# **Utah Code Ann. § 63A-16-214**

Current through May 1, 2024 of the 2024 General Session.

***Utah Code Annotated* > *Title 63A Utah Government Operations Code (Chs. 1 — 19)* > *Chapter 16 Utah Technology Governance Act (Pts. 1 — 11)* > *Part 2 Chief Information Officer (§§ 63A-16-201 — 63A-16-214)***

**63A-16-214. Zero trust architectures — Implementation — Requirements — Reporting.**

**(1)** As used in this section:

**(a)** “Endpoint detection and response” means a cybersecurity solution that continuously monitors end-user devices to detect and respond to cyber threats.

**(b)** “Governmental entity” means:

**(i)** the state;

**(ii)** a political subdivision of the state; and

**(iii)** an entity created by the state or a political subdivision of the state, including an agency, board, bureau, commission, committee, department, division, institution, instrumentality, or office.

**(c)** “Multi-factor authentication” means using two or more different types of identification factors to authenticate a user’s identity for the purpose of accessing systems and data, which may include:

**(i)** knowledge-based factors, which require the user to provide information that only the user knows, such as a password or personal identification number;

**(ii)** possession-based factors, which require the user to have a physical item that only the user possesses, such as a security token, key fob, subscriber identity module card, or smart phone application; or

**(iii)** inherence-based credentials, which require the user to demonstrate specific known biological traits attributable only to the user, such as fingerprints or facial recognition.

**(d)** “Zero trust architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy that employs continuous monitoring, risk-based access controls, secure identity and access management practices, and system security automation techniques to address the cybersecurity risk from threats inside and outside traditional network boundaries.

**(2)** This section applies to:

**(a)** all systems and data owned, managed, maintained, or utilized by or on behalf of an executive branch agency to access state systems or data; and

**(b)** all hardware, software, internal systems, and essential third-party software, including for on-premises, cloud, and hybrid environments.

**(3)**

**(a)** On or before November 1, 2023, the chief information officer shall develop uniform technology policies, standards, and procedures for use by executive branch agencies in implementing zero trust architecture and multi-factor authentication on all systems in accordance with this section.

**(b)** On or before July 1, 2024, the division shall consider adopting the enterprise security practices described in this section and consider implementing zero trust architecture and robust identity management practices, including:

**(i)** multi-factor authentication;

**(ii)** cloud-based enterprise endpoint detection and response solutions to promote real-time detection, and rapid investigation and remediation capabilities; and

**(iii)** robust logging practices to provide adequate data to support security investigations and proactive threat hunting.

**(4)**

**(a)** If implementing a zero trust architecture and multi-factor authentication, the division shall consider prioritizing the use of third-party cloud computing solutions that meet or exceed industry standards.

**(b)** The division shall consider giving preference to zero trust architecture solutions that comply with, are authorized by, or align to applicable federal guidelines, programs, and frameworks, including:

**(i)** the Federal Risk and Authorization Management Program;

**(ii)** the Continuous Diagnostics and Mitigation Program; and

**(iii)** guidance and frameworks from the National Institute of Standards and Technology.

**(5)**

**(a)** In procuring third-party cloud computing solutions, the division may utilize established purchasing vehicles, including cooperative purchasing contracts and federal supply contracts, to facilitate efficient purchasing.

**(b)** The chief information officer shall establish a list of approved vendors that are authorized to provide zero trust architecture to governmental entities in the state.

**(c)** If an executive branch agency determines that procurement of a third-party cloud computing solution is not feasible, the executive branch agency shall provide a written explanation to the division of the reasons that a cloud computing solution is not feasible, including:

**(i)** the reasons why the executive branch agency determined that a third-party cloud computing solution is not feasible;

**(ii)** specific challenges or difficulties of migrating existing solutions to a cloud environment; and

**(iii)** the total expected cost of ownership of existing or alternative solutions compared to a cloud computing solution.

**(6)**

**(a)** On or before November 30 of each year, the chief information officer shall report on the progress of implementing zero trust architecture and multi-factor authentication to:

**(i)** the Public Utilities, Energy, and Technology Interim Committee; and

**(ii)** the Cybersecurity Commission created in Section 63C-27-201.

**(b)** The report described in Subsection (6)(a) may include information on:

**(i)** applicable guidance issued by the United States Cybersecurity and Infrastructure Security Agency; and

**(ii)** the progress of the division, executive branch agencies, and governmental entities with respect to:

**(A)** shifting away from a paradigm of trusted networks toward implementation of security controls based on a presumption of compromise;

**(B)** implementing principles of least privilege in administering information security programs;

**(C)** limiting the ability of entities that cause incidents to move laterally through or between agency systems;

**(D)** identifying incidents quickly; and

**(E)** isolating and removing unauthorized entities from agency systems as quickly as practicable, accounting for cyber threat intelligence or law enforcement purposes.

**History**

2023 ch. 484, § 1, effective May 3, 2023.

Utah Code Annotated

Copyright © 2024 All rights reserved.

**End of Document**