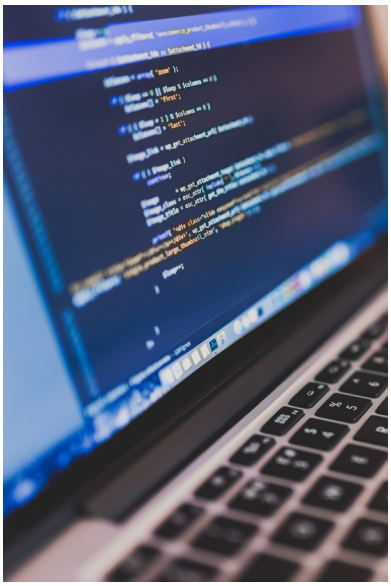
A GUIDE TO NYS SHIELD ACT COMPLIANCE

AVALON Cyber

AVALONCyber

NYS SHIELD Act



Under the **NYS SHIELD Act,** a breach is now considered **any unauthorized access.**

A Brief Introduction to the NYS SHIELD Act

The New York State Stop Hacks and Improve Electronic Data Security (NYS SHIELD) Act was signed into law in July 2019 and went into effect in March 2020. However, many organizations, understandably, may have pushed preparations aside due to the COVID-19 pandemic. But it's crucial that every business – large and small – that handles the private information of New York State residents moves forward and adopts a cybersecurity program that helps reduce the risk of a data breach.

Let's take a closer look at what this legislation is and what you need to do to comply.

The NYS SHIELD Act:

- Amended the New York General Business Code 899-aa and adds Section 899-bb to expand consumer privacy protections and consequences of a data breach.
- Was created to protect New York State consumers by requiring companies to develop, implement, and maintain "reasonable safeguards" to protect the security, confidentiality, and integrity of "private information."
- Expanded the definition of "private information" to include new items like biometric data, such as fingerprints and retinal scans, and the combination of usernames, passwords, and security questions.
- Broadened the definition of "breach" – previously, only unauthorized acquisition of data was considered a breach; however, under the SHIELD Act, a breach is now considered **any unauthorized access.**
- Applies to businesses operating within New York State, as well as any business, nationally or internationally, that stores, processes, or transmits a New York resident's private data.
- Changed when notifications are triggered, which means more breaches will be reportable and, therefore, more consumer/customer notifications will be required.

AVALONCyber

NYS SHIELD Act

The NYS SHIELD Act, **expands the list of key data elements** protected by the law.

Now, we'll address a few questions to help you better understand this new law.

What is Private Information?

The NYS SHIELD Act redefined "private information," expanding the list of key data elements protected by the law to include:

- Personal information ("any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person") in combination with a variety of traditional non-public personally identifiable information (PII), such as:
    - Social security number
    - Driver's license number or non-driver identification card number
    - Account number, or credit or debit card number, in combination with any required security code, access code, password, or other information that would permit access to an individual's financial account
    - Account number, or credit or debit card number, if the number can be used to access an individual's financial account without additional identifying information, security code, access code, or password
    - Biometric information, such as a fingerprint, voiceprint, retina or iris image, or other unique physical or digital representation of biometric data used to authenticate a person's identity
- Username/email address in combination with a password or security question/answer that permits access to an online account

Here are some real-life examples:

- You call your favorite restaurant in Buffalo, NY and place an order. They ask for your charge card number, expiration date, and the security code on the back of the card. That restaurant now has your private information under the SHIELD Act regulations and needs to protect it.

AVALONCyber

NYS SHIELD Act

The **safeguards your business must** take when developing your **cybersecurity program** can be broken down into three categories: **administrative, technical, and physical.**

- You pick up your son from daycare, but before you can retrieve him and bring him home, you need to scan your fingerprint to prove your identity. That daycare center has your biometric data and better update their cybersecurity program to comply.
- You own several apartment buildings in Rochester that house hundreds of tenants. Since you store their private information, including names, social security numbers, driver's license numbers, and bank statements, you need to develop a cybersecurity program, even though you've never had one before, to secure that data.
- Your software company, located in Cleveland, Ohio, just had a business in Albany place an order. Since they plan to order additional goods and services from you, their purchasing agent stored the company's billing information on your site. Congratulations, you're now under orders to become SHIELD-compliant!

What are Reasonable Safeguards?

