SmartSuite

Framework / Financial Services Regulation / Global Privacy Regulations

South Carolina Insurance Data Security Act (SC IDSA)

The South Carolina Insurance Data Security Act (S.C. Code Title 38, Chapter 99) requires insurance licensees to run a written security program and report cybersecurity events in 72 hours.



What it is

The South Carolina Insurance Data Security Act (2018 Act No. 171, codified at S.C. Code Title 38, Chapter 99) is the state law that requires every licensee of the South Carolina Department of Insurance to run a written information security program, investigate cybersecurity events and notify the Director of Insurance within 72 hours of determining that a qualifying event has occurred. It has been in effect since January 1, 2019, with the information security program required from July 1, 2019 and third-party service provider oversight from July 1, 2020.

At a glance

PUBLISHER
South Carolina General Assembly (2018 Act No. 171); enforced by the South Carolina Department of Insurance

TYPE
Regulation

VERSION
2018 Act No. 171 (H.4655), S.C. Code Title 38, Chapter 99, as amended by 2019 Act No. 6

EFFECTIVE
January 1, 2019 (information security program by July 1, 2019; third-party provider oversight by July 1, 2020)

DOMAIN
Financial Services Regulation

FAMILY
Global Privacy Regulations

REGION
South Carolina

INDUSTRY
Insurance

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: scstatehouse.gov/code/t38c099.php

Why it matters

- **Defined terms that set the scope** Section 38-99-10 defines cybersecurity event, nonpublic information, licensee, third-party service provider and multifactor authentication, so the duties attach to specific data and specific events.
- **A written program with named measures** Section 38-99-20(D) lists eleven security measures, from access controls and encryption of nonpublic information in transit and on portable devices to audit trails and secure disposal.
- **Board and management accountability** Section 38-99-20(E) requires executive management to report in writing to the board at least annually on program status, risks, provider arrangements, test results and events.
- **A 72-hour regulatory clock** Section 38-99-40 requires notice to the Director no later than 72 hours after the licensee determines that a cybersecurity event has occurred, with thirteen content items.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports SC IDSA

Chapter 99 Requirement Library

Load sections 38-99-20(A) to (I), the eleven security measures in (D)(2) and the investigation and notice duties as requirements with owners, status and linked evidence.

Risk Assessment and Annual Control Review

Run the section 38-99-20(C) threat identification and sufficiency assessment as a record, and schedule the at-least-annual assessment of key controls, systems and procedures.

Third-Party Service Provider Oversight

Track each provider's due diligence, contractual security measures and the nonpublic information it holds under section 38-99-20(F) in Third Party Risk Management.

Cybersecurity Event Investigation and Notice

Log events, run the section 38-99-30 investigation, compute the 72-hour deadline from the determination date and assemble the thirteen section 38-99-40(B) items for the Director.

Incident Response Plan

Maintain the written plan required by section 38-99-20(H) with roles, communications, remediation and the post-event revision record.

Board Report and February 15 Certification

Assemble the annual written report to the board under section 38-99-20(E) and the domestic insurer's certification to the Director, with the five-year record retention it requires.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · GLBA Safeguards Rule (16 CFR Part 314) · 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

South Carolina Insurance Data Security Act (2018 Act No. 171)

Provides the full legal text enacting Chapter 99 of Title 38, establishing data security and breach notification requirements for insurance licensees.

scstatehouse.gov/sess122_2017-2018/bills/4655.htm

South Carolina Acts and Joint Resolutions, 2018 – Insurance Data Security Act

Provides the official published act as part of the 2018 session laws, confirming enactment, effective date, and legislative language.

scstatehouse.gov/Acts%26JointResolutions/2018/2018Acts%26JointResolutionsVolumeI.pdf

Bulletin 2020-04: Third-Party Service Provider Guidance (South Carolina Department of Insurance)

The Department's guidance for licensees on the third-party service provider requirements of the Insurance Data Security Act.

doi.sc.gov/DocumentCenter/View/12756/Bulletin-2020-04-SC-Insurance-Data-Security-Act-Third-Party-Service-Providers-Guidance

Frequently asked questions

Who is a licensee under the South Carolina Insurance Data Security Act?

Section 38-99-10(9) defines a licensee as any person licensed, authorized to operate or registered, or required to be, under South Carolina's insurance laws, which covers insurers, producers, agencies and other registrants. It excludes purchasing groups and risk retention groups chartered and licensed in another state and licensees acting as assuming insurers domiciled elsewhere. Section 38-99-70 exempts licensees with fewer than ten employees, including contractors, from the section 38-99-20 program requirement.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What must the information security program contain?

Section 38-99-20 requires a comprehensive written program based on the licensee's risk assessment, with administrative, technical and physical safeguards. The licensee designates who is responsible, identifies and assesses threats, and determines the appropriateness of eleven listed measures, including access controls, an asset inventory, encryption of nonpublic information in transit over external networks and on portable devices, secure development, multifactor authentication, testing and monitoring, audit trails and secure disposal. A written incident response plan, provider oversight and staff training complete the program.

When must a cybersecurity event be reported to the Director?

Section 38-99-40(A) requires notice no later than 72 hours after the licensee determines that a cybersecurity event has occurred, when South Carolina is the insurer's state of domicile or the producer's home state, or when the event involves nonpublic information of at least 250 South Carolina consumers and either triggers notice to another regulator or is reasonably likely to materially harm a consumer or the licensee's operations. The notice is filed electronically with the thirteen items in subsection (B) and updated as the investigation continues.

Which licensees must certify compliance each year?

Section 38-99-20(I) requires each insurer domiciled in South Carolina to submit a written statement to the Director by February 15 certifying compliance with section 38-99-20, to keep the supporting records, schedules and data for five years, and to document any areas that need material improvement together with the planned remediation. The Department of Insurance states that the first certifications were due February 15, 2020.

How does the Act relate to the NAIC model law and to HIPAA?

The Act enacts the NAIC Insurance Data Security Model Law (MDL-668), and the Department of Insurance states that South Carolina was the first state to pass it; the chapter's structure of definitions, program, investigation, notification, confidentiality and exemptions follows the model. Under section 38-99-70(A)(3), a licensee subject to HIPAA that maintains an information security program under HIPAA's rules is treated as meeting section 38-99-20 if it certifies its compliance in writing.

License included / downloadable: Yes The Act is South Carolina state law, published free in the South Carolina Code of Laws on the General Assembly's site; the platform links to the official text.

Full framework page and mappings: smartsuite.com/frameworks/south-carolina-insurance-data-security-act-sc-idsa