NYS SHIELD ACT

TPCA TECHNOLOGY GROUP
THE POWER OF LISTENING

WHAT IS THE SHIELD ACT?

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act is a New York State law that mandates the implementation of a data security program, including proactive and ongoing measures such as risk assessments, monitoring, workforce training, and incident response planning and testing.

WHO IS REQUIRED TO FOLLOW THIS ACT?

All employers, companies and organizations (private, public and non-profit), regardless of location, that collect or maintain personal or private information of New York State residents.

WHAT IS CONSIDERED PERSONAL INFORMATION?

Any information that can be used to identify a person, such as name, number, personal mark, or other identifier.

WHAT IS CONSIDERED PRIVATE INFORMATION?

Any personal information in combination with any of the following data elements (when either the data element or the combination of the personal information and the data element is either not encrypted or is encrypted with an encryption key that has also been accessed or acquired):

- Social security number
- Driver's license number or non-driver identification card number
- Account number, credit or debit card number in combination with any security code, access code, password or other information that would permit access to an individual's financial account
- Biometric information, such as fingerprint, voice print, retina or iris image
- Email address or a username in combination with a password or security question and an answer that would permit access to an online account

WHAT IS REQUIRED IN ORDER TO ACHIEVE COMPLIANCE OF THIS ACT?

A data security program needs to be implemented that includes at least the following:

Administrative Safeguards

- Designates one or more employees to coordinate the security program
- Identifies reasonably foreseeable external and internal risks
- Assessment of existing safeguards in place to control the identified risks
- Trains and manages employees in the security program's practices and procedures
- Selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract
- Has a process for implementing adjustments to the security program based on business changes and/or new circumstances

Technical Safeguards

- Risk assessments of network design, software design, along with information processing, transmission and storage
- Implementation of measures to detect, prevent and respond to system failures and attacks
- Regular monitoring and testing of the effectiveness of key controls, systems and procedures

Physical Safeguards

- Prevention, detection and response to intrusions
- Assessment and protection of risks associated with the storage of information
- Disposal of information within a reasonable amount of time after it is no longer needed for business purposes by erasing that information so it cannot be read or reconstructed

ARE THERE ANY EXCEPTIONS FOR SMALLER BUSINESSES?

The SHIELD Act does ease certain regulatory burdens on smaller businesses, allowing them to scale and subsequently adopt "reasonable" administrative, technical and physical safeguards that are appropriate based on the organization's size, complexity, nature and scope of its activities, along with the sensitivity of the information collected.

According to the SHIELD Act, an organization is considered a small business if it meets any one of the following:

- Fewer than 50 employees
- Less than $3 million in gross annual revenue in each of the last 3 fiscal years
- Less than $5 million in year-end total assets in accordance with GAAP

ARE THERE ANY CONSIDERATIONS FOR BUSINESSES THAT ARE ALREADY COVERED BY OTHER ACTS OR REGULATIONS?

If businesses are covered and regulated by the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and/or the New York Department of Financial Services (DFS) cybersecurity regulations, being that these acts and regulations are considered to be more comprehensive and already include the conditions mandated by the SHIELD Act, these businesses are deemed to be in compliance with the SHIELD Act as long as they are in FULL compliance with these other acts and/or regulations.

WHAT DEFINES A BREACH AND WHAT HAPPENS IF THERE IS A BREACH?

With the SHIELD Act:

- A breach is defined as unauthorized access of data or unauthorized acquisition of data
- A data breach involving more than 500 New York State residents requires the submission of documentation to the state's Attorney General within 10 days of a breach determination
- All businesses that experience a data breach, regardless of where the business is located, must notify New York State residents whose information may have been compromised in the most expedient time possible and without unreasonable delay

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Failure to implement and maintain a compliant data security program is enforced by the New York State Attorney General and may result in the minimum injunctive relief and civil penalty of $5,000 for each violation, or $20 per failed notification for a maximum penalty of $250,000.

WHAT DOES PCA TECHNOLOGY GROUP RECOMMEND IN ORDER TO COMPLY WITH THE REQUIREMENTS OF THIS ACT?

The SHIELD Act does not mandate specific safeguards but instead states that a business will be deemed to be in compliance with this standard if it implements a data security program that includes all of the elements enumerated within the SHIELD Act. Accordingly, PCA Technology Group recommends the following to ensure compliancy:

- Cybersecurity User Awareness Education*
- Endpoint Management & Monitoring*
- Antivirus Protection*
- Anti-Malware & Anti-Ransomware Protection*
- Internal & External Vulnerability Scans*
- Multi-Factor Authentication (MFA) for Microsoft 365 Hosted Exchange*
- Comprehensive Firewall Implementation*
- Comprehensive Business Continuity & Disaster Recovery (BCDR) Implementation*
- Risk Assessments
- Advanced Security Information & Event Management (SIEM) Monitoring
- Dark Web Monitoring
- Multi-Factor Authentication (MFA) for VPN Connectivity & Other Software
- Company Password Policy
- Remote Access Policy & Procedures
- Employee Acceptable Use Policy
- New & Departing Employee Checklists
- Incident Response Plan (IRP)

* Included or provided with PCA Technology Group's Managed Services Agreement (MSA)