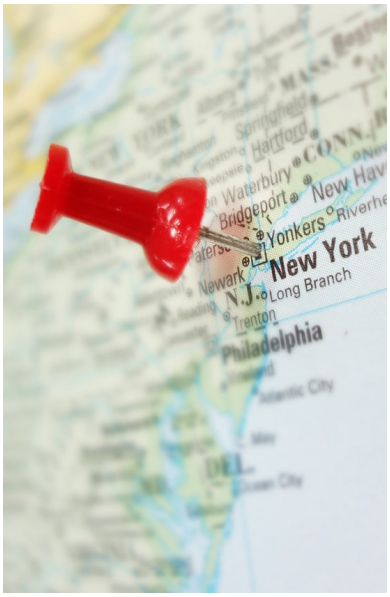
While the SHIELD Act doesn't cite specific "reasonable safeguards" to employ, it does say that a business will be in compliance if and when it implements a data security program. The safeguards your business must take when developing your cybersecurity program can be broken down into three categories: administrative, technical, and physical.

Administrative safeguards

- Designating one or more employees to coordinate the security program
- Identifying external and insider risks
- Assessing current safeguards to control identified risks
- Offering workforce cybersecurity and procedural training
- Selecting service providers to maintain appropriate safeguards and requires those safeguards by contract
- Adjusting the program when necessary

AVALONCyber

NYS SHIELD Act



It is important to know that **you don't need to be in New York** to be **affected by the NYS SHIELD Act.**

Technical safeguards

- Assessing risks in your network and software design
- Examining risks in your information processing, transmission, and storage
- Implementing measures to detect, prevent, and respond to system failures
- Regularly testing and monitoring the effectiveness of key controls, systems, and procedures

Physical safeguards

- Assessing the risks of private data storage and disposal
- Detecting, preventing, and responding to intrusions
- Developing protections against unauthorized access to or use of private information during or after collection, transportation, and destruction or disposal of the information
- Disposing of private information within a reasonable amount of time after it is no longer needed by erasing electronic media, so information can no longer be read or reconstructed

Must My Business Comply with the SHIELD Act?

If you or your company owns or licenses computerized data that includes private information of a resident of New York State, then, yes. It is important to know that you don't need to be in New York to be affected by the NYS SHIELD Act. You don't even have to do business in New York. You just need to own or license private information of a New York State resident.

If you do, this breach notification law applies to your business, even if you're not in a regulated industry, such as retail, financial, healthcare, or certain service industries. If you are in a regulated industry and are certified compliant with the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), the Gramm-Leach-Bliley Act (GLBA), or the NYS Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500), you may already be compliant with the SHIELD Act.

AVALONCyber

NYS SHIELD Act

After a breach, you should talk to your attorney or contact a lawyer who specializes in data privacy.

When Do I Need to Report a Breach?

The new law goes beyond reporting a breach in which information was acquired. Now, if there are "indications that the information was viewed, communicated with, used, or altered (e.g., ransomware) by a person without valid authorization or by an authorized person," you must report the incident to your New York State resident customers.

If the incident affects over 500 residents of New York, your business must provide the written determination to the NYS Attorney General within ten days after the determination. If notice of the security breach is made to affected people according to the breach notification requirements under GLBA, HIPAA, HITECH, and/or NYDFS 23 NYCRR Part 500 (or any other data security rules, regulations, or statutes administered by federal or New York State government), no further notice to those people is required as part of the SHIELD Act. However, a notice should still be provided to the NYS Attorney General, the Department of State, the Division of State Police, and consumer reporting agencies.

If you are required to provide notification of a breach, including breach of information that is not "private information" as defined by the SHIELD Act, to the Secretary of Health and Human Services pursuant to HIPAA or HITECH, you must provide notification to the NYS Attorney General within five business days of notifying the Secretary.

After a breach, you should talk to your attorney or contact a lawyer who specializes in data privacy. Additionally, reach out to a cybersecurity company, as their experts can assist you immediately following the breach and guide you through recovery.

NOTE: If private data was inadvertently disclosed by someone with the proper access to that data and it has been determined that this will not result in the misuse of that data or emotional or financial harm, you must document this and keep it on file for five years, but do not have to report the breach.

What If I Don't Disclose a Breach?

If you fail to report a breach that resulted in access to private data by someone without authorization, two things could happen:

AVALONCyber

NYS SHIELD Act

- For data breach notification violations that are not reckless or knowing, the court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses; or,
- For knowing and reckless violations, the court may impose penalties of the greater of $5,000 or up to $20 per instance with a cap of $250,000.

