Acceptable Use & Security Policy

Applies To:	All	Policy Number:	ITS-0028
Issued By:	AVP for IT	Policy Version Number:	3.0
Date Issued:	January 1, 2009	Last Review Date:	January 1, 2016
		Last Revised Date:	March 1, 2018

Scope

This policy applies to all persons accessing and using University of Detroit Mercy (the "University") computing, networking, telephony and information resources of the University. These persons include students, faculty, staff, persons retained to perform University work, and any other person extended access and use privileges by the University given the availability of these resources and services, and in accordance with University contractual agreements and obligations.

All members of the University community share in the responsibility for protecting information resources for which they have access or custodianship.

This policy covers all computing, networking, telephony and information resources procured through, operated or contracted by the University. This policy also covers any computing device connecting to and utilizing University information resources. Such resources include computing and networking systems including those that connect to the University telecommunications infrastructure, other computer hardware, software, databases, support personnel and services, physical facilities, and communications systems and services.

The University expects users to act in a responsible, ethical and legal manner consistent with the mission of the University.

Agreement to Terms & Conditions

By virtue of usage, users agree to the terms and conditions set forth by this policy, the policies documented on the ITS website (http://www.udmercy.edu/about/its/policies), the acceptable use policy of the University's internet service providers and all applicable international, federal, state, local and University policies.

Use is a privilege that may be revoked and not a right.

Policy

1. General

a. Use only those information technology resources you are authorized to do so, and use them only in the manner and to the extent authorized.

b. Accounts, passwords and access to University information technology resources must not be shared under any circumstances. All users of these resources must respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Users must not leave access information readily available for discovery.

c. Faculty, staff and students are expected to provide and maintain accurate data about themselves (i.e. date of birth, address, etc.) when updating personal information on any University systems.

d. All University community members requiring access to University records are required to submit signed paperwork and a FERPA agreement form approved by their immediate supervisor to obtain access. All paperwork is filed in the ITS offices and retained until separation from the University.

e. Access is granted and governed according to the ITS-0008 Account Privilege Policy which includes details related to the termination of access as well.

f. Users must respect the finite capacity of University resources and limit use so as not to consume an unreasonable amount of resources or to interfere unreasonably with the activity of other users. The reasonableness of any particular use will be judged in the context of all the relevant circumstances. If the situation warrants, ITS will with or without prior notification take necessary steps to balance usage by limiting or disconnecting the network connection.

g. Where online storage is permitted on University resources, users are only to store University related files. Personal files, graphics, music collections, etc. should only be stored on personal media.

2. Communications

a. Email is one of the official mediums by which the members of the University communicate with each other. Students, faculty and staff are all expected to read email regularly to receive University communications.

b. All University related communications are to originate from an @udmercy.edu domain account. Official University communications are to be sent to a student's @udmercy.edu account from the sender's @udmercy.edu account. Students are required to regularly review their email per policy ITS-0024. Reviewing email from a third-party client (mobile or desktop) does not eliminate the requirement to review email from the University's official system since email delivery cannot be guaranteed to third-party clients.

c. Communications to the University community at large must adhere to the University's Mass Communications Policy as documented in ITS-0019 guidelines.

d. The University maintains the right to review all incoming and outgoing email using tools for analysis of SPAM and virus infected messages and maintains the authority to stop such messages when possible. The proliferation of these messages originating from the University may lead to stoppage of services to all.

e. The University at any time may overtake an individual's University email account and may assign a new address.

3. Anti-Spam Prevention Statement

a. **Introduction**
It is critical for all @udmercy.edu email account users to know that personal or confidential information may be sought by email. Always be on the lookout for unscrupulous messages and scrutinize each email message that requests any personal or confidential information. It is very unlikely that you should legitimately need to provide such information through email.

b. **Spoofed/Forged Messages**
In the course of using your email account, you may receive messages that appear to be from someone you know or receive a seemingly official request for personal or confidential details. Messages like this are coming from "spoofed" addresses and, should you reply, it is unlikely the message will be routed to the apparent sender.

