INSTITUTIONAL POLICY: GA-31

Category:	General Administration
Subject:	Acceptable Use of Information Technology Resources
Effective Date:	November 9, 2010
Last Revision Date:	May 16, 2014
Applicability:	Employees, Students, and Others Utilizing WVSOM Information Technology Resources

GA 31-1. Authority

1.1 W. Va. Code § 18B-1-6

1.2 W. Va. Code R. § 133-4

GA 31-2. Purpose

The purpose of this policy is to provide, promote, and establish the secure, ethical, and legal use of information technology ("IT") resources, including data, devices, software, and electronic communications for all constituents of the West Virginia School of Osteopathic Medicine ("WVSOM"). This includes staff, faculty, students, alumni, Statewide Campus entities, WVSOM Board of Governors members, vendors, guests, and others utilizing WVSOM's IT resources. In order for WVSOM to maintain the highest standards and the most innovative and quality-based technologies, adherence to acceptable IT resources usage is critical.

GA 31-3. Definitions

3.1 "Chain Letters" means letters instructing the recipient to send out multiple copies, so that its circulation increases in a geometrical progression as long as the instructions are followed.

3.2 "Cloud" means shared computer resources outside of WVSOM's internal Network accessed securely via the internet for virtual applications such as email.

3.3 "Content" means any information, data, text, software, music, sound, photographs, graphics, video, messages, or any other material that may be uploaded, posted, emailed, or otherwise transmitted by a user of WVSOM's IT resources.

3.4 "Firewall" means a combination of hardware and software used to prevent unauthorized access to Networks when certain security criteria are not met.

3.5 "Gateway" means an entrance into a Network.

3.6 "Network" means a group of interconnected computers, computer peripherals, and other technology resources which is constructed in a particular topology for electronic access and communication to other technology resources based on certain protocols and rules.

3.7 "Personally Identifiable Information" or "PII" means all information that identifies, or can be used to identify, locate, contact, or impersonate a particular individual. PII also includes Protected Health Information ("PHI") as that term is defined below. PII is contained in public and non-public records. Examples may include but are not limited to a specific individual's: first name (or initial) and last name (current or former); geographical address; electronic address (including an e-mail address); personal cellular phone number; telephone number or fax number dedicated to contacting the individual at his or her physical place of residence; social security account number; credit and debit card numbers; financial records, including checking, savings and other financial account numbers, and loan accounts and payment history; consumer report information; mother's maiden name; biometric identifiers, including but not limited to, fingerprints, palm prints, facial recognition, full face image and iris scans; driver identification number; birth date; birth, adoption or death certificate numbers; physical description; genetic information; medical, disability or employment records, including salary information; computer information, including information collected through an internet cookie; and criminal records and history. When connected with one or more of the items of information specified above, PII includes any other information concerning an individual that, if disclosed, identifies or can be used to identify a specific individual physically or electronically.

3.8 "Polling" means a process which is repeated and continuously trying to gather data that can compromise Network operations.

3.9 "Protected Health Information" or "PHI" is a subset of PII and means, with regard to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") covered entities (*see* 45 C.F.R. §106.103), individually identifiable health information, including demographic information, whether oral or recorded in any form or medium that relates to an individual's health, health care services and supplies, or payment for services or supplies, and which identifies the individual or could reasonably be used to identify the individual. This includes information that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual including, but not limited to, preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care as well as counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; or the past, present, or future payment for the provision of health care to an individual; and which includes identity information, such as social security number or driver's license number, even if the name is not included, such that the health information is linked to the individual. Protected Health Information does not include records covered by the Family Educational Right and Privacy Act, 20 U.S.C. 1232g, and employment records held by the entity in its role as employer.

3.10 "Pyramid Schemes" means plans or promotions organized whereby fees, dues or anything of material value is paid or given by members of the plan to any other member of the plan, which provides for the increase in such membership through a chain process of members securing other new members and thereby advancing themselves in the group to a position where such members in turn receive fees, dues or things of material value from other members (see W. Va. Code § 47-15-1, *et seq.*)

3.11 "Server" means a larger capacity computer which is being used for a specific purpose such as print, email, web or file services, or the hosting of specific applications such as Student Information Systems.

3.12 "Spam" or "Spamming" means unsolicited e-mail sent over the internet.

3.13 "Spoofing" means a technique used in hacking to gain unauthorized access to a restricted technology resource by pretending to be a trusted source.

3.14 "Stalk" means a course of conduct (i.e., repetitive and/or menacing pursuit, following, harassment and/or interference with the peace and/or safety of another) directed at a specific person that is unwelcome and would cause a reasonable person to feel fear.

3.15 "Standard Cryptographic Techniques" means methods used by information technology to encrypt data at rest (in storage) or in transmission from one system to another that prevents unauthorized access to sensitive data. The encryption methods will change over time as techniques are rendered ineffective and necessitate stronger mathematical algorithms to protect the data.

3.16 "Sync" means the process of sharing data, specifically passwords, to another WVSOM application (i.e., email) to avoid maintaining multiple passwords.

