# **Burns Ind. Code Ann. § 4-13.1-1-1.5**

Current through P.L. 4-2024 of the Second Regular Session of the 123rd General Assembly.

***Burns’ Indiana Statutes Annotated* > *Title 4 State Offices and Administration (Arts. 1 — 38)* > *Article 13.1 Office of Technology (Chs. 1 — 3)* > *Chapter 1 Definitions (§§ 4-13.1-1-1 — 4-13.1-1-5)***

**4-13.1-1-1.5. “Cybersecurity incident” defined.**

**(a)** “Cybersecurity incident” means a malicious or suspicious occurrence that consists of one (1) or more of the categories of attack vectors described in subsection (b) and defined on the office’s Internet web site that:

**(1)** jeopardizes or may potentially jeopardize the confidentiality, integrity, or availability of an information system, an operational system, or the information that such systems process, store, or transmit;

**(2)** jeopardizes or may potentially jeopardize the health and safety of the public; or

**(3)** violates security policies, security procedures, or acceptable use policies.

**(b)** A cybersecurity incident may consist of one (1) or more of the following categories of attack vectors:

**(1)** Ransomware.

**(2)** Business email compromise.

**(3)** Vulnerability exploitation.

**(4)** Zero-day exploitation.

**(5)** Distributed denial of service.

**(6)** Web site defacement.

**(7)** Other sophisticated attacks as defined by the chief information officer and that are posted on the office’s Internet web site.

**History**

P.L.134-2021, § 2, effective July 1, 2021.

Burns’ Indiana Statutes Annotated

Copyright © 2024 All rights reserved.

**End of Document**