STATE OF MONTANA
DEPARTMENT OF CORRECTIONS
POLICY DIRECTIVE

Policy:	**DOC 1.7.7 Computer Security**
Chapter 1:	ADMINISTRATION AND MANAGEMENT
Section 7:	Information Systems
Effective Date:	May 1, 1997 Page 1 of 6
Revised:	January 24, 2020
Signature:	/s/ Reginald D. Michael

I. POLICY

In accordance with section 2-15-114, MCA, the security responsibilities for Department data lie with the department director. The director adopts the Enterprise POL-Information Security Policy and the policy's appendices as the Department's standard information security policy.

II. APPLICABILITY

All divisions, facilities, and programs of the Department of Corrections.

III. DEFINITIONS

Department Employee – The term includes paid employees or contracted persons (temporary or permanent), volunteers and interns who are paid or donate time or services to the Department, contractors, on-site vendors and individual service providers, e.g. delivery, maintenance, vendors, etc. who may not be contracted to the Department and whose assignment is primarily on Department premises, e.g. facility or program offices.

Device – Any electronic device including a computer, laptop, tablet, and smartphone. When the term is used in reference to a computer, a device is any internal or external hardware peripheral that attaches to a computer to send, receive, or process data.

Download – To copy software programs, games, screen savers and other such items from the Internet to a Department IT resource. Download does not include the copying of text documents from the Internet to a Department IT resource.

External Media Device – USB drives, digital cameras, multimedia players, smartphones and tablets, DVD's or CD's.

Information Technology (IT) Resources – Any computer system, including but not limited to, computers, servers, printers, smartphones, tablets, laptops, and networks.

Internet – An electronic communications network that connects computer networks and organizational computer facilities around the world.

Public Record – Information that is fixed in any medium and is retrieval in usable form for future reference, and designated for retention by the state records committee, judicial branch, legislative branch, or local government records committee.

SummitNet – The State of Montana's telecommunications nucleus network or backbone connecting agency, university, grades K-12, library, and local government networks. SummitNet provides connectivity to the Internet.

IV. DEPARTMENT DIRECTIVES

A. Acceptable Uses for IT Resources

1. Department employees may only use IT resources to carry out their official duties in accordance with 2-2-103(1)(2), MCA. Employees who deviate from these standards are subject to the penalties provided for in 2-2-103(1)(2), MCA.

B. Device Use

1. Access to IT resources in the form of devices and facilities are issued in accordance with performing assigned duties for the benefit of the people of Montana. Users of State of Montana IT resources and facilities are personally responsible for their conduct and behavior in the use of assigned resources.

2. Acceptable personal use includes e-mail for essential personal communication such as messages to family members, significant others, teachers, doctors and day-care providers to communicate work schedule changes, status, or other personal business. Acceptable Internet use includes personal information gathering during lunch breaks and nonworking hours, as long as it does not interfere with staff productivity or preempt any business activities. Violation of this section may lead to employee discipline, up to and including termination. There is no expectation of privacy while using the State IT resources. All activity can be logged, monitored, and reviewed.

3. Employees are expected to comply with all applicable IT-related contractual and license agreements. Staff should check with the IT bureau for guidance.

4. Work related files and electronic information pertaining to official Department related business must be stored on State approved storage services to ensure the document(s) are backed up. Storing data solely on a local computer drive including the desktop is prohibited.

5. Use of cloud-based services unapproved for department related data storage, transfer, etc. is prohibited.

6. Employees must never attempt to gain access to, disclose, or remove any user ID, information, software, or file that is not their own and for which they have not received explicit authorization to access.

7. Staff may not interfere with, encroach on or disrupt others' use of the State's shared IT resources. For example, by
   a. playing computer games, streaming non-work-related video, sending excessive messages, attempting to crash or tie up a State computer; and
   b. damaging or vandalizing State computing facilities, equipment, software, or computer files.

8. Staff shall not transfer, or allow to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.

9. Staff shall not intentionally transmit, display, view, archive, store, transfer, edit, or record nudity, erotic content or sexual content, unless the information is needed to conduct official duties deemed appropriate by the Department.

10. All hardware and software, including downloaded software, must be authorized, and purchased and installed by authorized staff prior to use.

11. Employees may not connect non-State-owned storage media (USB storage devices, external or internal hard drives), including personal mobile devices (iPads, Kindles, smartphones, etc.) to the workstation or internal network.

12. IT resources may not be used for private, commercial, or political purposes.

13. Remote Access including VPN services to the State's internal network must be authorized by a supervisor and utilize State approved software. Utilizing VPN services to connect to state networks and resources from personally owned computing devices is prohibited.

14. Employees must report missing or stolen IT hardware immediately to their supervisor and the Department's Service Desk.

15. Staff must notify the Service Desk and their supervisor in the event of a security incident or if the IT device is acting unusual, e.g. slow performance or response times, unexpected pop-up advertisements, etc.

16. Devices must be locked before leaving them unattended. Staff must log off devices at the end of the day unless permission has been received to run a job or process.

