Preparing for a SHIELD Act Safeguards Review

Map private information, responsible staff, service providers and safeguard records to prepare for a focused business review.

Edition 2026-11-03 · Online at newyorkcomputerforensics.com/guides/shield-act-review/

The first task is to identify the review you are preparing for. The SHIELD Act establishes data security obligations, but a request described casually as a PII audit may instead come from a customer, insurer, regulator, transaction team or internal auditor. Obtain the actual request, applicable standards, entity scope and period. This guide focuses on the reasonable safeguards framework in New York General Business Law 899-bb and the related private information definition in 899-aa. [New York General Business Law 899-bb] [New York General Business Law 899-aa]

Identify the private information and the people responsible for it

Map the information the organization owns or licenses, the people it concerns and the systems and providers that handle it. Identify the business owner and the legal basis for the scope determination. Keep the statutory term private information distinct from broader internal labels such as PII. A useful inventory explains the actual data elements, why the organization retains them and who can authorize access or disposal.

The current statutory definition includes specified combinations involving identifiers and sensitive data, as well as online account credentials. The 2025 revision also includes medical and health insurance information. Assess the actual data against the current wording, including the encryption conditions. Information stored by a vendor is assessed the same way. [New York General Business Law 899-aa]

Organize the safeguards record around how the business operates

The statute describes administrative, technical and physical safeguards. Use those categories to organize the record, then make each item specific to the business. Identify the person coordinating the security program, foreseeable risks, existing safeguards, staff training, provider arrangements and the process for adjusting the program after changes. Record who owns each control and what evidence will demonstrate its operation. [New York General Business Law 899-bb]

For technical preparation, request a scoped view of identities, access restrictions, relevant logging, system maintenance, recovery arrangements and control testing. For physical preparation, examine how devices and records are stored, transported and disposed of. Keep actual evidence separate from a written policy, and pair the disposal policy with the record showing how each retired computer was handled.

Build a data flow and provider register

Follow representative information from collection through use, sharing, storage and disposal. Include email, cloud collaboration, business applications, backups, paper records and exported files where relevant. Identify the organizations and people who can change access or retention. Note personal devices, shared accounts

© 2026 Global Digital Forensics, Inc. All rights reserved.

and informal transfer methods that sit outside the central system inventory.

For providers, identify the services used, the relevant data, contractual safeguards and available assurance evidence. Read the coverage and exceptions in each report against the customer's own configuration. Where the organization and provider share responsibility, record the boundary clearly. Ask who can preserve records, assist with an incident and demonstrate deletion when the service ends.

Apply small business treatment accurately

Section 899-bb provides a proportionate approach for qualifying small businesses, tied to factors including size, complexity, activities and information sensitivity. The technical record should show why the chosen safeguards fit the actual risks. [New York General Business Law 899-bb]

A small organization shows accountable ownership and evidence that important protections work across fewer systems and people. A concise register and a practical review process fit that scale. Keep open gaps and the plan for addressing them visible to the people who can make the necessary decisions.

Prepare an incident decision process that keeps pace with the facts

Identify how suspected unauthorized access is reported, who can authorize containment and who determines notification obligations. Preserve a factual chronology and the relevant records while the notification requirements are evaluated. Access is established from the records that capture it, read alongside alerts and file locations.

Section 899-aa requires notice to affected New York residents within 30 days after discovery of the breach, with notice to the Attorney General, the Department of State and the State Police, to the consumer reporting agencies when more than 5,000 New York residents are notified and, for a DFS covered entity, to DFS under 23 NYCRR 500.17, so the technical review moves at the same pace. Bring the trigger, the recipients, any exceptions and law enforcement considerations to the owner of the notice decision as soon as the facts allow. [New York General Business Law 899-aa]

Produce a practical review package and improvement record

Prepare the scope statement, data flow register, control owner list, relevant policies, provider record and representative operating evidence. Add an exceptions register with a reason, owner, action and review date for each open item. Identify documents based on interviews or provider statements and distinguish them from records the team inspected directly. Keep sensitive information out of broad circulation and use an agreed secure method for necessary sharing.

Before delivery, check that a reviewer can connect each material assertion to its source. Retain the delivered version and the decisions about remediation or accepted risk. The result gives the organization and its advisers a clear factual account on which to base compliance and notification decisions.

Information Gathering Q&A Checklist

Use this Q&A with the people who own the systems and the relevant legal or business decisions. Mark unknown or not applicable answers explicitly. Record an owner, a confirming source and the date.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Record who controls access to each source and how a secure handoff can be arranged, and keep completed copies with the matter records the company maintains.

What review are you preparing for, and who asked for it?

Record whether the request comes from a customer, insurer, regulator, transaction team or internal audit, with the standard, entity scope and period it names.

Answer:

Owner, source, date and open questions:

What data elements and New York resident information are within the reviewed scope?

Map each data element against the current section 899-aa definition, including biometric, medical and health insurance information and online account credentials. [New York General Business Law 899-aa]

Answer:

Owner, source, date and open questions:

Which systems, providers and paper records hold that information?

List business applications, email, cloud storage, backups, exported files and paper records, with the owner of each.

Answer:

Owner, source, date and open questions:

Who coordinates the security program, and who owns each safeguard?

Name the coordinator and the owners of administrative, technical and physical safeguards, and the evidence each owner can produce. [New York General Business Law 899-bb]

Answer:

Owner, source, date and open questions:

Which service providers handle private information, and what do their contracts require?

Record the provider, the data, the contractual safeguards and the assurance reports you hold.

Answer:

Owner, source, date and open questions:

© 2026 Global Digital Forensics, Inc. All rights reserved.

How are devices, media and paper records disposed of, and where is the proof?

Collect disposal records, certificates and the person who approves retirement of equipment.

Answer:

Owner, source, date and open questions:

Does the business qualify as a small business under section 899-bb?

A small business has fewer than fifty employees, less than three million dollars in gross annual revenue in each of the last three fiscal years or less than five million dollars in year end total assets. Record which test applies and how the safeguards are scaled to it. [New York General Business Law 899-bb]

Answer:

Owner, source, date and open questions:

Who decides breach notification, and how fast can the facts be assembled?

Name the decision makers and the path to notify affected residents within 30 days of discovery, the Attorney General, the Department of State, the State Police, the consumer reporting agencies when more than 5,000 residents are notified and, for a DFS covered entity, DFS. [New York General Business Law 899-aa] [NYDFS Cybersecurity Regulation]

Answer:

Owner, source, date and open questions:

Primary sources and further reading

Sources checked November 3, 2026.

1. New York General Business Law 899-bb https://www.nysenate.gov/legislation/laws/GBS/899-BB
2. New York General Business Law 899-aa, current 2025 revision https://www.nysenate.gov/legislation/laws/GBS/899-AA
3. New York Attorney General SHIELD Act overview https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
4. NYDFS Cybersecurity Regulation, 23 NYCRR Part 500, including notice under 500.17 https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500

© 2026 Global Digital Forensics, Inc. All rights reserved.

Scope Your Assessment

The first call is a free consultation with a senior security lead. We review the systems, the review or audit you face and its timing, and recommend the assessment depth that answers it. Requests are handled in confidence.

Call (800) 868-8189, 24/7 · New York office (212) 561-5860

Email info@evestigate.com or request your consultation at newyorkcomputerforensics.com/contact.

© 2026 Global Digital Forensics, Inc. All rights reserved.