GA 31-4. Shared IT Resources

4.1 The WVSOM academic atmosphere encourages the sharing of knowledge and the collaboration that should occur in the educational and research environment. Access to systems and Networks, owned or operated by WVSOM, carries certain responsibilities and obligations and is considered a privilege, not a right. When utilizing IT systems, users must value the physical facilities, the integrity of the IT resources, and all license and contractual agreements related to the IT resources.

4.2 Due to the shared nature of WVSOM's IT resources, users must:

4.2.1 Be considerate of others and refrain from monopolizing systems;

4.2.2 Avoid overloading Networks with excessive data, degrading services, wasting computer time, as well as connection time, disk space, printers, and other peripherals associated with IT;

4.2.3 Only use resources for authorized purposes;

4.2.4 Protect user IDs and passwords from unauthorized use;

4.2.5 Use only IT resources which the users are authorized by WVSOM to access;

4.2.6 Only use legal versions of copyrighted software in compliance with vendor license requirements;

4.2.7 Report unauthorized use, damaged systems, and malfunctioning software to the IT Department; and

4.2.8 Refrain from IT resource use that is unrelated to official WVSOM business and the activation of unauthorized devices, which may compromise and/or consume Network bandwidth or disrupt other institutional services.

GA 31-5. Ownership of IT Resources

5.1 WVSOM IT Resources. The computers in the library, training labs, Statewide Campus sites, departments, and at employee work stations, along with the campus Network, Servers, switches, routers, cabling, attached peripherals such as printers, telephones and voicemail, other hardware, and software are the property of WVSOM. Therefore, WVSOM determines who has access to these IT resources. Overuse or abuse of these IT resources can result in denial of access or a reduction of use for the benefit of other users and mission critical applications, and may subject the individual to administrative action, up to and including dismissal from WVSOM, termination of employment, termination of the vendor contract, or other equivalent action as applicable.

5.2 Software Licensing. WVSOM owns or has purchased licenses for software utilized on WVSOM's IT resources. In addition to campus-wide service agreements for specific software vendor licenses purchased by the IT Department, other departments may request purchase of specially licensed software. Licenses are normally purchased by the number of intended users. Therefore, it is a violation of software license agreements to make copies of software without permission. Users shall abide by the software license agreements and never make copies of software on WVSOM-owned IT resources that someone else has purchased and owns.

5.3 Copyright. Ownership of copyright-protected material belongs to the copyright holder. WVSOM requires that all WVSOM constituents including, but not limited to, staff, faculty, students, alumni, Statewide Campus entities, WVSOM Board of Governors members, vendors, guests, and others utilizing WVSOM's IT resources comply with federal copyright law and WVSOM's copyright policy concerning any copyright-protected material.

5.1 Issuance and Ownership of Student Laptop Computers

5.1.1 Each entering student shall be issued a WVSOM system-compatible laptop computer upon matriculation.

5.1.2 Students are responsible for the maintenance and upgrading of their WVSOM-issued laptop computer in compliance with WVSOM specifications for their class.

5.1.3 Unless otherwise authorized in advance, WVSOM is not responsible for the cost of students' off-campus internet access to the WVSOM Network.

5.1.4 WVSOM will retain ownership of students' WVSOM-issued laptop computers until the students graduate from WVSOM and upon confirmation that the students have satisfactorily discharged all financial obligations to WVSOM.

(i) Students may not sell, auction, transfer or encumber the title to their WVSOM-issued laptop computer prior to their graduation from WVSOM and confirmation that the students have satisfactorily discharged all financial obligations to WVSOM.

(ii) In the event a student's WVSOM-issued laptop computer is lost or stolen prior to graduation, the student will be responsible for acquiring a replacement laptop computer. The replacement laptop computer must be from the same

manufacturer with equivalent specifications as the student's original WVSOM-issued laptop computer and the student will incur the costs associated with acquiring the replacement laptop computer.

(iii) Should a student leave WVSOM prior to graduating, the student must return the WVSOM-issued laptop computer and any other related property owned by WVSOM in the possession of the student to the Vice President for Academic Affairs and Dean.

GA 31-6. Acceptable IT Usage Course

All WVSOM employees and students shall complete the Acceptable IT Usage Course in the Learning Management System before utilizing their WVSOM account for Network and email access.

GA 31-7. Data Protection

7.1 Laws and Regulations. WVSOM is governed by state and federal laws and regulations concerning the collection, use, and disclosure of certain information. All individuals governed by this policy shall at all times comply with these laws and regulations, which include, but are not limited to, the following:

7.1.1 The Federal Educational Rights and Privacy Act ("FERPA"), available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html. FERPA requires that WVSOM protect each student's educational records, including placement, medical, financial, disciplinary, and academic information, and provides that, with certain exceptions, a student's educational records cannot be disclosed without the written consent of the individual student.

7.1.2 The Health Insurance Portability and Accountability Act ("HIPAA"), available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html. HIPAA requires that individuals' protected health information be protected and safeguarded against unauthorized use and disclosure.

