DEPARTMENT OF MILITARY AFFAIRS
STATE HUMAN RESOURCES
PRACTICE AND PROCEDURE MANUAL

STATUS: (X) FINAL ( ) DRAFT	BULLETIN NO: 2.105
EFFECTIVE DATE: 10/11/99	PAGE: 1 OF 3
REVISED: 11/10/2020	

SUBJECT: Internet Use and Management

SECTION: Information Management

I. PRACTICE

A. Statement of Policy and Purpose

The Department of Military Affairs (DMA) will use the Internet/World Wide Web (WWW) as an effective, efficient, and timely source of information, method of communication, and vehicle for data collection, information dissemination, and delivery of services to DMA clients and customers. Because of legal, security, and user productivity issues associated with Internet use in the workplace, the DMA has adapted the following policy regarding Internet/World Wide Web use by state employees. All staff must comply with this policy and the policies for any host machines to which they are granted access.

The design of DMA's computer system is such that we sometimes suffer bandwidth constraints that interfere with the efficient operation of the system. Bandwidth constraints involve the ability of telecommunications circuits to bear network traffic. Some constraints occur in our local circuits and some constraints occur at gateways upstream of our network. Increasing network traffic, such as increasing web use and downloading files via the Internet can quickly overload the bearing capacity of our system. Traffic generated at the user level travels upstream and combines with the traffic of other users until it is funneled into only a few large capacity gateways. Required bandwidth at the lower echelons sometimes grows quicker than the ability of the higher echelons to increase bandwidth to accommodate increased requirements. When we overload the system with a mix of official and unofficial traffic, the entire system is degraded. The system does not distinguish between critical business applications and unnecessary use. That is why is it important that we limit our use of bandwidth to essential uses that achieve our required business purpose.

The Information Management Directorate has the ability to monitor Internet/WWW sites that users visit using agency computer equipment. By using the equipment, users give consent to such monitoring.

Conscientious use of our computer system will avoid overburdening communication systems and avoid making it necessary to use scarce resources to eliminate service disruptions and system degradation that could easily be avoided.

II. PROCEDURE

A. Internet Use

Internet resources are to be used in a manner consistent with the administrative, informational, instructional, and research objectives of the department. Appropriate use of resources is limited to the official work of the department and its mission. Government-provided resources shall not be used for private, personal, or nonofficial use.

Inappropriate use of the Internet/WWW may be grounds for disciplinary action. Internet/WWW users must use our resources responsibly and abide by acceptable standards of professional and personal conduct. Internet/WWW access will not be used in a way that would interfere with official duties, reflect adversely upon the organization (such as uses involving pornography and sexual gratification related sites or other uses that are incompatible with public service) or further any unlawful activity or personal commercial purpose. Examples of inappropriate use of resources include, but are not limited to, any use that violates state and/or federal laws, any use that is unethical in nature, distribution of unsolicited advertising, propagation of computer viruses, distribution of chain letters, attempts to make unauthorized entry to another network node, and recreational or personal activities. Internet/WWW access is provided at government expense to conduct government business.

Employees shall respect the privacy of others. Do not seek information about, obtain copies of, or modify electronic information belonging to other users unless explicitly authorized to do so.

Passwords should not be shared with unauthorized users nor should employees use passwords not belonging to them unless specific authorization is given.

Copyright laws, licensing agreements, and trade-secret laws that control the distribution and use of programs, databases, and other electronic information resources should be strictly observed.

Be aware of the classification of information contained in data files or correspondence that is transported using Internet access. Do not exchange private or confidential information in un-encrypted form.

Employees may use access to the Internet/WWW for occasional and incidental personal use providing such use:

a. Does not contribute to significant degradation of the system. For example, employees are not permitted to regularly access the Internet/WWW for unofficial purposes during their lunch or break periods because the compounded effect of that use would be to cause the system to degrade to where it would not function properly for users with an official purpose.

b. Does not interfere with the organization's operation. For example, employees are expected to perform official duties during work hours and would not be permitted to access the Internet/WWW for unofficial purposes.

c. Does not incur additional expense to the government. Note that all WIARNG small sites (principally unit armories below battalion level) are dial up sites which require that a long-distance call be made (via computer) to access the Internet/WWW. Making a long-distance call to access the Internet incurs an additional expense to the government. It is just like using a government telephone to make a personal long-distance telephone call, only it is done via computer and modem.

B. Downloadable Software Applications

Downloadable software applications (including Internet browser plug-ins and tools) typically become locally resident on a desktop computer hard drive and may produce technical problems by conflicting with other software applications required for DMA business needs. As is appropriate for any software loaded on any DMA computer, only WIAR-IM staff should perform software installs or provide specific instructions for others regarding such installations. WIAR-IM staff must precede such software installations with testing, documentation, and training to ensure compatibility with DMA's computing environment and manage technical support resources to meet DMA's business needs. All staff requests for tools to better meet business needs should be reviewed by WIAR-IM staff for assessment.

Attachment:

See P&P No. 2.110 for Receipt Certification