

WEST VIRGINIA CODE: §5a-6B-4

§5A-6B-4. Responsibilities of agencies for cybersecurity.

State agencies and other entities subject to the provisions of this article shall:

- (1) Undergo an appropriate cyber risk assessment as required by the cybersecurity framework or as directed by the Chief Information Security Officer;
- (2) Adhere to the cybersecurity standard established by the Chief Information Security Officer in the use of information technology infrastructure;
- (3) Adhere to enterprise cybersecurity policies and standards;
- (4) Manage cybersecurity policies and procedures where more restricted security controls are deemed appropriate;
- (5) Submit all cybersecurity policy and standard exception requests to the Chief Information Security Officer for approval;
- (6) Complete and submit a cyber risk self-assessment report to the Chief Information Security Officer by December 31, 2020;
- (7) Manage a plan of action and milestones based on the findings of the cyber risk assessment and business needs; and
- (8) Submit annual reports to the Chief Security Information Officer no later than November 1 of each year beginning on November 1, 2023. The report shall contain an analysis and evaluation of each agency or entity's cybersecurity readiness, ability to keep user data safe, data classifications, and other steps that the agency or entity has taken towards information technology modernization that are consistent with the objectives of §5A-6-4d and §5A-6-4e of this code.