March 2018

Information Security

A TOOLKIT TO PROTECT LEGAL AID ORGANIZATIONS

LSC America's Partner for Equal Justice
LEGAL SERVICES CORPORATION

in partnership with idealware

MAP MICHIGAN ADVOCACY PROGRAM

Table of Contents

AUTHORS
DAN RIVAS
ANGELA TRIPP

Introduction

Good intentions or a commitment to your organization's mission won't protect your data.

Ancient cities were built behind walls. A few still survive today—Mdina in Malta and Xi'an in China are two of the most spectacularly well-preserved walled cities—but many more had perimeter walls that came down or were breached by invaders. The ancient walled city of Jerusalem has been conquered many times. Palermo in Sicily once had a wall. Today it is known as the most conquered city in the world.

Many people use the language of walled cities when talking about IT security. A "data breach" implies that there was a gap in a wall. Consultants and software vendors both talk about keeping "invaders" out. Until a few years ago, IT professionals talked a lot about "perimeter security."

Today, information is incredibly mobile. Staff members have computers in their pockets and want to be able to take their work everywhere they go. If your security strategy is focused on building bigger and better walls, you're going to overlook other, more likely threats.

According to a 2016 survey by the Ponemon Institute, 55 percent of organizations reported that negligent or malicious staffers caused a data breach or security incident. The biggest threat your organization might face is sitting right down the hall or even across the room—it's your colleagues.

Good intentions or a commitment to your organization's mission won't protect your data. Your organization needs to develop infrastructure, processes, policies, and training that reduce the chances that someone will make a mistake and that help everyone become more security smart.

This toolkit will show you how to establish an organizational culture that prioritizes security and empowers all staff members to protect important data. We'll help you assess your data to ensure you're efficiently protecting what matters most, provide information about security infrastructure basics, help you write policies that clarify what is and isn't acceptable, discuss training approaches that foster security awareness, and provide a security audit questionnaire that you can use.

Assessing Your Data

Maximizing security for every bit of data isn't practical or cost effective. Most organizations prioritize the protection of particular kinds of data.

Not all data needs to be treated equally. For example, do you really need to encrypt, back up in three locations, and severely restrict a draft of a 300-word blog post?

Let's walk through a process for assessing your organization's data.[1] This process is best carried out by a committee of people who are responsible for different kinds of data. Their individual experiences and perspectives can help you better understand exactly what data your organization has and what you need to know about that data.

WHAT DATA DO YOU HAVE?

List all the different types of data that belongs to your organization. For example, you probably have contact information for donors or clients. If you have a website, each page or blog post is data. You probably also use Google Analytics or a similar tool to track website user data. List every kind of data you can think of in the worksheet on the next page or create your own spreadsheet for this exercise.

HOW MUCH DO YOU CARE ABOUT IT?

Consider each data type you've listed. Give it a score between one and 10 reflecting how important you think it is to your organization, 10 being the most important kind of data. "Importance" is somewhat subjective, but you can think of it in terms of operational importance (how critical is it to your work) and reputational importance (how important is it that the information is not exposed).

DO YOU HAVE EXTRA DATA LYING AROUND?

In the digital age, data can have a long life and can quickly be moved around. If you have data that is not critical to your work, but you cannot afford to expose, consider deleting it or moving it to deep storage to reduce your risk.

---

1 Adapted from NIST Special Publication 800-30: Guide for Conducting Risk Assessments http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf and resources created by RoundTable Technology

WHAT COULD HAPPEN TO IT?

Generally, there are three things that could happen to your data. It could be exposed (loss of confidentiality), lost (loss of integrity), or made inaccessible (loss of accessibility). This is generally known as the "CIA triad." We'll apply this in the next two sections.

More specifically, there are many ways data could be exposed, lost, or inaccessible. Some of the most common incidents include:

- Physical theft of equipment or printed files
- Natural disaster (flood, earthquake, fire, etc.)
- Improper disposal of equipment or printed files
- Inappropriate use of software (employees or others with access to software)
- Phishing (employees tricked into providing access or information)
- Insecure mobile devices
- Spying via software that tracks activity or keystrokes
- Spying via WiFi connection
- Hacking through remote access to your network
- Vandalism through malicious viruses or adware
- Ransomware (software that prevents access to machines or networks until a ransom is paid)
- Denial of Service attacks (bots flooding your website with traffic and causing it to crash)
- Social engineering (someone without authorization convincing authorized personnel to hand over information or access to systems)

HOW LIKELY IS IT TO HAPPEN?

How likely are you to lose your donation records? What are the chances that you won't be able to access your social media accounts? Using the worksheet on Page 6, consider how likely each of the three data incidents is to occur to each data type. Label each one "likely," "moderately likely," or "unlikely."

Not sure how likely an event is? When it comes to hacking and malicious action, look to the most recent industry statistics. For example, according to Wombat, 85 percent of organizations experienced phishing attacks, so the chances are very high that someone at your organization will receive a phishing email and be tempted to click on it. Contrast that with denial of service attacks, which are fairly rare, but are always very intentionally targeted. If your organization doesn't have many techie enemies, you probably don't have to worry about denial of service attacks. But if you're angering hackers or foreign governments with a history of cyberwarfare, then your odds of a denial of service attack might be a lot higher.

HOW BAD WOULD IT BE IF IT HAPPENED?

Some data would be very bad to expose. For example, if your donor's credit card numbers and home addresses were exposed, your organization you might lose a lot of donors and no longer have enough revenue to continue operations. At the other end of the spectrum, you might lose blog posts from 2010 and shrug your shoulders because they were outdated anyway.

Consider each data type and data incident and rate them on a scale of one to 10, with 10 being the worst-case scenario.

