that you wish to include in your organization's policy. Are there any other roles or types of employees at your organization not listed below? Use the extra lines to list anyone else this policy should cover.

"This policy applies to the following:"

- ☐ Full-time employees
- ☐ Part-time employees
- ☐ Contractors
- ☐ Consultants
- ☐ Temporaries
- ☐ Volunteers
- ☐ Interns
- ☐ Board members

☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____
☐ _____

Exceptions: (fill this section out after you've completed the brainstorming exercise at the end of this worksheet.)

_____

_____

_____

_____

_____

What Kinds of Personal Devices Are Approved For Work Use?

While allowing staff members to use their personal devices can be convenient for both them and the organization, it's important to set limits for what devices can or cannot be brought from home. The first concern is security—if staff members are using their smartphones to send confidential email to clients, for example, what if a phone gets lost in a public place? Another concern is where it makes sense to rely entirely on staff members to use their personal devices to do their work. The option to use personal devices over equipment provided by the organization is convenient, but if the expectation is that employees will use only personal devices for work, are you asking too much of them? Think about how to strike these balances as you craft your BYOD policy.

Go through the list below and check off each type of personal device that you will allow as part of your BYOD policy. Use the extra lines to list any other technology or equipment this policy should cover. Remember that it's best to be specific about what is or is not allowed.

- ☐ Laptop computers
- ☐ Desktop computers
- ☐ Smartphones
- ☐ Tablets
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Repercussions and Consequences of Policy Violation

What are the consequences of noncompliance? Many organizations make a broad statement that ends with "including termination." How specific do you want to be about this? Use the lines below to draft the consequences you feel would be appropriate for violating your organization's Bring Your Own Device Policy.

Are there limits you wish to set for which devices can be used during work hours? Will only those devices you defined above be permitted during work hours? Do the guidelines imposed by your organization's Acceptable Use Policy apply to personal devices as well? Use the lines below to define any limits you wish to impose.

For the purposes of this policy, how will you define the hours or circumstances that qualify as work hours?

Considerations

Are there any exceptions to these restrictions you wish to allow? Do staff members need to get permission from a specific person for these exceptions?

Will you have a separate wireless connection for guests or people using their home devices at work? If so, a splash page should be set up to explain the rules to anyone connecting to the network and that requires users to agree to those rules before they can fully connect to the network. Not every app or website used by someone on their personal device will be appropriate for use at work. Use the lines below to describe sites or apps that staff members are prohibited from using on their personal devices during work hours.

Whether a device is owned by an employee or the organization, something will eventually go wrong with it. If a staff member needs to use that device for work, they'll need to solve the issue quickly. What kind of IT support will you provide for personal devices? Will you place limits on the amount of support a staffer can receive?

Will you require all personal devices used for work to have a robust anti-virus solution installed? Many larger organizations and for-profit companies with BYOD policies now use Mobile Device Management (MDM) software to both provide work-specific apps for smartphones and to monitor usage or enforce policies.

If you do choose to use Mobile Device Management software on smartphones that staff members bring from home, you'll need to specify the conditions when this software will be used. For example, will you use it to delete all organization data from said devices when an employee leaves the organization? Use the lines below to define when and how your organization will use MDM software, including the data you will have access to and how you will manage or monitor that data.

While a BYOD policy can mean that your organization doesn't need to spend the money to provide these devices to staff members, it's not very fair to not support the devices at all. Will you reimburse staff members for the use of personal devices? How much? How will you calculate the amount to reimburse? Are there devices or uses exempted from the reimbursement policy?

In order to protect information that's accessible using devices brought from home, you may want to define a set of security expectations that staff members must implement and follow as part of the privilege of using personal devices. These precautions may be as straightforward as requiring that passwords are set on any devices used for work. You may also want to consider other potential risks. For example, is it appropriate for staff members to use smartphones that have been "jail broken"—that is, modified to bypass manufacturer restrictions on software that can or cannot be installed. What configuration settings will you require?

We've provided a few statements around device security that you may wish to consider for your organization. Select any that you want to include as part of your BYOD policy. Use the extra lines to list any other security guidelines staff members need to follow for their personal devices.

