WaTech
Washington Technology Solutions

Network Security Standard Background

New, Update or Sunset Review? Replaces IT Security Standard 141.10 (5.1-5.4)

What due diligence was conducted to determine the content of this policy/standard? If this is an update or sunset review, provide information as to what changes were made, if any, as well as reasons behind the policy/standard content.

Most of the original standard is the same. Changes were made based on workgroup and community feedback to improve clarity for what is required to secure an enterprise network that is made up of cloud services, enterprise IT application on-premises, microservices, heterogeneous platforms, edge computing devices, and other assets.

Updates to this standard draw from the Center for Information Security (CIS) Control List, NIST SP 800-207 Zero Trust Architecture, NIST SP 800-215 Guide to a Secure Enterprise Network Landscape.

What is the business case for the policy/standard?

Using network controls to protect data assets is not only an industry standard, but also common-sense measures built into existing technical solutions.

What are the key objectives of the policy/standard?

Establishes layered network security controls to ensure confidentiality, integrity, and availability.

How does policy/standard promote or support alignment with strategies?

This standard supports efficient and accountable government by strengthening IT architecture and security by creating secure, resilient and innovative technology solutions for the state. It also optimizes service delivery to provide the best customer experience possible through continuous improvement.

What are the implementation considerations?

Most requirements are not changing, just being reorganized, and clarified. However, some agencies may need training and possibly more resources to come into compliance.

How will we know if the policy is successful?

Specific: Agencies will ensure network controls are appropriately configured.
Measurable: Agencies will monitor and check that controls are implemented.
Achievable: Agencies already have tools available to achieve these goals.
Relevant: Network security is the first line of defense.
Timebound: This standard is effective when adopted.
Equitable: Network security protects all agency assets, ensuring all agencies have secure access to protected data.