ACCEPTABLE USE FOR COMPUTER RESOURCES

Directive 3 - 107

Date Issued: April 2016 Amends/Cancels: 3-107 Issued March 2014

I. PURPOSE

This directive outlines acceptable use of the computing systems and equipment owned and operated by the State of Maryland.

II. POLICY

A. It is the policy of the Department of General Services Maryland Capitol Police (MCP) that members use all computing resources that are owned or leased by the State, including, but not limited to computers, software programs, and Internet accessed by any of these software programs and equipment in a professional, ethical and legal manner.

B. State owned or leased computing resources will be only be utilized by members to accomplish and support the mission of the Department by promoting communication and information gathering and sharing, and conducting Department business more efficiently.

C. All members utilizing State owned or leased computing resources will adhere to all guidelines, rules, regulations and directives issued by the Maryland Department of Information Technology (DoIT).

III. DEFINITIONS

A. COMPUTER RESOURCES - The definition of computer resources includes any computer, server or network provided or supported by the State of Maryland and the DoIT. Use of the computer resources includes the use of data/programs stored on State of Maryland owned computing equipment, data/programs stored on magnetic tape, floppy disks, flash drives, CD/DVD's or other storage media.

B. INAPPROPRIATE MATERIAL – Any material that is inconsistent with the goals, objectives and policies of the Department of General Services and/or the Maryland Capitol Police.

C. OBSCENE MATERIAL – Any material that the average person, applying contemporary standards, would find, taken as a whole, appeals to prurient interest (Material having a prurient interest is defined as material having a tendency to excite lustful thoughts (Monfred v.State, 1961);

1. depicts or describes, in a patently offensive way, sexual conduct as defined in Criminal Law, Section 11-101(d) of the Annotated Code of Maryland; or

2. taken as a whole, lacks serious literary, artistic, political or business value.

D. USER - An employee of Department of General Services (DGS) utilizing State owned or leased computer resources.

IV. PROCEDURES

A. RESPONSBILITIES

1. User Responsibilities:

   a. All utilization of computer resources that are owned or leased by the State may be monitored and recorded. Users consent to such monitoring and recording.

   b. Users are responsible for protecting any information used and /or stored on their DoIT accounts. Employees will be familiar with DoIT guidelines on protecting user accounts and information using the standard system protection mechanisms.

   c. Users will report any weaknesses in computer resource security, any incidents of possible misuse or violation of this policy to their supervisor.

2. Supervisors Responsibilities:

   a. Upon being notified of security issues and/or misuse supervisors will immediately report the incident DoIT.

   b. If the misuse reported is being perpetrated by MCP personnel, the supervisor will complete a Form 176 “Complaint Against Personnel” and forward it to their Commander per procedures outlined in Directive 5-102 and 5-105.

3. DoIT Responsibilities:

   In the event that any monitoring reveals possible evidence of criminal activity or user misconduct, DoIT will notify the Chief of Police and provide him or his designee with any and all possible evidence.

B. COMPUTER RESOURCE SECURITY

1. While using computing resources, users are cautioned not to reveal their names, addresses, telephone numbers or other personal information to other persons via e-mail or any other form of communication.

2. Users will not:

    a. reveal any personal information of other employees to anyone.

    b. attempt to access any data or programs contained on computer resources for which they do not have authorization or explicit consent of the owner of the data/program, the Chief of Police or his designee, or DoIT.

    c. divulge Dial-up or Dial-back modem phone numbers to anyone.

    d. share their DoIT account(s) with anyone. This includes sharing the password to the account, providing access via a host entry or other means of sharing.

    e. Attempt to log-in to another users account without authorization from the Chief of Police or his designee or DoIT.

    f. make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

    g. make copies of system configuration files or program files for personal use or to provide to other people/users for unauthorized purposes.

    h. purposely engage in activity with the intent to: harass other users, degrade the performance of systems, deprive an authorized user access to a computer resources, obtain extra resources, beyond those allocated, circumvent DoIT computer security measures, or gain access to a system for which proper authorization has not been given.

    i. download, install, or run software programs, security programs or software utility programs without the approval of the DoIT.

    j. attempt to repair, upgrade or modify any computing resources. All problems should be reported to DoIT.

    k. copy or download any intellectual property protected by copyright onto State owned or leased computer resources.

C. ELECTRONIC COMMUNICATIONS:

1. Electronic communication facilities (such as e-mail or internet) are for authorized government use only.

2. Electronic mail communications (Email) are not considered confidential and may also be monitored. Users acknowledge that they have no reasonable expectation of privacy with regard to any email message, whether or not it is marked “Private” or “Confidential.”

2. Users shall not:

    a. send or forward chain email messages or jokes;

b. transmit illegal, malicious, threatening or obscene materials;

c. transmit communications containing harassing, slanderous or libelous statements;

d. conduct political campaigning or soliciting;

e. purchase or make inquiries pertaining to trades, auctions or other personal commerce to include, but not restricted to, stocks, bonds, e-commerce, travel, reservations, etc;

f. send inflammatory, critical or derogatory messages of the type known as “Flaming”;

g. send junk e-mail such as advertisements to news groups, lists or unknown third parties known as “Spam”;

h. transmit of any inappropriate and/or obscene material of any type or form;

i. use of profanity, vulgarities, swearing or any other inappropriate language;

j. transmit or receive of communications that discriminate based on gender, race, color, religion, ethnic or national origin, political beliefs, marital status, age, sexual orientation, social and family background, linguistic preference, or disability;

k. misrepresent themselves or their identity;

l. disseminate in any manner any communications that contain information that has been classified as law enforcement sensitive or confidential unless the recipient is a law enforcement officer or other authorized person.

D. INTERNET USE

1. Internet resources are provided to support the mission of the department and will not be utilized for other purposes.

2. Internet usage may also be monitored by DoIT. Users acknowledge that the improper, unauthorized use of the Internet, including, but not limited to, visiting or viewing inappropriate or obscene material will lead to disciplinary action.

2. Use of any information obtained via the Internet is at the user’s own risk. Users must consider the source of any information obtained and evaluate the validity of that information. The State of Maryland accepts no responsibility for the accuracy or quality of information obtained through Internet access.