DMA Policy: **1-0250**
Name: **INFORMATION SYSTEM SECURITY**
Reference: **MOM 1-0250; 2-17-503, MCA; 2-15-114, MCA; 45-6-311, MCA; 2-2-121, MCA; Internet Services Policy; Electronic Mail Policy; Transmission Policy**

Approval Signature: John E. Walsh

Effective Date: **September 1, 2008**

INFORMATION SYSTEM SECURITY

This policy applies to all Department of Military Affairs employees and contractors using a state computer. Each program manager will ensure that all program employees/contractors review this policy and sign an annual Computer Use Consent Form **(Appendix A)**.

Each user of the State of Montana's computing and information resources should realize the fundamental importance of information resources and is responsible for the safe keeping of these resources.

Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those on the state network and those on networks to which state systems are connected.

Each user is responsible for having knowledge of the state and department policies concerning security and care for their computer. It is the responsibility of the department to educate its management and staff about these policies; to educate its employees about the dangers of computer abuse and its threat to the operation of the state computer network; and educate its management and staff about proper ethical behavior, acceptable computing practices, and copyright and licensing issues.

Each user of the State of Montana's computing and information resources must act responsibly. Each user is responsible for the integrity of these resources. All users of state-owned or state-leased computing systems must be knowledgeable of and adhere to agency policies, respect the rights of other users by minimizing unnecessary network traffic that might interfere with the ability of others to make effective use of this shared network resource, respect the integrity of the physical facilities and controls, and obey all federal, state, county, and local laws and ordinances. All employees must abide by these policies, relevant laws and contractual obligations, and appropriate ethical standards.

State computing facilities and User IDs are to be used for the job-related activities for which they are assigned. State computing resources are not to be used for the following:

- private commercial purposes,
- non-state-related activities (including games or software that is not required for an employees job responsibilities), or
- Non-state standard software. Exceptions can be granted by ITSD for the use of software for which a state standard exists.

All department employees or contractors with the department who have access to the Internet, e-mail, or other online services, will sign a consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources. Privacy in using the state's computer systems is not guaranteed. Therefore, employees should not have any expectations of privacy when using the Internet, e-mail, or other computer services.

MISUSE OF COMPUTER RESOURCES

The following items represent, but do not fully define, misuse of computing and information resources:

- Using computer resources to create, access, download, or disperse derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory materials.
- Down-loading, installing, or running security programs or utilities which reveal weaknesses in the security of the state's computer resources unless a job specifically requires it.
- Use of computers and User IDs for which there is no authorization, or use of user IDs for purpose(s) outside of those for which they have been issued.
- Attempting to modify, install, or remove computer equipment, software, or peripherals without proper authorization. This includes installing any non-work related software on State-owned equipment. All newly purchased computer hardware and software must have approval before the purchase is made. In addition proper authorization must be obtained prior to the installation, modification or removal of computer equipment, software or peripherals. Authorization will be requested using the Computer Hardware/Software Authorization Form **(Appendix B)**.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the state. (That is, if you abuse the networks to which the state has access or the computers at other sites connected to those networks, the state will treat this matter as an abuse of your computing privileges.)
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- The use of computing facilities, User IDs, or computer data for purposes other than those for which they were intended or authorized.

- Sending fraudulent e-mail, breaking into another user's e-mailbox, or unauthorized personnel reading someone else's e-mail without his or her permission.

- Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions or journal vouchers, or fraudulent electronic authorization of purchase requisitions or journal vouchers.

- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.

- Taking advantage of another user's naïveté or negligence to gain access to any User ID, data, software, or file that is not your own and for which you have not received explicit authorization to access.

- Physically interfering with other users' access to the state's computing facilities.

- Encroaching on or disrupting others' use of the state's shared network resources by creating unnecessary network traffic (for example, playing games or sending excessive messages); wasting computer time, connect time, disk space, or other resources; modifying system facilities, operating systems, or disk partitions without authorization; attempting to crash or tie up a state computer; damaging or vandalizing state computing facilities, equipment, software, or computer files).

- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.

- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.

- Knowingly transferring or allowing 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.

STATE STANDARDS FOR INFORMATION TECHNOLOGY PASSWORDS

State agencies and their employees shall follow these standards when establishing passwords for users, networks, computer systems or other information technology resources:

- Passwords must be at least 6 characters long;
- Passwords must contain at least one numeric and one alphabetic character;
- Passwords must not be obvious or easily guessed (userID, user's name, address, birth date, child's name, spouse's name);
- Passwords must be changed at least every 60 days;
- Passwords must not be reused for at least 4 cycles;
- Passwords must not be written down where they can be found by unauthorized personnel;
- Passwords must not be shared with other individuals.

REPORTING AND DISCIPLINARY ACTION

Users will cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines in handling diskettes and external files in order to maintain a secure, virus-free computing environment; follow agency procedures and guidelines for backing up data and making sure that critical data is saved to an appropriate location; and honor the acceptable use policies of any non-state networks accessed.

Users will report unacceptable use and other security violations to their immediate supervisor and to the department Information Technology Manager located in CSD.

Misuse of the state's computer resources may result in an agency taking disciplinary action appropriate to the misuse, up to and including termination.

DEPARTMENT OF MILITARY AFFAIRS
COMPUTER USE CONSENT FORM

I _____ have read the Department of Military Affairs computer use policy and agree to comply with all terms and conditions. I agree that all network activity conducted while doing state business and being conducted with state resources is the property of the State of Montana.

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

Signed_____

Date_____

Appendix A

DEPARTMENT OF MILITARY AFFAIRS
COMPUTER HARDWARE, SOFTWARE, PERIPHERALS
INSTALL/MODIFY/REMOVE
REQUEST FORM

☐ INSTALL ☐ MODIFY ☐ REMOVE

Description of hardware, software, peripheral to be installed, modified or removed:

ESTIMATED COST:

REVIEWS AND APPROVALS

Requested By:	Date:
Supervisor Approval:	Date:
IT Manager Approval:	Date:

Appendix B