# 2022 Legal Aid Security Toolkit

Submitted by GravityWorks on Mon, 02/17/2025 - 8:35 AM


The legal services community has not been immune to cybersecurity incidents over the past years. Indeed, a significant number of programs have been compromised and significantly impacted by cyber attacks each year. As with the broader non-profit, business, and government communities, the incident rates and stakes are growing within our community. To enhance security in the legal aid community, LSNTAP and Just-Tech, LLC have partnered to develop the 2022 Legal Aid Security Toolkit to help educate the broader community on current cybersecurity technologies and practices.

Executive directors and management may use this toolkit to better understand why security is important for their organization, to start conversations with their IT staff or vendors, to consider their own role on cybersecurity, and to help plan organizational initiatives that will improve security and the protection of confidential data. IT responsible program staff may use the toolkit to help analyze their organization's security and identify areas for improvement. IT staff may also find resources that they may share with others within their organization to help raise awareness with management and staff as well as increase buy-in for enhanced security practices and technology. The toolkit also has information for advocates and other program professionals to help them learn more about security, their role in building a more secure organization, and steps they can take to enhance their security at work and at home.

This toolkit may serve as a check-up or jumping off point for legal aid programs depending on where they are on their security journey. For some providers, the toolkit may help their efforts to be more intentional and focused on managing for better security. It is not an all-encompassing guide. Instead, it is intended to be informative about higher-priority practices and technologies within the reach of legal aid. This toolkit is not a substitute for working with cybersecurity professionals. You may find this toolkit valuable on its own or it may supplement or enhance your organization's work with security professionals.

# 1. Security Toolkit: An Overview of Topics in Cyber Security

Submitted by GravityWorks on Mon, 02/17/2025 - 8:38 AM

### How To Use This Toolkit

This toolkit serves as a jumping off point for legal aid programs to start being more intentional about their security practices. It includes information from LSNTAP's 2021 Seasons of Security webinar series as well as additional information about security compiled from experts on the subject. It is not intended to be the complete and final answer to your organization’s security practices. It is a resource to get the conversation going and to move towards a more secure environment. But it does include some immediate and concrete suggestions for every organization, no matter where they are in the process of thinking through cybersecurity issues.

### Overview

At its most basic, cyber security in legal aid is about making reasonable efforts to protect confidential data, ensure business continuity, and ensure business recovery after a cyber incident all while enabling an organization to serve its clients and mission. Cyber security needs will vary somewhat by organization based on the data they collect, who they work with, how they interact with data and the services they provide clients. But there are some issues and subjects that are pertinent across most legal aid organizations.

This section is a great place to start; it provides an overview of many of the topics we will cover, with links to other parts of the kit for more information. As the content covered by the toolkit expands, the information here will be updated to reference new material on this site.

## Staying Up to Date of Cyber Security Technology and Practices

Legal Aid providers need to actively keep up with current and emerging security technologies and practices that may need to be implemented within their programs. A few current security technologies and practices for providers to consider or implement include:

- Next generations firewalls (NGFW) provide additional services beyond basic inspection and management of web traffic that firewalls have provided for 30 years. NGFWs have functionality such as Intrusion Detection Systems and Intrusion Prevention Systems (IDP/IPS), anti-virus scanning, limiting access by geography (Geo IP Filtering/Blocking), and Virtual Private Network (VPN) functionality. For more on these technologies see Next Generation Firewall, Intrusion Detection System, Virtual Private Network, and Geo-Blocking.

- Multi-factor authentication 1(MFA) provides controlled access to organizational networks, systems, and data. MFA better protects sensitive or confidential data from simple password compromise schemes and phishing attacks.

- Endpoint Detection and Response (EDP) software monitors endpoints (laptops/desktops/servers) with automated response to a wider variety of security threats than traditional anti-virus software.

- Offline server image and file backup solutions make it harder for malicious software and actors to encrypt or destroy backup copies of your data while also enabling faster and more tailored recovery that may be needed after a cyber security incident or system failure.

- Segmentation of the office network environment into multiple logical networks can make it harder for malicious software or actors to move across your network environment or even across an individual application once they have gained initial access to your network or application.
  1Enterprise-wide MFA typically also makes use of single sign on technology to reduce the number of times users have to sign in when accessing multiple systems within an organization or across their cloud services.

## Access Control and Account Management Practices

By improving the management, configuration, and access to existing technology, legal aid providers can significantly increase security and also mitigate the risks associated with a cyber breach. This work may include:

- Locking down software, hardware, and cloud service configuration to restrict access, eliminate default account access, or eliminate services and functions that are not immediately needed or actively managed and monitored.

- Active user management by limiting place, time, and duration of access (e.g., disabling summer intern accounts promptly after summer ends); limiting permissions within and across applications; and monitoring for abnormal access and use of systems.

- Configuring systems to log access and use by staff and volunteers.

- Maintaining current infrastructure by keeping current, actively supported versions of hardware and software in place along with patching and updating software as recommended by product vendors.

## Managing Office and Home Technology

Cyber security typically includes managing office technology and home office technology. Providers work to protect the physical security of technology to reduce loss or theft of hardware and data. They work to keep known, insecure hardware and software out of the work environments. They try to keep unauthorized devices (e.g., unknown laptops, hard drives, phones, USB storage keys) from adding significant cyber security risks out of their environment. Especially in the age of Covid-19, organizations are starting to actively manage personally owned devices (POD) that are used for work purposes by establishing appropriate access restrictions for untrusted devices, minimum software requirements and creating mechanisms for monitoring or interrogating access and use of organizational systems. In managing equipment, organizations should have preventive measures in place to protect against lost or stolen equipment. Such measures may include the use of full-disk encryption that helps ensure data on devices are inaccessible to unauthorized persons, mobile device management that helps keep the devices configured in secure manner and, in some instances, can erase lost or stolen devices.

## Building a Security Culture

Perhaps one of the most crucial elements of strong cyber security is building and maintaining a cyber security culture among your staff and volunteers. End users can be a great asset to maintaining the security of your systems and data, but that does not happen without sustained effort. In fact, most cyber incidents rely on user actions to stop the advance of

attacks. Security culture work typically includes:

1. Technology training and security training
2. Testing or auditing user skills and responses to cyber attacks
3. Supervision and monitoring of technology use by staff and volunteers
4. Developing, implementing, updating, and enforcing security-related tech policies

## Understanding the Organization's Collection, Use, and Storage of Sensitive or Confidential Data

1. Legal aid organizations generally have significant and diverse needs to collect, use, and retain data. That data needs to be kept secure. Legal Aid providers need to inventory, document, analyze, and control the sensitive and confidential data it works with organization wide. This work typically includes:
2. Tracking data collected across the organization and across the range of technology systems (e.g., CMS, HR, Fundraising, Self-help tools, email, Website)
3. Documenting who has access to the data and how the data moves or is shared inside and outside the organization
4. Understanding how the data is securely stored, backed-up, and securely destroyed across all its systems
5. Examining why the data is necessary for the work as well as why and when it needs to be shared
6. Ensuring that policies and practices are developed and consistently followed to govern the life cycle of confidential and sensitive data
   Learning how technology might assist the organization in working more securely with data and helping to ensure compliance.

## Managing Security for IT Staff, Contractors and Vendors

Technology professionals pose additional risks for organizations as they typically have access to a broad array of systems and data and typically have permissions to make potentially disastrous changes to your technology environment. To help address these risks providers may work to:

1. Ensure staff and contractors are properly trained and competent to do the technology work required
2. Limit permissions and privileges to the extent practical
3. Implement logging, audit tools, and develop a reporting mechanism on the work being done
4. Invest in ongoing security training for tech staff
5. Work to eliminate single points of failure due to loss of IT personnel

## Comprehensive Documentation of the Technology Environment

Maintaining up to date documentation helps ensure that an organization can properly implement new technology, reduce the risks of technology that may not be properly managed or integrated, and more competently and quickly recover from a cyber security incident.