7.1.3 The Gramm-Leach-Bliley Act, available at http://www.ftc.gov/privacy/privacyinitiatives/glbact.html. The Gramm-Leach-Bliley Act regulates the privacy surrounding personally identifiable financial information, including credit card and bank account numbers.

7.1.4 Certain additional state and federal laws and regulations applicable to this policy are available at http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx.

7.2 Protections for Retrieval and Use of Data. Because of the sensitive nature of student, employee, patient, donor, and other related information at WVSOM, extreme care and precautions should be taken in the retrieval and use of data. Only data that users covered under this policy are authorized to view should be accessed. Access to PII and PHI will be authorized based on job function and the necessity to perform work-related duties. Usernames and accounts with passwords will be assigned by the IT Department for authenticating and subsequent authorization into the appropriate systems containing PII

and PHI. Proper utilization of usernames, accounts, and passwords is essential to the protection of data.

7.3 Passwords

7.3.1 Passwords should not be "guessable" and should be changed frequently. When creating passwords, the following rules apply:

(i) Passwords must be at least nine characters in length;

(ii) Passwords may not contain the user name or any part of the user's full name; and

(iii) Passwords must contain at least one upper case letter, one lower case letter, and one number. For example, Ghravc469 is a valid password.

7.3.2 Users must commit passwords to memory and must never store passwords in close proximity or easy access to the user's computer system. If the user's system is left unattended, the user should log out of applications and the user's account. Users should also create a password protected screen saver.

7.4 Storage and Destruction

7.4.1 Electronic media that is still in use must be kept in a fire-resistant, locked cabinet, if available, or other secure location. Electronic media that is no longer used must be properly destroyed or written with blank data. Before the IT Department surpluses old equipment, hard drives must be removed and drilled or written with blank data.

7.4.2 The IT Department maintains nightly backups of Servers and file shares used by WVSOM. Users are highly encouraged to store information containing PII within the data center Server environment. Any user information that is not backed up by the IT Department should be backed up to electronic media by the user. For students, backups are solely their responsibility. If a user is unsure of the proper backup procedures to follow, the user should contact the IT Department for assistance.

7.4.3 Security measures must be extended to laptops, flash drives, and other mobile computing devices (i.e. smartphones, tablets) which can contain sensitive data that may not be on-site in a secured office. The user must protect electronic data against theft and unauthorized use and disclosure, both on-site and off-site of WVSOM's main campus and Statewide Campus. Users may only store data with PII or PHI on mobile devices if necessary as part of the user's employment or education at WVSOM and only upon approval of the individual's immediate supervisor. This includes electronic files, emails, and all other records relating to students, employees, patients, alumni, donors, and others. If data containing PII or PHI must be stored on a mobile device, then the user must only store that much PII or PHI as is necessary and must password protect and encode the mobile device with data encryption for maximum security of the data. All data transmitted in or out of WVSOM information systems shall utilize, to the fullest feasible extent, Standard Cryptographic Techniques.

GA 31-8. Installation of Hardware/Software

8.1 Certain computer hardware/software installations require local administrative authority, which is typically reserved for the IT Department. However, specific requests for local administrative authority may be submitted to the Director of IT for review using a request form. If the request is approved, the user assumes all responsibility and actions occurring under the administrative account. The user is prohibited from changing the local administrator password.

8.2 System modifications that are reserved for the IT Department include:

8.2.1 Direct registry additions or modifications by running REGEDIT.EXE or an equivalent utility;

8.2.2 Installation of WVSOM approved and licensed software, software upgrades, and service packs;

8.2.3 Installation of all hardware and hardware drivers including printers, scanners, PDAs, speakers, and other peripherals;

8.2.4 Changes to Network settings including internet protocol addressing, destination name Servers, Gateways, and workstation names;

8.2.5 Installation of any software that has the effect of changing the workstation's basic operating system or changing application components which may degrade Network access and throughput; and

8.2.6 Installation and configuration of workstation Firewall software.

8.3 Installations that are strictly prohibited by the end user include:

8.3.1 Applications that use constant and repeated Network and/or internet Polling;

8.3.2 Applications that block or mask workstation identification including applications that create virtual private Networks;

8.3.3 Applications that broadcast to random addresses or open addresses;

8.3.4 Software that utilizes Network sniffing applications that have the effect of Spoofing or masking Network identification;

8.3.5 Software that is considered to be Spamming or spawning in nature; and

8.3.6 Workstation and local area Network management.

8.4 Approval and Legal Purchase of Software. All software that has been legally purchased and/or registered must be approved by a WVSOM administrator prior to the installation of the software on any WVSOM hardware. Any software that is installed and/or used on any WVSOM hardware without both administrative pre-approval and proof of legal status can and will be removed. Software that has not been legally purchased is not permitted to be installed on any WVSOM hardware.

8.5 Responsibility for Unapproved Software and Damage

8.5.1 Any damage or loss caused by the improper installation or use of software on any WVSOM hardware that has not been purchased or approved by WVSOM is the sole responsibility of the person(s) installing and/or using the software.

