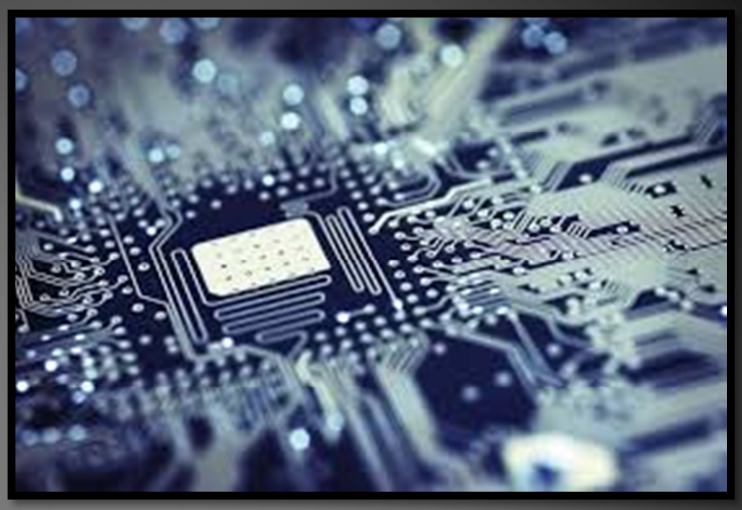

ITS Policies, Procedures, and Guidelines

William G. Dumire

Executive Director

Waynesburg University

51 West College Street

724-852-3413

10/30/2013

Contents

Purpose

- Waynesburg University Information Technology Services provides computing, networking, information, and communication resources to end-users in an effort to fully support and further enhance our faith, teaching, research, and service activities.

- Access to our Information Technology resources is conditionally granted to faculty, students, and staff.

- The ITS Executive Director is responsible for safeguarding our Information Technology resources (including but not limited to our equipment, software, networking infrastructure, and data) as well as facilitating end-user IT Security Awareness training.

- All WU faculty, staff, and students have a shared responsibility to protect our information resources.

- In order to keep up to date with the latest information on WU's ITS security policies and awareness efforts, WU faculty and staff will be required to take the WU IT Security Awareness Training on an annual basis. Additional information will follow shortly.

Declarations

- As members of Waynesburg University, faculty, staff, and students are bound by all of the procedures, policies, standards, guidelines, and laws as presented.

- ITS policies are not intended to circumvent, change, or nullify any of the institutional policies established by the President or Provost offices. Our policies serve to further enhance, ensure full compliance, and further protect our faculty, staff, students, and Waynesburg University.

- It should be noted that our policies may be amended to keep in line with changes in technology, federal and state law, and/or as part of the regular review process for all policies and procedures related to Information Technology Services.

Why We Have IT Policies

- To fully support and further enhance WU's faith, teaching, research, and service mission.

- To provide faculty, staff, and students with sound, reliable, and fully functional IT related equipment and software.

- To protect our substantial financial investments related to our Information Technology resources and systems.

- To identify and close any security gaps that could lead to a breach of confidentiality.

WU End-User Network Security and Support Services Policies

Due to federal, state, and local security regulations and guidelines, all computers connecting to the Waynesburg University computer networks shall adhere to the following standards:

- All Windows-based computers will connect/join to the WU domain
- All computers (Windows, non-Windows workstations) must adhere to the following restrictions:
    - Screensaver will be enabled with 15 minute timeout. Will require login upon waking. Lab/Classroom computers will be enabled with a 45 minute timeout.
    - All unattended computers must be locked or logged off.
        - PC - Depress the Ctrl-Alt-Delete keys simultaneously to lock or logoff
        - PC - Depress the "Windows" Key and "L" to lock
        - Mac - Activate a locked screensaver or logoff
- Windows-based computers: Windows Updates will be enabled and automatically installed on a user's computer nightly. If the computer is off at the daily installation time, updates will be installed upon restart. A reboot will be required for updates to take effect and must be initiated by the end-user at least once a week.
- Automatic updates must be enabled on all other workstations.
- All Windows-based computers must run anti-virus/anti-spyware with latest updates.
- WU ITS provides central firewall protection to all users of the WU Network. Local firewall can be disabled.