HOW WILL YOU KNOW?

How often do you use or check the data? Do you have any monitoring software or procedures in place? Describe the most likely way you would identify an incident. For example, if you maintain servers on the premises, it's smart to check the activity logs periodically to see if any suspicious activity has occurred. Similarly, many Cloud services will let you see who has logged in or accessed a file and from what location. Many services also allow you to set alerts if a new computer accesses a system or a valid login is entered from an unfamiliar location.

HOW WILL YOU RESPOND?

This is a big question that requires more discussion. We'll talk about it more when we review incident response and disaster recovery policies.

Now look at your results across all seven questions. Assessing risk is more art than science, but you should be able to see what data is most and least important to your organization. From there, you need to make a lot of judgement calls. How much do you invest to protect the data that is moderately at risk? There's no easy formula to tell you where to draw the lines or what to spend, but this process at least lets you know how to prioritize your security investments.

In the next section, we'll talk about the protections most legal aid organizations have in place and how to scale them up for larger organizations.

Worksheet: Assessing Your Data

Complete this worksheet to decide how to prioritize the security measure you'll take to protect your data.

Data Type	How Much Do You Care About It? (1-10)	What Could Happen To It?	How Likely Is It To Happen? (likely, moderately likely, unlikely)	How Bad Would It Be If Happened? (1-10)	How Will You Know What Happened?	How Will You Respond?

Security Infrastructure

There are a number of steps any organization can take to reduce the chances that their organization will lose, expose, or be unable to access data. All of these suggestions are affordable for small organizations without full-time IT staff and scalable for large organizations.

DOCUMENT MANAGEMENT

Documents are a critical part of every attorney's work. Fortunately, it's easier than ever to access documents at the office or on the road. On the flip side, easy access brings risks. Are documents being kept from the wrong people? Are your clients protected even when you're on the road? Are your digital documents organized so that they're easy to search, but don't reveal sensitive data?

Your case management system probably has document management features that allow you to organize the documents related to a particular client. Most legal aid organizations also have a file sharing system that allows staff members to work on word processing documents, spreadsheets, and more, and save those documents on organization-wide servers. Cloud solutions that are popular with legal aid organizations include GSuite and Microsoft SharePoint with Office 365.

Whether you maintain your file sharing system on the premises using your own file servers or outsource your file sharing system to the Cloud, it's important to think through a few questions.

Who will have access to which files?

Most server software or Cloud-based services allow you to set permissions for individual users. Think carefully about what staff members need access to which files. Why? Even if case files are in your case management system, you may have sensitive data in spreadsheets or other files. The more accessible each file is, the greater the chance it can be lost or exposed. You also run the risk of inviting conflicts that contaminate your case.

Convenience and collaboration are useful and necessary, but be careful and very intentional about how convenient it is to retrieve files and what level of collaboration is appropriate.

What files need extra protection?

Case files, personally identifiable data, and other sensitive data need extra protection. User permissions, encryption, and more may be available through your Cloud service provider or can be installed separately.

Will staffers access files from home?

If you need to provide remote access, a virtual private network (VPN) can allow staffers to access and save files securely through an encrypted connection. Tthere are dozens of VPN providers available, but research them carefully. Not all providers are as secure as advertised. Also, you should know that setting up a VPN is a technical task that is best done by an experienced IT professional.

What are the standards for describing documents?

Many legal aid offices need their digital documents to be searchable. For example, if you need to create a brief, but want to save time, you can pull one up that has already been created and edit it according to your own needs. Clear standards that describe the topics or type of document–without revealing specific case information–will make documents easier to find and help everyone be more productive.

Do you need to be in the Cloud?

Do you manage multiple offices or have attorneys who travel a lot? A Cloud-based system usually provides both web access and allows you to "map" the file share to your computer's drive so that the files appear as if they were part of your computer's file storage. All reputable services should use Hypertext Transfer Protocol Secure (HTTPS) to transmit your files and file information. HTTPS means that all communications between your browser and the website are encrypted.

UPDATES AND PATCHES

A decade ago or more, updates from Microsoft and other software vendors were risky. You could run the update and find that an integration no longer works or your server is incredibly slow. IT professionals often waited weeks or months to update software until they were sure that the bugs had been fixed.

Today, you can't take that risk. Ransomware commonly exploits known vulnerabilities that are easily fixed with a patch or an update. Delaying an update can ultimately cost thousands of dollars and cripple your organization. Weigh that against a couple hours of troubleshooting or a webcam not working and the choice should be clear.

Update and patch your software and devices as soon as you receive a notification. If you rely on individuals to run updates on their own devices, build in a way to check on them to make sure they have the latest version. Organizations with a strong IT presence can set servers and devices to run updates

automatically. Just make sure to choose a time of day when it will be least disruptive to staff members and IT staff will be available to troubleshoot as needed.

FIREWALLS

A Firewall is not exactly a wall—it's more of a gatekeeper that decides what information can pass based on predefined rules. You can install a firewall at any point where networks or devices meet—including routers, switches, and computers—to guard against intrusions from hackers and malicious software.

Firewalls have become increasingly sophisticated in recent years. Network-based Firewall appliances protect your entire organizational network by screening out malicious activity or information before it reaches your computers. While a Firewall appliance may be as simple as a home or office router from TP-Link, Linksys, or Netgear, these will only detect the simplest attacks. Enterprise products allow for more active management, are better at identifying and filtering data, and often come with support. Cisco's Meraki and FirePOWER, Dell's SonicWALL, and net generation firewalls (NGFWs) from Palo Alto, Fortinet, and Check Point all earn high praise from experts.