8.5.2 Any civil or legal penalties arising from the use of illegal or unapproved software are the sole responsibility of the user of that software.

GA 31-9. Email

9.1 WVSOM's Email Accounts

9.1.1 WVSOM's email services are handled in the Cloud by the Microsoft Office 365 platform at www.outlook.com/osteo.wvsom.edu. The email services require logging on via an internet browser or a local setup to the Outlook application to download messages to the computer. WVSOM no longer maintains email Servers locally and has entered into a Terms of Use agreement with Microsoft regarding email services. For additional information concerning this agreement, please visit http://www.microsoft.com/online/legal/v2/en-us/mos_legal_home.htm. User accounts may be suspended or discontinued based on violations of Microsoft's Terms of Use Section 2.a.iii. or this policy.

9.1.2 User accounts are assigned for incoming students once the second confirmation deposit is made to WVSOM. User accounts for employees are created once the hire notification has been sent by the WVSOM Human Resources Department. The accounts are created and passwords will Sync from an Active Directory database to the user's email account. Users should never need to change the passwords from within the Outlook application. Passwords should only be changed via the IT password change link. All official WVSOM email will be sent to the Outlook account to which the user has been assigned. Users do have the option to forward mail from the WVSOM account to any valid email account with another internet service provider (i.e., Hotmail, Yahoo).

9.1.3 The user shall maintain the confidentiality of the user accounts and passwords, and is fully responsible for all activities that occur under the user's password or account. The user shall (i) immediately notify the IT Department of any unauthorized use of his or her password account or any other breach of security, and (ii) ensure that he or she exits from his or her account at the end of each session. All email communications are the responsibility of the user who originated the Content. WVSOM will not be liable for any loss or damage arising from any user's failure to comply with this policy.

9.1.4 Users are placed on notice and should understand that there is no right of privacy in email communications, whether sent or received internally or externally, or in the monitoring of traffic to accounts. Accounts may be monitored by the IT Department as warranted without notice to the user, but only upon completion of the following procedure:

(i) The WVSOM administrator or supervisor will secure permission to monitor the email account from WVSOM's General Counsel, or, in the absence of such General Counsel, WVSOM's President.

(ii) An appropriate form with the signature of WVSOM's General Counsel will be presented to the system administrator allowing the system administrator to proceed to monitor the email account.

9.1.5 Circumstances that may cause user accounts to be monitored under Section 9.1.4 above include, but are not limited to, the following:

(i) When a user makes a complaint about communications made to his or her account;

(ii) When a user's traffic generates interference with or a breakdown of the proper functioning of IT resources or equipment;

(iii) When a change of service is requested; or

(iv) When a WVSOM administrator believes a user is using the WVSOM email service in violation of this policy.

9.1.6 Office 365 does perform Spam and phishing filtering. Characteristics of each email message are reviewed at the Outlook Gateway to determine legitimacy. An email that has a high rating is deleted, mid-level ratings are sent to the junk mail folder, and valid emails will be placed in the user's inbox. Only specific accounts have been given authority to send out mass emails (i.e, Admissions). Unless the use of a WVSOM group email list is necessary, mass emails should not be sent and may be rejected for delivery by Outlook.

9.1.7 All email communications, unless subject to a specific statutory, common law, or other applicable privilege, are subject to discovery and production, when relevant, in civil litigation, and to the West Virginia Freedom of Information Act. The federal Electronic Communications Privacy Act (18 U.S.C. § 2510, *et seq.*) will, in some instances, provide such a privilege to electronic mail which has not been opened, and WVSOM will observe and follow the requirements of all applicable state and federal statutes relating to privacy concerns in electronic mail. The Electronic Communications Privacy Act does not, however, establish a general right to email privacy in the workplace. The West Virginia Electronic Mail Protection Act (W. Va. Code § 46A-6G-1, *et seq.*) provides sanctions for unauthorized bulk mail transmissions.

9.1.8 While email account holders may expect reasonable access to email, access cannot be guaranteed at all times and in all circumstances.

9.1.9 Email accounts having no user activity (i.e., no user login to the service or email forwarding) will be considered for deactivation. If possible, the user will be notified in time to make an appeal. Requests for reactivation must be made in writing to the service administrator.

9.1.10 Complaints about email communications made to a user's account must be in writing and submitted to the IT Department.

9.1.11 Upon termination of a user's affiliation with WVSOM, the user's email account will be terminated and all information not retained by the user's supervisor will be deleted.

9.2 Email Account Access by Others

9.2.1 Under certain circumstances, authorized employees of the IT Department may, in the course of their professional duties, access users' email for legitimate management or maintenance purposes and will promptly designate in writing the identities of all such users to the Director of IT.

9.2.2 If a WVSOM administrator or supervisor believes that access to a user's email account is required for the conduct of WVSOM business, the user is not available, and a system administrator is required to access the user's email account, the following procedure will be followed:

(i) The WVSOM administrator or supervisor will secure permission to access the email account from WVSOM's General Counsel, or, in the absence of such General Counsel, WVSOM's President.

(ii) An appropriate form with the signature of WVSOM's General Counsel will be presented to the system administrator allowing the system administrator to proceed to access the email account.

