

State Information Technology Policy

Notice and Consent

Use of this Government Computer System constitutes consent to monitoring of the system. Please use this technology responsibly. The contents and communications of this information system, including electronic mail (E-mail) and Internet access, may be monitored for inappropriate use. Inappropriate use may result in disciplinary action up to and including termination of employment.

Purchase and Acquisition

The Director of Information Management (DOIM) will review all purchases and acquisition of computer equipment and peripherals for this agency, in order to meet user and network requirements. All offices must coordinate with DOIM through their supervisory chain for purchase of computer systems or software and use of personal software (e.g., use of AOL on a government laptop). Violation of this policy may result in disciplinary actions.

Computer Use Policy

- Government provided hardware and software are for conducting official government business. Supervisors may authorize personnel to use government resources to further professional and technical knowledge if it is determined to be in the best interest of the agency.
- You are accountable and responsible for any transmission you generate, forward, copy, or distribute.
- Electronic communications are not confidential.
- Use of electronic communication (E-mail and Internet) are subject to official agency monitoring, and misuse may result in disciplinary action or criminal prosecution.
- The following activities involving the use of government computer hardware/software or network systems are specifically prohibited:
 - Storing, processing, displaying, sending, or transmitting language or material that is derogatory, discriminatory or offensive (e.g. hate or racist literature or symbols), obscene (pornography or sexually explicit), or sexually harassing material.
 - Storing or processing copyrighted material (including cartoons) unless approved by the author or publisher.
 - Activities for personal or commercial financial gain (e.g. sale of commercial or personal property).
 - Participating in "Chat Lines" or open forum discussion
 - Using another person's account or identity
 - Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.
 - Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).
 - Installing, copying, storing, or using unauthorized software.
 - Permitting any unauthorized individual access to a government owned or operated system.
 - Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.
 - Simultaneously being connected to the local area network AND a dial-up Internet service provider (e.g. AOL). This opens the system to outside intrusion.
 - Processing of classified information on any system not approved for classified information.
 - Connection of any non-agency owned equipment with out the written permission of the DOIM.
- Prior to an individual being granted access to a government network, they will sign a statement acknowledging they have reviewed and understand the provisions of this policy. Each individual's immediate supervisor is responsible to ensure that this occurs prior to system access.

I have read and understand this policy. I understand all information, including personal information, placed on or sent over this system may be monitored.

Signature

Date