VIRUS PROTECTION

Antivirus software serves two roles: to stop malicious software—known as viruses or "malware"—from reaching your computers; and to "disinfect" computers of malware that has already been installed. While antivirus software is typically installed on individual laptops and computers, there are also solutions designed to protect email servers and file servers.

There are many basic, low-cost virus protection packages that will provide a layer of security to help you catch the most common malware. These include AVG, Panda, and Avast. But as with firewalls, more sophisticated software has emerged. At least two products—Code Black and SentinelOne—have been certified to replace traditional antivirus software. These systems use "whitelisting" controls that allow you to choose to only allow traffic that's proven to be safe, endpoint security to validate users, and pattern recognition to detect unusual activity. Pricing varies by the size of your organization, but a midsized nonprofit can expect to pay hundreds of dollars per year—a cost justified by the critical protection these products provide.

BACKUPS

Backing up files is critical in case of damage, loss, or theft, but file backup is a process more than it is a single piece of software. A good backup process contains three elements: ease of use or automation, offsite or Cloud storage to prevent your backups from being destroyed along with your primary data, and the ability to retrieve those files and restore your data.

For individual users, newer versions of both Windows and Mac OS include file backup and recovery tools that can be used with either external hard drives or with Cloud-based storage. There are also a number of third-party Cloud-based backup and recovery options available for individuals. Unlike simple storage options, these systems help automate the process so that it is not dependent upon

HOW SAFE IS THE CLOUD?

One of the largest misconceptions surrounding Cloud-based software is that since the data isn't stored on a computer in your office, it's more vulnerable to threats. In fact, chances are that big software companies have more resources to back up your data, keep your software up to date, and protect you against threats than you do. Organizations that lack highly-trained IT staff are likely much safer in the Cloud than using minimally maintained on-premise servers.

users remembering to make copies of files. They also include tools to create disk images of an entire computer—including applications, data, and personal settings—to make it easier to get back up and running after a loss.

Some tools, such as iDrive, offer free backup services for small amounts of data, but paid tools offer more capacity and more robust, sophisticated features. Versioning—the ability to roll back to previous versions of specific files—is a mid-level service included in some paid solutions, including Carbonite. MozyPro (now part of Dell), Crashplan, and JungleDisk offer software and storage to make both local and Cloud-based backup possible. A number of organizations are also moving to Datto, a backup-and-recovery service.

To back up an entire office of computers or a network, a common solution is what's called a Network Attached Storage, or NAS, device—essentially multiple hard drives in a single cabinet or rack that stores redundant copies of data. If your staff works in the field using laptops or mobile devices, they can also back up to a NAS system remotely over the internet.

A local backup is usually faster than Cloud-based storage when recovering an entire file system, but is not sufficient to protect against fire or other damage to the office. When selecting backup and recovery software for an office or network, consider layering in Cloud-based storage to securely store files offsite.

One of the most cost-effective ways to store backups is in what is typically called "deep freeze" storage. The most popular option is Amazon's Glacier. It allows you to store backups for $0.004 per gigabyte per month. The catch is that if you want to retrieve your backup quickly, you'll need to pay $0.03 per gigabyte, plus other costs. If time is not a factor, then you can pay $0.0025 per GB to retrieve your data in five to 12 hours. Many organizations view deep freeze storage as a third layer of redundancy and not as their primary backup.

Note: Even if your Cloud database or other Cloud-based file storage vendors keep backups of your data, you should still keep your own backups. While most Cloud vendors are very reliable, they can lose data. If you can't afford to lose a particular data set, redundant backups are critical.

Once you have a technology solution in place, you still need to think about the processes for backing up data.

- How frequently will you back up data?
- How many backups will you keep and in what intervals? For example, an organization might keep a backup for every day of the current week, one backup from the previous week, one from the previous month, one from the previous quarter, and one from each of the previous years. The amount of data you have, the cost of storage, and the importance of your data will help drive these decisions.
- What backups will you store in "deep freeze" versus more accessible locations?
- Do you know how to restore a backup? Do periodic "dry runs" to make sure your backup restores properly and make sure to document the procedures. It's advisable to include a copy of your backup restoration procedures in your incident response guide or policy handbook.

SECURE CONNECTIONS

If you're using a wireless router, you need more than a firewall to secure your connection. The first is to set a password. Many routers come with a default login and password—often "admin" and "password." Create a unique password that is made up of many characters and includes numbers and symbols. It's a good idea not to broadcast your Service Set Identifier (SSID), which is the name of your WiFi network, as it can act as a kind of password into your network—you can set this option in the router's administrative setup screen.

It's also a good idea to encrypt your wireless access point so that data cannot be easily intercepted as it is transmitted across the network or to other networks. WiFi Protected Access 2 (WPA-2) is a common solution.

FILE ENCRYPTION

For staff who use laptops, the risk of theft or loss can lead directly to data being compromised. Encrypting hard drives is a relatively easy, straightforward way to protect laptops. It won't protect against network intrusions or hackers, but it will protect against anyone who has physical access to your computer. It works by "scrambling" data so that it can only be viewed and read if you have an encryption key to unscramble it. Most Operating Systems, including Windows 10, Mac OS X, and Linux, have some form of encryption built in, though it's not enabled by default. There are a number of third-party encryption tools available, as well.

WEBSITES

As discussed above, an HTTPS certificate that encrypts data transmitted between your website and the user's browser is now a must-have feature. Also be aware that, if your website uses forms or Ja-

vaScript, it might be vulnerable to attacks that inject code that allow the user to modify your database or steal information. The article "Nine security tips to protect your website from hackers" has good information for DIY website builders or beginning coders.