(iii) The user whose email account has been accessed will be notified as soon as possible by copy of the above-referenced form. Where necessary to ensure the integrity of investigation into the use of WVSOM IT resources, such notice may, with the approval of WVSOM's General Counsel, be delayed until such time as the integrity of the investigation would no longer be compromised.

9.3 General Email Provisions

9.3.1 As with other WVSOM resources, email is made available to employees and students to further the teaching, research, and mission of WVSOM. Use of WVSOM's email services, therefore, is intended to be in furtherance of such goals and mission and not for extracurricular purposes. Users may not use email for entrepreneurial activities except in cases of WVSOM-sanctioned activities. Users who wish to solicit goods and services or to offer them to other members of the WVSOM community may use approved bulletin boards or employee newsletters.

9.3.2 No one may be added to an email mailing list for any purpose other than official WVSOM business without the individual's consent. Mailing lists may be used only for their intended purposes.

9.3.3 All materials sent by WVSOM email must be attributed to the individual, office, or organization sending the material.

9.3.4 All Content whether publicly posted or privately transmitted, is the sole responsibility of the person from whom such Content originated. WVSOM is not responsible for Content that users upload, post, email or otherwise transmit via WVSOM's email service. The IT Department does not control the Content posted via WVSOM's email service; therefore, the IT Department does not guarantee the

accuracy, integrity, or quality of such Content. Users must be mindful that, by using WVSOM's email service, they may be exposed to Content that is offensive, indecent or otherwise objectionable. WVSOM will not be liable in any way for any Content including, but not limited to, any errors or omissions in any Content, or for any loss or damage of any kind incurred as a result of the use of any Content posted, emailed or otherwise transmitted via WVSOM's email services.

9.3.5 WVSOM does not pre-screen email Content. However, WVSOM has the right, in its sole discretion and without obligation, to refuse or move any Content that is available via its email service. WVSOM may remove any Content that violates the terms of service. Users must evaluate, and bear all risks associated with, the use of any Content, including any reliance on the accuracy, completeness, or usefulness of such Content. In this regard, users may not rely on any Content submitted to WVSOM or other parts of WVSOM's email service.

9.3.6 WVSOM may preserve and disclose Content if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to:

(i) comply with legal process;

(ii) enforce the terms of service;

(iii) respond to claims that any Content violates the rights of third parties; or

(iv) protect the rights, property or personal safety of WVSOM, its users and the public.

9.3.7 The technical processing and transmission of WVSOM's email service, including user Content, may involve:

(i) transmissions over various Networks; and

(ii) changes to conform and adapt to technical requirements of connecting Networks or devices.

9.3.8 Email messages will be delivered to the addressees and will not be censored or interfered with in any way by WVSOM, unless WVSOM determines that a message contains a feature that will be harmful to software or equipment, such as a virus or worm.

9.3.9 Individually-addressed email communications may not be intercepted by a third party, except as noted in Section 9.1.4 and 9.1.5 above. This does not prevent persons who have legitimately received electronic mail messages from forwarding such messages to third parties.

9.4 System Demands and Reallocation of Email Resources and Quotas. The WVSOM email service is established as a means to transfer electronic communications between interested parties. It does not exist as a permanent repository for these communications and it is expected that the user will remove the communications from the Server using the industry standard tools in a timely manner.

9.5 Email Service Prohibitions. Each WVSOM email service user is prohibited from using WVSOM's email service to:

9.5.1 Upload, post, email or otherwise transmit any Content that is unlawful, harmful, threatening, abusive, harassing, deceitful, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially or ethnically objectionable;

9.5.2 Upload, post, email, or otherwise transmit any Content that the user knows, or reasonably should know, could cause harm to a minor;

9.5.3 Impersonate any person or entity including, but not limited to, a WVSOM administrator, forum leader, guide or host, or falsely state or otherwise misrepresent the user's affiliation with a person or entity;

9.5.4 Forge headers or otherwise manipulate identifiers in order to disguise the origin of any Content transmitted through WVSOM's email service;

9.5.5 Upload, post, email or otherwise transmit any Content that the user does not have a right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements);

9.5.6 Upload, post, email or otherwise transmit any Content that infringes any patent, trademark, trade secret, copyright, or other proprietary rights of any party;

9.5.7 Upload, post, email or otherwise transmit any unsolicited or unauthorized advertising, promotional materials, Spam, Chain Letters, Pyramid Schemes, or any other form of solicitation;

9.5.8 Upload, post, email or otherwise transmit any Content that the individual suspects, knows or has reason to know contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

9.5.9 Interfere with or disrupt WVSOM's email service, Servers, or Networks connected to the local WVSOM Network, or disobey any requirements, procedures, policies or regulations of Networks connected to WVSOM;

9.5.10 Intentionally or unintentionally violate any applicable local, state, federal, or international law or regulation, including, but not limited to, regulations promulgated by the U. S. Securities and Exchange Commission, any rules of any national or other securities exchange (including, without limitation, the New York Stock Exchange, the American Stock Exchange or the NASDAQ);