_____ Initial

Spammers have learned that they can simply reuse official looking communications they receive from banks or other entities and merely change links to create a very authentic looking message. Although the links and the corresponding websites may look authentic, odds are that the fake message has led you to a fake website and will collect any personal or confidential information you submit.

c. **Impersonating ITS**
Some people can be so devious as to impersonate your IT department's email address and create false scenarios to fool you into giving up your credentials. Perhaps you have seen requests appearing to come from your IT department asking for your user code and password to ensure that your account will continue to properly function after an upgrade or expansion in your account. Please understand that an IT department doesn't need your account credentials for these or any scenarios. ITS will never ask for your password or other confidential information. If ITS were ever to need this information, ITS would speak directly to you or meet with you as you enter your credentials. ITS does not want to take on the liability of knowing your login credentials – ever!

_____ Initial

d. **What to do if you receive one of these messages**
If you receive one of these suspicious messages and are unsure as to whether it is legitimate or not, forward a copy to its@udmercy.edu and request to validate the authenticity of the message.

e. **Mistakenly giving up your credentials and some potential ramifications**
If you receive a message and mistakenly give up your credentials, ITS strongly suggests you immediately login to your account to change your password. If you are unable to login to your account, this generally means that the scammer has changed your password and is using your account, as well as possibly all of your contacts, for spamming or other illicit purposes.

_____ Initial

If you use your TitanConnect for direct deposit, scammers may try to take advantage of you financially by changing your direct deposit account information to an account that is not yours.

If you are an employee, scammers may use your credentials to review your online W2 forms to obtain additional information, potentially exploiting other areas of your life.

Scammers may go so far as to change your security questions and answers. Once you regain access, they can simply get back into your account by answering the security questions they set up.

Scammers may set up an auto-forward to send all incoming email to the scammers account for unknown reasons.

Anyone that has mistakenly given account credentials should immediately contact the ITS department so we can take the necessary steps to regain access to your account and stop the exploitation.

Should you give up your credentials more than once, ITS may implement permanent restrictions on your account, may require additional authentication factors or may completely eliminate your access. Access is a privilege and not a right.

f. **Impact of Mistake to University Community**
When you make the mistake of giving up your credentials, you are not just hurting yourself – you're negatively impacting all members and potential members of the University community. Often, major sites like Gmail, Yahoo, Comcast, etc. will see large streams of spam messages coming into their domain from the violated @udmercy.edu account and blacklist any future messages from @udmercy.edu addresses. Essentially, the University is cut off from sending communications to potential students, alums or others, who interact with members of the University community via email.

4. Information Security

a. **Information Classification**
In order to ensure that information about members of the University community is properly protected, all information will be classified in one of three categories: Protected, Sensitive and Public. Information that is classified as Protected or Sensitive data will receive additional protections.

i. <u>Protected data</u>
Protected data is any data that contains personally identifiable information concerning any individual and is regulated by local, state, or federal privacy regulations, or by any voluntary industry standards or best practices concerning protection of personally identifiable information that University chooses to follow.

These regulations may include, but are not limited to:

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)

- Payment Card Industry Data Security Standards (PCI DSS)
- General Data Protection Regulation (GDPR)

ii. Sensitive data
Sensitive data is any data that is not classified as Protected data, but which is information that the University would not distribute to the general public. This classification is made by the department originating the data. Examples of the types of data included are: budgets, salary and vendor information.

iii. Public data
Public data is any data that the University is comfortable distributing to the general public. For department-specific data, this classification comes from the department. If data is created jointly by more than one department, the involved departments should jointly classify the data. If they are unable to come to a consensus, then the data must be classified as Sensitive Data. For University-wide data, this classification can only come from the Office of the President, the Registrar's Office, Marketing & Public Affairs, the Division of Academic Affairs, or Institutional Research. Examples of the types of data included are: department faculty lists, department addresses, press releases, and the University web site. Any University data that does not contain personally identifiable information concerning any individual, and that is not Protected data or Sensitive data, may be classified as Public data.

