JAY INSLEE
Governor

STATE OF WASHINGTON

# Office of the Chief Information Officer

1500 Jefferson Street SE • Olympia, Washington 98504-1501

November 21, 2017

**TO:** Agency Heads
Agency CIOs

**FROM:** Rob St. John
Acting State Chief Information Officer

**SUBJECT: NEWLY ADOPTED TECHNOLOGY POLICIES/STANDARDS**

On November 9, 2017, the Policy and Portfolio Subcommittee of the Technology Services Board (TSB) recommended approval of several policies and standards. Based on this recommendation, these policies/standards have been adopted, pending approval by the full TSB. The adopted policies and standards are now posted on the Office of the Chief Information Officer (OCIO) website at www.ocio.wa.gov and are in effect.

**Project Approval and Oversight Policy**
An interim change to Policy 121 – IT Investments Approval and Oversight Policy formalizes the recent adoption of a new IT investment assessment tool. With this new tool, the terminology for final assessment results changes. Rather than being a Level 1, 2 or 3 project, an investment is either 'under oversight' or 'not under oversight.' The material clarifies that the OCIO can independently escalate concerns to a project sponsor or agency head when necessary.

**Project Go-Live Readiness Decision Governance Standard**
Premature implementation of a solution can create issues that could have been avoided. Examples are disruption to the business, dissatisfied users, unserved customers, negative press coverage and exposure to legal risk. Among other things, Standard 121.10 – Project Go-Live Readiness Decision Governance requires projects under oversight to define go-live criteria early in the project and assign responsibility for collecting and tracking go-live data. It identifies the Executive Sponsor as the person to make the go-live decision in consultation with the Steering Committee. Because some projects have a higher profile or potential for impact, the standard notes projects may be required to brief the OCIO prior to go-live.

The OCIO Consultants will work with in-flight projects to determine how to apply this new standard with a goal of having all projects compliant by May 5, 2018.

**Security Standard Updates**

Standard 141.10 – Security Information Technology Assets is updated to raise awareness of where and when the standards apply, introduce new encryption requirements to further protect the states most confidential data and to otherwise maintain alignment with IT security. The encryption requirements have been updated such that all systems storing or processing Category 3 or 4 data outside the State Governmental Network (SGN), or any new system storing or processing Category 3 or 4 data within the SGN, implement encryption. While many agencies are already moving in this direction, until encryption becomes truly ubiquitous, agencies may need to allocate more money and staffing resources to meet the updated requirements. You may wish to consult with your agency Security Officer for an assessment of potential agency impacts and actions.

**NG 9-1-1 Geospatial Data Standard**

New Standard 161.07 – NG9-1-1 Geospatial Data adopts the National Emergency Association data standard used to coordinate all Next Generation (NG) 911 programs across the country. Use of this standard assists 911 dispatch to locations that cross jurisdictional boundaries or used non-landline communications to report emergencies. The Military Department has primary responsibility for ensuring standards are met in the Emergency Services IP Network, the backbone of the NG911.

**Commonly Used Software Policy and Standard**

Policy 186 – Commonly Used Software Product Retirement Policy and Standard 186.10 – Commonly Used Software Standard have been updated as a result of a sunset review. While agencies should generally use software that is supported by the manufacturer, the policy and standard focus on those products used widely across state government. You may wish to consult with your agency CIO to understand agency use of unsupported software and management of associated risks until the software can be upgraded or replaced.

Policy 142 – Windows XP End of Life is recommended for rescission. It is redundant to Policy 186 and Standard 186.10.

**IPv6**

The industry is moving to a new version of internet protocol addressing called IPv6. IPv6 replaces IPv4. This change is necessary because all available IPv4 addresses are nearly used up. IPv6 addresses are longer and also allow a whole host of improvements. The migration to IPv6 is not an option, it is where the world is headed. The new Statewide Migration to IPv6 sets December 2020 as the target for all state agencies to complete planning activities and December 2025 as the target for completion of migration. More communications about IPv6 and its importance will be available in the coming months.

Please share this information with others within your organization. If you have additional questions regarding this material, contact Sue Langen at (360) 407-8686. Thank you in advance for your support and consideration.