- ☐ Staff members must enable passwords (or comparable log-in settings) on all devices used for work purposes.
- ☐ Passwords for personal devices must follow the same minimum requirements and policies as any organization-issued equipment.
- ☐ Staff members must encrypt any organization files or data stored on personal devices.
- ☐ For personal devices, staff members must follow the Acceptable Use policies that specify when computers and other devices must "time out" or require log-in after a period of inactivity.
- ☐ Staff members cannot use any personal devices for work purposes that have been modified to bypass factory settings on the software that can be installed (i.e. "jail broken").
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

How soon should staff members report a lost or stolen personal device? In the event that a staff member loses a device used for work, or if their device(s) are stolen, how soon does the staff member need to report that breach to the organization? Will you measure that timeframe in hours or days?

The security precautions in a staffer's home, hotel room, or neighborhood coffee shop may not be as strong as the precautions taken at your office. Therefore, it's useful to define the minimum expectations that each staff member should follow when using their own devices at home or on the road. We've provided a few common security standards organizations may require of staff members using their own devices from home or remotely. Select any that you want to include as part of your BYOD policy. Use the extra lines at the bottom of the list to record any other steps staff members need to follow.

- ☐ Staff working from home must enable an internet firewall while using their home connection for work.
- ☐ Staff members must use a wireless router at home that follows strong password and encryption standards.
- ☐ Staff members must use a Virtual Private Network (VPN) when using an open wireless internet connection (e.g. at a coffee shop, hotel room, etc.).
- ☐ _____
- ☐ _____
- ☐ _____

If staffers download software on a personal device they use for work, who owns the license—the staff member or the organization? How will you manage licenses for software used on personal devices? How will you address the licenses for software installed on personal devices when the staff member leaves the organization?

Exceptions to this Policy

Finally, you should consider what exceptions may need to be made to this policy for certain roles or staff members. For example, if you wanted to prohibit staff members from installing new software on their workstations, or performing hardware maintenance themselves, you would need to make exceptions for IT staff—the people at your organization who are responsible for computer maintenance.

Use the lines below to brainstorm any exceptions to the policy. When are exceptions allowed? Who must approve any exceptions?

Once you've finished brainstorming, write down the conditions and proper protocol for exceptions to this policy in the Exceptions section at the beginning of this worksheet.

WORKSHEET 3:
Data Security Policies for IT Staff ▶▶▶

While you've already defined your general policies for staff members, you'll need to define more specific guidelines for how IT workers must protect the security and integrity of sensitive data, and the devices that store it. In this worksheet, you'll identify what data is confidential, essential to your work, or otherwise sensitive, and define a policy to ensure that data is handled appropriately, routinely backed-up, and monitored for proper handling.

Who Does This Policy Affect?

As with all policies, you'll need to define who at the organization your Data Security policy affects. Below, we've listed roles typically covered and left space for anyone not listed who this policy should cover.

"This policy applies to the following:"

- ☐ IT staff
- ☐ IT contractors
- ☐ System admins
- ☐ User admins
- ☐ Program officers
- ☐ Accounting/bookkeeping staff
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____
- ☐ _____

Exceptions: (fill this section out after you've completed the brainstorming exercise at the end of this worksheet.)

Data Policies

Every organization creates, collects, and stores a large amount of data. Even if you're not actively measuring performance or outcomes, you still have donation receipts, contact or other personal information from clients, and financial information such as staff salaries, budgets and expenditures, and tax records.

Not all data is the same—it varies widely by source, content, and how it can be handled. Some of your data may need to be kept secure for legal or ethical reasons. If you provide direct services, for example, HIPAA requires that any information that could be directly connected to an individual client needs to stay private from unauthorized access. Other data—such as your annual budget or tax records—need to be shared with the IRS and grantmakers (and it doesn't hurt to make that information available to donors or the public on your GuideStar profile). Therefore, you'll need to identify and classify the different types of data at your organization before you can define any policies on how to secure and backup that information.

In the table below, list the different types of data your organization currently stores. Then, for each type of data, check the box to mark whether that data is confidential (could expose personal details about clients, constituents, or staff members), essential (necessary for your organization to function), or "open" (data that could be lost or shared publicly without compromising constituent privacy or impeding organization work).

Type of Data	Confidential?	Essential?	Open?

Data Backup

Backups are an essential part of data maintenance for every organization. Regular and up-to-date backup files are your organization's insurance against data loss as a result of disaster—natural or human-made. While we all hope to never need the backups, maintaining an archive of your data (ideally outside of the office) ensures that you can keep working even after a hurricane or a burglar strikes. For each of the following prompts, brainstorm how you want to address them as part of your data security policy and write down your answer.