iv. Default classification of data
Any data that contains personally identifiable information concerning any individual or that is covered by local, state, or federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that the University chooses to follow, is automatically classified as Protected Data. All other data is classified as Sensitive Data by default.

b. **Access Privileges to Data**
Access to University data is very highly restricted and only provided on a need-to-know basis dependent upon the requestor's position within the University.

i. **Requests**
Requests for permission for access to data must be submitted in writing via the ITS Account Application form and include signed acceptance of this Acceptable Use & Security policy and signed Acceptance of the Applicable Privacy Policies (FERPA, HIPAA, etc.).

Permission requests will be evaluated on a case-by-case basis and require the approval of the respective custodian of the requested data before ITS will grant such access.

ii. **Audit**
On an annual basis, as required by the University's external auditors, the ITS department will perform an audit of all access levels for all user accounts on the TitanNet and TitanConnect systems. This audit involves the review by supervisors of their employees access and signed communication back to ITS of any required changes or signed communication that no changes are required at this time.

iii. **Access Changes and Revocation**
Access privileges may be revoked at any time for any reason by the custodian of the information or the employee's supervisor.

Employee access privileges will automatically be revoked at time of job change or at time of separation from the University per ITS-0008 Account Privilege Policy.

c. Users should also be aware that their uses of University resources are not completely private. While the University does not routinely monitor individual usage of its resources, the normal operation and maintenance of the University's resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service.

d. The University, at its discretion, may disclose the results of any general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings or in litigation.

5. Hardware

a. **Device Security**
All devices (workstations, desktops, notebooks, etc.) procured through, operated or contracted by the University which are the property of the University will be configured by the ITS Help Desk as a standard work computer (the "Work Computer"). In a very limited number of cases for users in specific technical areas involving software development, a device may be set up as a development computer (the "Development Computer").

i. Setup of the Standard Work Computer by the ITS Help Desk

1. The Work Computer will utilize one of the University supported standard operating systems and configured to automatically accept university approved critical and security patches for the operating system and applications at the schedule set by the University.
2. The Work Computer will comply with the ITS Password Standard as defined in the section on Password Standards & Management within this document.
3. The Work Computer will comply with the Antivirus Standard within this document.
4. The Work Computer will have the personal firewall enabled and will filter inbound traffic to the host with a "deny all" policy.
5. The Work Computer will have disabled unneeded services, e.g. SMTP or FTP
6. The Work Computer will be affixed with a University inventory barcode that may not be removed.

ii. Setup the Development Computer by the ITS Help Desk

1. The Development Computer will be set up such that the user cannot connect to the University's network or TitanConnect services. Users should not attempt to connect to University systems and ITS will block access via Access Control Lists.

2. Under no circumstances is University information to be stored on a Development Computer.
3. Users of Development Computers are solely responsible for all aspects of management of the computer including security, patch management and backup.
4. ITS provides only two services for Development Computers.
    a. Restoration back to the initial base development environment.
    b. Facilitator for covered hardware repair with the hardware vendor.

iii. Required Practice

1. Users must lock their computer or logout prior to leaving their device to prevent unauthorized access.
2. Users must turn their computer off when away for an extended period of time.

b. **Server Security**

i. Setup of Services
The installation of servers on the University's network requires the prior approval of the Associate Vice President for Information Technology. The build script, start-up and shut-down procedures must be documented and on-file with the Associate Vice President for Information Technology prior to connectivity to the University network and beyond. It is recommended those requiring connectivity of servers consult with the Associate Vice President for Information Technology.

