

W. Va. Code § 5A-6C-3

Current through all 2024 Regular Session Legislation.

Michie's™ West Virginia Code > Chapter 5A. Department of Administration. (Arts. 1 — 12) > Article 6C. West Virginia Cyber Incident Reporting. (§§ 5A-6C-1 — 5A-6C-4)

§ 5A-6C-3. Cyber Incident reporting; when required.

- (a) Qualified cybersecurity incidents shall be reported to the Cybersecurity Office before any citizen notification, but no later than 10 days following a determination that the entity experienced a qualifying cybersecurity incident.
- (b) A qualified cybersecurity incident meets at least one of the following criteria:
 - (1) State or federal law requires the reporting of the incident to regulatory or law-enforcement agencies or affected citizens;
 - (2) The ability of the entity that experienced the incident to conduct business is substantially affected; or
 - (3) The incident would be classified as emergency, severe, or high by the U.S. Cybersecurity and Infrastructure Security Agency.
- (c) The report of the cybersecurity incident to the Cybersecurity Office shall contain at a minimum:
 - (1) The approximate date of the incident;
 - (2) The date the incident was discovered;
 - (3) The nature of any data that may have been illegally obtained or accessed; and
 - (4) A list of the state and federal regulatory agencies, self-regulatory bodies, and foreign regulatory agencies to whom the notice has been or will be provided.
- (d) The procedure for reporting cybersecurity incidents shall be established by the Cybersecurity Office and disseminated to the entities listed §5A-6C-2 of this code.

History

2021, c. 149, effective July 5, 2021.

End of Document