How often will you back up your data? It's important to consider how frequently major changes or updates to the data may take place and how much new data may be lost. Many organizations will back up all their data on a weekly basis, or you could set different backup schedules for different types of data. Records that change infrequently, such as your tax information, could backup every month or so, while information you update regularly—such as client records or case notes—could be backed up nightly or even hourly.

While storage space is fairly inexpensive, you don't want or need to keep every backup file you ever create. How many backup versions will you keep and on what schedule? For example, an organization might keep a backup for every day of the current week, one backup a week for the current and previous month, and one backup for each month for the previous year. It's important to consider how far back a user might need to go to find records that were accidentally deleted.

How will you store backups? In the past, organizations relied on physical tape backups—every week, a staff member was in charge of backing up the data and taking the tapes home to store safely outside of the office. Nowadays, we have an abundance of cloud-based file storage and backup solutions available that can run automatically and be accessed from anywhere. Your policy should define where backups will be stored, whether that be in the cloud or on physical media. Will you maintain both physical and cloud-based backups? If so where will the physical backups be stored? Will you maintain an additional physical backup off site?

As mentioned before, organizations in the past needed to assign a staff member to manually initiate backups and ensure that the files were stored safely. While this is still an option, we now have access to affordable services that can automatically backup up files on a schedule, and save the backups to a secure, off-site server. How will your organization handle backup procedures? Will backups be scheduled automatically, or will someone need to remember to start them? Who will be responsible for making sure backups take place regularly and are saved properly?

Testing backups by restoring random files is the best way to ensure your backups will work in their time of need. Will there be a person assigned to periodically restore files from backups for testing purposes? How often will these tests occur?

Will you require your server room be locked at all times? Who will have access to the room? Server rooms typically require air conditioning, which can sometimes fail causing equipment to overheat and suffer damage. If you are a tenant in a building, will the landlord have access to the room in case of an emergency?

Password Storage

Whether you store passwords locally on an encrypted device, in the Cloud on dedicated servers, or using a service such as LastPass, your organization needs to think about how it will access those passwords if an IT staff member is unable to come to work or is fired.

How will IT store passwords and encryption keys to ensure that they are accessible in an emergency?

Software Installation

A computer is useless without the software needed to get the job done. In addition to the office software, accounting tools, and databases you'd typically expect, your staff members may need additional apps for specific tasks, productivity, or convenience. But who should be in charge of installing that software—your IT staff or the staff members who need the software?

Are individual staff members allowed to download software to the computers or other electronic devices they use for work?

While most applications your staff members will want to install will pose little threat to your organization's security, that doesn't necessarily give your staff carte blanche to install whatever they want. At a minimum, software installed on work computers should be for work-purposes—video games are almost certainly off-limits. Do you want to make a list of approved software or provide other guidelines for what should and should not be downloaded?

If IT must download software, what are the procedures for requesting and carrying this out?

Installation is only part of adding applications to a computer. The software that your organization needs often requires licenses, or activation keys, in order to run. (Installation may be free, but activation typically costs money.) For some software, the license fee provides a key, which can only be used once. Other software may use a Multiple Activation Key (MAK), which can be used a certain amount of times before expiring. How will you track which licenses have already been used and how many are left?

Update Protocol

Most applications are not "set it and forget it" products. Software vendors often provide regular updates or "patches" that protect against new security risks, provide additional functionality, or allow it to be compatible with newer versions or different file types. Therefore, you'll need to ensure that these updates are regularly installed, whether by dedicated IT staff or by the staff members using the software.

Who is expected to install software updates? Will your IT staff be responsible for updates or the staff members using the software? If staff members are responsible for updates, how will you monitor whether or not the updates are being made?

If your IT staff is responsible for installing software updates, what are the procedures? Are updates installed manually or will they be automated? What considerations need to be specified about disruption to staff?

Equipment Replacement

Servers, PCs, and other devices do not last forever. Some organizations use IT equipment until it fails, which can be inefficient in the long run and potentially disruptive. Here are a few questions to consider.

How are you tracking warranties?

Do you have a schedule for which devices to replace when?

What is your process for selecting and purchasing new equipment?

Data in Motion

For organizations with a large volume of confidential or otherwise sensitive information that is sent between multiple systems or outside the organization to clients or third-party providers, it may be necessary to monitor how that data is handled in transit. You may look into implementing a software package on your servers to monitor and scan data sent between your systems or to outside parties to ensure that confidential or restricted information is handled properly, or that staff are not sending data to unauthorized parties.

