

10100-P110: Security Policies, Standards & Procedures

I. PURPOSE

This policy sets forth the process to be followed by Information Technology Coordinating Committee (ITCC) in establishing and implementing statewide technology policies, standards, and procedures for entities of the executive branch of Wyoming state government.

II. SCOPE

This policy applies to all executive branch agencies, boards and commissions. All information technology policies, standards, procedures or guidelines affecting the executive branch of Wyoming state government at the enterprise level are subject to this policy.

III. POLICY

Information technology policies, standards, procedures and guidelines shall be established in accordance with this policy.

A. CATEGORIES – Information for which new policy proposals are presented.

New policy initiatives shall be characterized within one of the following three categories:

1. Policy - A prescribed or proscribed course of action or behavior which is to be followed with respect to the acquisition, deployment, implementation or use of information technology resources. Policies are intended to be comparatively enduring so where possible technology issues that are subject to periodic change should be addressed as standards. Likewise, administrative details that may also subject to frequent change are more appropriately included in procedure documents.
2. Standard - A specific prescribed or proscribed technical approach, solution, methodology, product or protocol which must be used in the design, development, implementation or upgrade of information technology systems architecture (e.g., hardware/software/services).
 - a. Standards are intended to establish uniformity in common technology infrastructures, applications, processes or data.
 - b. Standards may be developed as a subset of, and within the context of, a broader technology policy. Standards may define or limit the tools, proprietary product offerings or technical solutions which may be used, developed or deployed by executive branch entities.
3. Procedure - A set of administrative instructions for implementation of a policy or standard. Procedures in some cases will be internal documents of the administrative unit charged with responsibility for implementing enterprise programs (i.e. ITD or State Archives). If so they are intended to clarify how

10100-P110: Security Policies, Standards & Procedures

policies and standards will be carried out and are presented to policy making bodies to for review and comment only.

B. GOALS

Standards and policies shall wherever possible:

1. promote consistency in the automation of the State's common infrastructure systems,
2. eliminate duplicate IT efforts by multiple executive branch entities,
3. ensure continuity of ongoing State operations,
4. promote administrative efficiencies relating to development and maintenance of common data,
5. enable the State to realize its full market power from using a statewide, enterprise approach to the procurement of technology solutions, and
6. narrow the number of technologies supported by executive branch entities.

C. CRITERIA FOR STANDARDS - In order to be considered for designation as a statewide technology standard, a proposed technology solution should:

1. meet the programmatic and technical needs of the majority of executive branch entities in core functionality,
2. reflect industry trends or "best of breed" recommendations,
3. offer potential for long life cycle, minimizing the risk of technological obsolescence,
4. be evaluated against the size and scope of existing deployments among executive branch entities (existing embedded install base),
5. be evaluated in terms administrative and fiscal resources required for implementation, and potential for cost savings or cost avoidance, and
6. be available under an enterprise or volume purchasing agreement, which reflects the aggregate buying potential of executive branch entities.

D. DEVELOPMENT OF POLICIES AND STANDARDS

1. The ITCC, primarily through its Policy and Standards Subcommittee, will facilitate stakeholder collaboration in the development of policies and standards. Stakeholders include those entities that may be potentially subject to, or impacted by, the outcome of the policy or standard. Such collaboration may include, but is not limited to:
 - a. Use of the Policy and Standards Subcommittee and it's subcommittees or workgroups;
 - b. Use of other existing ITCC subcommittees, workgroups or forums;
 - c. Establishment of new workgroups comprised of interested parties;
 - d. Establishment of technical committees to provide expertise in the development of the policy/standard, including but not limited to,
 1. the preparation of technical standards and specifications,
 2. assisting in the preparation of a business case analysis of proposed alternatives,
 3. laboratory testing of different alternatives.

10100-P110: Security Policies, Standards & Procedures

2. Many policy proposals will require not only the writing of policies, but also the designation of standards and/or the development of procedures. If a policy proposal includes related standards or procedures, it is preferred that all relevant documents be submitted to the Policy and Standards Subcommittees at the same time as a policy proposal.

E. REVIEW & APPROVAL

1. Policy and Standards Subcommittee Review and Approval
 - a. After being developed by a workgroup, a proposed policy or standard shall be submitted to the Policy and Standards Subcommittee for consideration at one of its regular meetings
 - b. If the Policy and Standards Subcommittee finds it necessary to make significant or substantive changes to the documents based on their review, the Policy and Standards Subcommittee will normally return the policy proposal to the workgroup for reconsideration. However, changes may be made by the Policy and Standards Subcommittee without further review by the workgroup.
 - c. A policy proposal will be approved by the Policy and Standards Subcommittee upon motion, second and majority vote of the subcommittee membership present. After approval it will be presented to the ITCC for their consideration.
2. ITCC Review and Approval
 - a. Through their participation in the ITCC, executive branch entities will be notified that a new policy, standard or procedure is being considered. Pertinent documents will be made available to ITCC members and other interested parties.
 - b. The policy proposal will be placed on a review period so that the information can be disseminated to interested parties, giving them a chance to make comments raise issues or ask questions. The policy or standard will be considered for approval no sooner than the next regular ITCC meeting after it was placed on review. The review period may be extended by the ITCC at its discretion.
 - c. After completion of the review period, the policy proposal will be considered for approval.
 - d. If the ITCC finds it necessary to make significant or substantive changes to the documents based on their own review or on input received during the review period, the ITCC will normally return the policy proposal to the Policy & Standards Subcommittee for revision. However, changes may be made by the ITCC without further review by the subcommittee.
 - e. A policy proposal will be approved by the ITCC upon motion, second and majority vote of the ITCC membership per ITCC Voting and Quorum requirements as outlined in Chapter V of the ITCC Charter, after which it will be submitted to the Information Technology Policy Council (ITPC) for final approval.