C. Passwords

1. Passwords will be strong, with a minimum of 12 characters. Staff are required to have a combination of upper and lower case with special and numerical characters contained in their passwords.

2. Passwords may never be shared with anyone.

3. Personal information should never be used in a password (e.g., SSN or date of birth).

4. Staff must always secure their password(s). Passwords may not be written down (e.g., taped to monitor or under keyboard).

D. Internet

1. Internet usage is provided for the opportunity it gives state employees and contractors to accomplish their job duties.

2. Internet access must be used for conducting state business, however, employees are allowed non-excessive personal use of internet.

3. Department system administrators, management, and appropriate Department of Administration personnel may monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected.

E. Electronic Mail (Email)

1. Email may only be used for conducting state business, however, supervisory staff may allow incidental, non-excessive personal use of Email.
2. Email is considered public record. Employees should have no expectations of privacy.
3. State email accounts may not be used to sign up for non-work-related website accounts, mailing lists, etc.
4. Personal email account(s) may not be used for work-related business.
5. State email may not be used to circulate chainmail, spam, etc.
6. State email may not be used to send sensitive information to other parties unless authorized by agency and appropriately encrypted.
7. Employees may not use email to send inappropriate materials such as:
   a. sexually offensive, explicit; or
   b. harassing or discriminatory; or
   c. gruesome, violent, or sadistic.

F. Social Media

1. If staff use of social media is authorized it may only be used for work-related purposes.
2. Work-related social media communications should be professional and consistent with the agency's mission and the position's responsibilities,

G. Mobile Device Management

1. Granting of Mobile Device access to State of Montana IT resources will be managed by the Department's IT bureau.
2. State information managed from a mobile device requires authentication, which must include either a device passcode or user password.
3. Passcodes are required to follow the state policy for passwords. This includes biometrics. See previous section regarding appropriate password information.
4. Jailbroken or "rooted" devices will not be allowed to enroll in the enterprise MDM solution.
5. If a device becomes compromised while it is enrolled, state information will be removed, and the device will not be allowed access to the State network or State information. Access will not be restored until the device has been wiped or receives a factory reset.

H. Security Training

1. The Department provides mandatory security awareness training to new employees, as well as annual security training to all staff.

I. Sensitive Information

1. State of Montana Level 2 and 3 data classifications must be appropriately handled, marked, stored, and transmitted. See *Montana Operations Manual, GDE-Data Classification*.
2. Staff must ensure any personally identifiable information is saved to an appropriate location (e.g. encrypted location).
3. Sensitive information may not be stored, transferred, or copied to unauthorized locations.
4. Employees must utilize the State of Montana File Transfer Service or OneDrive for Business or Enterprise Approved encrypted email for any transfer needs of sensitive information.
5. Information that is sensitive, may only be stored on State-owned portable devices and portable storage if there is an approved business need or requirement.
6. If a position requires access to sensitive information, an Elevated Privileges Acknowledgement form will be signed by designee and approved by management prior to being granted access.
7. Sensitive information may not be transported outside of the United States on portable devices or portable storage.
8. Protect IT devices containing sensitive information (e.g. flash drives, computers, cell phones, etc.) until the device is destroyed or sanitized using approved tools or equipment.
9. Report lost, stolen or compromised information to immediate supervisor and Information Security Manager.

J. Multi-Factor Authentication

1. Multi-Factor authentication is the state standard for access to State of Montana computer systems. It is achieved through use of RSA physical fob or soft token.
2. The Department in partnership with the State Information Technology Services Division (SITSD), is responsible for distributing and managing RSA fobs. One fob will be issued to each employee or service provider who requires it for their position along with their User ID.
3. Fobs are not to be shared with other individuals.
4. Employees and service providers are responsible for the physical security of the fob at all times in order to prevent unauthorized access.

5. Lost, stolen or misplaced fobs must be reported immediately by calling the Service Desk or SITSD Service Desk at (406) 444-2000. The employee's manager must request a replacement fob or temporary passcode.

K. Compliance

1. Compliance is shown by implementing this Enterprise Acceptable Use of IT Resources 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 document can be made by submitting an Action Request form. Requests for exceptions are considered by submitting an Exception Request form to DOA_SITSD. Changes to policies and standards will be prioritized and acted upon based on impact and need.

V. CLOSING

Questions concerning this policy should be directed to the Department's Chief Information Officer (CIO).

VI. REFERENCES

This section contains content or links to supporting documents or sources.
POL-Information Security Policy POL-Information Security Policy - Appendix A (Baseline Security Controls)
POL-Information Security Policy - Appendix B (Security Roles and Responsibilities)
POL-Information Security Policy - Appendix C (Blocked Sites and Rules of System Usage forms) POL-Information Security Policy - Appendix D (Cyber Security Framework link to Baseline Security Controls)
Section 2-15-114, MCA
Section 2-17-534, MCA

VII. ATTACHMENTS

None