N.M. Stat. Ann. § 9-27A-3

Current through all chaptered acts of the 2024 Regular Session.

Michie's ™ Annotated Statutes of New Mexico > Chapter 9 Executive Department (Arts. 1 — 29A) > Article 27A Cybersecurity Act (§§ 9-27A-1 — 9-27A-5)

9-27A-3. Cybersecurity office created; security officer; duties and powers.

A. The "cybersecurity office" is created and is administratively attached to the department of information technology. The office shall be managed by the security officer.

B. Except as required by federal law, the cybersecurity office shall oversee, in a fiscally responsible manner, cybersecurity- and information security-related functions for agencies and may:

(1) adopt and implement rules establishing minimum security standards and policies to protect agency information technology systems and infrastructure and provide appropriate governance and application of the standards and policies across information technology resources used by agencies to promote the availability, security and integrity of the information processed, transacted or stored by agencies in the state's information technology infrastructure and systems;

(2) develop minimum cybersecurity controls for managing and protecting information technology assets and infrastructure for all entities that are connected to an agency-operated or -owned telecommunications network;

(3) consistent with information security standards, monitor agency information technology networks to detect security incidents and support mitigation efforts as necessary and within capabilities;

(4) as reasonably necessary to perform its monitoring and detection duties, obtain agency system event logs to support monitoring and detection pursuant to Paragraph (3) of this subsection;

(5) in coordination with state and federal cybersecurity emergency management agencies as appropriate, create a model incident-response plan for public bodies to adopt with the cybersecurity office as the incident-response coordinator for incidents that:

(a) impact multiple public bodies;

(b) impact more than ten thousand residents of the state;

(c) involve a nation-state actor; or

(d) involve the marketing or transfer of confidential data derived from a breach of cybersecurity;

(6) serve as a cybersecurity resource for local governments;

(7) develop a service catalog of cybersecurity services to be offered to agencies and to political subdivisions of the state;

(8) collaborate with agencies in developing standards, functions and services in order to ensure the agency regulatory environments are understood and considered as part of a cybersecurity incident response;

(9) establish core services to support minimum security standards and policies;

(10) establish minimum data classification policies and standards and design controls to support compliance with classifications and report on exceptions;

(11) develop and issue cybersecurity awareness policies and training standards and develop and offer cybersecurity training services; and

(12) establish a centralized cybersecurity and data breach reporting process for agencies and political subdivisions of the state.

History

2023, ch. 115, § 3, effective July 1, 2023.

End of Document