UW–Madison Police Department

Policy: 11.5
SUBJECT: COMPUTER USE
EFFECTIVE DATE: 06/01/10 **REVISED DATE: 04/17/19; 11/19/19**
REVIEWED DATE: 02/01/17 **STANDARD: CALEA 11.4.4, 41.3.7**

INDEX:

11.5.1 COMPUTER USE – GENERAL
11.5.2 COMPUTER USE
11.5.3 USE OF SOFTWARE
11.5.4 USE OF HARDWARE
11.5.5 USE OF MOBILE DATA COMPUTERS
11.5.6 REMOTE CONNECTIONS
11.5.7 COMPUTER USE – PASSWORD PROTOCOLS
11.5.8 PHYSICAL SECURITY OF COMPUTERS
11.5.9 INTERNET USAGE AND EMAIL
11.5.10 CELLULAR PHONES

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 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

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. 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.

C. 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 their exclusive use and is not permitted to be used by others (i.e., friends, family members, guests).

D. The protection of University IT resources depends heavily on each user's careful handling of the "keys" (accounts, access, and passwords) to these resources, [redacted]. Employees are responsible for the security of the "keys" provided to them.

E. Department members are responsible for their own network account, regardless of who actually uses it; therefore, they are responsible for logging off the network upon completion of their computer activity.

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 [redacted] f 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 Director.

11.5.2 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 Director.

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

[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. UWPD personnel shall abide by all Terms of Service as stipulated by the site or software; this includes, but is not limited to, a prohibition of falsely identifying oneself on a site or sites other than for investigatory purposes, infringing on copyrighted material, and violating the privacy or rights of other users.

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. shall

H. IT resources shall not be used for commercial, investment, consultant or extensive non-business use.

I. Department employees shall not use computer resources for making any campaign contribution in support of any person for political office or to influence a vote in any election or referendum.

11.5.3 USE OF SOFTWARE

A. Only properly licensed and IT Director-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 Director documenting the need, the proposed software, the anticipated results, and ongoing support options and costs.

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

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

[redacted]

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

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

[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

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 potentially 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

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

B. Police patrol officers and route security officers shall 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 shall 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

[redacted]

11.5.7 COMPUTER USE – PASSWORD PROTOCOLS

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

immediately to IT staff.

B. [redacted]

C. Passwords must be kept private, [redacted]

D. Passwords shall not be shared, stored, transmitted, or transported in an unsecured manner.

E. Personnel should not check or configure options that allow a password to be saved, if the website or program contains CJIS related material.

11.5.8 PHYSICAL SECURITY OF 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. [redacted]

11.5.9 INTERNET USAGE AND EMAIL

A. There is no expectation of privacy in using department internal email, external email or internet services on State-owned computers. All use of State computers, whether official or personal, is subject to public disclosure laws and can be discoverable in all court proceedings.

B. External Email (Wiscmail) correspondence outside the Department shall contain the employee's contact information including email address, business address and a UWPD phone number.

C. [redacted]

D. Employees should contact UW-Police IT if they have questions about an email attachment. Due to the risk of computer virus attacks, employees should not open email attachments from unknown sources.

E. Employee Internet use shall not disrupt or interfere with the work of other network users or adversely affect internet service of the department.

F. Employees must check and respond appropriately to their department internal e-mail(s) and assigned VoIP voicemails (if assigned) each day they are on duty.

G. [redacted]

H. Employees are strictly prohibited from using any personal cellular phone or similar device as a media storage device for the storage or transportation of any UWPD business information.

11.5.10 CELLULAR PHONES

A. Squad Cellular Phones

1. Squad cell phones are to be used as a tool to enhance police operations and are not intended to reduce in-person contact

2. Officers shall use squad cell phones for official business only. Cell phones allow officers to make calls from the squad instead of returning to the station and shall be used instead of a personal device.

3. Squad cell phones shall be used for official business in cases when it would not be appropriate to use the radio or MDC.

4. Needed repairs or service to squad cell phones shall be reported promptly to the Vehicle Maintenance Team. Notification should be made using the established computerized reporting system.