

South Carolina Insurance Data Security Act (SC IDSA)

South Carolina's Insurance Data Security Act mandates insurers adopt security programs and notify breaches to protect consumer nonpublic information.



What it is

The U.S. South Carolina Insurance Data Security Act is a state-level cybersecurity regulation that helps insurance companies safeguard nonpublic information and mitigate risks associated with data breaches. The regulation establishes standards for the protection of sensitive consumer data maintained by licensed insurers, agencies, and other licensees operating in South Carolina.

Enacted by the South Carolina Department of Insurance, the Act applies to all entities required to maintain licenses under state insurance laws. It sets out requirements for developing information security programs, managing third-party service providers, conducting risk assessments, and reporting cybersecurity events. Focus areas include cybersecurity controls, data protection, risk management, and incident response.

At a glance

PUBLISHER

National Association of Insurance Commissioners (NAIC)

TYPE

Regulation

VERSION

2018

EFFECTIVE

January 1, 2019

DOMAIN

Financial Services Regulation

FAMILY

Global Privacy Regulations

REGION

South Carolina

INDUSTRY

Insurance

ADOPTION MODEL

Regulatory Compliance

IMPLEMENTATION COMPLEXITY

Moderate

Source: <https://www.scstatehouse.gov/code/t38c099.php>

Why it matters

- **Strengthen data security controls** Implement robust security measures to better safeguard policyholder information from unauthorized access, loss, or misuse.
- **Enhance regulatory compliance** Align organizational practices with state-mandated requirements, supporting compliance efforts and reducing the risk of regulatory penalties.
- **Improve incident response readiness** Require timely detection of and response to security events, minimizing the impact of data breaches or cyber incidents.
- **Increase accountability and oversight** Promote essential roles and documented policies that clarify organizational responsibilities for information security and risk management.

How SmartSuite supports SC IDSA

Written Information Security Program (WISP)

Structure written information security program (WISP), policies, roles, and oversight aligned to regulatory expectations.

Risk Assessment and Safeguard Implementation

Track risk assessments and implementation of administrative, technical, and physical safeguards.

Nonpublic Information Scope and System Tracking

Track nonpublic information, systems, and processing activities subject to insurance data security requirements.

Insurance Data Access and Security Controls

Manage user access, authentication, encryption, and safeguards protecting sensitive insurance data.

Cybersecurity Event and Regulatory Notification Management

Track cybersecurity events and manage investigation, response, and regulatory notification requirements.

Insurance Cybersecurity Compliance Reporting

Provide dashboards showing security posture, incident readiness, and compliance with insurance cybersecurity regulations.

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 — Guidance for Licensees Regarding Third-Party Service Providers

Provides official Department of Insurance guidance on third-party oversight requirements under the South Carolina 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

What is the U.S. South Carolina Insurance Data Security Act used for?

The U.S. South Carolina Insurance Data Security Act establishes minimum standards for data security in the insurance industry within South Carolina. Its purpose is to protect sensitive consumer information handled by insurance licensees and ensure robust cybersecurity practices.

Is compliance with the South Carolina Insurance Data Security Act mandatory?

Yes, the Act is mandatory for all insurance licensees authorized or required to operate under South Carolina law. Noncompliance can result in regulatory enforcement actions and penalties from the state Department of Insurance.

Who does the South Carolina Insurance Data Security Act apply to?

The Act applies to all entities licensed, authorized, or registered under the South Carolina insurance code, including insurers, agents, and other licensees. Certain limited exemptions exist for licensees with fewer than ten employees or those covered by HIPAA.

What are key requirements under the South Carolina Insurance Data Security Act?

Key requirements include the development of a comprehensive information security program, routine risk assessments, implementation of safeguards to protect nonpublic information, and breach notification protocols. Licensees must also exercise due diligence in selecting and overseeing third-party service providers.

How should organizations implement the South Carolina Insurance Data Security Act?

Implementation starts with formal risk assessment and the creation of an information security program tailored to organizational risks and operations. Ongoing employee training, technical safeguards, and written incident response plans are also required components.

How does the South Carolina Insurance Data Security Act relate to other regulations like NY DFS or GLBA?

While the Act shares similarities with the NY Department of Financial Services Cybersecurity Regulation and the Gramm-Leach-Bliley Act (GLBA), it applies specifically to South Carolina insurance licensees. Organizations may leverage overlapping controls to streamline compliance with multiple frameworks.

What are ongoing compliance and reporting requirements for the Act?

Licensees must annually certify compliance to the South Carolina Department of Insurance and maintain relevant documentation and records. They are also required to notify the Commissioner within 72 hours of discovering a cybersecurity event involving nonpublic information.

How would SmartSuite support U.S. South Carolina Insurance Data Security Act compliance?

SmartSuite can help organizations manage South Carolina Insurance Data Security Act compliance by centralizing risk tracking, documenting and monitoring required controls, facilitating evidence collection for audits, and maintaining audit readiness. Its reporting tools support ongoing compliance status and regulatory notifications.

License included / downloadable: Yes South Carolina's Insurance Data Security Act statute text is publicly available on the state's official government website. License included with platform

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