WaTech
Washington Technology Solutions

Encryption Standard Background

New, Update or Sunset Review? Update.

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.

In discussion with agencies, the requirement to use FIPS mode for category 3 and 4 data may cause functionality issues with some applications. We changed this requirement to apply only when necessary by federal requirements.

What is the business case for the policy/standard?

- Encryption protects state data from exploitation by making data unreadable and unusable to unauthorized viewers.
- Encryption confirms authenticity of the data source.

What are the key objectives of the policy/standard?

The key objective of this standard is that agencies encrypt data and storage media using industry standards.

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

Encryption of data stored or in transit maintains information confidentiality and integrity, including confidential information requiring special handling. Alignment with these strategies supports compliance with statutory and regulatory requirements specific to the type of information stored or transmitted.

What are the implementation considerations?

- Agencies will need to map the risk of their data to their agencies based on classification.
- Agencies will need to select the appropriate encryption algorithm commensurate with the risk.
- Agencies will need education and support from WaTech.

How will we know if the policy is successful?

Specific: Agencies will be able to apply encryption commensurate with the risk of the information being protected.

Measurable: The SDR workload is reduced long-term because risk assessments are performed regularly.
Achievable: Agencies will map the risk and encryption needs of the different classifications of their data.
Relevant: Encryption and protection of data is increasingly important with new developments in cyber crime.
Timebound: The standard is immediately effective.
Equitable: Encrypting data protects everyone's interests.