

Nev. Rev. Stat. Ann. § 480.930

This document is current through the end of legislation from the 82nd Regular Session (2023). This document incorporates revisions received from the Legislative Counsel Bureau for NRS Chapters 1 to 220. This document is current through the end of legislation from the 34th and 35th Special Sessions (2023), subject to revision by the Legislative Counsel Bureau.

Nevada Revised Statutes Annotated > Title 43. Public Safety; Vehicles; Watercraft. (Chs. 480 — 490) > Chapter 480. Administration of Laws Relating to Public Safety. (§§ 480.010 — 480.950) > Security of Information Systems (§§ 480.900 — 480.950)

480.930. Office to prepare and update statewide strategic plan regarding security of information systems; use of information by private entity; state agencies with cybersecurity policy required to test adherence to policy by employees and submit results to Office.

1. The Office shall prepare and make publicly available a statewide strategic plan that outlines policies, procedures, best practices and recommendations for preparing for and mitigating risks to, and otherwise protecting, the security of information systems in this State and for recovering from and otherwise responding to threats to or attacks on the security of information systems in this State. The statewide strategic plan prepared and made available pursuant to this subsection must not identify or include information which allows for the identification of specific vulnerabilities in the information systems in this State.
2. The statewide strategic plan must include, without limitation, policies, procedures, best practices and recommendations for:
 - (a) Identifying, preventing and responding to threats to and attacks on the security of information systems in this State;
 - (b) Ensuring the safety of, and the continued delivery of essential services to, the people of this State in the event of a threat to or attack on the security of an information system in this State;
 - (c) Protecting the confidentiality of personal information that is stored on, transmitted to, from or through, or generated by an information system in this State;
 - (d) Investing in technologies, infrastructure and personnel for protecting the security of information systems; and
 - (e) Enhancing the voluntary sharing of information and any other collaboration among state agencies, local governments, agencies of the Federal Government and appropriate private entities regarding protecting the security of information systems.
3. The statewide strategic plan must be updated at least every 2 years.

4. A private entity may, in its discretion, make use of the information set forth in the statewide strategic plan.
5. Each agency of the State Government that has adopted a cybersecurity policy shall test the adherence of its employees to that policy on a periodic basis. Such an agency shall submit the results of the testing to the Office annually for consideration in the update of the statewide strategic plan.

History

2017, ch. 307, § 13, p. 1635, effective July 1, 2017; 2019, ch. 392, § 12, p. 2474, effective June 5, 2019.

Nevada Revised Statutes Annotated
Copyright © 2024 All rights reserved.

End of Document