USA Faculty/Staff Computer Use Policy

User Privileges and Responsibilities

Authorization. In general, USA colleges and departments are responsible for the allocation of computer resources for their faculty and staff. ***No one should use any University computer or network facility without authorization from the appropriate personnel in that office or department.*** University computers and networks are to be used for University purposes, i.e., to further the educational programs of the University. Any attempt to disrupt, degrade or improperly gain access to University computer resources is prohibited. Unauthorized wiring, altering or damaging of University-owned computer equipment, including network hardware and software, is also prohibited.

IDs/Passwords. No one should share their password with another person, nor obtain another person's password by any unauthorized means. Deliberately and inappropriately observing, recording, accessing, using or transmitting passwords, account numbers, e-mail addresses, phone numbers or credit card numbers belonging to other people is strictly prohibited.

Administrative Devices. An "administrative device" refers to a thin client or microcomputer used to access administrative computer systems (e.g., Student Information Systems and Financial Systems). Access to administrative devices is limited to individuals engaging in official University business. All persons given unique passwords and sign-ons are required to sign a Statement of Accountability, which states that this information is not to be shared with any other individual. (Authorized personnel should see Information Systems Security Policy for further details concerning use and misuse of administrative devices.)

Email. The University email systems are to be used for University business only -- not for personal business or personal gain. Users have full responsibility for all messages they transmit through the University's computers, networks and systems. Consequently, all laws and rules against fraud, harassment, obscenity, etc., which govern all University communications also apply to email. Abuse of the email system may be grounds for disciplinary action, up to and including termination.

No Spam. "Spam", the practice of mass-broadcasting unsolicited email (e.g., commercial advertisements, chain mail, pornographic materials, political

lobbying, hate speech, racial diatribes, and religious proselytizing), ***is strictly prohibited at USA***.

Viruses. Users are advised NOT to download email attachments as these may contain malware or viruses that could infect University computers and/or networks. It is illegal to knowingly replicate or transmit computer viruses, or otherwise deliberately damage the systems or files of other people. Users should install university provided Anti-Virus software to provide protection against malware.

Confidentiality and Security. No one without specific authorization may read, alter, or delete any other person's computer files or email, even if the equipment and software have that capability. ***No email system is completely secure***. Consequently, email should not be used to transmit computer passwords, credit card numbers, or other confidential information about students or employees. Routine maintenance of the email systems may require or inadvertently lead to viewing some pieces. The CSC will respect the privacy of such mail, and will not reveal its contents to any other parties. However, if activities in violation of law or University regulations are discovered through this procedure, the CSC may report such information to the appropriate authorities. Departments are advised that information subject to confidentiality regulations should not be transmitted via these electronic media without prior written approval from the appropriate administrative offices.

No "Hacking" or "Cracking". Deliberately invading the privacy of others by attempting to gain unauthorized access to any account or system is strictly prohibited.

Internet. All computer accounts provided to faculty/staff are intended for the University's work. Many University departments do encourage their employees to use the Internet to educate themselves, provided time and equipment are available. As a University employee, you are accountable for how you use your time on the job. In consideration of other network users, employees should limit bandwidth-intensive activities (e.g., playing or downloading network-based games, music or video) to those that are required as part of their employment. University employees are prohibited from using University equipment for private money-making enterprises. Due to the real danger of transmitting computer viruses, extreme care should be taken in downloading executable files from the Internet onto University computers. It is unacceptable to use University equipment or networks to view, download,

post, print or send pornography, or other sexually explicit, profane, obscene, hostile, or blatantly offensive and intimidating material, including hate speech, threats, harassing communications (as defined by law), or information that violates any state or federal laws. Using University equipment/networks for the sale of weapons, drugs or illegal substances is strictly prohibited.

Web Pages. All web pages running on University-owned servers must adhere to USA's Web Policies, which can be viewed in their entirety from the USA Web Services web site . These policies govern the management of those electronic documents that represent USA and are accessible on the Internet. Individual University departments are responsible for the accuracy and integrity of the contents of their web pages, and have full responsibility for what they publish. The Web Services office periodically reviews USA web sites and links to ensure that the University is being represented appropriately and that all official symbols are being used correctly. Any objectionable content found in USA web sites or links will be subject to laws and rules against fraud, harassment, obscenity, etc.

Software Licensing (copyright laws). All faculty/staff should be aware that uploading or downloading copyrighted material, violating the intellectual property rights of others, or illegally sharing trade secrets is strictly prohibited at USA. All reproduction and use of computer software on University equipment or by University employees or students in pursuit of University business or instruction must be in accordance with copyright law (as set forth in Title 17, United States Code) and the manufacturer's condition of sale. (See the USA Software Policy, printed in its entirety at the end of this document.)

Violations/Consequences
In addition to all guidelines in the policies stated here, all USA employees are subject to the policies and disciplinary procedures outlined in the Staff Employee Handbook and the Faculty Handbook. Violations of any USA computer policies incur the same types of disciplinary measures as other University policies or state or federal laws (up to and including criminal prosecution).

Revised: August 10, 2016