DRAFT

1.1 Appropriate Use of Information and Technology Resources

OVERVIEW

This policy is part of the Information Security Program and is guided by the Information Security Program Charter. It is intended to support the protection of Montana Legislative Branch information resources from illicit or damaging activity.

Effective information security is a team effort involving the participation and support of all Montana Legislative Branch employees, contractors, vendors, and others who deal with information and information systems. It is the responsibility of all users to know these guidelines and to conduct their activities accordingly. Inappropriate use may expose the Montana Legislative Branch to a variety of risks, including virus attacks and compromise of network systems and services, as well as issues of legal liability.

PURPOSE

This policy describes both appropriate and inappropriate use of information, computing, and communications resources and thus provides the user with basic parameters of acceptable use. This policy applies to information stored on or transferred via computers, networks, telephones, or other communications devices, as well as the usage and protection of the physical assets themselves.

SCOPE

This policy applies to all employees, contractors, vendors, or others who may utilize, possess, or have access to Montana Legislative Branch information and technology resources.

DEFINITIONS

"Information Systems" are an organized collection of hardware, software, supplies, policies, procedures and people, which store, process and provide *access* to information.

"Permanent work area" means the area where an employee regularly receives instructions or directions from the supervisor/employer.

"Personal Media" is personally acquired transmission tools used to store and deliver information or data, such as but not limited to: USB drives, CDs, Floppy Disks, etc.

"Sensitive data" means information that is not releasable to the public.

"Software" is the instructions for a computer, which are organized into sets called programs.

"Spam" means commercial e-mails (junk mail) that are unsolicited by the receiver.

POLICY

The use of Legislative Branch information and technology resources imposes certain responsibilities and obligations on users.

All equipment (hardware/software) purchased by the Montana Legislative Branch is considered property of the Montana Legislative Branch. Data residing on Montana Legislative Branch information systems is also the property of the Montana Legislative Branch. This equipment and the information contained within are to be used for official state business only. Limited personal use may be allowed in coordination with the appropriate division director's guidelines.

All users are responsible for complying with Legislative Branch policies regarding use and protection of information and technology resources. Failure to properly use or protect Legislative Branch information or technology resources may subject the user to prosecution under state or federal law.

1.1.1 General Use and Ownership

All data created or stored on Montana Legislative Branch systems remains the property of the Montana Legislative Branch.

For security purposes, certain authorized individuals within the Montana Legislative Branch may monitor equipment, systems, and network traffic at any time. Therefore, users of the Montana Legislative Branch information systems have no expectation of privacy while using these systems.

The Montana Legislative Branch reserves the right to audit networks and systems on a periodic basis to ensure compliance with this and other policies.

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Division directors are responsible for creating written guidelines concerning personal use of Internet/intranet systems. In the absence of such guidelines, employees should be guided by Branch policies on personal use, and if there is any uncertainty, employees should consult their supervisor or division director.

Employees are required to complete initial/annual training and review this policy. Employees are also required to sign an appropriate use form acknowledging that they understand the policy and the rules governing the appropriate use of information systems and communications resources.

1.1.2 Security and Proprietary Information

Use of encryption for sensitive data storage or transmission is required.

Passwords and account information are considered sensitive data and should remain secure at all times and should not be shared with other personnel.

All computer systems should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less. This setting must not be modified or extended beyond 15 minutes without written approval from the Legislative Branch ISO. If the system is left unattended, the user will activate the screen lock feature. Users must log off and power down their computer systems at the end of each duty day.

Portable computers are especially vulnerable to loss of data--special care should be exercised to secure the system and the data contained within the system when it is not being utilized in your permanent work area. Do not leave portable computers unattended or out of the user's control.

Postings by employees from a Montana Legislative Branch e-mail address are not allowed unless posting is in the course of official business duties.

Employees may not open e-mail attachments from unknown senders. Such messages often contain malicious code intended to disrupt or disable system operations. If you are unsure about an e-mail attachment but still believe it may be work-related, do not open it, instead contact an IT support technician to help determine if the attachment is safe before proceeding. Any time you get a strange e-mail message from an unknown sender that you believe is spam, insert the original message as an item into a new message and send it to "Spam Reports". Then delete the original message from your In Box.

Only information systems owned by the Montana Legislative Branch are allowed to connect to the Montana Legislative Branch's internal network. All Montana Legislative Branch information systems may operate only approved virus-scanning software with a current virus database, and the virus-scanning software must remain operable at all times when the system is turned on.