ii. The ITS department has the exclusive right to operate core network services, such as Firewalls, Intrusion Prevention Systems, DHCP, DNS, BOOTP, email, WIFI access point and all other core network services. Upon the discovery of rogue services, ITS will immediately take down the service. Users must not operate network management services (DNS, DHCP, etc.) and network traffic monitoring devices (i.e. Sniffers).

iii. ITS maintains the primary MX record for the University's email services. All requests for an MX record are to be submitted in writing to the Associate Vice President for Information Technology.

iv. The University reserves the right to monitor network traffic within the University's domain and implement packet management solutions to allocate resources as appropriate.

v. Excessive use of University storage will be monitored and reviewed with users as appropriate.

vi. System logs are required to enable effective troubleshooting of system problems and are a required component of the incident response process. All systems that store, transmit or process University Protected data shall abide by the ITS Log Management Standard.

vii. Physical Security
All University owned production level servers must be housed in the Information Technology Services data center, network closet or hot-site location. Servers are to be secured into standard racks with appropriate UPS backup power, environmental controls and fire-suppression.

Exemptions to this requirement must be obtained from the Associate Vice President for Information Technology.

c. **Disposal Requirement**
All University owned computers are required to be properly retired and disposed of by the University's Information Technology Services department. Information Technology Services practice is to remove and physically destroy all hard-drives for systems that will be recycled for further use within the University.

Under no circumstances may a previously used hard drive used to store University data be removed from the University's environment.

d. **Relocation of Equipment**
In the event a University device is to be relocated, the ITS Help Desk is required to coordinate the move of the device. The ITS Help Desk will ensure the network DHCP servers are reconfigured to allow for network access at the new location.

6. Data Encryption Policy

All systems that store University Protected data will encrypt the data using appropriate encryption techniques. This policy requires the use of private keys to encrypt the data.

Individuals who, because of their job function, are responsible for using a private key (primarily University system administrators) will be designated as "key custodians." No key custodian will have knowledge of a majority of the private keys.

Any private keys created during the encryption process will be maintained via a key management procedure specific to that system. This procedure is determined by the key custodians, and must include the following items:

- Require split knowledge and dual control of private keys, so that at least two key custodians are required to install a single key component or enter a passphrase, for the generation or installation of an encrypting private key.
- An individual who is not serving as a key custodian must be present during the installation of the private key to witness the installation and sign the ITS Key Management Log. The witness will then submit the ITS Key Management Log to the Associate Vice President for Information Technology.
- Require that key custodians sign the ITS Key Management Responsibilities Form, indicating they understand their key management procedures and responsibilities.
- Restrict private keys to the fewest number of key custodians possible.
- Store private keys securely in the fewest possible locations.
- Generate strong keys and securely distribute them to the appropriate key custodians.
- Change private keys at least annually, or as deemed necessary, whichever comes first.
- Replace all known or suspected compromised private keys immediately.
- Securely destroy all private keys that are changed and re-encrypt the data with new private keys.

7. **Anti-Virus Requirement**
   Viruses and other malicious programs can compromise the confidentiality, integrity, and availability of information resources.

   All University owned computers are required to have the University's standard anti-virus solution installed and activated. All are to be connected into the University's central anti-virus management console where automatic updates and settings are managed.

   All student owned computers connected to the residence hall network must also comply with the requirement for regularly updated anti-virus software.

8. **Password Standards & Management**

   a. **User Passwords**
      All user passwords are required:

      i. to be at least eight characters
      ii. contain at least one letter and one number
      iii. to be changed every 90 days

   b. When a password is changed, it cannot be set to any of its previous 10 values.

   c. Under no circumstances should a user password be shared with anyone – even trusted entities such as the ITS Help Desk Staff or your supervisor. If you need to share access to your account with your supervisor or for support purposes, you should be present and enter your own password when necessary. Supervisors may not demand employees provide their password but may work with ITS when such a need arises.

