Md. Public Utility Companies Code Ann. § 5-306

Current through all legislation from the 2023 Regular Session of the General Assembly.

Michie's™ Annotated Code of Maryland > Public Utilities (Divs. I — II) > Division I. Public Services and Utilities. (Titles 1 — 15) > Title 5. Powers, Duties, and Prohibitions. (Subts. 1 — 5) > Subtitle 3. Duties of Public Service Companies. (§§ 5-301 — 5-306)

§ 5-306. Reporting cybersecurity incidents.

(a) In this section, "zero-trust" means a cybersecurity approach:

(1) focused on cybersecurity resource protection; and

(2) based on the premise that trust is never granted implicitly but must be continually evaluated.

(b) This section does not apply to a public service company that is:

(1) a common carrier; or

(2) a telephone company.

(c) A public service company shall:

(1) adopt and implement cybersecurity standards that are equal to or exceed standards adopted by the Commission;

(2) adopt a zero-trust cybersecurity approach for on-premises services and cloud-based services;

(3) establish minimum security standards for each operational technology and information technology device based on the level of security risk for each device, including security risks associated with supply chains; and

(4)

(i) on or before July 1, 2024, and on or before July 1 every other year thereafter, engage a third party to conduct an assessment of operational technology and information technology devices based on:

1. the Cybersecurity and Infrastructure Security Agency's Cross-Sector Cybersecurity Performance Goals; or

2. a more stringent standard that is based on the National Institute of Standards and Technology security frameworks; and

(ii) submit to the Commission certification of the public service company's compliance with standards used in the assessments under item (i) of this item.

(d)

(1) Each public service company shall report, in accordance with the process established under paragraph (2) of this subsection, a cybersecurity incident, including an attack on a system being used by the public service company, to the State Security Operations Center in the Department of Information Technology.

(2) The State Chief Information Security Officer, in consultation with the Commission, shall establish a process for a public service company to report cybersecurity incidents under paragraph (1) of this subsection, including establishing:

(i) the criteria for determining the circumstances under which a cybersecurity incident must be reported;

(ii) the manner in which a cybersecurity incident must be reported; and

(iii) the time period within which a cybersecurity incident must be reported.

(3) The State Security Operations Center shall immediately notify appropriate State and local agencies of a cybersecurity incident reported under this subsection.

History

2023, ch. 499, § 1.

End of Document