WaTech
Washington Technology Solutions

Access Control Policy Background

New, Update or Sunset Review? Sunset Review. Replaces 141.10 6.1,6.2

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.

Changes were made based on workgroup and community feedback to improve clarity for agency adoption and accountability.

Updates to this policy draw from NIST 800-53r5 and CIS controls.

What is the business case for the policy/standard?

Controls are necessary to ensure that only authorized individuals can access information systems and data assets.

What are the key objectives of the policy/standard?

- Requires agencies to exercise principles of least privilege when providing system access.
- Requires management of user accounts on system components.

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

Access control strengthens IT security and by aligning the business need with the technical privileges given, minimizing impacts of any security breaches.

What are the implementation considerations?

There were not substantial changes that would require major changes, but agencies may need guidance and support to ensure they are applying the policy as intended.

How will we know if the policy is successful?

Specific: Agencies will use principles of least privilege when assigning permissions.
Measurable: Agencies will monitor access and keep records of changes.
Achievable: Agencies have tools available to support these standards but may need additional training.

Relevant: Access control is a tool to limit damage if a threat actor gets credentials.
Timely: The policy is effective when adopted by the state CIO.
Equitable: Agencies of all sizes are at risk for cybersecurity attacks, and all agencies can limit the risk through appropriate access controls.