- Passwords will be minimum of 8 characters in length
    - Effective January 15th, 2014, mandatory password change will be required every 90 days
    - Three Password history (Password reuse is not permitted for 3 cycles)
    - Account will be locked after 3 unsuccessful login attempts. Account will remain locked for a period of 30 minutes and then unlock.
    - Strong Passwords are required meeting WU ITS complexity requirements.
        - Not contain all or part of the user's account name
        - Be at least eight characters in length
        - Contain characters from three of the following four categories:
        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters, (!, @, #, $, etc.)
        - Password must be different from previous three passwords
- File / Print sharing between individual desktop PCs is prohibited. Central storage is provided by Information Technology Services.
- Due to security issues relative to access, dissemination, and retention of FERPA and other confidential information, the use of external file sharing/storage applications/sites (i.e. Drop Box, FolderShare, etc.) is strictly prohibited.
- POP3 is disabled for all WU email accounts due to security issues.
- No network hubs permitted on the WU Network.

- No external remote control access software is permitted on the end-user's computer for the purpose of remote access to WU related computers (i.e. gotomypc.com, logmein.com).
- All infrastructure equipment (ie. routers, switches, wireless equipment, network appliances, network storage devices (NAS, SAN, etc.)) is provided and maintained by WU Information Technology Services only. Departments are not permitted to install and maintain infrastructure equipment.
- To help provide for a more reliable and secure computing environment, it is important for end-users to keep their computers, operating systems, and application software up to date. Although, we don't always recommend moving to the latest cutting-edge technology we do encourage keeping computers updated at a reasonable pace. Doing so enables a better support infrastructure and system security.

Account Usage / Password Policies

Computers, laptops, applications and systems that produce, maintain, transmit or permit access to University data or data entrusted to the University must be protected, at minimum, by an electronic account or other approved authentication mechanisms. Each individual granted access to WU resources will be assigned his or her own unique electronic account(s) or authentication mechanism(s) for the purpose of accessing and using authorized information and/or resources. Except for the departmental accounts, discussed in the next bullet, sharing of accounts is prohibited.

Departmental accounts are accounts shared by multiple, but individually authorized individuals for a specific purpose, such as managing classroom audio/visual access, a departmental electronic mail account, or a computer that must operate in a continuous processing state. An account manager must be identified for each departmental or system account. The account manager must establish formal mechanisms for granting, tracking and terminating individual access and activity.

Guest accounts may be provided to allow temporary access to University resources for a specific purpose and period. The parties authorizing and issuing the guest accounts must establish formal authentication, accountability and tracking procedures. All guest accounts must be created with an expiration date and time. Guest accounts must be disabled immediately upon the expiration date.

Passwords are provided for the individual use of the authorized user.

- Passwords must be treated as highly confidential and may never be revealed, distributed, or otherwise compromised.
- User must not attempt to interfere with IT resources or attempt to circumvent or disable the security of any IT resource.
- Do not post your password where it can be easily observed or found:
    - on your computer monitor
    - on or under a phone
    - on a room or office wall

    - on a message board
    - under your keyboard
    - under your mouse pad
- Always change "default" passwords at the time of your first login attempt.
- Avoid using these as your password:
    - First Name
    - Last Name
    - Car Tag
    - WUID
    - PIN
    - Birth Date
    - Phone Number
    - SSN
    - Credit Card Number
- **Avoid using the same password for multiple accounts** - While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your MyConnect account. Your MyConnect password(s) should differ from that of any non-work related sites. ***(For example, never use the same username or password for Facebook that would tie back to your WU Myconnect account).***
- By changing passwords on a regular basis, you limit the password life. If your password is compromised, a limited password life will reduce the amount of time that a user has to access the data and resources that belong to you or are assigned to you. Passwords must be changed every 90 days.
- If you suspect your password has been compromised, change the password for all accounts associated with the compromised password immediately.
- If you suspect that your work account is compromised, contact your immediate supervisor and our ITS Help Desk at (724) 852-3413.

Resource Usage Policies

If you observe or have knowledge of unauthorized access or divulgence of the confidential information, including educational records protected by FERPA, business asset data, proprietary, or private information, you will report it immediately to your supervisor.