Will you scan traffic as it moves onto other servers?

What software will you use?

What is the threshold for triggering a response? Does it vary depending on how the data is classified?

If you notice unusual or suspicious traffic on your servers, refer to your data breach policy for the appropriate responses to take.

Additional Security Considerations

Depending on the nature of your organization's work, you may need to follow additional security guidelines for specific types of data.

Payment Card Information (PCI)

For nonprofits dependent on individual donations to fund their programs or general operations, it's imperative that donors can trust that you will protect their payment information. If you accept donations by credit card, that means you'll need to comply with Payment Card Information, or PCI, guidelines to ensure that cardholder information and credit card information is securely handled and encrypted.

The easiest solution is to not process credit cards directly—instead, utilize a PCI-compliant third-party payment processor or merchant account to actually charge a donor's card. But if your organization still runs credit cards on paper slips that need to be deposited to a bank, you'll need to take extra precautions to protect your donors' information.

On the lines below, define what additional steps you will take to protect any Payment Card Information.

Personally Identifiable Information (PII)

Identity theft is a serious concern, and an expensive hassle for your constituents. Your organization needs to take extra precautions to ensure that your constituents Personally Identifiable Information (PII)—such as social security numbers or financial information—are protected from unauthorized access. On the lines below, define what additional steps you will take to protect PII.

Health Insurance Portability and Accountability Act (HIPAA)

If your nonprofit deals with health records, it will need to comply with- HIPAA. You can read more about the rules on the U.S. Department of Health and Human Services website: https://www.hhs.gov/hipaa/for-professionals/index.html

Based on HIPAA, what additional steps will you organization take to protect health records and constituent data?

Will your IT staff be required to obtain HIPAA certification?

Student Records (PER)

If your organization provides educational services or otherwise works with actively-enrolled students, you'll need to protect their educational records—including personally identifiable information, evaluations, grades, admissions records, or financial aid records—from unauthorized access. On the lines below, define what additional steps you will take to protect student records.

Protected Health Information (PHI)

If your organization provides physical or mental health services (medical checkups and exams, therapy or counseling sessions, etc.) you will need to take steps to ensure that any information that links an individual with their condition is secured from unauthorized access. In addition to protecting the trust between a patient and their health provider(s), unauthorized release of information related to a patient's condition can cause irreparable damage to their social or professional lives. On the lines below, define what additional steps you will take to protect any Protected Health Information.

Exceptions to this Policy

Finally, you should consider what exceptions may need to be made to this policy for certain roles or staff members. For example, if you wanted to prohibit staff members from installing new software on their workstations, or performing hardware maintenance themselves, you would need to make exceptions for IT staff—the people at your organization who are responsible for computer maintenance. Use the lines below to brainstorm any exceptions to the policy—when are exceptions allowed? Who must approve any exceptions?

Once you've finished brainstorming, write down the conditions and proper protocol for exceptions to this policy in the Exceptions section at the beginning of this worksheet.

WORKSHEET 4:
Incident Response Policy ▶▶▶

While adopting and rigorously following security best practices and guidelines for acceptable use of electronic equipment offers significant protection, no policy will ever eliminate the risk of a security breach. The precautions we take against compromised or easily guessed passwords, malware, and phishing attempts only serve to reduce the likelihood.

In this worksheet, you'll work through identifying what needs to happen after a potential security breach.

In the following chart, we've provided a list of different roles or positions to help you brainstorm and collect the names the right people you need to form a response committee. Then, in the second chart, we've provided a list of necessary responses to security incidents. In the middle column, write down which role from the first chart is in charge for each response. Then, in the right column, identify how soon after the incident each response needs to happen. Is this an action that needs to be taken in a matter of hours, or over the following few days?

Roles At Your Organization	Names and Contact Information
Executive Director (committee chair)	
Senior IT Staff	
HR	
Communications Director	
Membership Director	
Staff members involved or affected	
Finance	
Legal	

Response	Who is in Charge?	Who is in Charge if the Primary Person is Not Available?	How Soon Does This Happen?
Diagnose a breach			
Remove access			
Repair or replace any technology damaged			
Review liabilities			
Communicate with staff			
Communicate with public			

WORKSHEET 5:
Disaster Recovery Policy ▶▶▶

When and where disaster strikes isn't something that your organization can control. What you can control is how quickly your organization gets back up and running. This worksheet will guide you through developing a recovery plan that prioritizes your most essential services—and the technologies needed to support those services—to help your organization maintain a cool head and get back up and running as efficiently as possible.

