Policy Number: 317 – Information Technology Use
Effective Date: June 26, 2020
Revision Date: June 26, 2020
Approved By: Denis Otterness, Chief of Police

317.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of Montana State University Billings Police Department (Department) information technology resources, including computers, electronic devices, hardware, software and systems.

317.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site, portable and mobile), electronic devices, hardware, software, and resources owned, leased, rented or licensed by Montana State University Billings and/or the Department that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones (including cellular and satellite), pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

317.2 POLICY

It is the policy of this Department that members shall use information technology resources, whether issued or maintained by the Department, in a professional manner and in accordance with this policy and the information technology policies of the Montana Board of Regents and Montana State University Billings.

317.3 PRIVACY EXPECTATION

Department members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any internet site that is accessed, transmitted, received or reviewed on any Department computer system.

The Department reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the Department, including the Department email system, computer network and/or any information placed into storage on any Department system or device. This includes records of all key strokes or web-browsing history made at any Department computer or over any Department network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through Department computers, electronic devices or networks.

However, the Department may not require a member to disclose a personal user name or password or open a personal social website, except when the employer has specific information about activity by an employee and access is reasonably believed to be relevant to the investigation of allegations of work related misconduct (§ 39-2-307, MCA).

317.4 RESTRICTED USE

Department members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Department members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to a Department supervisor.

Department members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

317.4.1 SOFTWARE

Department members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, Department members shall not install any unlicensed or unauthorized software on any Department computer. Members shall not install personal copies of any software on any Department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of Information Technology (I.T.) staff and with the authorization of the Chief of Police, or their designee.

No Department member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on Department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by Department members should only occur as a part of the automated maintenance or update process of Department or State-approved or installed programs by the original manufacturer, producer or developer of the software. Any other introduction of software requires prior authorization from I.T. staff and a full scan for malicious attachments.

317.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to Department-related activities. Data stored on or available through Department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or Department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

317.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to Department-related activities. Internet sites containing information that is not appropriate or applicable to Department use, and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a Department member's assignment. Downloaded information from the internet shall be limited to messages, mail and data files.

317.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty, or in conjunction with specific on-call assignments, unless specifically authorized by the Chief of Police. This includes the use of telephones, cell phones, texting, email, or any other off-the-clock work-related activities. This also applies to personally owned devices that are used to access Department resources

317.5 PROTECTION OF SYSTEMS AND FILES

All Department members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of computer systems.

Department members shall ensure Department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content

shall meet the prescribed standards required by the computer system, or as directed by a supervisor, and shall be changed at intervals as directed by I.T. staff or a supervisor.

It is prohibited for a Department member to allow an unauthorized user to access the computer system at any time or for any reason. Department members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

317.6 INSPECTION AND REVIEW

The Chief of Police, or their designee, may request I.T. staff inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, as authorized under the policies of the Board of Regents and the University.

I.T. staff may extract, download, or otherwise obtain, any and all temporary or permanent files residing on, or located in, the Department computer system as authorized under the policies of the Board of Regents and the University.