## Addressing Management's Role on Cyber Security

Management has a critical, ongoing role in maintaining a more secure environment. Management's technology oversight role is broad but certainly includes assessing and auditing, supervising tech staff, technology planning, developing, and implementing policies, technology budgeting, inventory management of hardware, and software and services.

## Third Party Audits and Testing

Security Audits and Penetration Testing of technologies that serve the organization and client communities are growing in importance. Major factors affecting the need for third party audits are increasing complexity (e.g.t echnology environments on-site and in the cloud, rapid changes to technology environments, development of new security attacks, and the need to

prioritize security improvements and risk mitigation strategies). Third party audits help identify new and emerging security risks and solutions to better manage the risks. They are done regularly since the organization's technology environment and its use are not static. Auditors work with providers to develop action plans to address identified deficiencies

### Insurance

Procurement and maintenance of cyber liability insurance is a critical part of cyber security. Insurance helps cover the substantial costs of managing and responding to a cyber security incident. It is a key part of an organization's risk management strategy. Insurers are increasingly driving critical security improvements within organizations to reduce insurance claims.

#### Cyber Incident Preparation and Response

Preparing to detect, log and respond to cyber security incidents of varying types and severity helps minimize the disruption and risks associated with such incidents.

1. Technologies and services that actively monitor for and/or interrupt current and emerging cyber security compromises
    1. Security Information and Event Management (SIEM) services that use software, security personnel, and/or artificial intelligence to detect and respond to events on your network, systems, and application that may relate to a cyber attack
    2. Endpoint detection and response software (EDR) may be part of a SIEM solution or stand on its own to help identify an attack, stop the attack, report the behavior, and / or recover from the attack
    3. Extensive and durable logging, typically to a cloud-based repository, of access attempts, access granted, application access, as well as the movement of users and data across the technology environment
    4. Security policies and training that cover identification and reporting of incidents that might indicate or lead to a cyber security incident (e.g., loss of equipment, clicking on unknown or dangerous links)
2. Developing an incident response policy and related protocols that includes incident handling, data capture/reporting, activation of response, communications, alternative solutions/services/resources, and cyber liability insurance.
3. Cyber incident response and recovery work
    1. Following incident response policy
    2. Interrupting the incident and stemming the damage
    3. Communicating internally and externally
    4. Getting help
    5. Forensic analysis
        1. Establishing the path for the compromise
        2. Establishing extent of access/compromise
        3. Establishing the likelihood of data exfiltration
        4. Establishing the path to securing the environment
    6. Managing the cyber incident
        1. Working with board, management, and staff
        2. Working with counsel on understanding the nature of the incident, internal/external communications, interaction with cyber criminals, and disclosure/compliance requirements
        3. Working with ransom negotiators
        4. Working with IT staff/contractors on interim and longer-term recovery
        5. Managing client services and staff needs/morale

## 2. Security Toolkit: Introduction

Submitted by GravityWorks on Mon, 02/17/2025 - 9:38 AM

#### Purpose

### The Problem

According to a study at the University of Maryland, cyberattacks are incredibly common and nearly constant: every 39 seconds, a computer connected to the internet is attacked. Legal aid programs are unfortunately no exception. Legal aid programs collect and store all sorts of client data through the process of representing people. These programs are just as susceptible to attacks on their security and their data as any other entities. In fact, some of our friends in the legal aid community have already experienced cyberattacks.

A breach can have a very high cost. The average cost of a data breach is $4.25 million (Cost of a Data Breach Report 2021). The average total cost of a data breach increased by nearly 10% from 2020 to 2021, and there's reason to believe this upward trend will continue. Because larger firms have largely started to address cybersecurity, attackers may now be targeting smaller organizations more often.

With attacks happening constantly, and with the high cost of a breach, the legal aid community must make conscious efforts to enhance security. We must all be prepared to take proactive steps to make sure our and our clients' data is safe.

## Why This Toolkit

We need to enhance security in the legal aid community. We have a duty to our clients not only to serve them, but also to protect their data. We need to take security seriously at every level, from offices just starting to protect themselves all the way to offices looking for the next innovation to add to their arsenals. We need a toolkit to help us all meet this obligation.

## Who is this Toolkit for?

This toolkit has something for everyone in a legal aid office:

- Executive Directors and management can use this toolkit to better understand why security is important for their organization and the steps needed to provide a more secure environment.
- IT staff can learn specific steps they can take to build a more secure environment and can find resources to share with others at their organization to help train staff and increase buy-in for enhanced security protection measures. Attorneys and advocates can learn more about security and why it is important, including some things they can do to enhance security as an individual.

**Background**

## Why Should Legal Aid Care About Cyber Security?

Cyberattacks are nearly constant and do not discriminate, any computer connected to the internet is vulnerable. But beyond the background threat, legal aid offices have even more reason to be concerned about cybersecurity. Legal aid providers need to keep client, employee, donor, volunteer, and other sensitive data confidential. Our clients, staff and volunteers deserve to have their identities and data protected by the legal aid providers they entrust.

Not only do attacks risk confidential data, cyber security incidents also typically disrupt law firm operations for days, or even months. In a 2020 breach, one Legal Aid experienced disruptions to computer services which prevented staff from directly accessing any files on the office servers for nearly three months. IT staff had to manually share files with people working remotely while they dealt with recovery from the breach. This kind of disruption cannot only impact staff productivity and morale, but it can also have a negative impact on services to clients, and even impact case outcomes.

Additionally, outside stakeholders are increasingly sensitive to cyber security of the organizations they interreact with, or even fund. State laws, regulations, and industry standards (including annual fiscal audits) are increasingly mandating that organization's take action on cyber security.

The threat environment has gotten worse for small and mid-sized firms, and non-profits are not at all spared. Cyber security risks and mitigation strategies are regularly changing, so legal aid providers need to keep focus on security just to keep up with expectations.

## What are Some of the Risks?

Many bad actors in the U.S. and abroad are working globally to look for ways to compromise your technology or your users. They do this for many different reasons. The most obvious reason is for financial gain (e.g., asking a ransom from offices to restore services, selling the data they access to other bad actors, using your data for further compromise, using your systems to attack other systems/organizations). Other attackers aim to harm or embarrass your organization for specific reasons (e.g., political, social, individual vendetta).

## Impact on Client Services and our Client's Lives

Cyber incidents can result in client data being stolen, which can have a severe negative impact on client's lives as a result.

Data theft could lead, for instance, to identity theft or destruction of credit. But attacks don't only expose confidential data, they also may interrupt any services that rely on computers or internet connection to work. This can include disrupting intake (even things like phone systems, case management systems, or web-based intake forms). It can also impact your organization's website and resources clients use for online learning and self-help.

Attacks can also interfere with ongoing client representation. Advocates might lose access to the data and systems they need to do their job representing people. They could also lose the ability to communicate with clients and with each other.

Finally, attacks can cause funders and stakeholders to distrust an office's security practices, which can lead to a loss of funding. And funding decreases also directly impact the communities we serve by decreasing the services we can offer.

## Philosophy, Approach, and Culture

The best way to start when thinking about cybersecurity is to remind ourselves that security is an ongoing process and a culture shift. It is impossible to be in a state of "cyber security" (or being "cyber secure"). Rather, we must prioritize ongoing learning and adjusting practices accordingly. This includes learning about current and emerging threats, learning about best practices and technologies to manage the risks, and learning about best practices and technologies to mitigate the harm and interruption of cyber incidents.

This also means that cyber security is a collective responsibility, shared by our whole community and across an entire organization. It can not simply be assigned to a staff member or contractor. Management at all levels are responsible for cybersecurity, both in practice and in creating a culture that takes the issue seriously.

Also, as with anything that is important for legal aid services and clients, an ongoing commitment to cyber security has a cost. Cyber security frequently requires organizations to make compromises between usability or functionality of their technology and the risk that the technology or data might be compromised. Safer practices might feel like more work or might feel like you are not using the technology to its full potential, but this trade-off might be required to secure the technologies that support access to and delivery of legal services. The tradeoff could also be financial: offices might have to pay for additional staff, contractors, software, or services to enhance their security.

In the end, balancing service needs against security requires that organizations stay informed and educated about their technology, the risks inherent in how they use it, and the tools and services that help reduce the associated risks.