MULTI-FACTOR AUTHENTICATION

Even the best passwords can get lost or captured surreptitiously. Multi-factor authentication allows you to use other kinds of unique information to make it harder for someone to access software or files. Common factors used for authentication include security questions, PINs, security tokens already in your device, and text messaging. Many phones now also can use fingerprint as an authentication factor. Many software and Cloud services offer multi-factor authentication. Services can also be purchased separately.

PHYSICAL LOCATION

Keeping your data safe starts with a secure office. What was true 100 years ago is still true today: Most security breaches are caused by natural disasters or improper activity by employees. Here are a few ways you can make sure the physical office space is configured to keep your data secure.

Lock the Door

It seems both trivial and obvious, but there's a lot of peace of mind to be found in just locking the door, especially if you share a building with multiple tenants. Many organizations have installed door handles that require you to type in a code before they will unlock. Even if you choose to leave the door to your office unlocked, you should make sure someone is by the door and takes on the responsibility of greeting people who enter. This is a good deterrent and can stop people who are hoping to stumble into an opportunity.

Within your office, you still want to consider locking up sensitive information. Your HR staff members, for example, should be the only ones who can access employee records. Your HR Manager should probably have a lock on his or her door and should lock up at the end of the day. If this is not possible, make sure any sensitive paper records are kept in a locked cabinet.

If you have a server on the premises, keep it locked and post a sign that says something like: "Server Room must be locked at all times. Contact the IT Director if you have questions or concerns."

Secure Equipment

If an intruder does enter your office, make it as difficult as possible to carry away valuable equipment. Use safety devices to lock laptops, computers, servers, printers, or any other device that contains organization data and that could easily be carried out of the office.

Log Off Machines

You wouldn't go to lunch and leave a file folder with sensitive papers flipped open on your desk, would you? That's essentially what you're doing when you walk away from your desk while your computer is open and accessible.

Every computer should be logged off at the end of the day. Consider installing automatic screen locks that kick in after a specific amount of time and require login information to unlock on every machine. This is especially important for workspaces in public areas.

Disaster Prevention

Flood, fire, earthquake—disaster can strike any office at any time. Many disasters can't be prevented, but the consequences can be minimized by considering what might happen.

FLOOD

Are your servers or computers on the floor? If so, even an inch or two of water can ruin them. Put them on secure stands or tabletops that are at least two inches off the ground. Similarly, power strips should be removed from the floor to prevent the risk of electricity flowing through the water and putting people at risk.

Floods are often slow-moving disasters, which means they can be planned for. If you know a hurricane is coming or the local river is close to spilling its banks, you can back up your data and shutdown all devices and servers before the waters rise or the power gets knocked out.

FIRE

Computers and servers generate a lot of heat. If a small server room isn't kept cool, a malfunctioning computer could lead to a big fire. Fans and ventilation are a minimum. If it's possible to control the temperature in your server room, it could provide a lot of peace of mind. Also, make sure you have a fire detector installed in your server room and fire extinguishers throughout your office.

If you have on premise data backup, consider keeping it in a fire safe or a fire cabinet. You might also consider installing a clean agent fire suppression system in your server room instead of water sprinklers. A good suppression system will prevent disastrous water damage to your equipment.

EARTHQUAKE

What will happen to your office if the ground begins to shake? Are there large or heavy objects that might fall on equipment (or people)? If so, consider rearranging your office or redecorating. Also, make sure your equipment is secured to a table or rack and not sitting on a high, narrow shelf.

QUIZ

Take a break from reading and test your knowledge of what you've learned so far.

1. What does HTTPS stand for?
   a. Human Transfer Technology Practice Security
   b. Hypertext Transfer Protocol Secure
   c. Hyper Technology Training and Problem Solving

2. Your server room should remain unlocked at all times.
   True
   False

3. According to a 2016 survey by the Ponemon Institute, what percentage of organizations reported that negligent or malicious staffers caused a data breach or security incident?
   a. 55 percent
   b. 90 percent
   c. 22 percent
   d. 30 percent

4. At a minimum, how many inches off the ground should you store your computer?
   a. 12
   b. 40
   c. 6
   d. 2

5. What's a firewall?
   a. A device to store your laptop in.
   b. A gatekeeper that decides what information can pass based on predefined rules.
   c. A highly-rated software system used to automate updates and patches.
   d. A website attack that overloads your web servers.

Answers: 1. (b.), 2. (False), 3. (a.), 4. (d.), 5. (b.)

Policies

Good policies establish expectations and provide guidance for how staff members can protect themselves and the organization's data.

The following worksheets can serve as a blueprint for the technology section of your organization's policy manual.

You might also consider a social media policy and an electronic file destruction policy. Examples of these and more can be found in the appendix to this toolkit.

Note: It's best practice to review your security policies annually and make revisions as needed.

Worksheet: Acceptable Use Policy

Your acceptable use policy covers how your staff members and other technology users at your office should use organization computers, software, and other equipment.

Purpose

Start off your acceptable use policy with a general statement on the problem that the policy is intended to address or prevent. This is also an opportunity to tie information security to your organization's larger mission.

Scope

Who does this policy affect? List all the roles or departments who are subject to this policy.

Equipment

What does this policy cover? List all equipment that the policy applies to.

Consequences

Clarify the range of punishments that may be applied to someone who willfully violates a policy.

Data Use and Ownership

This section is intended to clarify what data belongs to the organization and how staff members or others should use the data.

1. 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?

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

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

4. 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?

General Security Guidelines

1. Will every computer or device be set to hibernate or logout if not in use? How much time should pass before as user has to log in again?

2. Will you want to set guidelines for what attachments can or cannot be opened? Those guidelines can be by file type, recipient, etc.

3. 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?

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

Unacceptable Use

Below are common prohibitions included in an acceptable use policy.

