WaTech
Washington Technology Solutions

Security Logging Standard Background

Replaces IT Security Standard 141.10 (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 draws from NIST Special Publication 800-92, Guide to Computer Security Log Management.

What is the business case for the policy/standard?

- Security logs are a resource for reconstructing events and business recovery activities.
- Requiring agencies to log specific information ensures records are available when needed.

What are the key objectives of the policy/standard?

- Safeguard the resources used to detect, identify, and respond to security events, policy violations, and fraudulent activity.

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

This standard strengthens IT Architecture and security by ensuring that agency environments, and those environments which interconnect agencies to the State Government Network, maintain records of security events that may cause harm to state resources.

What are the implementation considerations?

- Agencies may need additional training and support on security log transmittal.
- Agencies will need to review and verify their security logging procedures align with this standard.

How will we know if the policy is successful?

- WaTech enterprise Security Information Event Management (SIEM) system will indicate the transmittal of security logging data.
- Agencies will possess up-to-date procedures that reflect the requirements of this standard.