DMA Policy: 1-0250
Name: INFORMATION TECHNOLOGY & SYSTEM SECURITY

Reference: DMA IT Policy Manual;
MOM Information Technology Policies

Approval Signature:
Effective Date: September 1, 2008
Last Revised: January 28, 2016

INFORMATION TECHNOLOGY AND SYSTEM SECURITY

This policy applies to all Department of Military Affairs (DMA) state employees and contractors (referred to as computer users) operating a state computer. All computer users must review this policy and the Information Technology Policy Manual, sign the Acknowledgment form and return to DMA Human Resources Officer. This policy and the IT policy manual are to be reviewed and signed on an annual basis.

All computer users must understand the importance of information technology and comply with safeguarding IT information and resources. Users and system administrators are responsible for guarding 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.

The Department is responsible for providing information technology education annually or as requested, to all DMA employees. The education should include and is not limited to:

- IT policies,
- The dangers of non-compliance and threat to the operation of the state computer network,
- Proper ethical behavior, acceptable computing practices, and copyright and licensing issues.
- Records retention, storage and purging files.

All computer users of state-owned or state-leased information technology and systems must be knowledgeable of and abide by all IT policies, relevant laws, contractual obligations, and appropriate ethical standards. Computer users must 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, and respect the integrity of the physical facilities and controls.

The DMA IT Policy Manual defines expectations for the following categories:

- Acceptable Use Policy,
- Email Policy,
- Ethics Policy,
- Password Protection Policy,
- Password Construction Guideline,
- Software Installation Policy,

- Wireless Communication Policy and Standards and,
- Workstation Security Policy.

REPORTING AND DISCIPLINARY ACTION

Computer users shall cooperate with system administrator requests for information about computing activities; follow agency procedures and guidelines 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 comply with the DMA IT Policy Manual.

Users will report unacceptable use and other security violations to his/her immediate supervisor and to the DMA Director's Office Information Systems Specialist.

Misuse of the state and Department computer resources may result in disciplinary action appropriate to the misuse, up to and including termination of employment.

ACKNOWLEDGEMENT FORM

I hereby acknowledge the receipt of the Department of Military Affairs Information Technology and System Security Policy and IT Manual. I am aware it is my duty to read and understand the policy and manual. I am also aware that failure to comply with any portion of the policy and/or manual is cause for disciplinary action up to and including termination of employment.

_____ _____

Employee's printed name Employee ID number

_____ _____

Employee's signature Date