- ☐ 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 not intended for you.
- ☐ 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

Passwords are one of the biggest vulnerabilities for an organization. Long, complex passwords are difficult to remember and inconvenient. As a result, many people choose short passwords that are easy to remember such as "password" or the organization's address. Your policy can establish minimum standards so that everyone knows what a strong password looks like and that they're expected to use only strong passwords.

1. What are your 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?

2. Are staffers required to change passwords periodically? How often? Can they repeat passwords? (Note: There is some debate about whether passwords need to be changed regularly. Many now believe that a longer window is permissible or that passwords should only be changed after a data breach or a vulnerability has been exposed.)

3. Describe a weak password. 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 most organizations try to avoid.

4. Does your organization use password management software? If not, are users allowed to use personal versions of password management software?

5. 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?

6. Will you periodically audit passwords by attempting to crack them?

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

8. Will all devices be required to have a password that locks the screen?

Email Use and Guidelines

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. These prompts can help you define those reasonable uses.

1. 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?

2. What level of confidential detail can be included in a forwarded email? What guidelines do you wish to share?

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

4. Will you monitor staff email? How frequently and at what level?

Exceptions

Are there any exceptions to this policy you can think of? For example, you might not monitor the email of certain departments due to the sensitive nature of the communications. Explain any exceptions here.

Worksheet: Personal Device Policy

The expectation to use personal devices for work continues to grow. Will you allow staff members to user personal computers or phones to access case files or contact clients? This section will help you sort out the questions you'll need to ask to protect your clients and your organization.

Purpose

Explain the thinking or philosophy that informed your policies on using personal devices for work. This may also be an opportunity to discuss the potential risks.

Scope

Who does this policy affect? List all the roles or departments who are subject to this policy. If any roles or departments are prohibited from using personal devices, state that here as well.

Equipment

What does this policy cover? List all personal equipment that the policy applies to.

Guidelines

1. Are there limits you wish to set for which devices can be used in the office during work hours?

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

3. Describe sites or apps that staff members are prohibited from using on their personal devices during work hours.

4. What kind of IT support will you provide for personal devices? Will you place limits on the amount of support a staffer can receive?

5. 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. Will you use mobile device management software?

6. 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.

7. Will you reimburse 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?

Minimum Standards for Personal Devices

If staff members will be using personal devices for work, you will want to be confident that they're using secure, reliable devices. Here are a few recommended minimum standards.

- ☐ 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").

Minimum Network Standards

If staff members will be doing work outside of the office, you need to be confident that they're transmitting data on secure networks. Here are a few recommended minimum standards.

- ☐ 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, at a minimum the same standards in place at the office.
- ☐ 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.).

Exceptions

Are there any exceptions to this policy you can think of? For example, are there times when a VPN is not required? Explain any exceptions here.

Worksheet: Incident Response Policy

Storms, hacks, accidents—there are a lot of ways your technology and data can experience a disaster. Your incident response policy should outline what happens when an incident occurs and how to get your organization back up to full operation.

Who's Involved?

After an incident, you want to assemble your Disaster Committee as quickly as possible. Here are the teammates you might want to be involved. Make sure to list current names and contact information.

Roles at Your Organization	Names and Contact Information
Executive Director	
Senior IT staff person or external IT contractor	
HR	
Communications Director	
Chair of Board of Directors	
Staff members involved or affected	
Finance	

What's Are Everyone's Roles?

Below are a few of the main roles and responsibilities after an incident. You may wish to add additional roles or responsibilities. Note that the highest position at your organization (CEO, Executive Director, etc.) is the chair of this committee and is responsible for overseeing all of these activities.

Response	Who is in Charge	How Soon Does This Happen?
Diagnose a breach		
Remove access		
Repair or replace any damaged technology		
Review liabilities		
Communicate with staff		
Communicate with public		

Is Everyone Safe?

If this is a physical disaster (versus a hack or catastrophic data loss), make sure anyone who might be in your office is safe and accounted for. Typically, the Executive Director contacts everyone in the disaster committee and assigns further contacts with the rest of the staff. It's a good idea to keep a paper directory with contact information for every staff member and declare a meeting spot if a physical disaster occurs at or near your office.

What if Essential Committee Members Are Not Available?

It's possible, especially in a natural disaster, that your Executive Director or top IT person will be unavailable. Who takes their place? What credentials or authority will a replacement need to fulfill their role in an incident? Note that the absence of one of these senior staff members may itself constitute an incident, triggering a committee meeting and other additional steps.

Call a Disaster Committee Meeting

How will you communicate in the event of a disaster? Consider multiple possible communication methods and list them all here. The Executive Director will determine which communication methods is appropriate for the situation.

Declare the Incident

When the Executive Director communicates with committee members, she will explain what happened and initiate the disaster response plan.

What Are Your Essential Functions?

If there's a disaster, what do you need to get up and running first? List all of your organization's functions and rank them so that in an incident you'll be able to quickly prioritize what to repair or replace.

Inventory

Write down an inventory of all equipment, systems, and hardware that you can use as a checklist when determining what needs to be fixed or replaced.

Processes

Are there workarounds or alternative processes that you can employ if the usual processes aren't possible? Document them here.

Contain the Infection

If the incident is malware, ransomware, or an intrusion of some kind, you'll need to contain the infection. Document the steps including: disconnecting compromised systems, collecting important data, gathering external intelligence, safeguarding all systems and media, and collecting logs. If you're dealing with ransomware and have accessible backups, you'll likely be able to wipe your servers or computers clean and reload all of your data.

Where Is Your Plan Stored?

Your plan needs to be accessible no matter what kind of incident you encounter. It's wise to keep it both in the Cloud and on premises. You should also have at least one paper copy in a secure place, possibly a fire safe or other secure storage location.

