CoreProtect™
ADVANCED CYBERSECURITY PROTECTION

powered by EscapeWire Solutions®

The New York State SHIELD Act Frequently Asked Questions

Companies that do business in New York State face ever-increasing regulation that imposes stronger cybersecurity requirements and more obligations on businesses handling private and personal information. Enter, the New York Stop Hacks and Improve Electronic Data Security Act, aka the SHIELD Act

New York State had breach notification requirements previously, but The SHIELD Act broadens the scope of information that could trigger a breach notification to consumers and also imposes stronger obligations on businesses to develop, implement and maintain "reasonable safeguards" to protect the **personal information** and **private information** of New York residents.

What is Personal information?

Personal information is defined as "any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person."

What is Private information?

Under the current law, **private information** is described 2 ways:

1. Any personal information (as described above) in combination with a variety of traditional non-public personally identifiable information
2. A user name/email address in combination with a password or security question/answer that permits access to an online account.

Under the SHIELD Act private information data elements include:

- Social security number
- Driver's license number or non-driver identification card
- Account number
- Credit or debit card number in conjunction with a Security code, Access code or Password
- Any other information that permits financial account access
- Account, credit card or debit card number that permits financial account access without additional identifying information
- Biometric information defined as data generated by electronic measurements of an individual's unique physical characteristics including but not limited to Fingerprint, Voice print or Retina or iris scan

CoreProtect™
ADVANCED CYBERSECURITY PROTECTION

powered by EscapeWire Solutions®

What Constitutes a Data Breach?

The regulation upgrades the definition of a **data breach** from "unauthorized acquisition" of data to "unauthorized access" of data.

"Access" creates a broader definition of data breach since bad actors do not need to extract data, just be able to access it.

The SHIELD Act requires notification of a data breach when the compromised data is

1. Computerized data containing "private information" of a New York resident, and
2. The compromised data is "reasonably believed" to have been accessed or acquired by a person without valid authorization.

Should a breach occur, the organization must provide notice to any affected individuals via: written notice, electronic notice, phone notification, or another notification method (such as email, a public posting, or an announcement via statewide media).

What are Reasonable safeguards?

The SHIELD Act promotes risk-based security procedures that are appropriate to the size and type business:

To comply with this requirement, an entity must either:

A. Have a compliant data security program under the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), New York's DFS cyber regulations, or other applicable federal or New York cybersecurity regulations; **OR**

B. In the absence of any other data security or privacy compliance requirements, businesses must implement a "data security program" that includes the following:

Administrative Safeguards

1. Designate one or more employees to manage the data security program
2. Identify reasonably foreseeable internal and external risks
3. Assess the sufficiency of safeguards to control risks
4. Provide employee training
5. Conduct due diligence on third-party vendors to ensure they have appropriate data security programs, and require "appropriate safeguards" by contract; and
7. Adapt the program to meet evolving threats

Technical safeguards

1. Assess risks in network and software design
2. Assess risks in information processing, transmission, and storage
3. Detect, prevent, and respond to attacks or system failures
4. Regularly test and monitor the effectiveness of key controls, systems and procedures.

Physical safeguards:

1. Assess risks of information storage and disposal;
2. Detect, prevent and respond to intrusions;
3. Protect against unauthorized access to or use of private information during or after the collection, transportation and disposal of the information; and
4. Disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

Who is required to comply?

The legislation applies to any person or business that collects or stores private information of a New York Resident. Compliance is required regardless of the entity's location and whether or not it conducts business in New York State.

There is no exemption for small businesses however, the safeguards need to be "appropriate" to the size and complexity of the business and the sensitivity of the data collected from or about consumers.

What is considered a small business?

The SHIELD Act defines a **small business** as "any person or business" that meets one of the following:

A. Fewer than fifty employees;
B. Less than three million dollars in gross annual revenue in each of the last three fiscal years; or
C. Less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles.

Are there penalties for failing to comply?

The SHIELD Act does not permit a private right of action. Rather, it provides for enforcement by the state's attorney general. Any organizations that fail to comply to the provisions the NYS SHIELD could face **up to $250,000 in civil penalties**.

Summary:

The SHIELD Act covers any and all persons or entities that have the private information of New York residents regardless of size or whether they are actually located in New York. It applies to for-profits and not-for-profits. Virtually every health care provider and payor in New York is already required to abide by the HIPAA and HITECH regulations covering security of personal health information, but they must become familiar with the SHIELD Act's provisions and make appropriate revisions to their data security compliance policies and procedures. Vendors and contractors with which private information is shared must also be in compliance with the SHIELD Act's requirements.

The full text of SHIELD Act (S.5575B/A.5635) can be viewed here »

CoreProtect™
ADVANCED CYBERSECURITY PROTECTION

powered by EscapeWire Solutions®

Now that I know about NYS SHIELD, where do I start?

Whether you are building a cybersecurity program or already have one in place, it can be challenging to be sure that all the proper protocals are in place, and kept current, in order to be compliant with NYS SHIELD.

In addition to the security measures listed in the the SHIELD Act — including designating dedicated security personnel, training all employees on security practices, and conducting regular risk assessments — we recommend that companies consider the National Institute of Standards Technology (NIST) Cybersecurity Framework to help identify "reasonable safeguards." The NIST Framework is a thorough and flexible set of best practices intended to guide organizations through the steps of creating a cybersecurity program.

The NIST Framework Core consists of five concurrent and continuous Functions:

IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:

- Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.
- Steps to take to protect against an attack and limit the damage if one occurs.

PROTECT

Once you've identified the different risks associated with your organization, you need to devise a strategy to protect yourself from these risks.

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

DETECT

- Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.
- Investigate any unusual activities on your network or by your staff.
- Check your network for unauthorized users or connections.

CoreProtect™
ADVANCED CYBERSECURITY PROTECTION

powered by EscapeWire Solutions®

RESPOND

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

Test your plan regularly

RECOVER

After an attack:

- Repair and restore the equipment and parts of your network that were affected.
- Keep employees and customers informed of your response and recovery activities
- Make improvements to processes, procedures and technologies.

CoreProtect™ Advanced Cybersecurity Protection

Cybersecurity Protection and Compliance Management

As you can see, there are many factors involved in implementing a compliant cybersecurity program. Most SMB owners simply don't have the time or expertise to effectively manage their cybersecurity let alone NYS SHIELD Act compliance. That's why EscapeWire developed our CoreProtect Advanced Cybersecurity Protection Program. CoreProtect follows the NIST Cybersecurity Framework and includes the most advanced cybersecurity for your networks, data and devices. Plus, with CoreProtect SMBs like yours have access to the assesments, documentation, policy creation, staff training management, and testing components that address compliance to NYS SHIELD.

For over 17 years EscapeWire has worked with SMBs from a wide variety of industries to address their technology and cybersecurity needs. If you have questions or would like assistance becoming NYS SHIELD Act compliant, contact us today. We will work with you to achieve complaince while meeting the unique needs of your business.