Technology Triage

After a disaster, your organization will likely have many services and technologies to get running again, and time will be in short supply. Therefore, it's essential to identify which technology or procedure you need to get back on line first, to reduce downtime and recover efficiently. Because multiple services your organization provides may require the same technology or software, identifying which systems are essential for the most services can help you focus recovery efforts more efficiently.

In the table below, identify each of the services your organization provides and the internal processes that help the organization run smoothly. Then, in the right column, write down all the software, hardware, and other technologies needed to support each. Keep in mind that much of what you write down will also depend on making sure your power and internet are back online.

Service	Software/ Technology Required

Now that you've identified the technology needed to get each service or process running, look over the list again. Are there systems or devices that support multiple services? The more services or processes that depend on a single technology, the more important it is for you to get that technology up and running quickly.

On the lines below, write down each of the technologies you identified above, ordered by your most essential services. This will give your team a prioritized list of what needs to get back on line first during your disaster recovery.

Disaster Recovery Priority: Essential Technologies and Services

Look over this list—does the order make sense for your organization? Does something seem out of place, or are you surprised by what appears to be most important? Use your best judgment—no one knows your organization better than you. Run this list by other staff members to get their input and make sure that this list accurately reflects your organization's priorities.

Data Restoration

Once your systems are back on line, you'll need to ensure that you're working with a complete copy of your data. This is why backup is an essential part of your data security policy. You'll need to make sure you know where your backups are stored and restore the most recent backup so you can get up and running as if nothing had ever happened.

Where are your files and data currently backed up?

What are the procedures for restoring a backup?

Cyber Security Insurance

Many organizations have a lot at stake if they get hacked. To reduce the risk to their organization and constituents, they purchase cyber security insurance.

Do you have cyber security insurance? If so, what does it cover?

How are you communicating your coverage to your constituents?

How can your organization make an cyber security insurance claim?

Replacing Lost/Damaged Equipment

In the event of a natural disaster or break-in, you'll need to replace computers, devices, or other equipment that may have been damaged or stolen. While insurance should cover the cost of replacing anything lost, you'll need the equipment well before you'll receive the insurance payout, and it's unlikely that your organization will be able to afford replacing everything at once in the wake of a disaster. Therefore, it's important to prioritize and replace the equipment most essential to your work first.

Look back at the essential services and the required technologies that you brainstormed earlier in this worksheet. What physical equipment or electronic devices are needed to support your critical services? In the wake of any disaster, those pieces of equipment should be the top priority to replace. For example, if the phone is the primary way your constituents contact your organization for services, it doesn't make sense to replace a broken or missing scanner first.

Think carefully about the equipment your organization needs to support services and processes. Consider getting input from IT staff, directors, program officers, or other stakeholders. Then, on the next page, write down the order in which equipment should be replaced.

In the rush to get your services back up and running after a disaster, you don't want to waste time trying to source replacement devices. You don't have the luxury of time to search around dozens of websites or brick-and-mortar stores to find what you need. To streamline the process, it's helpful to create a short list of approved vendors for replacing equipment. Where should you go first to replace a lost computer, phone system, or printer?

On the lines below, list the approved vendors, if any, for replacing stolen or damaged equipment.

Contingency Planning

The goal after any disaster is to get back up and running quickly. Unfortunately, there will always be some parts of disaster recovery that will be out of your control. The severity of a disaster and your organization's physical location can factor into how long your services are out. For example, while the City of New York was able to restore subway services following Hurricane Sandy in a matter of days, rural areas of New England were without power for a week or longer following a December 2013 ice storm. No matter how severe a disaster is, your constituents still need your services. While one or two days offline may be brief enough for people to manage, if your services are unavailable for longer durations, you'll need a contingency plan in place to make sure your constituents still receive the help they need.

In the table below, identify each of the services your organization provides. Then, in the right column, define the contingency plan for continuing each service, whether by your organization or by partnering with nearby service providers.

Service	Contingency Plan

Finally, while individual devices or simpler processes will be relatively simple to set up and get working following a disaster, more complex or involved systems may require a testing and implementation period—much like when you first implemented that system—before they're ready to go live once again. How much testing will you conduct before going back online with your systems and services?