Your company will be affected financially in either scenario, so it makes sense to minimize business and reputational risk and report all breaches as soon as possible.

I'm a Small Business Owner. Do I Still Need to Comply?

Your **cybersecurity program** should be appropriate for the **size and complexity** of your **business.**

In a word: Yes. The law states that if you have fewer than 50 employees and generated less than $3 million in gross annual revenue in each of the last three fiscal years, or less than $5 million in year-end total assets, you need to comply with the NYS SHIELD Act, but your cybersecurity program should be appropriate for the size and complexity of your business. You still need to implement appropriate administrative, technical, and physical safeguards, but they should match the scope of your business's activities, as well as the sensitivity level of the personal and private information you collect from or about your customers.

What If I Don't Set Up an Information Security Compliance Program?

If you fail to execute a SHIELD-compliant notification and cybersecurity program, the NYS Attorney General may bring an action to obtain civil penalties. If you or your business violates the notification requirements of the SHIELD Act, knowingly or recklessly, the court may impose a civil penalty of the greater of $5,000 or up to $20 per instance of failed notification, up to $250,000.

Keep in mind, that in addition to heavy fines, your company could experience additional problems, including a damaged reputation, which could drive away partners, vendors, and customers.

It's clear that a compliant cybersecurity program is a necessity if

NYS SHIELD Act

The **NIST CSF** is one of a few excellent frameworks that can be utilized for **developing or improving security operations,** as it is **proactive, rather than reactive.**

you want to maintain your business interactions with New York State residents.

Now, we'll move on to what your company needs to do to comply with the NYS SHIELD Act.

How to Comply with the NYS SHIELD Act

Setting up a cybersecurity program for your business is no small undertaking. You have to conduct an assessment of your IT environment to see where gaps may exist, write policies, provide training, review risks, build a team, possibly find and vet vendors to work with, etc. Even if you already have a robust program in place, keeping it current and ensuring that it's compliant with government or industry regulations, is challenging as well.

The first thing to do when building or updating your cybersecurity program is review your current privacy and security policies. If they already fall in line with the SHIELD Act requirements, you're all set. If not, you will need to update the documentation to ensure the program's policies and procedures meet the reasonable safeguards the new law requires. Once you have policies stating 'what' is required and procedures clarifying 'how' those requirements are implemented, you can work to ensure that those items are operating effectively within your environment.

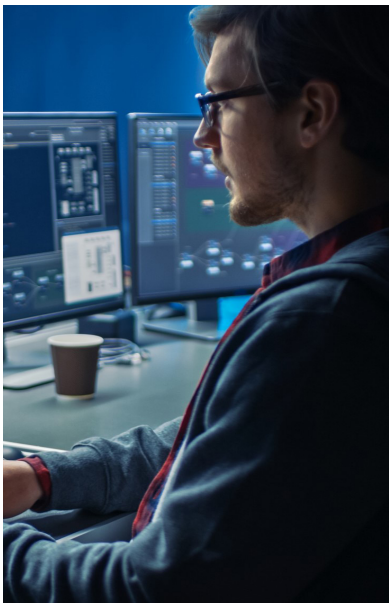
Map to a Framework

For your cybersecurity program to be deemed "reasonably safe," it should be mapped against a recognized framework. A framework is a series of documented processes used to define cybersecurity policies and procedures, such as the NIST Cybersecurity Framework (CSF), which was established by the U.S. National Institute of Standards Technology (NIST).

The NIST CSF is one of a few excellent frameworks that can be utilized for developing or improving security operations, as it is proactive, rather than reactive. Think of it as a recipe for success for a strong, secure cybersecurity program. It can, however, be tricky to implement on your own.

To help map your cybersecurity program to a framework, you may want to bring a chief information security officer (CISO) on board or

NYS SHIELD Act



Knowing exactly **what you need to secure and why,** helps you decide **how to protect it.**

use a third-party provider. If that's not in the budget, and it probably isn't for most small to medium-sized businesses, you can hire a virtual CISO, or vCISO.

A vCISO will guide you through the framework process and help you select the programs and services – like vulnerability assessments, training, monitoring, and incident response planning – that you need to keep your data safe and your business compliant.

Components of a Successful Cybersecurity Program

Risk Assessments

A risk assessment helps you determine what your company's potential threats and vulnerabilities are regarding the confidentiality, integrity, and availability of systems, assets, and processes, and which strategies you need to develop to mitigate the risk.