10100-P110: Security Policies, Standards & Procedures

3. ITPC Review and Approval
 - a. The ITPC will conduct any review of the policy proposal they deem appropriate. If the ITPC finds it necessary to make significant or substantive changes to the documents based on review of the proposal, they will normally return it to the ITCC for revision. However, changes may be made by the ITPC without further review by the ITCC.
 - b. A policy proposal will be approved by the ITPC upon motion, second and majority vote of the ITPC membership, per ITPC Voting and Quorum requirements as outlined in Chapter V of the ITPC Charter.
4. CIO Approval
 - a. Executive branch agencies shall be bound by a policy or standard upon its approval by the CIO.

F. PROCESS FOR IMPLEMENTING POLICIES AND STANDARDS

1. Policies and Standards Implementation – Executive branch entities are required to adhere to the policy and/or migrate to the standard as set out below.
 - a. New Systems Acquisitions - On or after the effective date of the policy or standard, executive branch entities acquiring new systems shall comply with the policy or standard.
 - b. Completion of Existing System Lifecycle - Unless otherwise set forth in the policy or standard, executive branch entities can continue to use existing systems for the remainder of the system's then-current life.
 - c. Major Upgrade or Replacement of Existing Systems – executive branch entities will be required to move to an established standard when an existing system requires major upgrade or a full replacement. Major upgrade shall include, but not be limited to, such things as:
 1. substantial redesign of an existing system;
 2. upgrades to a new major version release of a proprietary software product;
 3. other system modifications that involve substantial human or fiscal resources to implement.

G. EXCEPTIONS FROM POLICIES OR STANDARDS

1. Application For Exception
 - a. An executive branch entity must apply to the CIO for an exception by preparing a request for exception. The analysis (submitted in writing) shall establish a timeline for compliance or present a compelling argument which warrants the exception.
 - b. The request for exception shall be submitted to the CIO and must include, at a minimum, the following information:
 1. the specific state information policy, standard, or procedure requirement(s) that the agency feels they cannot comply with,

10100-P110: Security Policies, Standards & Procedures

2. a thorough explanation of the circumstances that prevent the agency from meeting the specific requirement,
 3. a cost/benefit analysis comparing the maintenance or implementation of a non-compliant system against the implementation of a compliant system,
 4. alternative measures or mechanisms that will be used to address the intent of the policy or standard and compensate for non-compliance,
 5. the consequences of not being granted approval for the exception,
 6. a plan and timeframe for moving into compliance with the policy or standard, and
 7. any other documentation requested by the CIO, Policy and Standards Subcommittee or the ITPC.
2. Review of Application for Exception
- a. The request for exception shall be reviewed to determine:
 1. the validity of the constraints that prevent the agency from meeting the policy, standard, or procedure requirement,
 2. whether the overall goals of the standard or policy serve the best interest of the state and out weigh the impact that compliance would have on the agency,
 3. whether the exception would violate other regulations, such as federal statutes, state law, or other state policies,
 4. whether the proposed alternative measures or mechanisms are appropriate and effective,
 5. whether other alternatives for compliance may exist, and
 6. whether the proposed plan and timeframe for moving into compliance with the policy or standard is reasonable.
 - b. Policy and Standards Subcommittee Review and Recommendation
 1. After being received by the CIO, the request for exception shall be submitted to the Policy and Standards Subcommittee for their review and recommendation.
 2. The Policy and Standards Subcommittee may request additional information from the agency to complete their review.
 3. The Policy and Standards Subcommittee will recommend approval or disapproval of the exception by motion, second and majority vote of the subcommittee membership present. This recommendation will then be presented to the CIO for his consideration.
 - c. CIO Review and Recommendation
 1. The CIO will conduct any review of the application deemed appropriate.
 2. The CIO may request additional information from the agency to complete his review.
 3. The CIO will approve or disapprove the application and advise the agency.

10100-P110: Security Policies, Standards & Procedures

3. Approved Exceptions
 - a. Term of the Exception
 1. All exceptions are considered temporary. All approvals for exceptions shall specify the duration of the exception, not to exceed three years.
 2. When an exception expires, a new application shall be submitted if the need for the exception continues.
 3. All exceptions will be subject to re-evaluation and review:
 - i. upon a change in the relevant policy or standard, and
 - ii. upon major upgrade or full replacement of the excepted system.
 - b. Review of Exceptions
 1. The CIO shall perform a periodic review of all active exceptions to determine:
 - i. if the exception is still needed,
 - ii. if technology, budget, personnel, or other resources are available for the agency to become compliant, and
 - iii. if the agency is following their plan to move into compliance.
 - c. Reporting on Exceptions
 1. The CIO shall provide a summary report of exceptions to the Information Technology Coordinating Committee (ITCC), and the Information Technology Policy Council (ITPC) at least annually.

H. REVIEW OF POLICIES AND STANDARDS

1. The CIO shall insure that all policies and standards are reviewed by the Policy and Standards Subcommittee on a regular basis for the purpose of verifying their currency and validity. All standards will be reviewed annually, and all policies will be reviewed every two years.
2. The CIO, the ITPC, the ITCC or any agency may request that the Policy and Standards Subcommittee conduct a review of a policy or standard at any time.
3. If, as a result of this review, the Policy and Standards Subcommittee determines that a policy or standard needs to be changed or rescinded, the document with the proposed revisions must follow the process outlined in section **E. REVIEW & APPROVAL** of this policy.

CIO Approved Date: 02/01/2010