Legal aid has been managing complex risks for years (financial mismanagement, compliance, malpractice, and even case decisions), and cyber security is another major risk for legal aid to manage that will likely be with our community for years to come.

## Benefits of Proper Security Planning and Management for Advocacy and Advocates (Lemonade)

### *Benefits for IT Staff*

The most obvious benefit to IT staff taking cyber security seriously is a decreased risk of successful security breaches. This reduces business interruptions. Any cyber incidents that do compromise the organization will likely be both identified and shut down more quickly. This early detection and preparedness can also reduce interruption time when incidents do occur.

A strong cybersecurity preparedness plan can also help with recovery. Organizations with the right technology and processes in place will increase the likelihood that IT staff can identify the cause or source of the compromise. This also increases the chances that the organizations will know the extent of access and the extent of any data that has been stolen. Finally, being prepared before an attack can also help staff debrief from any breaches to identify simpler solutions for securing routes of attack against future breaches.

### *Benefits for Management and Operations*

Enhanced cybersecurity also directly benefits management and operations staff. First, better cybersecurity preparedness can improve relationships with funders and stakeholders. Audits and reports for funders and boards often include questions about security. Being prepared can make these reports easier to prepare. It can also increase your organization's reputation as a responsible non-profit, both to stakeholders and to the larger legal aid community. Plus, better handling of incidents as they arise will mean less likelihood that an office needs to report or disclose a breach.

Being mindful of cybersecurity is also more economical. Preparing ahead of time typically costs a lot less and can be spread out over a longer period than emergency responses. Planned security work can be done in concert with other projects or timed for better pricing. When your organization considers cybersecurity (which you should), this can be more attainable

and more affordable if you are already taking these issues seriously.

***Benefits for Staff, Attorneys, and Advocates***

Staff, Attorneys, and Advocates will also feel the positive effects of better cybersecurity. They can feel safe that their own data, and the data of their clients, will not be accessed by bad actors and used for nefarious purposes. When things do go wrong in an organization that has taken steps to prepare for a breach, staff will not feel as disrupted. They will be able to get back to work faster after an incident.

## 3. Security Toolkit: Assessing Your Current Cyber Security Practices

Submitted by GravityWorks on Mon, 02/17/2025 - 9:47 AM

### Full Security Assessments

In addition to self-assessments to guide your cyber security decisions, your organization should also consider a more complete assessment, often conducted with the help of outside experts. Below is information on what a security assessment usually entails and what you can do after the assessment to apply what you learn.

### What is a Security Assessment?

A security assessment is an opportunity for your firm to look at your approach to technology and evaluate how secure you really are. This includes looking at your current security software, services, and practice, as well as your security training for staff and your general readiness for cyber security incidents. But it also includes analyzing the equipment and software you use, your technology is configured, your IT practices, your technology policies, and data management practices. It is always better to know where your office is vulnerable to attack before an attack happens so that you can not only prepare for attacks, but also make informed decisions about which risks are acceptable and which are not.

These types of reviews and assessments are typically done periodically, not just one time. Some large law firm legal technology experts liken security assessments to annual physicals. Your organizations's technology environment and practices are always evolving, and we are always seeing new vulnerabilities and exploitation techniques emerge. An assessment should be done at least every 2 to 3 years, though some recommend doing assessments annually.

The process usually starts with selecting a vendor, then a rigorous discovery process, followed by reports from the vendor and planning how to move forward from those reports and recommendations. Vendors who perform assessments, called auditors or assessors, typically help firms address questions they have and come up with solutions that work or better fit budget constraints while keeping firms informed about the impact of new approaches and solutions on associated risks. The end result should be a comprehensive plan to improve security over time, as well as a plan to assess those improvements as they are implemented.

**The Nuts and Bolts of a Security Assessment**

### Selecting a Vendor

Before your assessment can begin, you need to find an auditor or assessor. Talk to the legal community about who is doing these assessments. Look at the specific areas in which assessors might work (e.g. if you have concerns about inventory management specifically, you should find an assessor who has worked on inventory management solutions before). You can also seek grant funding help for your assessment (including from LSC, as described below).

### Discovery

Once you've selected your vendor, your assessor will start to collect information about your office to learn as much as they can about your organization's security vulnerability and practices. The size of this process can vary greatly, but around a month of discovery is not typical.

Your vendor will want a vast variety of information. Your assessor will review your organization's security policies (things like Window Server security, access and use policies, and your "bring your own device" policies). Your IT team and administrators will need to be involved in this process, and people from around the office might have to gather information for the vendor or participate in interviews. You will also likely have to give your assessors access to some of your technology and software with user accounts.

This phase of the assessment may also include internal and external "penetration testing," a type of testing where assessors

try to break into a organization's systems to see how secure they are. This kind of testing may be done more regularly than the fuller assessments. Assessors may also attempt phishing and social engineering attacks to see if your organization's users are particularly vulnerable to these methods of attack.

Doing all follow-up work and providing all information your assessors request is critical. In order to provide useful advice, assessors need an understanding of your business and practice. This increases the likelihood that they will uncover lurking vulnerabilities, but also that they'll propose strategies that are cost-effective and match with your organization's actual work and processes. For instance, in an office where advocates collaborate very often with users in Google Docs, an assessor must know not to suggest a policy requiring advocates to work only in the firm's Office 365 environment. Assessors can only know these details if the organization works closely with them during the discovery process.

### Outputs and Follow-Up with Assessors

When your assessor finishes gathering supporting information, they'll prepare reports for you, in which they'll identify and describe the vulnerabilities they've found and their relative risks. Assessors will typically make recommendations on the specific technologies in use, new technologies that might be implemented in your organization, changes to business practices, changes to the insurance you carry, and user changes to practices around user management and support.

Assessors will typically prepare multiple reports. First, they'll create a business-level report, a summary for non-technical audiences, that the office can share with leaders and committees. They'll also create more detailed technical reports. These actionable reports should be directed at IT staff to explain what's wrong and how to fix it.

### After Your Assessment

A security assessment is only a first step. Once the assessment is complete, you'll have a good idea of what to do next.

Start by reviewing the reports prepared by your assessor. Next, meet with the assessors to discuss their findings. This will also be a chance to ask any follow-up questions or get clarification on any of the findings.

Next, bring the findings to relevant members of your management team and to the right staff. Work with them to start developing a plan of action. It makes sense to start with low-cost items that you can implement quickly, but this is also the time to start planning for harder, more expensive, longer-term projects.

For long-term planning, you may have your local IT teamwork with the assessor to develop technical and operational solutions. As you take on more complex, long-term projects, track your progress and employ project-management strategies to make sure you are headed towards your goals and following the advice of your assessors. This may also include things like directed fundraising or changes to your planned budget.

#### Funding Through LSC

### Overview

LSC offers Technology Improvement Project (TIP) Grants. These grants fund technology related assessments, including an IT security audit. The maximum amount for funding is $35,000 if the project includes an IT security audit. Funding generally covers 12 or 18- month projects. Some offices have worked with general TIG applications before; TIP applications are shorter and simpler than full TIG application. TIP applications do not include a pre-application or invitation requirement.

### Eligibility

To be eligible for a TIP grant covering assessment, your office must be current LSC Basic Field-General, Basic Field-Migrant, or Basic Field-Native American grant recipients. Your office also must be up to date according to milestone and payment schedules on any existing TIG projects before starting a TIP project.

### To Apply

Applications are available in GrantEase, LSC's online grant management system.

- 2021 Application Guide
- Video Tutorial

## 3.1. Security Toolkit: Self-Assessment for Organizations

Submitted by GravityWorks on Mon, 02/17/2025 - 9:54 AM

### Self-Assessment for Organizations

Below is a self-assessment tool that can be used by any organization to help gauge the efficacy of their current security practices. We encourage anyone using this Toolkit to complete this self-assessment and use the questions to help drive your conversations between management and your tech team. The self-assessment is not comprehensive but seeks to prioritize security tools and practices that are of higher in priority for legal aid and within reach of most organizations. After the assessment be sure to return to the toolkit for information about some of the steps your organization can take to address issues that became apparent during the assessment.

