Stop Hacks and Improve Electronic Data Security Act (SHIELD Act)

General Info:

- Signed into law by NYS governor on July 25, 2019.

- Businesses should immediately begin the process to comply with the Act's requirements effective March 21, 2020.

- The law covers all employers, individuals or organizations, regardless of **size or location**, which collect private information on New York State residents.

- The law requires implementation of an information security program to protect "private information" defined as:
    - any individually identifiable information such as name, number or other identifier coupled with social security number, driver's or non-driver identification card number or account number, credit or debit card number in combination with any security code, access code, password or other information that would permit access to the individual's financial account, or biometric information (such as fingerprint, voice print, retina or iris image);
    - individually identifiable information coupled with an account number, credit or debit card number if circumstances exist wherein such number could be used to access an individual's financial account even without additional identifying information, or a security code, access code or password; or
    - a username or email address in combination with a password or security question and answer that would permit access to an online account.

- Small businesses of fewer than 50 employees, less than three million dollars in gross revenues in each of last three fiscal years, or less than five million dollars in year-end total assets may scale their data security program according to their size and complexity, the nature and scope of its business activities and the nature and sensitivity of the information collected.

- Organizations that are covered by and in compliance with the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), and/or the New York State Department of Financial Services cybersecurity regulations shall be deemed in compliance with the SHIELD Act.

- Failure to implement a compliant information security program is enforced by the New York State Attorney General and may result in injunctive relief and civil penalties of up to $5,000 imposed against an organization and individual employees for "each violation."

- The law broadly requires that “any person or business” that owns or licenses computerized data which includes private information of a New York State resident “shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.”

Reasonable Safeguards:

- “Reasonable Safeguards” are categorized as either (1) Administrative, (2) Technical, or (3) Physical.

SHIELD Act Requirement	Type of Safeguard	TAG Offering(s)
Designate one of more employees to coordinate the security program	Administrative	None
Identify reasonably foreseeable internal & external risks and assess the sufficiency of safeguards in place to control the risks	Administrative	Risk Assessment
Train and manage employees in the security program practices and procedures	Administrative	Security Awareness Training
Select Service Providers capable of maintaining appropriate safeguards and require those safeguards by contract	Administrative	Third Party Service Provider Management Policy
Assess risks in network and software design	Technical	Risk Assessment Network Assessment Remediation Work
Assess risks in information processing, transmission and storage	Technical	Risk Assessment Network Assessment Remediation Work
Detects, Prevents and Responds to attacks or system failures	Technical	Artic Wolf Managed Services Incident Response Policy Incident Response Plan Firewall, IDS, IPS Anti Virus / Anti Malware
Regularly tests and monitors the effectiveness of key controls	Technical	Vulnerability Assessment Penetration Testing
Protects against unauthorized access to or use of private information	Physical	Access Control Multi-Factor Authentication Password Manager Encryption