9.5.11 Stalk or otherwise harass another;

9.5.12 Collect or store PII, PHI, or other personal confidential data, unless such data is required as a part of the user's job responsibilities and only to the extent necessary for the user to perform those job responsibilities;

9.5.13 Participate in any non-WVSOM sanctioned or non-mission related activities;

9.5.14 Receive or attempt to receive any commercial or personal gain;

9.5.15 Execute or open email attachments that appear questionable (a user must contact the IT Department prior to executing or opening email attachments if the user is unsure about the legitimacy of an email and/or its attachment); or

9.5.16 Send mass emails, unless the use of a WVSOM group email list is necessary.

GA 31-10. WVSOM Web Site

10.1 The WVSOM website has been established to support the mission of the institution and is the sole property of WVSOM. All material posted on the website is subject to all applicable WVSOM policies and procedures and is subject to authorization and review by WVSOM.

10.2 Website Maintenance and Design

10.2.1 The IT Department will maintain the WVSOM Server and handle technical matters concerning the WVSOM website.

10.2.2 The Marketing and Communications Department, through its Web Master, will design and work with departments regarding website page Content and structure.

10.3 Website Rules and Regulations

10.3.1 WVSOM uses a Content management application to manage the WVSOM website. Access to the application is provided upon request and following training in its use.

10.3.2 Each page or section on the WVSOM website is the responsibility of the department or individual authorized to manage that page or section. All pages relating to the Office of Business Affairs are the responsibility of the Vice President for Finance and Facilities or his or her designees. All pages relating to any academic department or curricular matter are the responsibility of the Vice President for Academic Affairs and Dean or his or her designees. All pages related to general institutional matters and the Office of the President are the responsibility of the Web Master under the Director of Marketing and Communications. Posting to the website requires approval by the responsible administrator and the Web Master.

10.3.3 The website is divided into two domains: the public domain, which will be open to the general viewing public, and the internal domain, which will be accessible by Active Directory account and password only. Internal pages will be the sole responsibility of the author of the page. New web pages must be developed by the department or individual responsible for creating it. A template will be supplied and the Web Master will assist with the initial development.

10.4 Website Prohibitions. The following activities are prohibited on or using WVSOM's website and web pages:

10.4.1 Buying or selling of any non-sanctioned goods and services.

10.4.2 Purposefully accessing or transmitting profanity, pornography, generally obscene material, or links to any of the former.

10.4.3 Using any graphic, logo, or picture without the express consent of the creator.

10.4.4 Unauthorized advertising of other organizations and businesses.

10.4.5 Using web pages or the WVSOM server for personal pages.

10.4.6 Using the WVSOM website or web pages in any manner that has not been authorized.

GA 31-11. WVSOM Network Access

11.1 WVSOM provides both wired and wireless access to the Network. Network access is based on the Active Directory user accounts and Network groups that have been assigned to each user account. Issues with Network connectivity can be resolved by contacting the IT Helpdesk at 304-647-6246 or, for employees, logging a TrackIt ticket from the WVSOM website (https://my.wvsom.edu/TrackItWeb/SelfService/Login).

11.2 Any Network protocol or service which infringes on the WVSOM Network is banned (i.e., intentional route poisoning, illegal peer-to-peer file sharing, individualized domains, and non-authorized Servers). Hosts that are using or offering this type of service will be removed from the Network immediately.

11.3 In utilizing the user account for Network access to the internet, users should only access those internet sites that are needed for WVSOM mission-related work. Users should consider how their activity affects the overall Network and must guard their accounts against use by other individuals. Users will be held accountable for abusive activity associated with their account, including excessive bandwidth from file downloading. Abusive activity will result in the loss of Network privileges, and may result in other administrative action. The IT Department conducts ongoing audits to collect networking information and uses this information to analyze the state of the Network, discover and assess any abuses that may be occurring, and support the discontinuance of the offending Network behavior.

11.4 If a user encounters anyone trying to hack the WVSOM Network, Servers, or computers, steal identities and personal data including usernames or passwords, propagate viruses, phish, flood email Gateways with Spam, or attempt any other harmful or malicious behavior, the user must report it immediately to the IT Helpdesk.

11.5 Changing Network User Account Name

11.5.1 If a user changes his or her Network user account name, the user's email is also changed. Students will receive a Network user account during WVSOM's acceptance and deposit process, while employees will receive this during the employment orientation. The user is responsible for maintaining confidentiality of the Network user account, and is fully responsible for all activities that occur under the user account.

11.5.2 The Network user account name must be based on the user's name and can be changed due to marriage, divorce, or other legal name change. Requests for a Network user account name change will be processed as follows:

(i) For employees, requests must be processed through Human Resources, who will verify all legal documentation. For students, requests must be processed through the Registrar, who will verify all legal documentation.

(ii) The request is forwarded via e-mail to helpdesk@osteo.wvsom.edu.

(iii) The request must include what the account change should be, including the user's last name (i.e. John Smith will be JSmith).

