University of Wisconsin–Madison Police

Policy: 11.5
SUBJECT: COMPUTER USE
EFFECTIVE DATE: 06/01/10 **REVISED DATE: 12/31/11**
REVIEWED DATE: 05/01/14

INDEX:

POLICY:

Each employee is expected to protect the integrity of these resources and to know and adhere to University and Department rules, regulations, and guidelines for their appropriate use. Each University of Wisconsin–Madison Police Department employee is part of a network of IT users. Each has the ability to negatively impact the system, and therefore every other Department member, if the following guidelines are not strictly adhered to. It is important to remember that each workstation is not isolated but connected and that the actions of one impact us all.

DEFINITIONS:

Computer "hardware" refers to the mechanical, magnetic, electronic, and electrical devices constituting a computer system, such as the CPU, disk drives, keyboard, and screen.

Computer "software" refers to the programs used to direct the operation of a computer, as well as documentation giving instructions on how to use those programs.

PROCEDURE:

11.5.1 COMPUTER USE – GENERAL

The following establishes general procedures regarding computer use by Department personnel:

A. Computers, software, databases, e-mail accounts, Internet access, and other information technology (IT) resources are tools provided by the Department to employees to support the missions of both the University and the Department.

B. Each employee is expected to protect the integrity of these resources and to know and adhere to University and Department rules, regulations, and guidelines for their appropriate use. [redacted]

C. The Department IT staff shall provide training in the use of computers and software required for each position. Employees shall use computer resources in a manner consistent with their training to maintain a system that is secure, reliable, and predictable.

D. Access to University IT resources is a privilege granted to members of this Department to be used for appropriate University- and Department-related activities. Authorization for the use of IT resources is provided to each employee for his or her exclusive use and is not permitted to be used by others (i.e., friends, family members, guests).

E. The protection of University IT resources depends heavily on each user's careful handling of the "keys" (accounts, access, and passwords) to these resources, s[redacted] These "keys" should be changed frequently and their security protected to prevent unauthorized intrusions into the network. Employees are responsible for the security of the "keys" provided to them.

F. Playing or downloading/configuring any form of interactive material/game is generally prohibited. If there is a business value to interactive material, it should be checked by the IT Staff and approved by a supervisor.

G. If an employee believes a computer has become infected with a virus, malware, spyware or other malicious code, [redacted]

[redacted] If it is believed a data breech occurred from the malicious code, then it needs to be immediately reported to a supervisor or MOC and the IT administrator.

11.5.2 COMPUTER USE – MALICIOUS ACTIVITY

The following establishes prohibitions on malicious activity in regards to computer use:

A. Employees shall not obtain or use or attempt to obtain or use any hardware or software resources not assigned to them or without prior approval from the IT Administrator.

B. Employees must not alter or intentionally damage University or privately owned software or data or interfere with an authorized user's access.

C. [redacted]s [redacted]

D. Personnel shall not obtain or use—or attempt to obtain or use—passwords, IP addresses, or other network codes that have not been assigned to them as individuals or authorized for their use as University employees. Persons shall not obtain—or attempt to obtain—unauthorized access to computer accounts, software, files, or any other University IT resources, unless as part of a criminal investigation.

E. Users of University IT resources shall not send electronic messages with the sender's identity forged or send anonymous messages unless this action is part of an investigation.

F. Employees shall not access profane, obscene, inappropriate, offensive, or illegal material using University IT resources, unless accessing the material is done as part of an official police investigation or for training purposes.

G. In the interest of making the use of University and Department IT resources a natural part of day-to-day work of all members of the University community, incidental personal use is tolerated. However, IT resources will not be used for commercial or extensive nonbusiness use. Department employees shall not use computer resources to support the nomination of any person for political office or to influence a vote in any election or referendum.

11.5.3 USE OF SOFTWARE

The following establishes procedures regarding the use of software on Department computers:

A. Only properly licensed and IT Administrator-approved software may be used on Department computers.

B. Prior to the purchase of any new software, users who need specialized software must submit a request to the IT Administrator documenting the need, the proposed software, the anticipated results, and ongoing support options and costs.

C. The IT Administrator or designee will approve and load all software on the system in order to ensure compatibility with the system.

D. Copies of Department-owned software and/or docu-mentation will be made and distributed in accordance with the software licensing agreement.

E. [redacted].

F. Software malfunctions should be reported to the IT Administrator or designee in a timely manner.

G. Demonstration materials obtained from third parties are to be reviewed by the IT Administrator or designee prior to review or use in any Department computer. This includes CD-ROM material from vendors and other law enforcement agencies.

H. [redacted]. Data that does not need to be kept for business purposes, most notably video and other large files, should be deleted. Data

should not be retained longer than required for business purposes or according to open records laws and record retention schedules.

11.5.4 USE OF HARDWARE

The following establishes procedures regarding the use of Department computer hardware:

A. [redacted] Use of personally owned flash memory or other portable data storage devices in Department-owned computers is prohibited.

B. Computers are precision instruments and are easily damaged. Special care should be exercised to avoid using food, drink, sprays, physical force, or poten-tially damaging items in the area of computer equipment. Intentional damage to equipment is prohibited, except in the event destruction is authorized by IT staff.

C. Employees shall report damage, serious problems, and emergency maintenance needs immediately to the IT Administrator or designee during normal business hours and to the police OIC or manager on call after hours. Routine problems that do not prevent the accomplishment of required work may wait to be addressed during normal business hours.

11.5.5 USE OF MOBILE DATA COMPUTERS

The following establishes procedures regarding the use of mobile data computers:

A. Employees shall use the system as specified in training.

B. Police patrol officers and route security officers will sign on and off the MDC when beginning and ending their shifts, unless exigent circumstances exist.

C. Officers are responsible for making their own status changes from the MDC as these occur.

D. Dispositions will be completed upon returning to the MDC, unless exigent circumstances exist.

E. All communications are expected to be professional. Communications are subject to open records law and may be monitored by supervisors.

F. Police officers and route security officers assigned to vehicle patrol or a security route should use vehicles equipped with an operational MDC unless exigent circumstances exist.

G. Only personnel specifically authorized and trained may access state and federal databases.

H. Printers attached to Mobile Data Computers are to be used exclusively for printing citations.

11.5.6 REMOTE CONNECTIONS

The following establishes procedures regarding remote connections to the Department:

A. [redacted]

B. [redacted].

11.5.7 COMPUTER USE – PASSWORD PROTOCOLS

The following establishes procedures regarding password protocols:

A. Each employee is assigned a unique identification (ID) number and is responsible for all business transacted and reading information/messages under his or her login ID. Any suspected misuse of accounts or passwords must be reported immediately to IT staff.

B. [redacted]

[redacted]

C. Passwords must be kept private, [redacted].

D. Personnel must lock or log off all systems when leaving them unattended for extended periods of time, including when leaving for the night. [redacted].

E. [redacted] Each employee must check his or her Department e-mail each day that s/he is on duty.

11.5.8 PHYSICAL SECURITY OF COMPUTERS

The following establishes procedures regarding physical security of Department computers:

A. Access to the computer and server rooms is restricted to authorized personnel.

B. Care should be taken to maintain the physical security of all computer equipment. Possible breaches of physical security (unauthorized access, lost or stolen devices, etc.) should be immediately reported to your immediate supervisor and the IT Administrator.