SmartSuite

Framework / Cybersecurity / Other

NAIC Insurance Data Security Model Law MDL-668 (2017)

NAIC MDL-668 establishes data security, risk management, and breach notification requirements for insurance companies and related entities.

What it is

The NAIC Insurance Data Security Model Law (MDL-668) is a regulatory framework that establishes data security requirements for insurance companies and related entities to protect consumer information and reduce cybersecurity risks. Its purpose is to drive adoption of effective cybersecurity programs and incident response processes within the insurance sector.

Published by the National Association of Insurance Commissioners (NAIC), this model law is adopted by U.S. state insurance regulators seeking to enhance data protection, risk management, and regulatory compliance across insurers, agents, and other licensees. The law addresses areas including cybersecurity controls, risk assessments, oversight of third-party service providers, breach notification, and ongoing compliance obligations.

At a glance

PUBLISHER National Association of Insurance Commissioners (NAIC)	TYPE Framework	VERSION NAIC Model Law 668
EFFECTIVE 2017	DOMAIN Cybersecurity	FAMILY Other
REGION United States	INDUSTRY Insurance	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://content.naic.org/model-laws

Why it matters

- **Strengthen information security governance** Drive adoption of documented cybersecurity programs, oversight, and risk management across insurance organizations and their third-party service providers.
- **Enhance regulatory compliance** Facilitate adherence to state-level data security obligations, reducing regulatory risk and streamlining compliance reporting to insurance regulators.
- **Improve breach response capabilities** Establish incident response practices and notification procedures, enabling prompt detection, containment, and reporting of security breaches.
- **Protect consumer information** Mandate security controls that reduce the risk of data compromise, helping safeguard sensitive personal and financial data entrusted to insurers.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NAIC MDL-668

Security Program Requirements Library

Organize governance, risk assessment, safeguards, and oversight requirements.

Risk Assessments and Treatment Plans

Run periodic risk assessments and track mitigation actions through closure.

Vendor Due Diligence and Contract Management

Manage vendor due diligence, contract requirements, and ongoing monitoring.

Incident Response and Notification Workflow

Track cybersecurity events, escalation decisions, and reporting readiness.

Evidence and Examination Readiness

Centralize policies, training, testing, and operating evidence tied to requirements.

Board and Leadership Reporting

Provide program status, open issues, and risk posture reporting for governance.

Common framework mappings

CIS Controls v8.1 | EU DORA | GLBA Safeguards Rule (16 CFR Part 314) | ISO 27001:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

NAIC Insurance Data Security Model Law (MDL-668)

Defines data security requirements for insurance entities to protect consumer information.

content.naic.org/model-laws/mdl-668

NAIC Cybersecurity Guidance

Provides implementation guidance for achieving compliance with the NAIC Cybersecurity Model Law.

content.naic.org/cipr_topics/cybersecurity.htm

Frequently asked questions

What is the NAIC Insurance Data Security Model Law (MDL-668) used for?

The NAIC Insurance Data Security Model Law is designed to establish data security standards for insurance companies and related entities. Its primary purpose is to protect consumer information and mitigate cybersecurity risks within the insurance sector by mandating robust data protection programs and incident response processes.

Is compliance with the NAIC Insurance Data Security Model Law (MDL-668) mandatory?

Compliance becomes mandatory when a U.S. state adopts the NAIC Model Law into its own insurance regulations. Insurers, agents, and other licensed entities operating in those states must adhere to the specific requirements set forth by the adopted version of the law.

Who does the NAIC Insurance Data Security Model Law apply to?

The law applies to all insurance licensees, including insurers, agents, brokers, and certain third-party service providers that handle nonpublic consumer information. Its scope covers any entity regulated by state insurance departments that has access to sensitive customer data.

What are the key requirements of the NAIC Insurance Data Security Model Law?

Key requirements include developing and maintaining a written information security program, conducting periodic risk assessments, implementing appropriate cybersecurity controls, managing third-party risk, and establishing breach notification processes. Assigning clear governance responsibilities to senior leadership is also required.

How should insurance organizations implement the NAIC Insurance Data Security Model Law?

Organizations should start by conducting a comprehensive risk assessment to identify cybersecurity threats and vulnerabilities. Based on this assessment, they must implement appropriate safeguards, train personnel, monitor controls, update policies regularly, and prepare formal incident response and notification procedures.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does the NAIC Insurance Data Security Model Law relate to other cybersecurity frameworks?

The NAIC Model Law aligns with broader U.S. data protection standards, such as those outlined by NIST and state-level privacy laws, but is tailored specifically for the insurance industry. It complements existing frameworks by focusing on regulatory oversight, sector-specific requirements, and integration with state insurance regulations.

What ongoing compliance activities are required under the NAIC Insurance Data Security Model Law?

Ongoing compliance requires regular review and updating of the information security program, continuous risk assessment, staff training, monitoring of internal and third-party controls, and timely incident reporting to regulators. Organizations must maintain documentation as evidence of their ongoing adherence to the law.

How would SmartSuite support NAIC Insurance Data Security Model Law (MDL-668) compliance?

SmartSuite helps organizations operationalize NAIC MDL-668 by mapping legal requirements to policies and controls, managing and tracking cybersecurity risk assessments, monitoring vendor risk, collecting compliance evidence, and automating reporting. These capabilities support audit readiness and streamline ongoing compliance management for insurance organizations.

License included / downloadable: Yes The NAIC Insurance Data Security Model Law is publicly available through the National Association of Insurance Commissioners.

Full framework page and mappings: smartsuite.com/frameworks/naic-insurance-data-security-model-law-mdl-668-2017