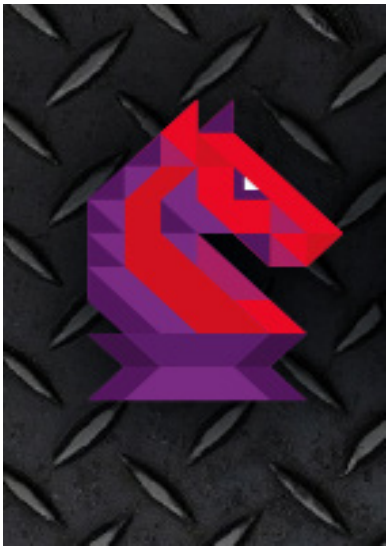
Knowing exactly what you need to secure and why, helps you decide how to protect it. Once you discover the gaps or events that are more likely or impactful, you can address them. This could include developing new policies and controls, investing in new tools or people, or reviewing current controls around a given risk area more frequently to ensure it is still appropriate. Avalon Cyber can perform a risk assessment of your IT assets to help you gain an increased awareness of your organization, reduce the chances of a breach, and avoid regulatory issues, like for instance, the SHIELD Act.

Policymaking

Developing policies for your cybersecurity plan may seem like an overwhelming task. Where do you even begin? Luckily, there are many online resources, such as NIST.gov/cyberframework. There you'll find valuable information about the NIST framework, including uses and benefits, references, tools (including baseline policy language), and a roadmap to follow when creating or updating your security program. The SANS Institute is another fantastic resource where you can find written policies on remote access, software installation, data breach response, and even one that instructs employees about keeping a clean desk (to ensure that confidential material is locked up when not in use, rather than laying out in the open). The establishment of clear, documented policies are essential to any business and make up the

AVALONCyber

NYS SHIELD Act



basis for IT/IS security programs, laws, regulations, and standards. The experts at Avalon Cyber can help create or mature policies, procedures, and audit evidence needed to confirm controls are designed and operating effectively.

Security Awareness & Training

Avalon Cyber partnered with the world's largest security awareness training and simulated phishing platform to help our clients manage the ongoing problem of social engineering. Our innovative phishing simulation and training program allows your security team to launch best-in-class, fully automated simulated phishing attacks and run comprehensive security awareness training campaigns to help educate your employees and stakeholders.

Our **KnightVision MDR** service is a **24/7/365 monitoring solution** that screens **malicious behavior at the endpoint level,** which allows a team of cyber experts to alert you and **take immediate action to shut down a potential threat.**

Managed Detection and Response (MDR)

Our KnightVision MDR service is a 24/7/365 monitoring solution that screens malicious behavior at the endpoint level – meaning, desktop computers, laptops, and virtual servers – which allows a team of cyber experts to alert you and take immediate action to shut down a potential threat. Since most small and medium-sized businesses don't have the resources to detect and respond to intrusions themselves, an MDR service allows your company access to state-of-the-art detection tools and a team of trained professionals at a much more affordable price.

Vulnerability Assessments

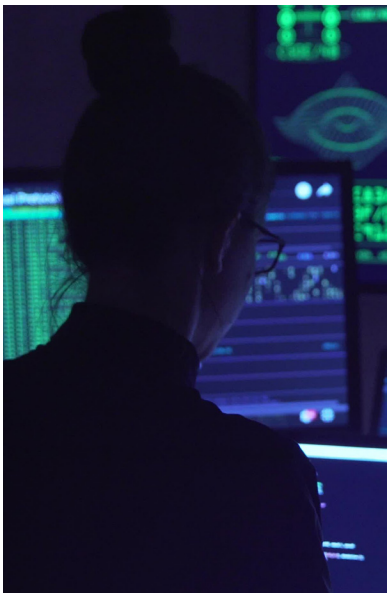
Avalon Cyber's expert engineers conduct internal and/or external scans to identify vulnerabilities and basic misconfigurations in your company's environment. Our team works with you every step of the way to develop a plan to address the most critical weaknesses and provide insights into the best way to implement improvements.

Penetration Tests

Our cybersecurity professionals safely simulate the actions of a cybercriminal targeting your network and attempt to exploit critical systems to access sensitive data. Penetration testing validates the efficiency of your currently deployed security resources and determines how well employees are following existing security policies. Once a penetration test is performed, remediation measures to help reduce exposures can be determined.