Click Here to start the Self-Assessment for Organizations

## 3.2. Security Toolkit: Self-Assessment for Individual Users

Submitted by GravityWorks on Mon, 02/17/2025 - 9:59 AM

### How are you keeping your devices secure (mobile phones, tablets, USB, laptops, desktops)?

Below is a self-assessment tool that individuals may use to start to gauge how secure their personal tech practices are. We encourage this assessment for anyone working for your organization. We also encourage all users to regularly participate in cyber security trainings geared for end users. After the assessment, you will be given recommendations on how you can improve your security practices.

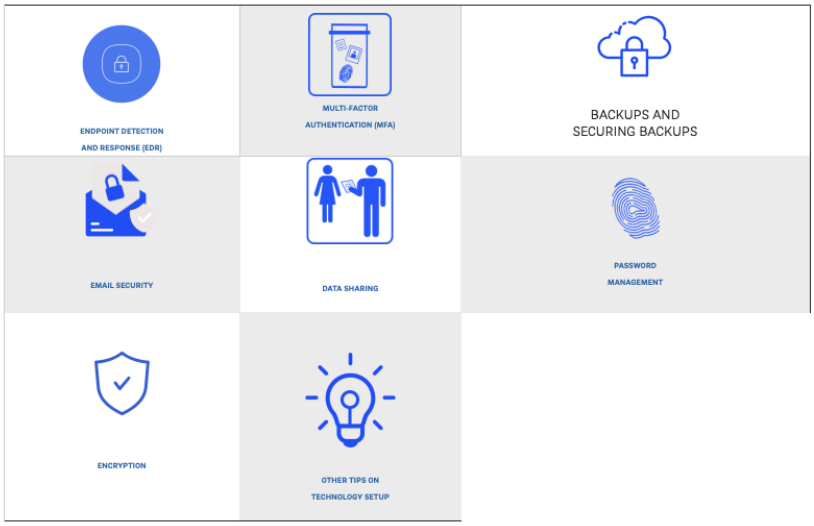
**Click Here to start the Self-Assessment for Individual Users**

## 4. Security Toolkit: Specific Security Topics: What to Look into and Why

Submitted by GravityWorks on Mon, 02/17/2025 - 10:00 AM

Below is a selection of topics in cybersecurity to guide you in thinking about your current security practices and what to do next. Each section has some information that all staff should know, including leadership and management, as well as some more detailed information that IT staff should know.

The toolkit also provides some suggested solutions and some guidance on pricing. These suggestions are not exhaustive. Pricing can be very complex depending on the packages and solutions you pursue, including how they dovetail with the products you already purchase (e.g. an expensive solution might not be as expensive when it's purchased as an add-on to an ongoing subscription you already pay for). Pricing can also vary depending on non-profit pricing and grant assistance. We've also included some outside general resources related to each topic.




- Endpoint Detection and Response (EDR)
- Multi-Factor Authentication (MFA)
- Backups and Securing Backups
- Email Security
- Data Sharing
- Password Management
- Encryption
- Other Tips on Technology Setup

# 4.1. Security Toolkit: Endpoint Detection and Response (EDR)

Submitted by GravityWorks on Mon, 02/17/2025 - 10:09 AM

### What Everyone Needs to Know

Endpoint Detection and Response (EDR) refers to a type of software solution that is the next evolution of traditional antivirus solutions. Attackers just don't stick to a single game plan anymore. They've adapted and modified their methods to be much more fluid. Today's cat and mouse game has evolved beyond the static lists that traditional antivirus solutions can deal with. EDR solutions continuously monitor what is happening with your office's network so that staff can rapidly investigate and stop potential security incidents.

### What IT Needs to Know

EDR provides deep visibility into the status of your network and allows for threat hunting capabilities to detect and block suspicious activities. It also gives you increased forensic capabilities, which allow for administrators to build a timeline of events to determine the impact of a breach. Additionally, many insurance companies are now requiring EDR solutions to be in place for organizations.

EDR is better than traditional antivirus because it can more organically respond to threats. Traditional antivirus software relies on a database of known attacks that needs to be constantly updated by vendors. These databases are good at detecting whatever the most recent attack was, but not so good at preventing new and emerging threats. EDR relies on event and behavior analysis, which helps it detect both known and unknown threats. EDR solutions can also provide you with a timeline of an attack, giving you information such as how it occurred and what it's trying to do, along with the capability to isolate, quarantine and remediate the infected endpoint(s). EDR can help you detect and respond to ransomware attacks, fileless attacks, and zero-day attacks.

Ransomware attacks are designed to encrypt your data and demand a ransom payment to unlock your files. This is now being combined with exfiltration techniques where attackers steal your data before they encrypt it and then threaten to release this information in the dark web if payment is not received.

Fileless attacks rely on what you already have in your environment, making it hard to detect and remove from your environment. PowerShell, for example, is a built-in Windows tool used by administrators but in the wrong hands, can be used to launch these types of attacks.

Zero-day exploits are new vulnerabilities that attackers have begun to exploit before developers have had a chance to

patch. This often leads to developers having to scramble to update their systems which can take days. These attacks are sudden and require immediate attention and/or action by IT administrators.

Again, EDR helps administrators detect and respond to all of these types of attacks.

### Solutions to Consider

Crowdstrike: Website, Pricing
SentinelOne: Website, Pricing
Checkpoint: Website, Pricing
VMWare: Website, Pricing

### Resources

"What is Endpoint Detection and Response" (Crowdstrike)
"What Is Endpoint Detection and Response (EDR)?" (McAfee)

## 4.2. Security Toolkit: Multi-Factor Authentication (MFA)

Submitted by GravityWorks on Mon, 02/17/2025 - 10:18 AM

### What Everyone Needs to Know

Multi-Factor Authentication (MFA) adds a second layer of security when logging into your account making it more difficult for cybercriminals to access your account. This means when logging in, you typically need to authenticate in two ways (e.g., password you know and a device or a code you have).

With this, cyber criminals will need more than just your password to access your account.
You can enable MFA for your own accounts, but your organization can also enable this extra protection for all people working at the office.

### What IT Needs to Know

MFA is quickly becoming standard practice to secure your information and data, and more firms and insurers are requiring MFA.

Your organization should enable MFA on any individual applications that have the option. You could also consider enterprise MFA solutions across all of your systems and applications. If your organization is using various applications for core operation (e.g., email, case management, time tracking, etc.), third-party MFA tools can be configured to cover all of these various services and identities. Additionally, many of the technologies your organization is already using will have MFA solutions built in. For instance, Google and Office 365 already have an option to enable MFA for your users. When you add MFA to these core applications and identity providers, you can combine the protections of MFA with single sign-on configuration to make access easier for the user and easier to manage for administrators.

Some MFA solutions include adaptive authentication. Adaptive authentication is a type of MFA that can be configured and deployed in a way that the identity service provider (IDP) system will select the right multiple authentication factors depending on a user's risk profile and behavior.

### Solutions to Consider

Okta: Website, Pricing
Duo: Website, Pricing

### Other Resources

"Multi-Factor Authentication (MFA): Implementation, Best Practices and Benefits" (Stealthlabs)

"Multi-Factor Authentication Best Practices & Solutions" (eSecurity Planet)
"Two-factor authentication: A cheat sheet" (TechRepublic)

# 4.3. Security Toolkit: Backups and Securing Backups

Submitted by GravityWorks on Mon, 02/17/2025 - 10:26 AM

## What Everyone Needs to Know

A “backup” is, in general, one or more copies of important data stored on your devices or servers, including virtual servers or virtual machines, as well as by your cloud-based service providers (email, case management, documents, fundraising, etc.) and is used in potential data loss situations to restore the original information. Data loss can occur for several reasons, including hardware failures, human error, ransomware attacks, or theft. Protecting backups from corruption, deletion, and unauthorized access is a critical task for IT administrators since backups help us restore from all kinds of disasters.