Security Awareness

Your data is only as safe as the weakest link at your organization. For most legal aid organizations that weak link isn't technology. It's people. Here are some ideas for improving security awareness at your organization.

PROVIDE TRAINING

Every organization should conduct an annual security awareness training. Your staff members want to do the right thing. Usually they don't realize they're taking big risks by leaving their computer unattended or setting a password such as "123456." A thorough curriculum that outlines the major threats and provides guidance on what to do is a good start. If you want to incentivize busy attorneys to attend your training course, consider offering CLE credit, if possible.

MAKE SECURITY PART OF REGULAR MEETINGS

Do you have regular staff meetings? You can use these to periodically discuss security issues. For example, a recent attack in the news can be a jumping off point to remind people of best practices or your organization's policies.

IT STAFF NEED THEIR OWN TRAINING

Security threats evolve quickly. You can invest in your organization's security and the careers of your IT staff by enrolling them in training and certification courses. The SANS Institute is widely considered the most authoritative source for information security training. The InfoSec Institute, Cybrary, and MIS Training Institute also offer respected training courses.

SECURITY EDUCATION SOFTWARE

Big training sessions are useful, but individualized training is more effective. Security Education Software allows you to tailor online security training for your staff and test their knowledge in multiple ways. What sets these systems apart from other eLearning tools is their feature set that allows you to send simulated threats to staff members and evaluate how they react. For example, you can send a fake phishing email to a staff member and through the administrator interface see that they clicked on the link in the email. On the user end, after clicking the scam

link, the staffer will be taken to a page that notifies them of their mistake and provides videos and other information to help him or her spot the scam and stop from clicking next time.

Wombat Security, KnowBe4, PhishMe, and PhishLine are the most popular systems. Pricing is typically per user (unique individuals receiving training). Small organizations might pay between $20-25 per user. Large organizations will typically pay less than $10 per user.

INCLUDE SECURITY IN PERFORMANCE REVIEWS

If you use security education software you'll get information about the user's security awareness and whether they're taking the threats seriously. That score can be incorporated into your annual performance review and could be used among the criteria for determining professional advancement or salary increases. If you don't use security education software, you can still provide quizzes or test users in other ways.

To help you promote security awareness at your organization, we've included a checklist in the appendix. Encourage your staff members to print it out and keep it handy. You might even use it to quiz staff members or review it at a staff meeting.

Conducting a Security Audit

How secure is your organization's data and how do you know?

For a thorough and impartial technical audit, you should contact a respected IT consultant. However, for a basic audit here are some questions and scoring to give you a sense of whether you're doing a good job of keeping your organization secure.

Complete this self-audit and give yourself points for every "yes" answer. Points are in parentheses.

_____ Have you conducted a thorough assessment of your data, including:

- Listing all of your data types? (1)
- Rating the importance of your data? (1)
- Documenting the most likely risk to your data? (1)

_____ Do you have document management security measures in place including:

- Controls on which users can access which electronic files? (1-5)
- Documented prioritization for which files need extra protection? (1)
- Passwords and other forms of authentication to access files? (5)
- Encryption available for some files? (1)
- VPN for remote access? (1)

_____ Are updates and patches installed promptly? (5)

_____ Are updates and patches downloaded automatically? (10)

_____ Do staff members have to download updates and patches themselves? (-3)

_____ Do you have firewalls installed in all routers and switches? (10)

_____ Do you have firewalls in all servers, computers, and other computing devices? (10)

_____ Are you able to monitor and adjust your firewall as needed, thereby providing protection beyond the factory settings? (2)

_____ Does every computing device have virus protection installed? (5)

_____ Does every device or piece of software that contains important data have a password, including:

- Computers? (10)
- Mobile devices? (10)
- Wireless routers? (10)
- Cloud software? (10)
- On-site software? (10)
- File share? (10)

_____ Is your wireless router protected with encryption? (10)

_____ Do you have backups both on the premises and in the Cloud? (15)

_____ Do you have "deep freeze" backups? (2)

_____ How confident are you in your ability to restore a backup if needed? (Score 1-10)

_____ Do you practice installing backups at least:

- Annually? (1)
- Quarterly? (3)
- Monthly? (5)
- Never? (-5)

_____ Do you monitor your data movement, checking logs for suspicious activity:

- Monthly? (1)
- Weekly? (2)
- Daily? (3)
- In real time? (5)

_____ Do all of your websites have HTTPS certificates? (1)

_____ Do you use multi-factor authentication for any devices or software? (1)

_____ Do you keep your office doors locked? (1)

_____ Do you keep your server room locked? If you don't keep a server on the premises, do you lock up sensitive paper documents so that an unauthorized individual can't access them? (10)

_____ Do computers log off users if they haven't used them within a certain amount of time? (5)

_____ Are all electronic devices on the ground floor at least two inches off the ground in the event of a flood? (5)

_____ Do you have fire boxes with sensitive equipment or documents inside? (1)

_____ Do you have cooling equipment in your server room? (5)

_____ Does your server room have a fire suppression system? (1)

_____ Do you have a written acceptable use policy in place that has been shared throughout your organization? (10)

_____ Do you have minimum standards for passwords that require:

- At least 14 characters? (3)
- Both capital and low-case letters? (3)
- Both numbers and letters? (3)
- A special symbol? (1)

_____ Does your organization require the use of a password manager? (3)

_____ Do multiple users share login information for some accounts (email, database, or other services)? (-1)

_____ Do you have a personal device policy in place (or prohibit the use of personal devices for work)? (5)

_____ Do you have an incident response plan:

- That assigns roles? (1)
- Provides clear instructions on how to assess and act on a data incident or disaster? (5)
- Includes a contact directory? (1)
- Includes a meeting place? (1)
- Accounts for contingencies such as IT staff or a director leaving the organization or becoming unavailable, including access to accounts and other sensitive information? (10)
- That's stored in multiple locations, on paper and digitally? (5)

_____ Do you have a social media policy? (3)

_____ Do you have an electronic file destruction policy? (3)

_____ Do you provide information security training to all staff members? (10)

_____ Do you invest in security education software? (3)

_____ Do you regularly discuss information security issues with teammates and staff? (3)

How did you do? Your total score is _____ out of 268 possible points.