AVALONCyber

NYS SHIELD Act



For immediate assistance, call **Avalon Cyber's Incident Response Team** at:

877.216.2511

Incident Response (IR) Planning

Avalon Cyber's incident response planning service helps you identify, protect against, detect, respond to, and recover from a cyber incident. Our team can guide you through plan creation and tabletop exercises, in which we run through various threat scenarios and practice how you would respond to those threats. We can also help you implement tools and technology to manage and mitigate security incidents. Remember, since threats constantly change, your IR plan will need to be modified and tested regularly. To further assist you, we offer an IR retainer program that allows you to have a cyber team on call 24/7/365.

Managed SIEM & SOC

Our KnightVision CAM (which stands for Compliance, Alerting, and Monitoring) combines a security information and event management (SIEM) platform, which collects, aggregates, and analyzes security event log data, and a managed security operations center (SOC), i.e., a team of cybersecurity experts who respond to detected threats immediately. It's Avalon Cyber's customizable, scalable, affordable solution that addresses a range of cybersecurity challenges, including regulatory compliance, threat detection, and incident response.

Data Breach Review & Notification

If you experience a cyber incident, you need to determine whether sensitive data was exposed as soon as possible. Avalon Cyber's experts provide data mining and hosting services using industry-leading software. We can help you establish what sensitive information was affected during the cyber incident and then identify whether you need to alert agencies and/or your customers. If customer notification is necessary, Avalon Cyber offers secure print and mail services that ensure your data breach notifications are processed and delivered promptly, accurately, and with the utmost respect for data privacy.

Virtual CISO (vCISO)

In this type of engagement, Avalon Cyber steps into the role of a virtual chief information security officer (vCISO) for companies that do not have the need or means to hire and pay for a full-time resource. Typically, this hybrid approach includes a few hours every month in which our experts become an extension of your team and provide support by overseeing the design, development, and integration of your cybersecurity program.

AVALONCyber

NYS SHIELD Act

When it comes to complying with the NYS SHIELD Act, you may have a lot of work to do, but you can rest assured knowing that there are experts out there who can make this task infinitely easier for you.

This chart lists the safeguards you must implement to comply with the SHIELD Act, alongside the services Avalon Cyber provides, which will help you achieve your goals.

	Requirements	Avalon Cyber Services
Administrative Safeguards	Designating employees to coordinate a security program Identifying internal & external links Assessing the sufficiency of safeguards to control risks Training employees in security practices Selecting secure service providers Adjusting your security program with changes in your business	vCISO Services Policy & Documentation Development IT Risk Assessment Security Awareness & Training Vendor Risk Management Gap Assessments & Remediation Services
Technical Safeguards	Assessing the risks in software & network design Assessing risks in information processing, transmission & storage Detecting, preventing & responding to incidents or system failure Testing & monitoring systems, controls & procedures	KnightVision CAM KnightVision MDR Vulnerability Assessments Penetration Testing
Physical Safeguards	Assessing risks of information storage & disposal Detecting, preventing & responding to intrusions Protecting against unauthorized access or use of information Disposing of private information after it is no longer needed	IT Risk Assessments Incident Response Tabletop Exercises
Breach Notifications	Determine whether information has been acquired or accessed by unauthorized person Disclose breach to apppropriate agencies and NYS residents	Data Breach Review Data Breach Notifications

AVALONCyber

NYS SHIELD Act

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

About Avalon Cyber

Avalon Cyber is a team of highly experienced cybersecurity strategists, who follow an approach founded in our industry experiences from both commercial and military sectors. Our deep understanding of governance, security, risk management, and compliance allow us to help you build a highly resilient cyber program, while simultaneously enabling productivity and the continued success of your business.

Our team has decades of experience in digital forensics, cybersecurity incident response, IT risk management, and enterprise information security leadership, and our experts have, or previously have held, top secret government clearances and possess key industry certifications including: CISSP, OSCP, GPEN, CISM, CISA, SSCP, CCNA, CCE, CFCE, EnCE, ACE, GXPN, OSCE, GSEC, ECIH, CCSFP, and SEC+.

We work with clients, from commercial and government organizations in industries that include financial services, legal, education, healthcare, manufacturing, and telecommunications, who are looking to partner with us to achieve a greater level of data security.

AVALONCyber

QUESTIONS?

For more information on our services, visit avaloncybersecurity.com.

To set up an appointment with one of our cyber experts, call **1.877.216.2511.**