WU end-users will not seek personal benefit or permit others to benefit personally by any confidential information educational records protected by FERPA ,business asset data, proprietary, or private information that they may have access to.

WU end-users understand that all information, regardless of the media on which its stored (paper, computer, videos, recorders, etc.), the system which processes it (computers, voice mail, telephone systems, faxes, etc.), or the methods by which its moved (electronic mail, face to face conversation, facsimiles, etc.) shall not be used inappropriately and shall not be removed from the premises without prior authorization. WU end-users also understand that all electronic communication may be monitored and subject to internal and external audit.

WU end-users understand that discussions regarding educational records, protected by FERPA, shall not take place in the presence of persons not entitled to such confidential information and shall not take place in public places (such as elevators, lobbies, off premises, etc.).

ITS would like to remind everyone that publishing confidential information or any other data that can be linked to a specific student's identity is not permitted. This information includes but is not limited to the following: Social Security Number (in whole or in part), Grades/GPA, and Test Scores. By publishing such information, faculty or staff may be violating a multitude of policies, regulations, and/or laws, such as those listed below. Impermissible disclosures place our students at risk for potential embarrassment, identity theft, or worse. Additionally, such disclosures place the University at risk for legal action or substantial fines. Ultimately, the person responsible for the disclosure is at risk for personal legal liability or other adverse action. Posting of grades are permitted only in an on-line secure environment (Blackboard).

WU computing resources shall not be used to copy software, cds, dvds, upload or download material that is copyrighted or protected under trademark / licensing laws unless express written permission has been obtained by the resource owner and placed on file with the appropriate office.

The downloading or ripping of pirated / illegal movies, music, and or other media files is strictly prohibited by federal law.

WU computing resources may not be used for preparing, storing, receiving, or distributing any information that is harassing, unethical, illegal, or may be deemed defamatory in nature. This includes, but is not limited to, pornography, racism, sexism, obscenities, acts of intimidation, or verbal /physical threats.

Installation of personal / non-business related software is strictly prohibited. Any attempt to change or modify computer settings or override existing security is strictly forbidden.

Additional computing safeguards will be installed as deemed necessary by WU Administration.

PC / Internet usage is for official work related activities.

Faculty and staff may not download personal / non-business related email attachments (ie, from hotmail, yahoo mail accounts, etc.), or visit websites that are unethical, illegal, or that may compromise data / system security.

De Minimis Usage: "One should not use University sources of email, Internet access, and other IT services for activities of an extensive nature that are unrelated to University purposes. Excessive use of systems for recreational Internet browsing, email, or game playing is to be avoided and may subject University employees to disciplinary action up to and including termination."

All users must be lawful and ethical in their system usage and are bound by WU policies, procedures, and guidelines.

Enforcement: "Although the University does not routinely monitor computer and network use, the University does reserve the right to monitor computer and network use for operational needs and to ensure compliance with applicable laws and University policies. The University considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on University systems or equipment that may be related to inappropriate use."

Guidelines for Appropriate Use of Internet, Electronic Networking, and Social Media

These guidelines are applicable to all faculty, staff, and students of Waynesburg University. The use of the internet or intranet includes, but may not be limited to, postings on blogs, instant messaging (IM), using social networking sites, sending or receiving e-mail, or postings to public media sites, mailing lists, and/or video sites. These guidelines apply whether an individual uses public or private computers or devices. Nothing contained in these guidelines shall supersede other University adopted policies, guidelines, or training relating to Information Technology Resources.

Background:

Faculty, staff, and students at Waynesburg University regularly use social and business networking websites and on-line communities to communicate with each other and with others external to the institution. It is expected that members of the WU community will act with honesty and integrity and will respect the rights, privileges, privacy, sensibilities, and property of others.

In accordance with HIPAA, FERPA, and WU ITS policy, please be advised that faculty, staff, and students are **not permitted** to post confidential patient information, including protected health information (PHI), educational records protected by FERPA, institutionally-owned asset data, confidential, proprietary, or private information on any social networking sites (Facebook, MySpace, Twitter, YouTube, etc.), personal / business related blogs, and/or instant messaging service.

Each member of the WU community is required to satisfactorily complete the annual WU Information Technology Security Awareness Training, which includes, but is not limited to, the appropriate usage of information technology resources and various forms of electronic media. Additional information will be sent on this in the near future.