Scoring Your Score

240+: You're doing nearly everything you can to keep your organization's information safe. Nice job!

200 – 239: You're doing a fine job, but there are a few areas you can focus on for improvement.

150 – 199: You're doing a lot right, but your organization is potentially vulnerable to a data incident. Consider making a checklist of issues to take on and working your way through them.

Less than 149: You might be taking very big risks. Immediate action is needed to reduce your vulnerability.

Conclusion

Perfect security may not be possible. But practical security is well within your reach.

You can't prevent all vulnerabilities or build a wall that will protect your organization from every threat. However, with knowledge, planning, strong policies, and training that raises expectations across your organization, you can prevent the vast majority of incidents. What's important is that you cannot become complacent. The threats and vulnerabilities keep shifting. Devoting a little time and attention to monitoring those developments and adjusting your security to meet new challenges will put your legal aid organization in the best position to serve your clients and protect them from embarrassment, surveillance, and legal jeopardy.

Did you find this TIG Toolkit useful? Please take a short survey to let us know what you thought of it to help guide future content:

https://www.surveymonkey.com/r/TIGtoolkits

Appendix A: Employee Security Checklist

Data security is everyone's job. Here are a few ways you can protect yourself and your organization from spying, vandalism, theft, and accidental data loss.

Your Workspace

_____ Don't leave sensitive documents out on your desk. Lock them away in a safe or a cabinet.

_____ When you dispose of documents that contain organization data, shred them.

_____ When you leave your workspace, take laptops and mobile devices with you or secure them.

_____ Log out of or lock your computer screen whenever you're going to be away for more than a few minutes.

Passwords

_____ Set a strong password that is at least eight characters long and combines letters and numbers. Including uppercase characters and symbols will also strengthen your password.

_____ Do not write down your password and keep it near your workstation.

_____ Disable browser features that auto-fill your passwords.

_____ Do not share login information or passwords with others.

Email

_____ Do not click on email links unless you're certain the email has come from a trusted source and that the content of the email is directly applicable to your work together.

_____ If your email program includes it, use the "preview" function to review attachments and determine whether they're safe.

_____ Sign out of your email client when you are not using it.

On the Web

_____ If your organization does not automatically install antivirus software and software patches, install them yourself and check for updates daily.

_____ Do not click on links unless you're certain they come from a trusted source. Look for slight changes to URLs that are intended to pass the site off as a legitimate source.

_____ Vigilantly watch out for spam on social media and messenger apps. Do not click ads that offer too-good-to-be-true deals.

_____ If a website asks you to transmit any data, make sure the URL says it is using "HTTPS," a more secure protocol than "HTTP."

_____ Avoid downloading new or untested browser plug-ins—they often contain vulnerabilities that could compromise your device.

Mobile Devices

_____ Download updates to your operating system and apps.

_____ Do not assume all apps are safe. Some apps are fake and are intended to compromise your device. Read reviews, seek out "editor's choice" picks, and look up the developer's profile to gauge your risk.

_____ Double check the source of any shared images, videos, or links.

_____ Download a device location app to help you find a lost or stolen device.

At Home/On the Road

_____ Make sure your home internet connect is password protected and has a built-in firewall.

_____ Install updates/patches on all devices you might use for work.

_____ Avoid sending sensitive data via public WiFi.

_____ Do not set your device to automatically roam for a WiFi signal—it may pick up an unsecure signal and compromise your device.

_____ If you use a remote desktop application, do not save login credentials and make sure it is updated every time you login.

Appendix B: Policy Templates and Samples

Use these policies as examples or templates to help you craft your own.

ACCEPTABLE USE POLICY

Brown University
https://it.brown.edu/computing-policies/acceptable-use-policy

SANS Institute
https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy

Maryland Legal Aid
https://lsntap.org/sites/all/files/MD-Policy%20-%20Acceptable%20Use.pdf

PASSWORD POLICIES

SANS Institute
https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

University of Michigan
https://www.michigan.gov/documents/msp/Password_policy_325048_7.pdf

Society for Human Resource Management
https://www.shrm.org/resourcesandtools/tools-and-samples/policies/pages/passwordpolicy.aspx

BRING YOUR OWN DEVICE POLICY

Legal Services of Central New York
https://lsntap.org/sites/all/files/policy_LSCNY%20IT.pdf

Community Legal Aid Services
https://lsntap.org/sites/all/files/policy_mobiledevice.pdf

IT Manager Daily
http://www.itmanagerdaily.com/byod-policy-template/

SOCIAL MEDIA POLICY

City of Seattle
http://www.seattle.gov/tech/about/policies-and-directors-rules/social-media-use-policy

Idealware
http://www.idealware.org/wp-content/uploads/2017/03/Idealware_sm_policy_template.doc

Kivi's Nonprofit Communications Blog
http://www.nonprofitmarketingguide.com/blog/2010/05/03/rough-draft-of-a-nonprofit-social-media-policy/

INCIDENT RESPONSE POLICY

Kansas State
https://www.k-state.edu/policies/ppm/3400/3434.html

State of Vermont
http://dii.vermont.gov/sites/dii/files/pdfs/Incident-Response-Policy.pdf

ELECTRONIC FILE DESTRUCTION POLICY

Lawyers Mutual
http://files.www.lawyersmutualnc.com/risk-management-resources/risk-management-handouts/file-management-retention-and-destruction/File_Management_Retention_and_Destruction.pdf

Washington State Bar Association
http://www.wsba.org/~/media/Files/Resources_Services/Ethics/Guide%20to%20Best%20Practices%20for%20Records%20Management%20310.ashx

Appendix C: Additional Resources

Here is some additional reading material to provide more information about security for your organization.

