corsica technologies

SHIELD ACT COMPLIANCE GUIDE

The New York Stop Hacks and Improve Electronic Data Security Act or SHIELD Act, was enacted on July 25, 2019, as an amendment to the New York State Information Security Breach and Notification Act. The law went into effect on March 21st of this year. SHIELD Act requires companies to implement and maintain reasonable security measures. Affected businesses must deploy safeguards to protect the security, confidentiality, and integrity of private information of New York residents including, but not limited to, secure disposal of data. The SHIELD Act introduces significant changes including.

UPDATING THE DEFINITION OF "PRIVATE INFORMATION"

SHIELD broadens the definition of "private information" to also include biometric information, account numbers, credit/debit card numbers, username/email addresses in combination with passwords or security questions and answers.

EXPANDING THE DEFINITION OF "DATA BREACH"

SHIELD expands the definition of "breach of the security of a system" to include unauthorized access of computerized data that compromises the security, confidentiality, or integrity of private information, and it provides sample indicators of access.

EXPANDS THE PROTECTION/TERRITORIAL SCOPE

SHIELD expands the territorial application of the breach notification requirement to any person or business that owns or licenses private information of a New York resident. Previously, the law was limited to those that conduct business in New York.

IMPOSING DATA SECURITY REQUIREMENTS

SHIELD requires companies to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information. A company should implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.

SHIELD ACT'S DATA SECURITY REQUIREMENTS

The SHIELD Act does not mandate specific safeguards, but it does provide several examples of best practices that are considered reasonable administrative, technical, and physical safeguards. These examples suggest the kinds of safeguards businesses should be adopting.

ADMINISTRATIVE SAFEGUARDS focus on internal organization, policies, procedures, and maintenance of security measures that protect consumer private information. Some administrative safeguards include:

- Designating individuals or teams responsible for security programs.
- Ensuring a risk assessment process is in place. This should identify reasonably foreseeable internal and external risks and assess your safeguards in place to mitigate those risks.
- Educating employees in best security practices.
- Maintaining and practicing disaster recovery and business continuity plans.

PHYSICAL SAFEGUARDS are measures, policies, and procedures to protect your organization's electronic information systems. Some physical safeguards include:

- Preventing, detecting, and responding to intrusions.
- Protecting against unauthorized access or use of private information.
- Assessing risks of information of storage and disposal of confidential information.

TECHNICAL SAFEGUARDS are measures that protect and control access to private information. Some technical safeguards include:

- Network and software security technologies.
- Risk assessments for the organization's information processing, transmission, and storage of data.
- Regular tests and monitoring effectiveness of key controls, systems, and procedures.
- Using multi-factor authorization and deploying encryption and data loss prevention tools.

WHAT ARE THE PENALTIES FOR FAILING TO COMPLY WITH THE SHIELD ACT?

If your organization fails to implement a compliant information security program, it can result in injunctive relief and civil penalties of up to $5,000 per violation.

If a cybersecurity incident does occur and involves the private information of more than 500 New York Residents, a written notice must be provided to the New York Attorney General within ten days after the determination. Businesses that fail to comply with this breach notification requirement can be held liable for the "actual costs or losses incurred by a person entitled to notice." In addition, if the organization violates this provision, a civil penalty could be enforced—the greater of $5,000 or $20 per instance of failed notification, up to a maximum of $250,000 fee.

Are you struggling to understand everything that comes with SHIELD Act? Corsica Technologies is here to help. Our dedicated security team can answer any questions you may have or can conduct a Security Posture Review to see where you stand. Please reach out to our team either *here* or call us at (855) 411-3387.

corsica technologies