Creating backups of essential data can ensure that attacks do not interrupt service. Backups can include:

- User data, such as individual user profiles and files.
- Organizational data, such as databases and configurations of your office’s case management systems or Windows login infrastructure.
- Full server images, which can make restoring from a cyberattack or system failure much less painful.

Backups are only as good as when and how they are created, so your organization should have a plan on how often to store backups and where to store them.

Most cloud-based services (e.g., email, documents, case management, donor management) backup your organizations data to help the service provider recover if their server or network environment is damaged or attacked. It is worth investigating what each cloud provider backs-up, how long the back-up data is preserved, and how you may recover data that is damaged or lost by your users or through a cyber incident. Your organization may decide that it wants to back-up some or all your cloud-based service data in addition to the backups provided by the service vendor. These backups might help programs meet their data retention policy requirements and protect against data that was lost or corrupted but not discovered until after the point at which the cloud service provider can recover the data itself. These backups might also make it easier and faster to recover specific data or make it practical to turn off accounts for users who have left the organization but who created data that needs to be retained.

## What IT Needs to Know

Backups should be stored in a secure location, physically and logically separate from the original data. During ransomware attacks that involve encryption of your current data, backups are a primary target for attackers since the attackers want to prevent you from being able to recover your data without paying the ransom. There are multiple storage options, including external hard drives, tape drives, and cloud-based storage.

There are critical considerations when planning for and storing backups. They include:

- How often should you perform backups? The timing of backups can greatly impact their usefulness. For instance, if you need to recover data but you only store backups once a day overnight, you could potentially lose a full day of work.
- What data is being backed-up? How do you ensure that the right data is being backed-up over time? Typically, organizations quickly evolve the systems they use and the locations of where the current data reside. Documentation and auditing are important to ensuring the right data is being protected with your backup solution.
- Does your backup solution allow for you to recover your data on a file basis as well as a server or virtual machine basis? It is very valuable to have a backup solution that allows both file-based and server-based recovery.
- How long will it take to restore your data? If you have a large amount of data, you may need local faster storage for faster recovery times. During a cyber incident, your organization may need to run one or more massive data restoration. The speed of recovery system is a very important factor to restoring services.
- If your backup is stored in the cloud, is there an option to recover to a temporary cloud server environment? How fast can that be done?
- How long will it take to restore your entire system if it is affected by an attack, a hardware failure, or a corruption? The extent of a breach will determine the time necessary to restore backups.

- What are the ongoing cost of the backup solutions (labor, hardware, subscriptions, cloud services, etc.)? Storage costs money, and so does IT staff time spent on maintaining backup systems.  How does your firm limit the growth of its data backup needs?
- How will you monitor backups to make sure they are working and backing up all the required data? Consider ways to do this automatically as part of your backup system.
- Is the backup data encrypted in case the backup is accessed in an unauthorized fashion?
- How will your firm secure access to your backup system or systems? You should ensure that backups are only accessible to authorized personnel, that the systems are protected with MFA, and that the data cannot be changed once it is backed up. This might mean limiting access to which human and service accounts have access to the backups, limiting the ability of those accounts to delete data before a certain date, and certainly working with the backup solution provider to explore further how to protect the data from cyber incidents.
- How often will you fire drill small, medium, and large recoveries?  Testing your recovery processes at least annually will typically reveal important information that your organization will want to act on promptly.
- Who is able to manage the recovery if your primary IT person(s) is not available?
- If your firm needs to maintain some period of time its compromised servers or systems for forensic analysis purposes, does your firm have a plan to recover to alternative hardware or cloud servers with sufficient capacity and performance?

Costs for implementing and maintaining a backup protocol can vary widely.  It is worth shopping around to find the right mix of features and cost. There is a significant investment of time to setup and do some initial testing of your backups.  For smaller, simpler technology environments, this might be in the tens of hours.  For larger, more complex environments it might be over 100 hours to implement and fully test.

### Solutions to Consider

- For backup of on-site servers, virtual machines and cloud backups of accounts, such as Microsoft 365 Email or SharePoint)
  -Datto: Website
  -Acronis: Website
  -Veeam: Website
- Microsoft Azure Site Recovery (Backups): Website
- Keepersecurity: Website

### Resources

"Backup & Secure" (USGS)
“Data Backup – What is it?” (Acronis)
"Azure Backup service documentation" (Microsoft)

## 4.4. Security Toolkit: Email Security

Submitted by GravityWorks on Mon, 02/17/2025 - 10:35 AM

### What Everyone Needs to Know

Developing an approach to email security typically involves multiple procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss, or compromise. Email can be used to infect a device with malware, spread spam, and target users with phishing attacks.

Attackers use deceptive messages (e.g., emails that look like they’re from a reputable source like Microsoft). They use these deceptive emails to entice recipients to part with sensitive information (e.g. to share account passwords), to open attachments (which might install hidden software on the user’s computer), or click on hyperlinks (which will also install malware on the victim’s device). Email is also a common way for attackers to gain access to a network and obtain valuable company data, often using “social engineering” (e.g., pretending to be an official representative from a company to get

passwords, information about security, etc.).

### What IT Needs to Know

While basic spam and antivirus email protection are useful in reducing email threats, standard email filtering is no longer sufficient. A dedicated advanced email security tool will offer improved spam and phishing protection, compared to the basic protection included by default with most email services. When looking at options for email security, look for solutions that can:

- Control device access
- Identify suspicious user behavior
- Improve spam and phishing protection
- Maintain communication confidentiality
- Protect against zero-day threats
- Provide real-time threat protection
- Stop ransomware attacks and other threats

As with many other technologies, the price for email security tools can vary greatly depending on how you contract and purchase the different services. As usual, consider services that integrate with your existing technology infrastructure and strategy to reduce setup time and cost.

### Solutions to Consider

- IronScales: Website, Pricing
- Proofpoint: Website, Pricing
- MS Defender: Website, Pricing
- Mimecast: Website, Pricing

### Resources

"The Transformation of Email Security" (Forbes)
"What is Email Security? Definition, Benefits, Examples & Best Practices" (Toolbox)

## 4.5. Security Toolkit: Data Sharing

Submitted by GravityWorks on Mon, 02/17/2025 - 10:42 AM

### What Everyone Needs to Know

Sometimes when doing your work, you will need to share information and data with other people both inside and outside of your organization. This can range from individual files to large-scale data sharing. Whenever data is shared beyond an individual, team or unit, there are some additional risks such as inadvertently sharing data with the wrong people or those who received the shared data further disseminate the data to others inappropriately. While there are specific tools to help organizations  While there are a range of technologies that help organizations manage inadvertent or inappropriate data sharing which are typically referred to as data loss presentation (DLP) technologies, there are some simpler steps that organizations can take while they consider more robust DLP solutions.

Those steps include developing written data sharing protocols that work across the organization but also for specialized units or practice groups.  Included in the protocols might be guidance on:

- types of data that may be shared internally and externally (this might lead to adata classification protocol) ,

- which entities or types of entities may receive shared data
- when it is appropriate to share data and whether specific permission is needed
- which technologies should be used to share data (e.g., encrypted files, encrypted email, regular email, open web links, login-protected web links)

Depending on how the organization proceeds in managing shared data, your staff will need to be trained on the protocols and the technology. Likely, your IT team may need to implement additional technologies such as secure email and file sharing tools. Generally, all users should use the technologies IT team provides to share data as opposed to using personal accounts (e.g. personal Dropbox, Google Docs, or private email systems such as ProtonMail). Avoiding personal solutions to more secure file sharing helped ensure secure as well as governance and control of the firm's data. Managers and decision-makers are urged to take data sharing security issues seriously.

### What IT Needs to Know

When it comes to data sharing, internally and externally, do you know the who, what, when, where, and why? Do you have the technology and protocols/policies in place to protect your data?

- Internally, do staff and volunteers only have access to data and files they are authorized to use?
- Do staff and volunteers have appropriate, limited access within the systems being used (e.g., case management, accounting, donor management, human resources)
- When sending out sensitive data, do you know what is being sent, who is it being sent to, and if it is being sent securely?
- Do you have the tools in place to know or log what data is being accessed by whom?
- Do you have the technology, polices/protocols, and training in place to help staff share data appropriately securely?
- Does the technology used for sharing data allow you quickly revoke the shared data or expiry the sharing of data based on time elapsed or some other variable?