What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk, Idealware's guide to nonprofit security basics.

http://www.idealware.org/reports/nonprofits-need-know-security-practical-guide-managing-risk/

Small Business Information Security: The Fundamentals, A thorough, straightforward guide created by the National Institute for Standards and Technology.

http://csrc.nist.gov/publications/nistir/ir7621/ nistir-7621.pdf

The SANS Institute, A computer security organization that provides training and certification for security professionals. Its website contains resources for experts and novices alike.

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

An Introduction to Threat Modeling, An overview of a security methodology that attempts to map out the threats, your assets, and the points where you can protect yourself.

http://web.mit.edu/tweilu/www/eff-ssd-mockup/ threatmodel.html

Mind the Gap, A presentation from Roger Hagedorn, Information Security Analyst for the City of Minneapolis, on the current security climate and how nonprofits can close the gaps in their protection.

http://www.slideshare.net/techfrogger

A Nonprofit's Guide to Antivirus Software and Malicious Program Defense, The basics for setting up your antivirus software.

http://forums.techsoup.org/cs/community/b/tsblog/ archive/2015/10/14/nonprofit-guide-antivirus- software-malicious-program-defense.aspx

Webinar: Training Staff in Basic End User IT Security, A recording and slides that outline the steps staff members can take to help their organization be safer from data loss or exposure.

http://www.communityit.com/resources/webinar-end-user-training/

Krebs on Security, A blog by Brian Krebs, an investigative journalist who has a knack for making security issues relatable and interesting.

http://krebsonsecurity.com/

Appendix D: About This Toolkit

This Toolkit is the result of a collaboration between Idealware and the Michigan Advocacy Program (MAP), funded through the Technology Intitiatives Grant Program of the Legal Services Corporation (LSC).

ABOUT IDEALWARE

Idealware, a 501(c)(3) nonprofit, provides thoroughly researched, impartial and accessible resources about technology to help nonprofits make smart technology decisions. Idealware's research publications, assessments, and training save nonprofits time and money by providing guidance that gives nonprofit leaders the knowledge and confidence they need to decide what's best for their organization.

ABOUT MAP

Through direct legal help and statewide advocacy, the Michigan Advocacy Program provides access to the justice system for those who need it the most. The Michigan Advocacy Program's direct service components are Legal Services of South Central Michigan, which provides free civil legal advice and representation to low-income and senior citizens in thirteen counties, and Farmworker Legal Services, which provides free legal assistance and referrals to migrant and seasonal farmworkers throughout the state of Michigan. The Michigan Advocacy Program also provides administrative services to a number of independent statewide programs, including the Michigan Poverty Law Program, the Michigan Immigrant Rights Center, the Michigan Legal Help Program, the Michigan Elder Justice Initiative, and the Crime Victim Legal Assistance Project.

ABOUT LSC

The Legal Services Corporation (LSC) is an independent nonprofit organization established by Congress in 1974 to provide financial support for civil legal aid to low-income Americans. LSC was founded on the shared American ideal of access to justice regardless of one's economic status. LSC is the largest single funder of civil legal services to the poor in the United States. LSC is a grant-making organization,

distributing more than 93 percent of its federal appropriation to eligible nonprofit organizations delivering civil legal aid. LSC also administers special grant programs supporting innovative practices in the areas of technology and pro bono engagement.

AUTHORS

Dan Rivas, *Idealware*

Dan is a versatile writer and editor who specializes in translating complex information into compelling stories. Prior to Idealware, he was a copywriter and editor at a marketing agency that serves large technology and financial services companies. He also has experience as a freelance writer and journalist, a census enumerator, a bookseller, and a college instructor. He is a graduate of Willamette University and the University of Michigan, where he studied anthropology and creative writing.

Angela Tripp, *Michigan Advocacy Program*

Angela is the Director of the Michigan Legal Help (MLH) Program, which is responsible for the statewide website for self-represented litigants (MichiganLegalHelp.org) and 15 affiliated Self-Help Centers around the state. In 2016, over 770,000 people visited the MLH website and over 86,000 people used its resources to complete legal forms. She has led the development and growth of MLH from its inception in 2011. She is also the Co-Director of the Michigan Poverty Law Program, the state support program in Michigan, and holds a J.D. from Northeastern University School of Law in Boston and a B.A. from the University of Cincinnati.

CONTRIBUTORS

- Melkis Alvarez-Baez, Director of Programs, *Nonprofit Coordinating Committee of New York*
- Peter Campbell, former CIO, *Legal Services Corporation*
- Roger Hagedorn, Information Security Analyst, *City of Minneapolis*
- Ken Montenegro, Information Technology Director, *Asian Americans Advancing Justice*
- Joshua Peskay, Vice President, *RoundTable Technology*
- Gail K. Reynolds, *CISSP*
- Eliot Sasaki, Research Editor and Writer, *Legal Services Corportation*
- James Snow, COO and CFO, *Prospect Park Alliance*
- Anna Steele, Senior Consultant, *Just-Tech*
- Larry Velez, Founder and CTO, *SINU*