(iv) The IT Helpdesk will notify the user to review and abide by this policy and give an activation date when the change will occur.

(v) If the request is being rescinded, it is the responsibility of the user to notify the IT Helpdesk prior to the activation date.

11.5.3 After establishing a new user account, the user will no longer be able to log onto the Network or send/receive email using the old account. All subscriptions and mailing lists to the old account must be canceled prior to the account change. New subscriptions and mailing lists must be activated using the new account name after it has become effective.

GA 31-12. SharePoint, Social Media, and General Online Collaboration Tools

12.1 SharePoint Sites Use and Security

12.1.1 SharePoint is part of Microsoft's integrated suite of business products. WVSOM maintains this web application tool as part of the Office 365 Cloud service, which also provisions email accounts. SharePoint is considered a social collaboration tool which can be used to create custom websites and sub-sites for short or long-term usage and with various levels of access for security. Within these sites, the sharing of calendars, events, announcements, surveys and informational Content is made possible, as well as the integration with databases and the production of workflows. Content inherent to each site, representing various WVSOM online communities, can be easily searched and audited with version control capabilities (i.e. Word and Excel files).

12.1.2 Requests for SharePoint sites will be made to the IT Department by submitting the SharePoint Site Request Form, which must include sufficient details for the provisioning of the initial template to create and maintain a SharePoint website. The template and site permissions will be based on the information gathered from the request. Upon approval, the requestor and the appointed site owner will be notified of the new site's availability, ownership responsibilities, and training options. Once the site template has been made available to the site owners, the site owners are responsible for site Content and security at various permission levels, including full control; view, contribute, update and delete; and read only. The IT Department will retain site administration over all WVSOM SharePoint sites and will provision/deprovision based on need, available storage, and adherence to WVSOM's policies and procedures.

12.1.3 All activity related to the creation, maintenance and utilization of any SharePoint site is governed by this policy. Users may never post any PII, PHI, student record-related data, information considered as WVSOM intellectual property, or any other confidential information on any WVSOM SharePoint public website. Only users permitted to access confidential information as part of their normal job function may be given permission in SharePoint to do so and only to the extent necessary for the user to perform the job function. WVSOM SharePoint sites will be directed to

internal use and for legitimate WVSOM purposes only. A SharePoint site may be opened to external third parties only after IT Department approval, which includes verifying the special affiliation or specific need to collaborate with WVSOM. Sites created under SharePoint should not be intended to replace WVSOM's public facing website or intranet site. Templates will be delivered with WVSOM branding. It is highly recommended that any additional design elements adhere closely to this branding.

12.2 Social Media Use and Security

12.2.1 As an institution of higher learning, WVSOM supports the value of online communities and maintains a strong commitment to academic freedom on these sites. To that end, respect, diversity, and an attitude of learning and transparency are guiding principles for Content postings and material review. The Marketing and Communications Department and the Media Services Department will maintain oversight of information published on WVSOM-hosted social media sites such as YouTube, Facebook and Twitter.

12.2.2 Social media sites that are associated with WVSOM will have general landing pages that appropriately represent departments or organizations under main pages established by the Marketing and Communications Department. In establishing these pages, the Marketing and Communications Department must be consulted for branding and published Content.

12.2.3 A WVSOM department or organization that has a social media site must appoint a page administrator to collaborate with the Marketing and Communications Department on an ongoing basis for managing updates and changes to site Content. Page administrators may never use these platforms to express individual opinions. Only WVSOM-sanctioned activities may occur in WVSOM branded social media sites. Sites are prohibited from political activity, private commercial transactions, or other non-WVSOM business activity. Sites shall not use logos and trademarks without appropriate authorization. Content shall adhere to all applicable fair-use and copyright law. This includes all photos, videos, or audio.

12.2.4 For each social media site associated with WVSOM, at least two administrative accounts must be made available. WVSOM social media accounts may not be accessed through personal accounts and only WVSOM email addresses may be associated with the accounts.

12.2.5 Content on social media sites should be brief, accurate, and relative to the target audience. Page administrators must review appropriate Content and remove Content that is objectionable or inappropriate, including factual inaccuracies, offensive language, the use of slander or profanity, and messages selling products or promoting commercial ventures. Page administrators must modify social media settings to limit the public access for posting of such information.

12.2.6 Social media site communications are considered public records. Posts published by employees and administrators and any responses by other employees, students, alumni, the general public, and others will become part of the public realm. For this reason, WVSOM social media sites must include this disclaimer:

"The views expressed on this social media site do not necessarily reflect the views of WVSOM, the West Virginia Higher Education Policy Commission, or the State of West Virginia. WVSOM has not reviewed or approved this personal Content and therefore accepts no responsibility. Further, communications via this social media site, whether by WVSOM employees, students, alumni, the general public, and others may be subject to monitoring and disclosure by third parties. Discretion should be used at all times. Personally identifiable information, protected health information, legal issues, and other confidential information should never be published to this site due to the lack of confidentiality and privacy on this site."