Guidelines:

1) Never post any protected health information (PHI) about an individual patient to any electronic media, other than the patient's electronic health record. "Protected health information" means information as defined by HIPAA which may identify an individual patient. This guideline applies even if the patient's information has been de-identified so that the only person who may be able to identify the individual is the patient himself.

2) Never post a photograph or image of a patient to any electronic media, other than the patient's electronic medical record. Use of cameras or cell phone cameras in the patient care setting shall be for the sole purpose of assisting in the care and treatment of the patient or for educational purposes. Any photographs taken in the patient care setting must be posted to the patient's electronic medical record.

3) Comply with all applicable institutional policies or guidelines regarding any use of information technology resources, including the use of institutional trademarks or logos.

4) Never post any information about colleagues or co-workers to any electronic media without their explicit written permission. Respect for the privacy of others is an important part of the professionalism of our WU community.

5) Never become an electronic "friend" of a patient in any electronic media or require that a patient become a "friend" of the health care provider in order to influence or maintain the patient-health care provider relationship.

6) Never misrepresent, in any electronic media, that an individual faculty, staff, or student is acting on behalf of Waynesburg University.

7) Maintain the professionalism standards of your profession in all aspects in the use of internet, electronic networking or social media.

8) Make sure you understand the permanency of published material on the Web.

9) Finally, please note that Facebook, Twitter, and other social networking sites are increasingly being targeted by cyber-criminals drawn to the wealth of personal information supplied by users. Data posted on the sites (i.e. name, date of birth, address, job details, email and phone numbers) is a windfall for hackers. Viruses on these networks can hijack the accounts of social networking site users and send messages steering friends to hostile sites containing malware, a malicious software often designed to infiltrate a computer system for illicit purposes. Malware can be used to steal bank account data or credit card information once installed on a personal computer. Another danger of social networking sites are the popular quizzes, horoscopes and games made available for free to users which can sometimes be used to hide links to hostile sites.

Examples of information that should not be shared on social networking, blog sites, and instant messaging services are:

- Posting of and/or the discussion of student grades, evaluations, course feedback, etc.
- Reviewing profiles of patients.
- Reporting on or about official medical activities and/or patient's personal health information. Requiring patients to participate in "social networking" activities to influence or maintain the provider/patient relationship.
- Participating in activities that may compromise the provider/patient or faculty/student relationship.
- Providing medical advice on social networking sites.

Enforcement:

All members of the WU community have a responsibility to ensure that these guidelines are adhered to appropriately. Any individual who becomes aware of a violation of these guidelines should approach his/her immediate supervisor for advice. If the issue is not addressed appropriately, the individual may complain in writing to the Provost or to the Executive Director of Information Technology Services.

Purchasing Policies

Regardless of funding source and prior to ordering, a Technology "Pre-purchase Questionnaire" form must be completed and submitted for review to Information Technology Services for all IT services, computing equipment, and/or software to be installed on the WU Network to ensure compatibility and compliance with WU Network policies and procedures. The form is located at: https://forms.waynesburg.edu/machform/view.php?id=261121

Approval and/or denial status will be sent to the requestor's email address within two business days with explanation where applicable. Once approval is received, your department may place the order for the approved IT services, equipment, and/or software.

Failure to complete this questionnaire and obtain approval prior to purchasing may result in the need to return non-compliant equipment and/or software or in the loss of funds.

Equipment Installation / Connections Policies

All computer / network equipment, that will be connected to the WU Network, must be appropriately registered with WU ITS before it can be installed / connected.

All windows-based computer equipment that will be connected to the WU Network must log on to the WU domain. Please reference the WU End-User Network Security Policy.

Users are not permitted to connect network hubs, routers, wireless access points, or any other infrastructure networking devices.

IT Resource Removal Policies

No IT resource is to be removed off-site without appropriate permission from your immediate supervisor.

Detailed documentation such as system model name, model number, and system serial number must be recorded along with the name of the individual checking out the equipment and sent to WU ITS at helpdesk@waynesburg.edu.

