

	Montana Operations Manual Policy	Category	Information Technology, Security
		Effective Date	10/30/2015
		Last Revised	Not Approved Yet
Issuing Authority	Department of Administration State Information Technology Services Division		
POL-Enterprise Mobile Device Management Policy			

I. Purpose

The [Montana Information Technology Act \(MITA\)](#) assigns the responsibility of establishing and enforcing statewide IT policies and standards to the Department of Administration (DOA). The purpose of this Policy is to implement the Enterprise Mobile Device Management Policy for defining actions to fulfill the responsibility.

II. Scope

This Policy applies to the CIO as required under [2-17-521\(4\), MCA](#), and to executive branch agencies, excluding the university system, as required under Section [2-17-524\(3\), MCA](#).

III. Policy Statement

This enterprise policy has been developed for the state's information systems based on the [Montana Information Technology Act \(MITA\)](#). This policy is in cooperation with the federal and local governments with the objective of providing seamless access to information and services to the greatest degree possible [2-17-505 \(3\)](#).

IV. Roles and Responsibilities

Roles and responsibilities are required by this policy and in accordance with [Appendix B - Security Roles and Responsibilities](#)

V. Requirements

To support Enterprise Mobile Device Management, this Policy requires that:

- A. Compromised devices, such as Jailbroken devices, will not be allowed to enroll in the enterprise MDM solution.

- a. If a device becomes compromised while it is enrolled, state data will be removed. Depending on type of enrollment, this could result in a factory reset on the device. Fully enrolled devices will undergo a full wipe of the device. Devices enrolled as BYOD will undergo a wipe that only removes data in the containerized MDM space.
- b. Compromised devices will not be allowed access to state data until the device has been wiped or received a factory reset.
- B. All access to State of Montana resources from a mobile device requires authentication, which must include either a device passcode or user password.
 - a. Password requirements are addressed in the POL-Information Security Policy – Appendix A (Baseline Security Controls) (IA-5).
 - b. Passcodes are required to follow the state policy for passwords.
- C. All mobile devices that access State of Montana data protected by federal or state regulation must enable encryption on all storage directly associated with the mobile device including Secure Digital (SD) cards and flash drives. If a device does not support encryption, that device will not be used to access such data.
- D. Non-State approved cloud services must not be used for any storage or duplication of state data protected by federal or state regulation, statute or law.
- E. Agencies must identify agency MDM administrator(s) for the purpose of administering the MDM from the solution admin console. Agencies will be responsible for agency owned devices in addition to agency BYOD participants.
- F. Agency MDM administrators must ensure end users are aware that State Data may be removed from BYOD mobile device in the event the mobile device is replaced, lost, stolen, or the end user terminates employment with the State of Montana. Agency MDM administrators must ensure end users are aware that fully enrolled mobile devices may have all data removed, including personal, in the event the mobile device is replaced, lost, stolen, or the end user terminates employment with the State of Montana.
- G. SITSD is responsible for creating and dispersing a template document that addresses terms of service for end users. SITSD will make this document available to agency administrators.
- H. Agencies are required to have end users sign and acknowledge an end user service agreement. Agencies will be responsible for storing these documents.
- I. All vendor recommended patches, hot-fixes, or service packs must be installed prior to mobile device enrollment and processes must be in place

to keep operating system and applications current based on vendor support recommendations.

VI. Definitions

Refer to the [Statewide Information System Policies and Standards Glossary](#) for a list of local definitions.

Mobile Device Management (MDM):

MDM is a way to ensure employees stay productive and do not breach corporate policies. Many organizations control activities of their employees using MDM products/services. MDM primarily deals with corporate data segregation, securing emails, securing corporate documents on device, enforcing corporate policies, integrating and managing mobile devices including laptops and handhelds of various categories. MDM functionality can include distribution of applications, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, ruggedized mobile computers, mobile printers, mobile POS devices, laptops, etc. MDM tools are leveraged for both state-owned and employee-owned (BYOD) devices across the enterprise.

Bring your own device (BYOD):

Refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Jailbreak:

Refers to the act of overcoming limitations in a computer system or device that were deliberately placed there for security, administrative, or marketing reasons.

VII. Compliance

Compliance shall be evidenced by implementing the Policy as described above.

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this instrument are made by submitting an [Action Request form](#). Requests for exceptions are made by submitting an [Exception Request form](#). Changes to policies and standards will be prioritized and acted upon based on impact and need.

VIII. Enforcement

Policies and standards not developed in accordance with this policy will not be approved as statewide IT policies or standards.

Enforcement for statewide policies and standards developed in accordance with this policy will be defined in each policy, standard or procedure.

If warranted, management shall take appropriate disciplinary action to enforce this Policy, up to and including termination of employment, consistent with current State Policy. The discipline policy can be found in the [MOM Policy System](#) (search for: 261). When considering formal disciplinary action, management will consult with their assigned Human Resource Specialist before taking action.

IX. References

A. Legislation

- [2-15-112 MCA](#) Duties and powers of department heads
- [2-17-505 MCA](#) Policy
- [2-17-512 MCA](#) Powers and duties department
- [Montana Information Technology Act \(MITA\)](#)

B. Policies, Directives, Regulations, Rules, Procedures, Memoranda

- Statewide Policy: [POL-Establishing and Implementing Statewide Information Technology Policies and Standards \(v.2\)](#)
- SITSD Procedure: [Conduct Policy for State Space and State Grounds in Helena \(v.2\)](#)

C. Standards, Guidelines