Acceptable Use Policy Background

Replaces IT Security Standard 141.10 (2.10)

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 agency adoption and accountability.

Updates to this standard draw from NIST 800-53 Security and Privacy Controls for Information Systems and Organizations.

What is the business case for the policy/standard?

- Mitigate cybersecurity risks.
- Reduce state exposure to illegal activities.
- Maintain productivity of employees while on the network or accessing the internet.

What are the key objectives of the policy/standard?

- Outline acceptable use of state IT assets.
- Protect state IT assets and workforce from risks that may result from the inappropriate or illegal use of the state IT assets.

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

Strategic Planning | Washington Technology Solutions

This standard supports efficient and accountable government by ensuring agencies are managing IT resources comprehensively.

What are the implementation considerations?

- Agencies will need to verify existing training aligns with the policy.
- Agencies can provide additional training internally or share materials statewide.

How will we know if the policy is successful?

- Acceptable Use violations can be monitored, and statistics reported.
- Employees report that they understand the training materials.