   d. **Administrative Passwords**
      All administrative passwords are required:

      i. to be at least twelve characters
      ii. may not be based on any word that is found in a dictionary
      iii. must contain at least two letters and two numbers

   e. When an administrative password is changed, it cannot be set to any previously used value.

   f. Server administrative passwords cannot be provided to student workers.

   g. **Service Passwords**
      All passwords used to allow servers to communicate with one another in an automated fashion require stronger passwords as they are infrequently changed. They must be at least 12 characters long.

   h. Service passwords cannot be provided to student workers.

   i. Service account passwords must be changed whenever the administrator responsible for the account leaves the organization or changes roles.

j. **Documentation of Administrative and Service Passwords for Business Continuity/Disaster Recovery**
For business continuity and disaster recovery purposes, all administrative and service passwords are to be provided to the AVP for IT at the time they are established or updated. The AVP for IT will store these passwords in a locked safe and at the secured storage location along with the University backup tapes.

9. Software

a. Software installations on Standard Work Computers may be scheduled by contacting the Help Desk.
b. Users must not install any software that the University does not have the right to use.
c. Users must comply with the law with respect to the rights of copyright owners in the use, distribution, or reproduction of copyrighted materials, including but not limited to music or video files.
d. ITS reserves the right to audit the use of software licenses for the sole purpose of compliance with licensing levels.
e. Should ITS discover or be notified of the installation of software in violation of copyright, ITS will immediately investigate and if warranted, remove the product from the computer. Removal may be accomplished through a simple uninstall or through the reimaging process. Prior to reimaging, the user will be afforded four (4) hours to backup any data before ITS wipes the unit clean.
f. All University software is to be acquired through the University's Procurement department according to the University Procurement Policies and a copy of all licenses with a legal backup copy are to be on file with the ITS department.
g. Where only a license is granted for a hosted solution, the license agreement must be on file with the ITS department. Electronic licenses should be directed to its@udmercy.edu.
h. When the installation of a new solution offers password level authentication, passwords are to be established according to the Password Standards & Management section within this document.

10. Hosted Solutions Requirement

a. All University contracted hosted solutions are required to include terms that provide immediate notification to the University's senior attorney in the event of a breach of data related to the University of Detroit Mercy.

b. Before signing an online agreement, the user is required to submit the agreement through the University's Contract Review Process regardless of whether there is an associated dollar value to the agreement or not.

c. Users must not use University resources for personal, commercial or non-profit purposes beyond the mission of the University without the prior written approval of their supervisor and the University of Detroit Mercy senior attorney. This includes prohibiting the use of clickable ads, pay-per-click banners, etc. on University sites.

d. Users or companies contracted to do business with the University must not register domain names to conduct University of Detroit Mercy business without prior written approval by the

Associate Vice President for Marketing and Public Affairs and the Associate Vice President for Information Technology.

11. Network Security

All networking devices procured through, operated or contracted by the University will be configured in accordance with the ITS Router and Switch Security Standard, the ITS Network Firewall Policy, or the ITS Wireless Access Point Policy, depending on type of device.

12. Backup Requirement

a. All University servers and devices containing University data are to have a backup plan on file with ITS, which includes the frequency of backup, the location of media, backup and restore procedures.
b. All data stored on backup media must be encrypted.
c. Once backup media reaches its end-of-life, the media is to be erased with a magnetic device and then physically destroyed such that it is no longer readable by any device.
d. The restoration of end-user files by ITS may only be performed at the request of the departmental director or Dean of Students with the permission of the University Senior Attorney (when appropriate) and/or the AVP for IT. Users should ensure they maintain their own backup and secure it in a safe location. ITS does not guarantee that its backup solutions capture all files at all times and therefore users should be cautious when using their files. Restoration fees may be charged back to the appropriate department for requests due to accidental or careless use.
e. Backup tapes will be rotated to an off-site location on a weekly basis.
f. All systems backed up must be tested on an annual basis to comply with auditor requirements.