To facilitate safe and secure file sharing, make sure you've implemented secure file sharing methods (e.g. file sharing solutions as part of your document management system). It is worth repeating the importance of documenting the data sharing protocols and training all used on data sharing. Finally, depending on the data being shared make use of email and file encryption technologies to help limit unauthorized entities for gaining access to shared data.

### Solutions to consider:

Mimecast: Website, Pricing
SharePoint: Website, Pricing
BOX: Website, Pricing
NetDocuments: Website
Microsoft Data Loss Prevention: Website

### Resources:

"6 Smart Ways to Share Files Securely" (Business News Daily)
"5 Steps to Becoming a Data Sharing Master" (TechBeacon)

## 4.6. Security Toolkit: Password Management

Submitted by GravityWorks on Mon, 02/17/2025 - 11:32 AM

### What Everyone Needs to Know

Passwords are still the primary lock used to protect access to systems and data. This is why applications always prompt users to create more complex passwords and to change passwords often. You should always change your password when it is recommended and follow the password guidance when you do (e.g., do not reuse passwords across different accounts, do not share your passwords with other people, etc.). The difficulty has now become having too many passwords, all needing to be unique. The more challenging this becomes, the less inclined people are to create complex secure passwords. One way to mitigate this is to use a password manager for both work and personal accounts, which will store your passwords in a secure vault so that you don't need to memorize them.

### What IT Needs to Know

Passwords present several challenges to IT staff. Organizations need to manage user access and permissions across multiple systems in their offices and in the cloud. As a result, users are responsible for multiple secure passwords and, potentially, multiple MFA solutions so users tend to make some password mistakes, e.g., they reuse passwords, choose an insecure password, neglect changing their passwords over time, share their passwords with other users. And when users leave the organization, the organization needs to retain access to its data on third-party systems.

There are a few ways that staff can address these challenges in password management. First, consider cybersecurity training for users to help them develop better password habits. You should also have policies on passwords (how often to change them, how to keep them secure, etc.).

Finally, consider a password manager. Password managers securely store multiple passwords, and they also help users create complex passwords that are harder to break. Password managers combined with single sign-on can greatly reduce the number of passwords users have to memorize, which will in turn lead to fewer passwords on post-it notes and fewer reused passwords. You can adopt an enterprise password-management solution and create accounts for all users, or you can add password managers to your user training and best-practice documents for staff. Be aware that some organizations also specifically tell users not to put work passwords into their personal password managers. Whichever you choose, be clear with users on what is expected of them.

### Solutions to consider:

keepersecurity: Website
BeyondTrust: Website
n-able passportal: Website

### Resources:

"Cybersecurity: What All Nonprofits Need to Know" (The Modern Nonprofit)
"Creating and Managing Strong Passwords" (CISA)
"NIST Password Guidelines" (n-able Passportal)

## 4.7. Security Toolkit: Encryption

Submitted by GravityWorks on Mon, 02/17/2025 - 11:41 AM

### What Everyone Needs to Know

Encryption is the conversion of data into an unreadable form that helps prevent unauthorized use of such data. Encryption helps ensure confidentiality and keep information secret from those not entitled to see it.
To encrypt data, you need software that uses a key or password to scramble the data, and you need that same key or password and compatible software to decrypt it as well. Most business websites encrypt their data with what is called public key encryption technology. When you see a website URL that starts with https://, the site is using public key encryptions. Encryption is used to help identify an entity such as a website, server, or user.
Encryption technologies are used to protect data and files that are stored in one place (data at rest) and data that is sent from one place to another (data in transit). The legal aid community is moving to more encryption of both data in transit (e.g., email, voice calls, video calls, web meetings, chat) and data at rest (e.g., hard drives, desktops, file servers, cloud servers, backups) to help protect the data against accidental or intentional access or dissemination of data in an unauthorized manner. (Legal Aid providers should also talk to their cloud service providers (e.g., case management, document, fundraising, accounting, HR, telephone) to understand how they encrypt data in transit and at rest.)
Data in transit includes confidential email, voice, or video communications. Lots of messaging services already include encryption (such as WhatsApp, iMessage). Email communications are typically not encrypted by default, but most email solutions either have options to encrypt emails or are compatible with technology to encrypt them. Google's email and

Microsoft 365's email solutions both have options for encryptions from Google and Microsoft as well as from third parties. Data at rest includes data on USB storage keys, hard drives, laptops, smartphones, servers, and backup files. Protecting data at rest is key for any office that wants to prevent data loss when equipment is lost or stolen. A stolen laptop that is encrypted is functionally the same as an empty laptop to a thief.

### What IT Needs to Know

When thinking about Encryption, you need to protect the data at rest and the data in transit. Data at rest means data that is housed physically on computer data storage in any digital form. This includes servers, desktop computers, laptops, smart phones, and tablets.  Data in transit is data actively moving from one location to another, such as across the internet or through a private network. This includes email, web, collaborative work applications such as Teams, and remote access technologies.
When possible, use services that already include encryption (e.g., web applications that use HTTPS instead of HTTP. Messaging applications with end-to-end encryption). If your technology does not include encryption built in, you can find secondary tools for encryption, both across applications and for sending specific encrypted messages.

### Solutions to Consider:

Proofpoint (email security and protection): Website
Office 365 (Built in tool): Website
BitLocker for Windows: Website

### Resources

"Azure data security and encryption best practices" (Microsoft)
"What is encryption? Data encryption defined" (IBM)
"What Is Encryption?" (Proofpoint)
"What Is Data Encryption: Types, Algorithms, Techniques and Methods" (Simplilearn)

## 4.8 Security Toolkit: Other Tips on Technology Setup

Submitted by GravityWorks on Mon, 02/17/2025 - 2:17 PM

4.8. Security Toolkit: Other Tips on Technology Setup

### Updates and Patching

IT staff should ensure that all software is up to date and properly patched. This can include device policies that push updates to all computers, but it should also include updates to core applications (e.g. case management systems). This might also require upgrading hardware as well, since older computers might not be able to support new software.

### User Accounts

Whenever creating user accounts on computers or in technology systems, IT staff should create standard accounts, not admin accounts. Every user should have a standard account. When a user needs admin level access, IT staff should create a separate account. IT should also have policies for onboarding and offboarding staff to ensure that former staff do not retain access to accounts after they depart.

### Wi-Fi

Staff should be trained not to use key applications over public Wi-Fi while outside of the office. Public Wi-Fi can be unencrypted and might reveal private data and information to others sharing that network.
Inside the office, you should separate your private staff network from your guest network. This way, outside users do not use the same Wi-Fi network that is handling your sensitive data and applications. You can also configure your Wi-Fi network with more security features, such as connecting users to your wireless network with unique logins or segmenting your

network depending on the user or group permissions by using VLANs.

### Remote Work

When building remote work technical capacity for staff and volunteers, it is helpful to start with the development of policies or protocols for remote work so that the organization build the right capacity, functionality, and security into the environment. If the organization already has remote work technology in place, it is still worth developing the policy and then work to comform the technology to support the policy. Have a telecommuting policy and have policies that explain how to use personal devices. This should include policies on which applications your staff are allowed to use and how to use them. You should also establish a communication plan for how to share information with your staff. Invest in the right technology tools to make remote work as secure and successful as possible.

You should also have a security plan for any remote work. In general, users should only be using the equipment provided by your organization to secure your data. Consider the other topics in this toolkit, as they can be even more important in remote settings (e.g., MFA and password policies). You can also use virtual private networks (VPNs) for remote access, which can provide direct secure access to your on-site technology even while off-site.