Only authorized Office of Legislative Information Technology employees shall install software via the Montana Legislative Branch network. In no case shall any user install software on any Branch information system. The IT Helpdesk will assist users in loading software that has been approved through the BCA process. The Network Manager is responsible to ensure compliance with all software copyright laws by coordinating software installations and software use monitoring.

Network Administrators perform regularly scheduled backups of information stored on the local area network file servers. The backup and recovery procedures ensure that adequate information exists to restore network files in the event of a server malfunction or damage to programs or data. Files maintained off the network drives (i.e., on the computer hard drive) are the responsibility of

the user. Users should place a copy of important files on the network drive to ensure that a copy of the file is backed up. Personal backup media (diskettes, CD-ROMs, USB flash drives, etc.) are not authorized for use on the Montana Legislative Branch network or information systems.

Do not store personal data or software on any system hard drive or network file server. Information found to be of a personal nature will be removed.

1.1.3 Unacceptable Use

The following activities (actual or attempted) are strictly prohibited with no exceptions.

Under no circumstances is a Montana Legislative Branch employee, contractor, vendor, or other person authorized to engage in any activity that is illegal under local, state, or federal law while utilizing information system resources owned by the Montana Legislative Branch.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

Unacceptable System and Network Activities

Intentional or negligent violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property or violations of similar laws or regulations. This limitation includes but is not limited to the installation or distribution of "pirated" software products that have not been appropriately licensed for use by the Montana Legislative Branch.

Intentional or negligent unauthorized copying of copyrighted material, including but not limited to digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Montana Legislative Branch or the end user (acting in an official capacity) does not have an active license.

Intentional or negligent introduction of malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) onto Montana Legislative Branch information systems, including any network or server.

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being conducted at home.

Using Montana Legislative Branch computing assets in procuring or transmitting illegal material or material that is in violation of sexual harassment or hostile workplace laws.

Performing any activity that might compromise the confidentiality, integrity, or availability of network communications. This activity includes but is not limited to accessing data of which the user is not an intended recipient or logging onto a system or account that the user has not been expressly authorized to access.

Attempts to subvert the security of any Montana Legislative Branch, Montana state, or any other network or network resource through the use or manipulation of any Legislative Branch information system. Such unauthorized activity includes attempts by individuals to crack passwords or otherwise induce unintended information systems activity for the purpose of gaining access to systems or accounts other than their own. Port or vulnerability scanning by unauthorized employees is prohibited; authorized employees will be informed in writing of their authority to perform such activity.

Executing any form of network monitoring capable of intercepting voice or data. Certain employees authorized to conduct this activity will be informed in writing of their authority.

Conducting private or personal for-profit or not-for-profit activities. This includes use for private purposes such as business transactions, private advertising of products or services, and any activity meant to foster personal gain.

Conducting any activity or solicitation for political or religious causes.

Attempts to modify or remove computer equipment, software, or peripherals without prior authorization.

Creating, accessing, or transmitting sexually explicit, obscene, or pornographic material.

Creating, accessing, or participating in online gambling.

Transmission or storage of sensitive data in plaintext form without the use of encryption.

Unacceptable E-mail and Communications Activities

Sending unsolicited e-mail messages outside the course of normal official business, including the sending of spam or other advertising material, to individuals who did not specifically request such material.

Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.

Creating or forwarding "chain letters" of any type.

Transmission of sensitive data in plaintext form without the use of encryption.

1.1.4 Enforcement

Any employee, contractor, vendor, or other person utilizing state information systems who is found to have violated this policy may be subject to disciplinary action, up to and including termination.

APPROPRIATE USE POLICY
ACKNOWLEDGEMENT

I have read the Montana Legislative Branch's Appropriate Use Policy and agree to comply with all terms and conditions. I agree that all network activity conducted while doing Montana Legislative Branch business and being conducted with Montana Legislative Branch resources is the property of the State of Montana.

Further I have completed the initial/annual training on the Branch's Appropriate Use Policy for information resources and agree to follow the rules contained in this policy. I understand that if I violate the rules, my network access may be revoked and I may face disciplinary measures, including possible termination.

I understand that the Montana Legislative Branch reserves the right to monitor and log all network activity, including e-mail and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

I have been given the opportunity to raise any questions and concerns regarding the content of the Montana Legislative Branch's Appropriate Use Policy.

_____ _____
Employee's Name (Print) Office

_____ _____
Signature Date

_____ _____
Manager's Name (Print) Office

_____ _____
Signature Date

This employee meets all requirements to receive network access

_____ _____
MLB Information Security Officer Date

This employee was granted network access on _____

_____ _____
IT Helpdesk Date