Delaware Cybersecurity Advisory Council

Audit and Compliance Standards

Standard	Industry Impacted	Regulation
Federal Information Security Information Act (FISMA)	• Federal agencies including contractors and third-party vendors used to support agency operations. • State agencies that administer federal programs.	Requires all federal agencies to ensure the security and safety of all agency information.
Family Educational Rights and Privacy Act (FERPA)	• Schools that receive funds under an applicable program of the U.S. Department of Education.	Federal law that protects the privacy of student education records.
General Data Protection Regulation (GDPR)	• Anyone who processes the personal data of EU citizens or residents • Anyone who offers goods or services to EU citizens.	This Regulation lays down rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data.
Gramm-Leach-Bliley Act (GLBA)	• Financial institutions that offer consumers financial products or services like loans, financial or investment advice or insurance	Requires financial institutions to explain their information-sharing practices to customers and to safeguard sensitive data.
Health Insurance Portability and Accountability Act (HIPAA)	• Entities and their business associates that create, receive, use, or maintain personal health information.	Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
IRS Publication 1075	• Federal agencies • State agencies • Local agencies	Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Tax Information (FTI)
North American Electric Reliability Corporation – Critical Infrastructure Protection Committee (NERC-CIP)	• Bulk electric suppliers	NERC Standards provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
Payment Card industry Data Security Standard (PCI DSS)	• All entities that store, process and/or transmit cardholder data.	Covers technical and operational practices for system components included in or connected to environments with cardholder data.

Sarbanes-Oxley Act (SOX)	• Publicly traded companies doing business in the U.S.	Establishes financial reporting standards, including safeguarding data, tracking attempted breaches, logging electronic records for auditing and proving compliance.
Transportation Security Administration (TSA) Pipeline Security Guidelines	• Owners/operators of TSA-designated hazardous liquid and natural gas pipelines or liquefied natural gas facilities.	Requires actions necessary to protect the national security, economy and public health and safety of the United States and its citizens from the impact of malicious cyber intrusions affecting the nation's most critical gas and liquid pipelines.