### Securing Home Technology

Legal aid staff members and volunteers, working from home are typically working in an environment with other users (e.g., family members, roommates, partners) and many different Internet-enabled technologies (e.g., desktops, laptops, tablets, smartphones, printers, Wi-Fi access points, routers, cable modems, game consoles, smart TVs, smart speakers, smart thermostats, home NAS/server, connected appliances, and IP cameras). It is important generally advisable that all equipment in the home be kept up-to-date with current software and firmware (a type of software that get more directly controls and manages specific hardware such as a router or a printer). Keeping equipment up to date helps protect legal aid and personal user data and systems as the updates frequently fix security bugs in the software or firmware. Typically, every equipment manufacturer has a website with current software and firmware to download. As needed, users should work with the equipment manufacturer's tech support to make sure they successfully are successfully updating their equipment. Users may also have equipment that is no longer supported (updated) by the manufacturer. Manufacturers may refer to such equipment as end-of-life hardware or equipment. When equipment is no longer support, newly discovered security risks for that equipment will not be fixed by the manufacturer which in turn makes the equipment more vulnerable. That equipment should ideally be replaced as soon as budget and time allow.

In addition to keeping equipment up-to-date, it is important that the equipment be configured securely. At a minimum, this would mean changing all default passwords to a new, more complex, longer password. It would also mean turning off any functionality that isn't needed (if a user has a home network attached storage (NAS) server for photos, videos, files, and backup that server might also have a built-in web server that is not being used and should be turned off) or leaving devices disconnected if not needed (e.g., if a user prints via a USB cable to their printer, they could turn off the printer's built in Wi-Fi connection). For network access devices such as cable modems, firewall, routers, and wireless access points, it is particularly important that users read all the documentation and communicate with the manufacturer or Internet provider's tech support to ensure that their configuration is as locked down as possible while allowing needed access for equipment inside the household.

While all equipment in a household may pose security threats to the user's work machine, users should pay particular attention to updating and securely configuring their cable modems, firewalls, routers, wireless access points, and other computers, tablets, and smartphones. For laptops and desktops, users should be running current anti-virus, anti-malware software from a trusted vendor and use built-in security configuration checks. Microsoft includes such tools in Windows 10 and 11 (Windows Security). Users might also consider security software for the tablets and smartphones.

## 5. Security Toolkit: Security Policies

Submitted by GravityWorks on Mon, 02/17/2025 - 2:24 PM

### What to Include?

Security policies may cover a wide variety of topics. You should have policies dedicated to specific security topics. Below is a list of common policies needed in legal aid organizations:

- Account Management and Password policy: guidance on what kinds of passwords to use and how often to change them.

- Acceptable use policy (AUP): help staff and volunteers understand what they should and should not do with the organization's technology, systems, and data.  AUP's may include requirements with respect to training, specifically security awareness training and testing.

- Remote work and remote access policies: what devices can/cannot be used; who can and cannot use a work device; how to create a secure remote environment; how to properly access organization networks remotely; and data handling practices to prevent data leakage.

- Data classification: clear descriptions of what kinds of data your organization retains and what security should be used for each kind of data. This may include which systems to use and whether/when encryption must be used.

- Data retention: schedules for how long your organization keeps data and in what forms, distinguishing between on-site data, backups, and off-site backups.
  Security breach and incident response plans: guidance on how to respond when the organization becomes aware of a possible breach (see the materials on what to do when you experience a breach below).

- Disaster Recovery Plan Policy: detailed plans on how to keep critical IT services and data available in the event of disaster and/or how to restore critical services in an acceptable time frame.

- Physical security: protect against property damage or theft by establishing rules for granting access to equipment, identifying sensitive areas, authorized personnel, the removal of equipment from the premises, and any required locks and/or video surveillance.

Security policies, like most policies, require sufficient staff and volunteer training as well as designating a role within the organization to be responsible for maintaining the policy, integrating the policy into practice, and driving compliance. Most security policies should be reviewed annually to make sure they are still applicable, that they conform with current good practices, and that they are otherwise sufficient.  There may be circumstances that arise that may call for an earlier review such as when the organization does a security assessment or suffers a security breach that highlights one or more weaknesses in current policies.

### Sample Security Policies

Company Cyber Security Policy Template
Security Policy Templates
IT security policies
30 Free IT Security Policy Templates for Businesses

## 6. Security Toolkit: Training

Submitted by GravityWorks on Mon, 02/17/2025 - 2:26 PM

### What, When, and How

Many offices already understand the value of training for substantive work and client services, but training practices should extend to how staff use technology. You should provide training for staff on the core applications your organization uses (e.g., Outlook, Word, Excel, your case management system). You should also provide training on using the organization's equipment. You should also provide training on using the organization's equipment and security awareness. In fact, funders and insurance companies now ask if you are doing this; some are even requiring it.

Security training should teach your staff how to keep your organization's data secure and how to share data externally in a secure way. Security training can also include "phishing tests," or tests that help staff identify suspicious emails before opening them.

**Resources + Trainers**

### Comprehensive Training Approach

- https://ltc4.org/training-services-providers/
- https://wilsonallen.com/services/training

### LegalServer Training

- help.legalserver.org/home/sitewide/legalservertraining

### Microsoft Office Training

- https://www.knowledgewave.com/
- https://support.microsoft.com/en-us/training

### Security Awareness Training

- KnowBe4
- Ninjio
- Phinsec

### Solutions to consider:

- KnowBe4
- Breachsecurenow
- Ninjio

## 7. Security Toolkit: When you Experience an Incident

Submitted by GravityWorks on Mon, 02/17/2025 - 2:32 PM

### When You Experience an Incident

Every cyber incident is different if for no other reason that each provider's technology environment and user practices are different than sister organizations. The process of dealing with and responding to an incident will vary. Here, we've outlined some of the common things to consider if (or when) an incident occurs. This outline is not one-size-fits-all. Instead, you can use these bullet points to think through what questions to ask and what actions to take. This outline can help organizations develop plans before an attack has ever occurred, and it can help organizations experiencing an attack to determine what to do next.

1. 1 Investigate whether you have been attacked/compromised immediately
    1. Helps to have a well-trained team of staff and volunteers who can serve as an early warning team on any suspicious behavior or changes to their environment
    2. Assume that any significant changes in performance, account access, or notifications from other organizations, your Internet or cloud providers that indicate strange behavior (e.g., lots of spam from your org, network congestion from your ISP, unusual Internet traffic patterns, etc.) are potentially signs of either an attack (DDOS) or a compromise (successful attack).
    3. Attacks or compromises might be seemingly limited but assume that they will grow/get worse.

4. Move quickly to assess and act; be prepared to take action before you are certain your systems have been compromised – may have a false positive which isn't the worse thing in the world.
5. Before an attack, your executive team should collect and verify contact information (personal email addresses and phone numbers) for all staff members. In the initial stages of a security incident, most systems will be considered untrusted and/or locked down thus preventing normal methods of communication.
6. Work with your security provider, your EDR vendor, your SIEM vendor or even use your firewall and system logs to help identify/confirm problems.
7. An attack with cryptoware may be noticed by users before it has completed its spread and encryption – so shutting down or cutting off access may limit damage.

