

# Quick Guide to Understanding & Implementing Florida's Cybersecurity Incident Liability Act (CS/CS/HB 473)

## INTRODUCTION

On March 5, 2024, in response to the growing number of cyberattacks and data breaches negatively impacting Florida's organizations and consumers, Florida's Senate passed House Bill 473, the Cybersecurity Incident Liability Act. The new law aims to encourage organizations to improve their cybersecurity measures to better protect data. In return, organizations who are breached will receive increased immunity for demonstrating compliance with the measures outlined in the bill.

## UNDERSTANDING HB 473

Florida's new law requires organizations to adopt and maintain strong cybersecurity frameworks, like NIST CSF, ISO 27001/2, HITRUST, SOC 1/2, CIS 18 Controls, or adhere to industry-relevant federal laws like HIPAA, a law for healthcare providers that is designed to protect sensitive patient data.

The expectations of the bill align with cyber insurers and some regulatory bodies and ideally, will help drive down the cost of cyber insurance for organizations that show good faith efforts towards mitigating attacks.

## WHO'S INCLUDED?

**COVERED BUSINESSES:** Any business that collects, stores, or uses personal information, regardless of size.






**THIRD-PARTY PARTNERS:** Organizations that manage personal information for another business.

## WHY SHOULD YOUR ORGANIZATION ACT NOW?

A notable aspect of HB 473 includes provisions for liability protections aimed at encouraging organizations to enhance their cybersecurity practices while also recognizing the efforts of those that effectively safeguard personal information. Here's an explanation of how these protections operate:

- EXEMPTION FROM LIABILITY:** Organizations that comply with the specified cybersecurity frameworks or standards, as outlined in Florida Statutes Section 501.171(3)-(6), are not liable for cybersecurity incidents, provided they have implemented a cybersecurity program that aligns substantially with these guidelines.
- COMPLIANCE CONSIDERATIONS:** Organizations should consider factors such as the size, complexity, and nature of their operations, as well as the sensitivity of the information they handle, when assessing their adherence to cybersecurity standards.
- NO PRIVATE CAUSE OF ACTION:** The law does not establish a private cause of action, meaning individuals cannot sue entities based solely on non-compliance with this section of the law.
- EVIDENCE OF COMPLIANCE, NOT NEGLIGENCE:** Failure to align with the law's requirements is not deemed evidence of negligence or considered negligence per se. Not doing anything won't "hurt you more" which is positive, however, it makes it more difficult to claim ignorance.
- BURDEN OF PROOF:** In legal actions related to cybersecurity incidents, entities covered by the law must prove a comprehensive compliance posture to benefit from the liability protections.

## GETTING STARTED:

-  **REVIEW AND ALIGN:** Start by assessing current cybersecurity practices against one of the standards mentioned (NIST CSF, ISO 27001/2, HITRUST, SOC 1 / 2, CIS 18) and adjust as necessary to ensure alignment.
-  **MAINTAIN DOCUMENTATION:** Keep detailed records of the cybersecurity program's compliance, including risk assessments and mitigation efforts. Without proof, it will be hard to substantiate a good faith effort has taken place to secure the organization and meet the spirit of the law.
-  **EDUCATE AND TRAIN:** Ensure all team members understand their roles in maintaining cybersecurity and compliance. All departments play a role in keeping a business safe, so proof of adequate training from top to bottom personnel is required.
-  **STAY CURRENT:** Regularly review and update cybersecurity practices to keep pace with changes in standards, laws, and the threat landscape. Through business changes, turnover, regulatory winds, M&A, new product development or regional office openings there are unlimited opportunities to inadvertently sidestep a requirement.
-  **REMEDIATION:** Be proactive in identifying and mediating your organization's risk. Remember, now that these issues are formalized, they will be considered evidence if they are not addressed and ultimately lead to an incident.

## CONCLUSION:

Traditionally, organizations have viewed cybersecurity investments as an added IT expense. Florida's Cybersecurity Incident Liability Act reframes this perspective into a financial risk reduction tool. The law incentivizes businesses to invest in strengthening their cybersecurity without having to reinvent the wheel by aligning processes with recognized frameworks. Given the frequency and severity of cyberattacks and data breaches, a proactive approach today can now lead to significant cost savings down the line.

In addition to not being faced with costly lawsuits, organizations who follow the intent of the law will be well positioned to meet or exceed cyber insurance requirements, qualifying for more favorable insurance premiums. The new law positions cybersecurity as a strategic investment by incentivizing good behavior over punitive damages.

## LET SDG HELP.

SDG's team of cybersecurity experts are available to guide you through Florida's Cybersecurity Incident Liability Act requirements to help ensure your organization is poised for exemption from lawsuits stemming from a data breach. Leveraging TruOps, SDG's powerful GRC solution, along with our Compliance as a Service (CaaS) team, SDG can provide end to end support by conducting initial assessments and identifying compliance gaps, to alignment and implementing recognized cybersecurity frameworks and controls.

We work with you to ensure policies, procedures, and documentation are appropriate and available, execute regular reviews and updates of cybersecurity practices, and provide thorough education and training for personnel – all customized to align with your organization's unique requirements. Additionally, SDG's full line of services supports remediation spanning vital areas including identity access management, secure cloud computing, as well as offensive and defensive cybersecurity strategies.



■ 55 North Water Street  
Norwalk, CT 06854

■ 203.866.8886

■ [sdgc.com](https://sdgc.com)

**For More Information Contact:**

[jaike.hornreich@sdgc.com](mailto:jaike.hornreich@sdgc.com) for guidance and support.