12.2.7 Posted Content may never violate WVSOM policies or procedures or state or federal law or regulations. Postings shall not reference or cite entities outside of WVSOM without written consent. Reports of Content violations must be reported to the Marketing and Communications Department and the Office of the General Counsel.

12.3 General Online Collaboration Tools Use and Security

12.3.1 All PII, PHI, and other confidential employee and student data shall be held to the highest security standards and procedures at WVSOM with regard to communication and file sharing using online collaboration tools. These online collaboration tools include applications for instant messaging, video conferencing, file sharing, and any other Cloud-based collaborative application.

12.3.2 Employees may only utilize WVSOM-approved online collaboration tools and shall not install third-party consumer grade applications. Employees and students shall have no expectation of privacy in the use of these online collaboration tools. Contents on these online collaboration tools may be properly disclosed for discovery or management purposes without the express permission of the user who authored the information. WVSOM is under no obligation to retain communications created with online collaboration tools such as instant messaging. However, these communications may be retained as evidence during investigations, audits and litigation. Communications created using online collaboration tools may be subject to access requests, including the West Virginia Freedom of Information Act.

GA 31-13. Prohibited Use of IT Resources

In addition to the other prohibitions set forth in this policy, each user of WVSOM IT resources is prohibited from using those resources to:

13.1 Use another person's user ID, passwords, and files;

13.2 Use computer programs to decode passwords;

13.3 Access any information without the express permission of the owner;

13.4 Attempt to circumvent or subvert system or Network security measures;

13.5 Engage in any activity that might purposefully cause harm to systems or to information stored on IT resources, which could create or propagate viruses, disrupt services, damage files, or make unauthorized modifications to WVSOM data;

13.6 Use WVSOM systems for commercial or partisan political purposes, including circulation of advertisements for products or for political candidates;

13.7 Make or use illegal copies of copyrighted materials or software, store copies on WVSOM IT resources, or transmit them over the WVSOM Network;

13.8 Use email or messaging services to stalk, harass, or otherwise intimidate another person (i.e., broadcasting unsolicited messages, repeatedly sending unwanted mail, or by using someone else's name or user ID);

13.9 Waste IT resources or Network resources, such as intentionally placing a program in an endless loop, printing excessive amounts of paper, or sending unsolicited mass mailings;

13.10 Use WVSOM's IT resources or Network for personal gain, including, but not limited to, selling access to one's user ID or to systems or the Network, or performing work with WVSOM assets in a manner not authorized by WVSOM;

13.11 Engage in any activity that would be related to copyright infringement, including illegal downloading and P2P file sharing;

13.12 Disrupt or interfere with the normal use of computers, computer-related equipment, data, or programs of individuals, the Network, or the WVSOM institution;

13.13 Attempt to breach security in any manner;

13.14 Use a computer account for a purpose other than which it is assigned;

13.15 Use equipment, data, or programs in performance of any act prohibited by this policy; or

13.16 Engage in any other activity that could compromise WVSOM's IT resources or that does not comply with the principles stated in this policy.

GA 31-14. Disciplinary Action for Misuse of IT Resources

14.1 WVSOM considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information residing on WVSOM IT resources allegedly related to unacceptable use, and to protect its Network from systems and events that threaten or degrade operations.

14.2 Users who violate this policy are subject to administrative action, including the disabling of the user's account, banning the user from access to WVSOM systems, and possible dismissal from WVSOM, termination of employment, termination of the vendor contract, or other equivalent action as applicable.

14.3 In addition to the administrative penalties set forth in this policy, WVSOM may seek civil remedies against violators of this policy for any fines, judgments, or royalties assessed against WVSOM for the violator's wrongful use of WVSOM's IT resources.

GA 31-15. Information and Privacy Disclaimer

15.1 Individuals using IT resources owned by WVSOM do so subject to applicable WVSOM policies and procedures and state and federal laws and regulations. WVSOM disclaims any responsibility and/or warranties for information and materials residing on non-institutional systems or available over publicly accessible Networks. Such materials do not necessarily reflect the attitudes, opinions, or values of WVSOM, its employees or students. Information on the WVSOM website is provided by employees, students, alumni, and organizations, and others. Although WVSOM strives to keep its web information accurate and up-to-date, accuracy cannot always be guaranteed. WVSOM is not responsible for errors or omissions in information provided via the WVSOM website or web pages. Visitors to the WVSOM website or web pages are responsible for contacting the appropriate person/department to verify information and should not rely on the information contained within the site or pages.

15.2 All activities relating to WVSOM's IT resources and Network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized administrators, including pursuant to the West Virginia Freedom of Information Act. There is no right of privacy when utilizing WVSOM-owned IT resources. WVSOM administrators may give to law enforcement officials any potential evidence of criminal activity found on these IT resources. Use of any WVSOM-owned IT resource by any user, authorized or unauthorized, constitutes consent to this monitoring, interception, reading, copying, capturing, and disclosure.

GA 31-16. Implementation of Policy

This policy shall be implemented using applicable WVSOM policies, procedures, and handbooks, and shall be governed by applicable local, state, and federal laws and regulations, and WVSOM policies, procedures, and handbooks.