Handling/Removal of Media Policies

Removal of any **unencrypted** media, from Waynesburg University, that contains identifiable patient information or any protected / confidential data violates WU ITS usage policy. Media types may include, but not limited to: Zip disks, USB devices, cds, and any other electronic type or hard copy format.

All users of WU Information Technology resources are directly responsible for ensuring that they use them in ethical and legal ways.

Infractions and/or violations of copyright, HIPAA, FERPA, or any other legal, ethical, or internal policy or procedure will be handled in accordance with federal and state law as applicable as WU Administration.

Email Policies

User Account Deactivation Policy for Termination Employees

- All user accounts shall be deactivated and removed from service on the employee's termination date. Any employee leaving WU should notify their important contacts of their new address prior to leaving WU. Personal email address book entries may be exported prior to employee termination date. Contact the WU ITS Help Desk if you need assistance with exporting your personal address books.

Work-related Communications

- Due to the sensitive and confidential nature of information that individuals have access to (including FERPA, HIPAA, and other proprietary / confidential data), all employees are required to use their officially issued email accounts for all work-related communications. Employees ARE NOT permitted to create or utilize personal email accounts to transmit work related information (e.g. Gmail, Yahoo, etc.)

Email forwarding policy

- Email forwarding outside of the WU domain is strictly prohibited. Therefore, faculty, staff, and students of the Waynesburg are not permitted to auto-forward email from their WU email account (account ending in @waynseburg.edu) to any other email account. This prohibits forwarding email to any personal email account (i.e. gmail, yahoo, etc.) due to the likelihood of an unauthorized disclosure.

Email Confidentiality Notice

- Due to the sensitive and confidential nature of the data that WU employees have access to, all faculty and staff are required to place the following WU approved "Confidentiality Notification" statement in their email signature line for all external email (email sent outside WU) communications:

> Confidentiality Notice: This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution by anyone other than the intended recipient(s) is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Email Scams and Phishing Policies

Please be aware of fraudulent email scams circulating our networks and NEVER reply to messages requesting your account information or any personal information. This type of email is known as "Phishing".

A phishing scam is one in which victims are tricked into providing personal information such as account numbers and passwords to what they believe to be a legitimate company or organization. In order to carry out this trick, the scammers often create a look-a-like website that is designed to resemble the target company's official website or simply asks the recipient to reply to an email with personal information. Be wary of any email that asks you to click on a link or reply with personal information such as banking details or any account information. Information submitted on these bogus websites or via email reply may be used by the scammer to steal funds from the user's accounts and/or steal the victim's identity.

Most legitimate companies/institutions would never request sensitive information from customers via email. The WU ITS department would never ask you to send personal information in an email or via website. Please DO NOT click on the links in these types of emails and NEVER REPLY with any personal information. If you have any doubts about the validity of an email, please contact the WU ITS Help Desk at (724) 852-3413 or at helpdesk@waynesburg.edu

WU ITS has a central anti-spam/anti-virus server in place. Unfortunately, these systems are not able to intercept all scam emails. It is important for end-users to be aware of these types of scams and immediately delete the email instead of replying.

If you have replied to a Phishing email, Information Technology Services recommends you change your password immediately. To change your password, contact our WU ITS Help Desk at (724) 852-3413.

Distribution List Usage Policies

The purpose of the "global" email address book and the “myConnect Bulletin Board” is to provide an electronic communications tool for the faculty, staff, and students of Waynesburg University.

Mass emails, from the email global address book, are not permitted for distribution by individuals. All such communications must be approved and sent directly by WU Administration.

Faculty, staff, and students will use email distribution lists and the “myConnect Bulletin Board” for official school related communications only.

No protected information will be transmitted across any WU distribution lists. This includes security numbers, grades, etc.

Abusive, racially demeaning, or offensive language, vulgarities, and or other inappropriate communications WILL NOT be tolerated.

Equipment / Media Disposal Policies

All computers, copiers, fax machines, and other electronic devices are required to have the hard drives sanitized (or destroyed) and/or memory erased before being re-assigned or surplused.

Departments wishing to surplus, re-assign (transfer), or return leased computers, copiers, faxes, electronic devices should contact the WU ITS Help Desk at (724) 852-3413 or at helpdesk@waynesburg.edu to make appropriate arrangements.

