

02-6--731-198

Rec'd
10/31/02
via Gail Swanson
@ training session



WASHINGTON MILITARY DEPARTMENT POLICY

Administrative Services Policy 00-004-02 **USE OF THE INTERNET, ELECTRONIC
MAIL AND COMPUTER SYSTEMS**

Effective September 1, 2002

Supersedes Administrative Policy 04-00 dated September 9, 2000

1. **PURPOSE:** To establish guidance for all employees on the use of the internet, internet access, electronic mail, and related computer systems.
2. **APPLICABILITY:** This policy applies to all employees of the Washington Military Department (WMD), which includes state employees, federal employees full-time, part-time, traditional guard members, and contractors. Commanders, managers, and supervisors are not authorized to make exceptions to this policy unless specifically authorized herein; however, they may impose tighter restrictions.
3. **REFERENCES**
 - a. Army Regulation 25-1, Army Information Management
 - b. Air Force Instruction 33-119, Electronic Mail Management and Use.
 - c. Air Force Instruction 33-129, Transmission of Information via the Internet.
 - d. ANG-PD 33-1, Internet and Electronic Mail Policy
 - e. ANGI 33-103, Internet and Electronic Mail Policy
 - f. RCW 42.52 Ethics in Public Service
 - g. WAC 292-110-010, Use of State Resources
 - h. Washington Executive Ethics Board Advisory Opinions 96-04, 97-04, 02-01, and 02-02
 - i. Governor's Executive Order EO-00-02
 - j. DA Pam 25-1-1 Installation Information Services
 - k. Joint Ethics Regulation 30-210
4. **ADJUTANT GENERAL INTENT:** As a state agency we are charged with ensuring that publicly purchased equipment and services are properly utilized and not misused. It is the intent of this policy to set guidelines that are clear, concise, and can be followed by all of our members regardless of status.
5. **POLICY:** Internet connectivity, electronic mail, and computer systems are provided primarily to send, receive, and store information of an official, work related, and nature. Unless specifically provided by this policy, public law, ethics guidance letters and/or government regulation, all other use is prohibited. Violation of this policy is a basis for adverse administrative and/or disciplinary action up to and including termination, involuntary separation, and prosecution under any or/and all applicable federal or

APPROVED
Executive Ethics Board

Date: 2/14/03

Use of Internet, Electronic Mail and Computer Systems

Administrative Services Policy 00-004-02

Page 2 of 3

state laws and codes. Use of department communications and Internet systems is subject to monitoring at any time. Users should have no expectation of privacy. Unless specifically designated, as an exception, all Department systems are for unclassified administrative use only.

6. **MONITORING AND REPORTING:** First-line supervisors will have the primary responsibility for ensuring employees' compliance with this policy, for reporting misuse, and in taking recommended appropriate corrective or disciplinary action. Technical assistance to the supervisors will be provided by the appropriate Information Systems Support Staff. The Information Systems (IS) Managers and their IS Support Staff are authorized to randomly audit usage to ensure compliance with applicable laws and directives. The IS Managers will maintain software and hardware capable of monitoring all use of the network.
7. **EQUIPMENT ATTACHED TO THE NETWORK:** All equipment attached to the network will be approved by the appropriate IS Manager. The use of personal equipment on the department systems is strictly forbidden.
8. **SOFTWARE:** All software used on department computers must be licensed and authorized by the applicable IS Support Staff. No department/division-furnished software, not specifically approved for use by the network manager, will be loaded to a workstation or server attached to the network. Public Domain and Shareware software will only be installed as approved by the appropriate IS Support Staff.
9. **VIRUS PROTECTION:** All equipment attached to the network will have a department/division licensed anti-virus software program with current virus data files installed and operational.
10. **PERMITTED ACTIVITIES:**
 - a. Use of internet, electronic mail, and computer services for official business.
 - b. Federal and state rules, policies, regulations and directives allow for de minimis, infrequent personal use of electronic mail, and computer services, provided it:
 - (1) Does not result in a cost to the organization
 - (2) Does not interfere with the performance of official duties
 - (3) Is short in duration and frequency,
 - (4) Will be confined to off-duty periods, such as breaks, lunch or after work
 - (5) Is not related to any outside business activity
 - (6) Does not distract from the conduct of official business
 - (7) Does not disrupt other employees and does not obligate them to make a personal use of state resources
 - (8) Does not compromise the security or integrity of organizational information, systems, or software
 - (9) Is used to assess potential or existing security holes or perform routine vulnerability scans on the network by each division's IS manager, and

APPROVED

Executive Ethics Board

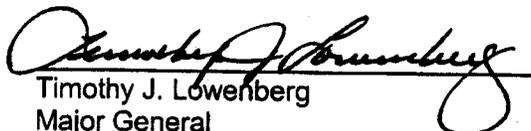
Date: 2/14/03

(10) Is not specifically prohibited in section 11 below.

11. PROHIBITED ACTIVITIES: The following activities are specifically prohibited:

- a. Sending or forwarding classified material on unclassified systems.
- b. Sending or forwarding virus warnings of any sort to anyone other than IS Support Staff.
- c. Sending or forwarding chain letters of any sort, harassing electronic mail, not required for official business.
- d. Fundraising activities not specifically authorized in references (3 above).
- e. Playing games, streaming video or music/radio stations on or over the Internet unless specifically permitted by the IS Manager/Support Staff.
- f. Subscribing to mailing lists and broadcast services that are not work related.
- g. Intentionally browsing to Internet sites or knowingly receiving, sending, forwarding or generating information of a sexual nature.
- h. Browsing to Internet sites whose contents are of a subversive or anti-government nature unless authorized, in writing by the individual's supervisory chain and the IS Manager, as part of official duties.
- i. Sending or forwarding unsolicited electronic mail or attachments of a political nature, including lobbying for support of a specific piece of legislation other than as a part of your official department business.
- j. Participating in Internet chat rooms that are not work or mission related. An example of a work related activity would be participating in an online training program that hosts an instructor/student chat room.
- k. The malicious or unrestrained use of any hacker tools or techniques is strictly forbidden.

12. This policy will be reviewed by the Information Technology Review Board (ITRB) annually. The ITRB will recommend changes and updates to the management team.


Timothy J. Lowenberg
Major General
The Adjutant General
Director, WMD

26 August 2002
Date

APPROVED
Executive Ethics Board

Date: 2/14/03