




SmartVault

The Ultimate Cybersecurity Checklist for Financial Institutions



Your institution is a cybercriminal's goldmine.

From Social Security numbers to birthdates, addresses, and banking information, your files have exactly what cybercriminals need to steal identities, file for fraudulent loans, commit credit card fraud, and more.

Following this checklist will help you build a robust cybersecurity program that protects your institution and customers' data from hackers.

Note that this is not an exhaustive list of what your security program should include. Check applicable regulations for additional information and compliance requirements.

Understand Cybersecurity Basics

Knowledge is key. Before you create new processes, you must understand the basics.

Learn general cybersecurity facts and the common ways cybercriminals gain access to data (malware, phishing, man-in-the-middle, ransomware, etc.)

Understand your obligations to comply with legal, regulatory, and industry mandates, like the Federal Trade Commission's (FTC) Written Information Security Plan (WISP) requirement, Gramm-Leach-Bliley Act (GLBA), and others

Stay updated on cybersecurity threats/risks and regularly review, test, and update your cybersecurity program (see below) to meet the latest recommendations

Evaluate Your Risks and Current Workflows

When you have a general understanding of cybersecurity, you can determine your business's unique risks.

Designate at least one employee who is responsible for your cybersecurity program

Identify vulnerabilities and risks that are specific to your business, such as unauthorized access, loss of data, and use/disclosure of information

Create an inventory of all the devices and hardware your business uses to handle data (i.e., desktop computers, cell phones, routers, printers, etc.), including what you use each for and where they're located

List the data your business handles, including both physical, hardcopy data and electronic data

Review your Business Continuity Plan to define potential data loss scenarios (i.e., a computer is stolen or hacked, data corrupted, hard copy paper files are destroyed in a fire, etc.) and outline how you monitor, test, and respond to these risks and threats

Every 11 seconds
a company is a victim
to a ransomware
attack, on average.

[\(Cyber Security Ventures\)](#)

95% of breaches
are caused by human
error, like clicking a
malicious link.

[\(World Economic Forum\)](#)

\$9.44 Million
is the average cost
of a data breach in
the United States.

[\(IBM\)](#)

Create a Cybersecurity Program

Take what you learned from the previous steps to create a strong cybersecurity program. Your program should, at a minimum, document everything below.

Data Collection and Retention

Identify how much data you store and for how long, where and how you store that data, and who has access to the data

Review the flow of data, considering what happens from when you receive the data to when you're ready to store it

Document as many details as possible about how your data is cared for and accessed

Identify all potential points of failure in your workflow

Ensure all data is encrypted during transit and at rest

Don't use emails to send or request sensitive data

Implement a secure document management system to request, send, and store data in the cloud

Data Backup

Identify what data you need to back up (the information your business couldn't function without)

Keep your backup data separate from your computer or network by using an external hard drive, USB, or, ideally, the cloud

Consider a vendor for cloud storage that provides automated data backup, follows strict security measures, and helps ensure you don't lose your data to a disaster, cyberattack, or human error

Destroying or Deleting Data

Destroy or remove data from computers, CDs, USBs, cells, and other electronic devices before you dispose of them

Shred paper documents that contain sensitive information

Data Disclosure

List the third-party companies that access your data and why

Define requirements for third-party data access (i.e., Two-Factor Authentication, password requirements, etc.)

Describe how you evaluate and confirm that third parties meet privacy standards

Comply with unauthorized disclosure regulations applicable to your business

User and Remote Access

Set access permissions based on employee roles and ensure your vendors provide strong access control options

Require Two-Factor Authentication

Create a process for Unsuccessful Login lockouts

Develop a remote access policy

Network Protection

Define user protocols and requirements:

- Require passwords to have at least 12 characters (a mix of letters, symbols, and numbers)

- Set passwords to expire regularly and ensure your vendors have appropriate password requirements and policies

- Remind employees not to use the same password for multiple devices or accounts

- Do not leave passwords or credentials on sticky notes, notebooks, etc.

- Consider using a password manager program to track passwords

- Require employees to lock computers before stepping away from their desks

- Remind employees to report suspicious emails, texts, or phone calls

Describe the process for adding new devices or software to your network:

- Confirm that all devices meet security requirements

- Designate an employee who approves each new software or device

- Develop a strategy for preventing staff from downloading risky apps

Describe how you monitor computer systems for hackers or unauthorized access

- Use firewall protection, anti-virus, anti-malware, and other security software that updates automatically

- Ensure third-party vendors automatically install patches that resolve software vulnerabilities

- Change the default admin passwords on your routers

- Require employees to install updates as needed on their hardware, computers, and devices

- Remind employees not to use public wi-fi for work

- Track activity across your documents, including who has accessed the data and when

Incident Response

- Create an incident response team with clear assignments, objectives, and responsibilities

- Develop a framework that outlines action items and procedures

- Document information about external resources and how/when to notify the appropriate persons of the data breach, like your staff, customers, the FTC, FBI, local law enforcement, etc.

