Montana Operations Manual *Policy*	Category	**Information Technology, Infrastructure**
	Effective Date	**04/01/2016**
	Last Revised	**Not Approved Yet**
Issuing Authority	**Department of Administration** **State Information Technology Services Division**	

POL-Information Technology Procurement Request (ITPR) Policy

I. Purpose

The purpose of this policy is to establish requirements for the review and approval of acquisition and/or development of information technology resources.

II. Scope

This policy applies to all state agencies subject to the exemptions in 2-17-516, MCA and 2-17-546, MCA.

III. Requirements

A. **General Requirement:** In accordance with ARM 2.12.204, regardless of project cost, all state agencies, including State Information Technology Services Division (SITSD), shall submit a request on required Department of Administration (DOA) forms for all information technology acquisitions or state agency development efforts pursuant to DOA policies, standards, procedures, and guidelines.

B. Executive Order No. 09-2016

1. Only SITSD can buy and deploy servers, storage, and cloud services, unless otherwise directed by the Budget Director and CIO.

2. An agency shall utilize enterprise systems including, but not limited to, enterprise content management (ECM), directory services, email, telecommunications (voice, video, and data) and state data centers to further their missions with the effective and efficient use of enterprise information technology.

3. The Executive Order covers the Executive Branch and exempts (but does not prohibit from participation) elected official agencies and those entities identified in 2-17-516, MCA.

C. Additional Requirements

1. Except as otherwise provided in this policy, an ITPR must be submitted for each IT procurement, including new purchases, contract extensions, amendments, and addenda.

2. In accordance with the policies and principles established in sections 2-17-505 and 2-17-512, MCA, and as further defined in ARM 2.12.204, DOA shall review the ITPR and, based on its review, approve or deny the request.
3. An IT procurement for which an ITPR was required but not submitted will be cancelled or denied pursuant to 2-17-514, MCA. The agency must then submit an ITPR, and SITSD staff review time will be charged to the agency. All SITSD staff time resulting from an unapproved IT procurement will be billed to the agency.
4. ITPRs are reviewed by the Technical Review Board (TRB) and the State CIO in accordance with this policy and as described in the PRO-Information Technology Procurement Request Procedure.
    a. Appendix A lists factors considered by the TRB in reviewing ITPRs.
5. See PRO-Information Technology Procurement Request (ITPR) Procedure for additional information regarding the ITPR review and TRB process.
6. To facilitate a prompt decision, the agency shall:
    a. ensure persons familiar with the agency's business needs and technical requirements attend meetings with SITSD staff;
    b. submit information with the ITPR demonstrating the business need or justification; and
    c. provide all information available to the agency. Withholding information may cause delays, lead to denial of the ITPR, or increase the cost of implementation.
7. Each agency shall provide SITSD a list of persons authorized to submit ITPRs on behalf of the agency. Only persons on the agency's authorized list are permitted to submit an ITPR.
8. To ensure notification for ITPR determinations, each agency must define its agency email distribution group. At a minimum, the email distribution group must include the agency IT CIO/Manager and the agency Contract Manager.
9. Before resubmitting an ITPR, an agency shall first meet with the State CIO or designee to review issues that led to the prior ITPR not receiving approval. This requirement applies whether the ITPR was denied, conditionally approved, or withdrawn by the agency.
10. Each agency shall maintain a FRM-Quarterly Agency IT Procurement Log Form of acquisitions made under the agency's delegated authority. **Each agency shall submit its FRM-Quarterly Agency IT Procurement Log Form to SITSD quarterly.**
11. State Procurement Bureau (SPB) statutes, administrative rules, and policies govern procurement in general.
    a. This ITPR policy does not exempt agencies from complying with SPB procurement requirements or the public contract provisions defined in Montana Code Annotated Title 18.

b. See GDE-Information Technology Procurement Request (ITPR) Delegated Authority Guideline for information about delegation agreements, coordination with SPB, and the FRM-Quarterly Agency IT Procurement Log Form.

D. Specific Examples. **NOTE: The examples provided are not an exclusive list of items that require or do not require ITPRs.**

1. An ITPR is required when:
   a. procuring:
      i. collaboration tools;
      ii. monitoring tools;
      iii. services that duplicate enterprise services or infrastructure;
      iv. IT SOWs;
      v. IT maintenance contracts;
      vi. IT staff augmentation;
      vii. IT RFPs; or
      viii. IT contract extensions;
   b. a software product is not listed on the approved software list (ASL); or
   c. purchasing from the Master IT Services Contract administered by the State Procurement Bureau (SPB).
2. An ITPR is not required when:
   a. a software product is on the ASL.
   b. an agency has previously received an ITPR approval for the same version of the software being purchased;
   c. purchasing from SITSD's Service Catalog;
   d. purchasing personal computers from Dell or HP, cell phones, and non-networked printers purchased from the SPB-approved term contract; or
   e. purchasing multi-functional/printer devices purchased or leased through the DOA-General Services Division (GSD) Print & Mail Services contract.

E. Approved / Denied Software Lists

1. Subject to State CIO approval, the Technical Review Board will create and maintain the Approved Software List (ASL) of acceptable IT software and products and the Denied Software List (DSL) of IT software and products unsuitable for use by state agencies.
2. State agencies can purchase any product on the ASL without submitting an ITPR.
3. State agency CIOs must submit a FRM-Quarterly Agency IT Procurement Log Form by the 10th of the month following the end of the quarter (January, April, July, October) detailing these software

purchase(s). The log aligns with the Legislative Finance Committee report and will be submitted to SITSD at ITRequests@mt.gov.

4. State agencies cannot purchase or use products on the Denied Software List (DSL).

IV. References

Note: *General information about roles and responsibilities, enforcement, references, and other material applicable to all IT instruments is provided in the POL-Information Technology Reference Policy.*

A. Legislation

1. Section 2-17-512, MCA
2. Section 18-4-402, MCA

B. Executive Orders and Administrative Rules

1. State of Montana Executive Order No. 09-2016
2. ARM 2.12.204
3. SPB Administrative Rules: ARM Title 2, chapter 5

C. Policies and Procedures

1. PRO-Information Technology Procurement Request Procedure
2. SPB Policies in the Montana Operations Manual: Procurement

D. Guidelines and Standards

1. GDE-Information Technology Procurement Delegated Authority Guideline

E. Forms, Memoranda, and Other References

1. FRM-Quarterly Agency IT Procurement Log Form
2. Approved Software List
3. SITSD's Service Catalog

Appendix A
The Technical Review Board considers the following in their review of ITPRs:

The TRB reviews all ITPRs to ensure the requests comply with the requirements established in 2-17-512, MCA, 2-17-518, MCA, 2-17-524, MCA, and ARM 2.12.204.

A. Business Case – What business need are you solving with this purchase?
B. Preferred Solution – Justification of why your choice is the best solution
C. Enterprise Services – Does your proposed solution compete with an enterprise service offering? If so, why is your choice a better fit than the enterprise service? Also, your agency will need to submit an Exception Request if your solution competes with an enterprise service.
D. Security – Are there known vulnerabilities with this solution? External cloud services that connect to SummitNet or host sensitive data require a risk assessment.
E. Alignment with State Strategic Information Technology Plan
F. Alignment with your Agency IT Plan