Once the WU ITS Help Desk has degaussed/sanitized the equipment, the equipment will be eligible for your department to surplus or re-assign(transfer) within the University.

The computer, or any hardware/software/licensure components, may not be transferred to an individual for personal gain or re-sell.

The WU ITS Help Desk has a CD, DVD, and mini disc data destroyer that will damage the cd/dvd/mini discs on both sides leaving data completely unreadable. Please contact the WU ITS Help Desk if you need assistance destroying CD, DVD, or mini disc media.

Surplused computers will be disposed of per WU policies and procedures. Please follow the appropriate guidelines for your hardware.

It is the responsibility of the department to ensure that all data is erased from computer hard drives, handheld computers, Personal Digital Assistants, Smartphones, cell phones, copier drives, fax, removable and external drives (ie. USB memory key, CD, DVD, floppy, external drives) before disposing or re-assigning the device. Please contact the WU ITS Help Desk for assistance.

Policy Breaches

Breaches of policy will be reported immediately to WU ITS Executive Director.

If WU Administrators believe that unethical or illegal activities have occurred, these processes will be followed:

> The user's access privileges will be temporarily suspended until further investigation can occur. The employee will be notified by their immediate supervisor that a potential breach has occurred.
>
> If a breach is found, WU Administrators will confer to determine appropriate action.

Audits

All WU ITS resources may be audited. Usage and activity records belong to the University, not to the individual user. Please Note: "Although the University does not routinely monitor computer and network use, the University does reserve the right to monitor computer and network use for operational needs and to ensure compliance with applicable laws and University policies. The University considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on University systems or equipment that may be related to inappropriate use."

All University equipment/systems may be subject to Freedom of Information Act (FOIA) or Electronic Discovery requests. E-Discovery refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

ITS Policies, Procedures, & Guideline Questions

Questions should be directed to Information Technology Services at (724) 852-3413 or at helpdesk@waynesburg.edu

Checklist to Protect Your Information Resources

- If you suspect that your computer is infected, please contact our WU ITS Help Desk **(724-852-3413)** immediately.
- Install critical operating system updates as prompted.
- Do NOT post account or password information around or near your PC.
- Whenever possible, avoid storing confidential information on DVDs, CDs, USB drives, or other portable media. If you absolutely must use DVDs, CDs, and paper when working with confidential information, shred the media or paper when you are finished using it. Additionally, make sure all information is encrypted prior to storage.
- Immediately retrieve from the printer/fax any papers containing confidential information.
- "Lock" all unattended workstations.
    - PC - Depress the Ctrl-Alt-Delete keys simultaneously to lock or logoff
    - Mac – Activate a locked screensaver or logoff
- I will not access confidential information, including protected health information (PHI), educational records protected by FERPA, institutionally-owned asset data, confidential, proprietary, or private information which I have no legitimate need to know and for which I am not an authorized user. This includes records of family members and friends.
- I will not in any way divulge, disclose, copy, release, sell, loan, review, alter or destroy any educational records protected by FERPA, institutionally-owned asset data, confidential, proprietary, or private information unless expressly permitted by existing policy.
- I will not utilize another user's password in order to access any system. I will not reveal my computer access code to anyone.
- I accept personal responsibility for all activities occurring under my password.
- All electronic email messages/instant messages/cellular phone calls/PDA entries/episodes of internet access/episodes of remote access/computer use occurring on institutionally-owned or issued computers/cellular or other phones/PDAs/pagers, whether for business purposes or incidental personal purposes, may be subject to WU's obligations to collect, preserve and produce electronically-stored information during litigation or certain legal investigations.
- WU cannot guarantee that incidental personal email/phone calls/pages/PDA entries/internet access/remote access will be exempt from collection, preservation or production under these circumstances.
- Only authorized users are permitted access to WU ITS resources.

- Authorized users may use ITS resources to carry out the responsibilities of their positions as employees and students, to conduct official school business, or in other activities sanctioned by Waynesburg University.
- All users must be lawful and ethical in their system usage and are bound by WU policy and procedures.
- All confidential, protected data, PHI, and educational records protected by FERPA must be stored on the WU secured servers.
- IT resources are not to be used to gain unauthorized or illegal access to other computers/networks/systems/files/data, regardless of the intention.