- Describe steps to re-secure devices, passwords, network, and data

- Develop a continuity plan

Ensure Employees Follow Processes

Your staff are your biggest risk when it comes to data breaches. They're also your first line of defense.

Develop an employee/contractor training policy:

- Create a training program based on your cybersecurity program

- Require new staff (full-time and temp workers) to read the cybersecurity program and complete training during onboarding and at least twice throughout the year

- Regularly remind employees of your policy and their legal obligation to protect customer data

Ensure all employees pass a background check and submit references

Develop and implement non-disclosure agreements and privacy guidelines

Ensure terminated or separated employees do not continue having access to network and data

Protect Your Data in a Vault

One of your top priorities should be implementing a document management system (DMS) that's integrated with a client portal. A DMS provides financial institutions with the organization, security, and efficiency they need to stay compliant and better serve customers. Here are things you should look for in a DMS:

- Bank-level security that'll protect your data with the strongest security measures
- Automated cloud backups for availability if your local systems are damaged, lost, etc.
- Version control and activity tracking to preserve history and access previous versions
- Encryption at rest and transit and robust access controls to restrict who can view, edit, and delete documents
- Mobile access so you can access and collaborate on documents from anywhere
- Indexing and search to quickly find documents
- An integrated client portal to collaborate online



Streamlining Executive Team and Board Alignment While Strengthening Security

To deliver on their commitment to its 125,000 members' financial success, Frontwave's Board and Executive Team must stay aligned through clear communication facilitated by the Executive Administrator (EA).

To make sharing and collaborating on documents easy and secure, the EA uses SmartVault, a cloud-based document management system. "Since I joined Frontwave three years ago, SmartVault has become engrained into my work managing board materials," the EA explains. "I enjoy using the system because it's user-friendly, and it's easy to navigate and find the documents we need."

SmartVault provides a centralized, secure location that empowers the EA to easily share and maintain confidential documents. "Sharing files via email poses a significant risk," the EA says.

"I appreciate how SmartVault enables us to be more secure by giving us one place to upload documents."

SmartVault's granular permissions, encryption, and other bank-level security measures help protect sensitive information, giving Frontwave and its members peace of mind that their data is protected from breaches and data loss.

[Read the Story](#)

6 Reasons You Need a DMS

Implementing a document management system and client portal can provide significant benefits for your financial organization, customers, and teams. Here are six:

1. Builds Your Community

Technology like document management and client portals allow smaller financial institutions to provide amazing service that feels super personalized – and it's this great service that keeps customers happy and encourages them to recommend you to their friends and neighbors. As you continue to scale and build relationships with the people in your area, they'll see your commitment to providing financial services that help their neighborhoods grow and prosper.

2. Simplifies Customer Collaboration

A DMS and client portal can solve everyday headaches you experience when working with customers, such as playing phone tag to remind them to complete a form or resending important information to a customer who lost your first email. These situations, while minor, are frustrating for both parties and make your business look disorganized and difficult to work with. Client portals give customers access to their own documents, so they can securely log in to access, share, review, complete, and eSign documents 24/7. This is more convenient than having to call or visit a branch during business hours, increasing customer satisfaction – which means increased referrals. Portals enable staff to share documents and information with customers instantly as well.

3. Makes Employees Happier (and More Efficient)

Using a DMS is a highly effective way to streamline your process, facilitate communication, and make your teams' experiences positive. Digitizing processes eliminates the need for physical files, helps staff save time on tasks, and makes it easy for employees across branches to collaborate. Having a central repository also makes it faster to retrieve files and provide excellent service. The ability to work remotely also gives staff flexibility.

4. Creates User-Friendly Processes

Traditional software requires everyone to spend time learning how to use it, which creates a major barrier to making even necessary changes. DMS and client portal platforms, however, are designed to be user-friendly, regardless of how tech-savvy a person is. Not only will you be able to come up to speed on the features quickly, but you can rest assured your customers and employees, regardless of their skill level when it comes to tech, will have an easier time as well. Upgrading to the cloud will also make your system more accessible.

5. Secures Your Data

Many DMS vendors have greater resources and invest heavily in ensuring their customers' data stays safe. You'll benefit from advanced security measures like automatic data backup, file versioning, activity tracking, bank-level encryption, and multi-factor authentication (MFA). And granular access controls let you be in 100% control of who accesses what folders and documents. These security standards create peace of mind for your team and customers and can help you meet the most stringent industry regulations with ease.

6. Keeps You Up and Running

Whether you experience a building fire, a computer malfunction, or someone accidentally deleting a file, the cloud makes it significantly easier for you to recover and get back up and running. Cloud providers store your data on multiple remote servers, which they maintain and back up regularly. They'll help you restore your data quickly. Better still, using the cloud actually reduces your vulnerability to disasters. Storing your information on remote rather than on-premise servers means that even if a flood or other weather event impacts your home or office, you won't lose everything.

Over 3 million people securely gather, store, share, and eSign documents in the cloud with SmartVault.

With SmartVault, you'll have a cloud-based document management system and client portal that prioritizes security and compliance and makes it more secure for you, your staff, and your customers to work together online.

Learn more or schedule a demo: www.smartvault.com