13. Data Retention Policy

The retention rate for storage of University information is governed by the University's Document Retention policy. ITS will electronically enforce this policy for the information stored within the University's information systems.

14. Development

a. **Forms Security**
All forms based development (Web, Oracle, etc.) must include the appropriate security measures to prevent the improper use of University servers. Injections that lead to abuse will result in the immediate termination of service upon discovery.

b. **Change Management**
All requests for changes to systems, applications or business processes are to be submitted in writing through the http://hd.udmercy.edu system. Changes will be reviewed by the appropriate authorities and, if deemed accepted, will be authored and tested within a test environment prior to implementation in production. In addition, back-out plans must be developed and all technical and end-user documentation certified prior to implementation in production.

c. **External Code**
Prior to the use of any external code, all licensing to grant such usage of code must be on file with the AVP for IT.

15. Physical & Environmental Security

Centralized computer facilities will be protected in physically secure locations with controlled access, in accordance to the ITS-0035 Access Control Policy. They will also have appropriate environmental safeguards. Departmental computers housing Sensitive or Public data may require physical and environmental security safeguards. All servers containing University Protected data must be housed in an approved ITS data center.

16. Separation or Job Change

Please reference ITS-0008 Access Privilege Policy for details regarding the status at time of separation or job change from the University.

17. Risk Assessment

Security incidents are more likely to occur when there are unknown and unaddressed risks and vulnerabilities in information systems. Therefore, risk assessments will be conducted on a regular basis.

18. Incident Response

Information security incidents have the potential to negatively impact members of the University community and to harm the University's reputation. Therefore, it is important that all information security incidents are handled confidentially and appropriately. All information security incidents will be handled in accordance with the ITS Incident Response Plan.

19. Flagrant Misuse

a. University resources (computers, network, etc.) are not to be used to breach security of any University or external computer.

b. Users must not knowingly attack or infect any other computer and must take reasonable action to prevent potential attacks or infections by using regularly updated anti-virus protection.

c. Users must not use University resources to scan internal or external sites.

d. Users must not use University resources to threaten, stalk or harass another individual.

e. ITS maintains the right to immediately disconnect any device that is disruptive to the network.

f. **External Access Violations**
Under no circumstances is access to University resources to be provided to anyone outside of the University community unless permission has been granted by the Associate Vice President for Information Technology. Users found to be providing access to any third party will immediately lose connectivity to the University's network.

20. User Training and Awareness

Effective information security requires a high level of participation from all members of the University and all must be well informed of their responsibilities. To facilitate this, information security awareness materials and training will be provided to the University community through several methods of delivery.

These methods may include, but are not limited to:

1. **Information Security Website** - ITS maintains a website at http://www.udmercy.edu/about/its/security providing information about Information Security concepts, best practices, advisories and relevant security articles. The website will be updated as needed.
2. **Information Provided via Campus Connection** – ITS works with Marketing & Public Affairs (MPA) to send out relevant security messages to the community via Campus Connection.
3. **Information Provided via Mass Email to the University Community** – ITS sends high priority messages to the University community via mass email distribution.
4. **Information Security Awareness Training Sessions** - ITS provides Information Security awareness sessions as part of its standard training offering as well as by request.
5. **Information Provided via New Faculty Orientation** - ITS presents Information Security materials to new Faculty at the New Faculty Orientation information sessions are current and appropriate.
6. **Information Provided via Student Orientation** - ITS presents Information Security materials included in SOAR information sessions.

21. Enforcement

Violations of this policy may result in some or all of the following:

1. Temporary or permanent loss of privileges
2. Disconnection or delisting from the University network
3. Judicial sanctions as prescribed by the Student Code of Conduct
4. Monetary reimbursement to the University or other appropriate service
5. Separation from the University
6. Prosecution under applicable civil or criminal laws

Signature: _____

Date: _____