Office of the State Public Defender
Administrative Policies
Human Resources

Subject: Computer Use	**Policy No.: 502**
Title	**Pages: 4**
Section:	**Last Review Date: 4-9-2020**
Effective Date: 11-01-06	**Revision Date: 4-9-2020**

1. POLICY

The state's computer system and all programs on it belong to the State of Montana and are provided for the conduct of state business. The use of the state's computer facilities for essential personal business must be kept to a minimum and not interfere with the conduct of state business. All Office of the State Public Defender employees are required to acknowledge that they understand and will adhere to this policy by signing the Employee Use of Information Technology Acknowledgement Form (Attachment A).

2. PROCEDURES

2.1 By using the state computer system, including but not limited to the Internet and communication systems (email, SMS/Text, etc.), employees understand that management may monitor, read and review any and all information accessed or stored in the system and/or on your assigned state computer.

2.2 The State of Montana has a business requirement to monitor or retrieve information on its computer system for a variety of reasons that include, but are not limited to, troubleshooting software problems, retrieval of work files, preventing system misuse and assuring compliance with software distribution policies.

Employees do not have a right to privacy in any materials created, accessed, sent or received on state computer equipment or systems whether password protected or not. Passwords may be overridden by the State.

2.3 Very limited, reasonable personal use of the state's e-mail system may occur to send a personal e-mail that does not contain foul, offensive, defamatory or pornographic information. Just like the use of the state telephone system, personal use of e-mail should be limited and brief. E-mail sent over the state system, whether personal or state work related, should be proper in its content. Personal use of information technology must not create cost to the state, interfere with the employee's duties, disrupt state business, or compromise the security or integrity of state government systems. The state's SMS/Texting platform is not to be used for personal reasons as it creates a cost to the state.

2.4 An employee may access a non-obscene, non-offensive Web site on break time only. *Use common sense and good judgment.* Misuse of the state

computer system by falsifying time sheets and recording non-work time as work time can lead to disciplinary action up to and including termination.

2.5 To ensure that the above guidelines are being met the state reserves the right to filter out or block inappropriate Internet sites and will from time to time conduct unannounced surveillance of any and all computer use by state employees. While the State will take steps to block offensive material and delete it when discovered, that does not mean that all accessible material is appropriate.

2.6 Documents deleted from any of your directories, including Outlook, may continue to exist and can be retrieved off the system. A list of all Internet sites accessed by employees is available to management when management requests it or computer security personnel observe and report inappropriate use to management.

2.7 Logon IDs and passwords (e.g., C numbers) are assigned to individuals for access to the Office of the State Public Defender data. The individual assigned an ID and password is responsible for the security of this ID. Passwords must be kept confidential. Under no circumstances should you share your Logon ID or password. You may be liable for unauthorized access of information using your ID and password.

2.8 Employees shall:

- **2.8.1** Abide by all copyright laws;
- **2.8.2** Protect data in their custody, including knowing if data is confidential;
- **2.8.3** Ensure that critical data is saved to an appropriate location;
- **2.8.4** Maintain a secure, virus-free environment including checking CD's and USB sticks for viruses before using them on a state computer;
- **2.8.5** Seek a system administrator before installing any software;
- **2.8.6** Protect equipment from theft and report any loss of equipment or information to their supervisor immediately;
- **2.8.7** Lock systems before leaving them unattended;
- **2.8.8** Notify managers or system administrators of anything unusual or if a computer may have a virus.

3. PROHIBITED USE

3.1 No one may use the state computer system or any of its programs for non-job-related purposes to access or send foul, offensive, defamatory or pornographic information.

3.2 The state has a zero-tolerance policy for sexual harassment. Accessing or sending harassing or derogatory information such as comments demeaning a person's sex, race, religion, disabilities and sexual orientation will not be tolerated.

3.3 Do not use a personal e-mail account outside of the of the state e-mail system (such as Hotmail) unless you have been granted an exception by the State

Information Security Officer. Downloading an outside system on to the state system can open the door to viruses and other serious problems.

3.4 Prohibited activities include but are not limited to:

3.4.1 Chain letters;

3.4.2 Unauthorized use of copyrighted materials including software;

3.4.2 Communications to solicit voluntary participation in athletic betting pools, political causes, religious causes or personal organizations.

3.5 The state computer system may not be used to conduct or operate a personal commercial business or "for-profit" or "non-profit" activities.

4. SITSD POLICIES

The following policies are also incorporated in the OPD policy by reference:

4.1 Employee Use of Information Technology:
POL-Information Security Policy – Appendix A (See PL-4, page 23)

4.2 Social Media:
https://montana.policytech.com/docview/?docid=228&public=true

4.3 POL-SummitNet Acceptable Use Policy
https://montana.policytech.com/dotNet/documents/?docid=685&public=true

5. CLOSING

This policy shall be followed unless it conflicts with negotiated labor contracts or specific statutes, which shall take precedence to the extent applicable.

If you have a question about a particular use ask your supervisor before you use the state computer system for that purpose and potentially expose yourself to disciplinary action.

Violation of any provision of this policy may result in disciplinary action up to and including termination.

Questions about this policy can be directed to your supervisor or to the OPD Human Resource Officer at:

Office of the State Public Defender
Central Services Division
44 West Park
Butte, MT 59701

(406) 496-6080

Employee Use of Information Technology

Information technology is essential to the State of Montana and each employee is responsible for the safe keeping of these resources. This policy outlines important areas of responsibility. Violations of this policy may result in disciplinary action up to and including termination. All employees shall read and sign this policy every year. Return to the Central Services Division.

Acceptable Use
The State of Montana uses information technology for conducting state business. Employees must not use technology for purposes other than those that would further their job duties. Incidental personal use is permitted. “Incidental” is defined as use that does not create cost to the state, interfere with the employee’s duties, disrupt state business, or compromise the security or integrity of state government systems. Employees may not violate law, rules, regulations, or policies using information technology while in the course of their duties, including copyright laws. This includes the duplication, transmission, or use of intellectual property without the proper agreements.

Security Responsibility
Employees shall:

- Protect data in their custody, including knowing if data is confidential;
- Ensure that critical data is saved to an appropriate location;
- Maintain a secure, virus-free environment;
- Seek a system administrator before installing any software;
- Protect equipment and report any loss of equipment or information immediately;
- Protect passwords and lock systems before leaving them unattended;
- Notify their manager or system administrator of anything unusual or if they think a computer may have a virus.

Privacy
Employees have no expectation of privacy when using state-controlled equipment or systems. State officials may access, read, copy, use or disclose information on state-controlled equipment and systems without prior notification.

Employee Signature
I have read the State of Montana’s computer use policies and agree to comply with the conditions within this document. I understand that all activity using state information technology resources may be monitored including monitoring of my communications, with or without notice; therefore, I have no expectation of privacy when using these resources.

I know that I may direct any and all questions about the policy to my supervisor or the Human Resource Officer before signing or at any time in the future.

Print Name: _____

Signed _____ Date _____