2. Consult and follow your cyber security incident response policy.

3. If you don't have a cyber incident response policy, consider:
    1. Communicating with your leadership via out-of-band phone, text, chat, etc.
    2. What your IT and leadership team understand about how the attack was able to gain access the environment is tentative knowledge and may be wrong.
    3. If you have cybersecurity insurance, contact your agent.
    4. If you have cybersecurity counsel or general counsel, contact them.
    5. Designating an incident captain, coordinator, or manager - typically/ideally not someone from the IT team.
    6. Communicating with your staff as appropriate on what they can expect and what they can communicate to others.
    7. With respect to communications, despite any initial conclusions with respect to the nature of the incident and its impact, the organization should expect those conclusions may be wrong or may represent only a partial understanding of the incident.
    8. Generally, don't communicate about a potential incident publicly or with third parties until advised by your leadership or counsel.
    9. Talking to your tech team / tech partners for additional assistance.
    10. Attempting to isolate and shutdown access to systems.
        1. Where possible maintain remote connectivity for IT to manage access.
        2. Restrict inbound and outbound firewall traffic to only IT personnel/remote connectivity from trusted public Ips.
        3. Limit or stop traffic across all endpoints. For instance, on virtual servers, disable the virtual NIC.
        4. Talk with your cloud service providers about limiting or stopping traffic (case management, document management, email, etc.)
        5. Reset all passwords, including administrators, users, service accounts, temp accounts, guest accounts, etc.
        6. Review user accounts for anything that may have been suspiciously added.
        7. Talk with your cloud service providers about doing the same (case management, document management, email, etc.).
        8. Collect and backup all log information from all systems including servers, firewalls, VPNs, email, etc.
        9. If there is a ransomware note or a malicious email, get a copy of it.
        10. Take screenshots of any unusual activity, such as logins from unknown accounts, antivirus/EDR pop-ups, configuration changes, etc.
        11. Create a detailed timeline of all events from the moment you became aware of the security incident.
        12. Be careful not to alter/delete any potential evidence that can be used by the forensics company.
        13. Attempt to identify the source of the security breach. The compromise may have occurred from malware, phishing email, misconfigured firewall rule, zero-day exploit, easily guessable password, etc. Check all servers and networking devices (i.e., firewalls, VPNs, email, etc.) for suspicious login activity.
    11. If you don't have cybersecurity insurance, you will likely need to:
        1. Get IT and legal help from partners who have worked on cyber incidents.
    12. Working quickly to mitigate the damage.
    13. Getting outside expertise to Investigate the incident, determine the extent of the damage, determine, to the extent possible, whether there was data access or exfiltration.
    14. Decide whether and how to negotiate with the criminals involved - there are firms that specialize in these negotiations.
    15. Plan for and securely restore technology services:
        1. Consult with your insurance/security/legal teams before proceeding.
        2. May need to do this on alternative physical or virtual network and system environment in case confidence is low that the security breach has been identified or if you need the affected environment for forensic analysis.
        3. Will likely need to greatly expand logging and monitoring of the environment.
        4. Likely need to install EDR software.
            1. May need to prioritize which services to restore.
        5. May want to avoid restoring unnecessary or out-of-date, insecure systems or network infrastructure.
            1. Assume that accounts and access can be compromised again.
            2. Consider MFA deployment across all systems on an expedited basis.
            3. Review privileges and limit to the extent feasible.
            4. Modify password policies to be more stringent, if necessary.
            5. Consider modifying any sharing policies/configurations that were previously in place (i.e., disable

sharing via anonymous links).
6. Adjust or implement stronger email security systems to protect against malicious attachments/links and email security attacks such as phishing and business email compromises (BEC).
7. Provide users with security awareness training.
8. Restrict who has remote access (if that is even possible with COVID).
9. Review firewall rules for any old/unused rules and disable them.
10. Revise firewall rules to be more restrictive.

6. Monitor electronically and with all users on high alert.
7. Decide what changes to make to improve security (to avoid a repeat attack).

16. Work on communications/compliance as necessary (regulators/government entities, funders, clients, employees, and the public).

4. Complications
    1. Backups are not comprehensive, up-to-date, and accessible.
        1. Not certain whether the backups have backed-up the security compromise – might be restore access/backdoor.
    2. Not enough capacity in the environment to setup the restored environment.
    3. It may take a long time to recover massive data, especially when restoring from cloud-based backups on slow internet connections.
    4. Criminals are posting exfiltrated data on the dark web/shame sites.
    5. Criminals sell reconnaissance information to other criminals. There is potential for another attack.
    6. Forensic analysis is inconclusive.
    7. Not enough/inaccessible IT documentation to rebuild the environment. May be missing installer packages for critical software or detailed configurations needed for certain connections/applications.
    8. Outdated IT credentials to access systems or networking devices.

## Have Insurance

Cyber insurance is essential in helping your organization recover after a data breach. Insurance can help with costs that can include business disruption, equipment damage, legal fees, public relations expenses, forensic analysis, and costs associated with legally mandated notifications. Insurance also helps companies comply with state regulations that require a business to notify customers of a data breach involving personally identifiable information.

Cybersecurity insurance policies can also cover customer notifications in the event of a breach, an option to monitor the information of anyone impacted for a specified period, and payment of costs incurred in the recovery of compromised data.

## Identification of an Incident

Typically, most legal aid providers identify a possible incident when system performance or access issues, including access to files, becomes an issue that users bring to their IT team. It also happens that another user working for another organization in the community gets spam from the legal aid organization contacts the users they typically work with to alert them, or some law enforcement agency reaches out to inform the provider that they may be a victim of an incident. (It is important that such a notification by third parties be screened as possible cyber-attack itself.)

Generally, the earlier an incident is identified, the better. Early identification helps limit access, damage, and costs while improving the ability of forensic experts to determine the cause of the incident and the security lapses that need to be addressed. Increasingly, organizations are using more sophisticated tools, such as endpoint detection and response (EDR) software, and security services, such as third-party provided security information and event management (SIEM) services, to monitor and identify incidents earlier and intervene more quickly to stop an incident before the access or damage is more significant. Any monitoring might lead to false positives that might in term lead to unnecessary stress and response. It is important to work with your IT team/partner to tune any monitoring tools to reduce the number of false positive alerts. Typically, this work takes weeks or possibly longer after new systems are implemented. Similarly, training users on cyber security awareness will help improve the quality of user reporting on odd email and performance issues.

## Common Cyber Attacks

The FBI recently released its 2022 report on 2021 Internet Crime that is worth reading or skimming to get a better sense of the prevalence of different cybercrime. Another great resource is from Fortinet, a security hardware, software and services firm, on the top 20 cyber-attack types. Visit their web page for a plain language understanding of the different attack types and what organization can do to help prevent them.

## Exercise: Sample Incident and Response

Below is a fact pattern describing a typical data breach. It outlines several actions taken by a member of staff in one column, and in the second column it outlines a list of places to review from the toolkit while considering the fact pattern. Try to spot the things the member of staff has done that increase risk. Think about what you would do in that situation. Use the fact pattern as a tool for discussing security with the rest of your office.

| Fact Pattern | Issues |
| --- | --- |
| You are working on an immigration case with a pro bono attorney at a private law firm. There is a sudden emergency that requires documents to be filed urgently. You need to get more confidential client information immediately to meet the deadline and share it back with the pro bono counsel. | • External data sharing |
| This has all unfolded, while at the airport with your family, as you head to your cousin's wedding. You think, "I've got time, 6-hour plane ride—I'll get it all done in no time". You log into the airport's public Wi-Fi and begin downloading the client's data and texting the client about the documentation that is outstanding. | • Wi-Fi, Encryption, Data sharing, and Personal Devices |
| In flight you connect to the free in-flight airplane wireless network, login to your 365 Webmail to review the document from the pro bono lawyer and save it on your laptop. You also; | • Wi-Fi and Passwords |
| • Remote into your firm's terminal server and find a few documents that you need to reference.<br>• Use the email client to email those documents to your Gmail account, so that you can easily download them onto your Mac.<br>• Your client sends MMS texts to you with copies of their documentation and additional documents are emailed from their yahoo account – you can easily airdrop the images on to your Mac. | • Remote Work<br>• Email security<br>• Personal devices and Encryption |
| Finally, you've made it through the 6-hour flight and to the hotel. You decide to wrap things up at the Starbucks in the hotel's lobby. You have a few email exchanges between the pro bono attorney and your client, and you e-fax all documents to immigration services. Now, it is time to get some rest. The next morning, while everyone prepares for the wedding, you receive an--alert your Gmail has been signed in at a different location.<br><br>Congratulations, enjoy the wedding! | • Wi-Fi, Passwords and MFA |

## 8. Security Toolkit: 2021 Security Webinar Series

Submitted by GravityWorks on Mon, 02/17/2025 - 2:45 PM

Security is important to our organizations and to our clients. The security of our organizations is not the job of one person; it's on all of us. We all have an ongoing responsibility to ensure we are operating in a secure environment to protect client data and confidential organizational data. Legal aid organizations need to continue to learn more about the latest security recommendations, improve the security of their technology, and its management, as well as help users navigate technology more securely. Together we can work to enhance security in the legal aid community.