ADDITIONAL READING ▶▶▶

- *What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk,* Tech Impact Idealware

  https://offers.techimpact.org/reports/nonprofits-need-know-security-practical-guide-managing-risk/

  This free report cuts through the fear and uncertainty surrounding security issues, showing you how to assess your risk, explain the basic protections, and discuss building a culture that values security.

- *Information Security Policies,* The University of Florida

  https://it.ufl.edu/policies/information-security/

  A listing of helpful articles, templates, and guidelines on information Security policies from the University of Florida Information Technology Department.

- *Information Security Policy Templates,* SANS

  https://www.sans.org/security-resources/policies

  This resource from the SANS Institute provides a robust set of templates for information security policies, covering twenty-seven important security requirements.

ABOUT THIS REPORT

Authors

Dan Rivas, Lead Researcher

Dan Rivas is a writer and editor who has worked with nonprofits, local governments, and large companies to research and communicate ideas that move communities forward. He lives in Portland, Oregon.

Karen Graham, Managing Director of Education and Outreach, Tech Impact

Karen is a sought-after speaker, trainer, writer, and consultant with expertise in technology leadership and innovation, nonprofit software, and digital strategy. As Tech Impact's Director of Education and Outreach, she leads the Idealware team of researchers, presenters, and writers who create technology information resources designed to help nonprofit leaders put their vision into action. Her past experience includes leading the technology consulting services and nonprofit technology learning and networking programs at MAP for Nonprofits, helping to build the nonprofit CRM/database solution provider thedatabank from a startup to a thriving software company, and various roles in arts and human services organizations. She holds an MBA in Nonprofit Management from the University of St. Thomas.

Contributors

Antonio Palumbo, Director of IT, National Development Council
Dan Hampton, IT Specialist, AHA Agency for their input and insights.

About Our Sponsors

Community IT

Community IT is among the Top 501 Managed Services Providers in North America and is a recognized leader in the nonprofit technology community. In 2020 Community IT Innovators was one of the only ranked MSPs serving exclusively nonprofit clients. Since 1993, our skilled and certified team of IT professionals has served the greater Washington DC nonprofit community, helping organizations of all sizes and capacities to advance their missions through the effective use of technology.

WizeHive

WizeHive serves some of the most important mission-based organizations—foundations, nonprofits, universities, associations, and government offices—with Zengine, its comprehensive, easy-to-use, and flexible grants management software. Humbled by the missions that drive their clients, it is their mission to design technology with grantee experience, impact reporting, and achieving your objectives in mind. Pairing the platform with dedicated and human service, one-on-one training, and continual educational opportunities, WizeHive serves as a partner continually innovating and collaborating for the good of your objectives.

About Tech Impact's Idealware

Tech Impact is a nonprofit on a mission to empower communities and nonprofits to use technology to better serve the world. The organization is a leading provider of technology education and solutions for nonprofits and operates award-winning IT and customer experience training programs designed to help young adults launch their careers. Tech Impact offers a comprehensive suite of technology services that includes managed IT support, data and strategy services, telecommunications, and cloud computing integration and support.

In 2018, it expanded its education and outreach capabilities by merging with Idealware, an authoritative source for independent, thoroughly researched technology resources for the social sector. Tech Impact's ITWorks and CXWorks training programs have graduated hundreds of young adults with the knowledge, skills and confidence they need to start their careers in the technology and customer experience industries. The organization also operates Punchcode, a coding bootcamp based in Las Vegas, NV. Learn more at www.techimpact.org.

About the Technology Learning Center

Tech Impact's Technology Learning Center, or TLC, is an expansive collection of technology education materials—just like this workbook—created exclusively for nonprofits. It includes hundreds of free publications and downloads, a free organizational tech assessment, and the most comprehensive curriculum of webinars, courses, and on-demand learning about nonprofit technology currently available. The vast majority of resources are free, and the remainder are priced within reach of even the smallest nonprofits. Give your tech knowledge a little TLC at https://techimpact.org/technology-learning-center.


GIVE YOURSELF
A LITTLE TLC
Introducing the Technology Learning Center
The most powerful and trustworthy technology education tool for the social sector.
www.TechnologyLearningCenter.org
TECHIMPACT®


9.15.20
TECHFORWARD
A VIRTUAL CONFERENCE EVENT
Join nonprofit leaders discussing mission-focused technology through case studies, workshops, expert speakers and more.
Hosted by:
TECHIMPACT®
LEARN.
MORE.