

New York SHIELD Act

S5575B

NY SHIELD Act requires businesses to implement reasonable data security safeguards and breach notification for New York residents' personal information.



What it is

The New York SHIELD Act (S5575B) is a state data protection and cybersecurity regulation that requires organizations to implement reasonable safeguards to protect the private information of New York residents. Its primary purpose is to reduce the risks of data breaches and enhance accountability for the security of personal data held by businesses and other covered entities.

Enacted by the State of New York, the SHIELD Act applies to any organization—regardless of location—that owns or licenses private information of New York residents. The law covers areas including administrative, technical, and physical security controls, expanding the definition of protected data and mandating prompt breach notifications. It addresses cybersecurity risk management and compliance oversight to strengthen personal data protection.

At a glance

PUBLISHER Office of the New York State Attorney General	TYPE Regulation	VERSION 2019
EFFECTIVE October 23, 2019	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION New York	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY Moderate

Source: <https://www.nysenate.gov/legislation/bills/2019/S5575>

Why it matters

- Strengthen data security practices** Encourage the adoption of administrative, technical, and physical safeguards to protect sensitive personal information from unauthorized access.
- Improve incident response readiness** Support prompt detection, reporting, and remediation of security incidents involving New York residents' private data.
- Enhance regulatory compliance support** Enable organizations to demonstrate adherence to state privacy laws, reducing legal exposure and enforcement risks.
- Increase audit and reporting readiness** Provide clear criteria for documenting security practices, making regulatory audits and internal assessments more efficient.

How SmartSuite supports NY SHIELD

Reasonable Security Controls Framework

Structure administrative, technical, and physical safeguards required to protect private information.

Data Inventory and Classification

Track private information types, storage locations, and systems subject to SHIELD Act requirements.

Risk Assessment and Safeguard Implementation

Manage risk assessments and track implementation of required security measures across systems.

Access Governance and Data Protection Controls

Manage user access, authentication, encryption, and secure handling of sensitive data.

Security Incident and Notification Obligation Tracking

Track security incidents and manage notification obligations to affected individuals and regulators.

Data Protection Compliance Reporting

Provide dashboards showing control effectiveness, breach readiness, and compliance with New York data protection requirements.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GDPR

HIPAA

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

State of New York – SHIELD Act (S5575-B) Legislative Text

Provides the full official statute text of the Stop Hacks and Improve Electronic Data Security Act as enacted.

legislation.nysenate.gov/pdf/bills/2019/S5575B

New York State Attorney General – SHIELD Act Compliance Page

Outlines official compliance requirements and breach notification procedures under the SHIELD Act.

ag.ny.gov/resources/organizations/data-breach-reporting/shield-act

New York Department of Financial Services – Cybersecurity Regulation Q&A on SHIELD Act Amendments

Provides official clarification regarding SHIELD Act amendments and notification requirements under 23 NYCRR § 500.1, § 500.17.

dfs.ny.gov/industry_guidance/cybersecurity

State of New York Department of State – Cybersecurity Advisory and Enforcement (DOS Portal)

Offers official guidance on data security obligations for New York entities under state law, including SHIELD-related enforcement context.

dos.ny.gov

Frequently asked questions

What is the New York SHIELD Act used for?

The SHIELD Act is designed to enhance the protection of private information for New York residents by requiring businesses to implement reasonable cybersecurity safeguards. It establishes data security requirements and expands the definition of private information subject to breach notification rules. The Act aims to reduce the risk of data breaches and improve incident response.

Is compliance with the SHIELD Act mandatory for organizations?

Yes, compliance with the SHIELD Act is mandatory for any business that owns or licenses private information of New York residents, regardless of whether the company is physically located in New York. Failure to comply can result in regulatory enforcement and significant penalties.

Who does the SHIELD Act apply to?

The SHIELD Act applies to all entities, whether large or small, that handle computerized private information of New York residents. This includes for-profit and not-for-profit organizations as well as third-party vendors processing data on behalf of covered entities.

What are the key requirements of the SHIELD Act?

The SHIELD Act requires organizations to implement "reasonable" administrative, technical, and physical data security safeguards. Key artifacts include written security programs, risk assessments, designated security personnel, employee training, and incident response procedures. The law also expands the definition of reportable data breaches.

How should organizations implement the SHIELD Act's security controls?

Organizations should conduct risk assessments to identify threats, develop policies and procedures aligned with the Act's safeguards, and assign responsibility for managing data security. Controls must be appropriate to the company's size, complexity, and the sensitivity of the data processed. Regular reviews and updates are encouraged to maintain effectiveness.

How does the SHIELD Act relate to other frameworks such as HIPAA or GLBA?

The SHIELD Act recognizes "compliant regulated entities" that already follow information security regulations such as HIPAA or GLBA as meeting its requirements. However, organizations are still required to comply with notification obligations and should ensure alignment between frameworks to address overlapping responsibilities.

What are the ongoing compliance requirements under the SHIELD Act?

Ongoing requirements include maintaining and updating security policies, continually monitoring risks, training staff, tracking incidents, and reporting breaches to affected individuals and, in some cases, to regulators. Organizations should regularly assess the effectiveness of their security measures and adapt them as threats evolve.

How would SmartSuite support New York SHIELD Act compliance?

SmartSuite can support SHIELD Act compliance by providing modules for risk tracking, documenting and managing required controls, and organizing evidence of compliance activities. The platform enables audit readiness through centralized policy management, facilitates incident tracking, and generates reports needed for regulatory reviews and breach notifications.

License included / downloadable: Yes The New York SHIELD Act (S5575B) is published by the New York State Legislature and is publicly available via official state government publications and websites. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-new-york-shield-act-s5575b-stop-hacks-improve-electronic-data-security