Huston-Tillotson University

Office of Information Technology Policies and Procedures Manual

July 2019

HUSTON-TILLOTSON
UNIVERSITY
1875 AUSTIN, TEXAS

Submitted by
Malcolm Haraway
Director of Information Technology

Table of Contents

1. Huston-Tillotson University Mission

HT nurtures a legacy of leadership and excellence in education, connecting knowledge, power, passion, and values.

2. Office of Information Technology Mission

The Department of Information Technology strives and dedicate ourselves to provide a secure technology-rich learning and working environment for Huston-Tillotson University. We are responsible for implementing, monitoring, and maintaining all university technology such as the campus network and wi-fi, computer systems, computer labs, servers and help desk support.

3. Objectives

- Deliver professional customer service and highly reliable IT services to our students, faculty, and staff.

- Create, implement, and maintain robust and secure IT infrastructures and software services to support Huston-Tillotson University in efficiency and productivity.
- Providing students with up-to-date resources and technology to assist and prepare them for their future.

- Ensure the availability of and access to information that enables Huston-Tillotson University to make timely, informed decisions by strengthening data and knowledge management.

- Ensure efficient and effective performance of core university functions and enterprise services.

- Build, develop, and retain a talented, diverse IT department.

4. Purpose

The purpose of the *Huston-Tillotson Information Technology Policies and Procedures Manual* is to provide a guide for employees and students in the planning, acquisition, use, and management of information technology and telecommunications resources at Huston-Tillotson University (HT). It assigns responsibility and defines the authority for implementing computer and network standards, operational standards, security policy and training, and is intended as a handbook for users, as well as an operations management tool.

The information technology resources at Huston-Tillotson University, including computers, printers, local /wide/wireless area and telecommunications networks, software, electronic mail (e-mail), web sites, video, telephony (faculty, staff, and student), voicemail, and cable services are the property of the university and are provided for use by authorized students, faculty, and staff. Individuals who utilize these resources accept responsibility for their proper use.

5. Scope

These policy and procedures apply to:

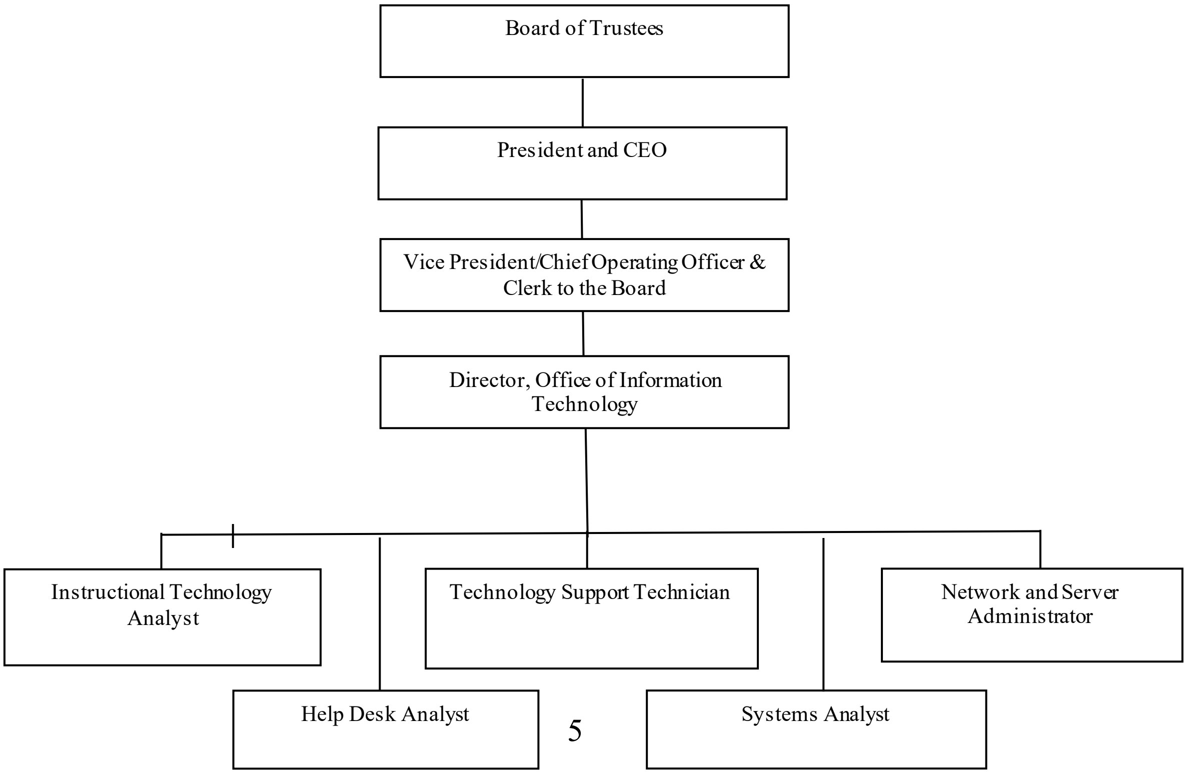
a. All university offices, sites, and learning centers.

b. All students, employees, consultants, contractors, agents and authorized users accessing Huston-Tillotson University information technology systems and applications.

c. All information technology systems or applications managed by Huston-Tillotson University that store, process, or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

6. Organizational Structure

Office of Information Technology Organizational Chart 2019-2020


Board of Trustees
President and CEO
Vice President/Chief Operating Officer & Clerk to the Board
Director, Office of Information Technology
Instructional Technology Analyst
Technology Support Technician
Network and Server Administrator
Help Desk Analyst
Systems Analyst

6.1 Director

The Director of Information Technology provides leadership, planning, and management for all areas of information technology including academic computing, administrative systems, voice and data communication, information technology security, training, and user support. The Director serves as a key resource in the collaborative development and implementation of the University's strategic information technology plan.

6.2 Network and Server Administrator

The Network and System Administrator is responsible for maintaining and administering our university's computer networks and servers. The primary duties include maintenance of computer networks, hardware, software, and other related systems, performing disaster recovery operations, protecting data, software, and hardware from attacks, and replacing faulty network hardware components when necessary.

6.3 Instructional Technology Analyst

The Instructional Technology Analyst serves as the coordinator for the seamless operation of the technical aspects of the distance education program, online learning, and classroom technology. The Instructional Technology Analyst is responsible for maintaining the university's equipment and the connections necessary to transmit and receive broadcasts from the institution.

6.4 Systems Analyst

The System Analysts is responsible for maintaining and improving computer systems and software for Huston-Tillotson University. These systems include and are not limited to Jenzabar CX, NuVision, JICS, Cognos BI, and Office 365. They will analyze system requirements, apply updates, maintain, and address any relevant problems. They perform standard testing and provide solutions to ensure high levels of performance and security.

6.5 Technical Support Technician

The Technical Support Technician is responsible for providing technical assistance and support related to computer systems, hardware, or software. Responds to queries, runs diagnostic programs, isolates problem, and determines and implements solution. They also provide backup support for other areas of operation.

6.6 Help Desk Analyst

The Help Desk Analyst provides direct contact with clients. This helps customers to work effectively on-site. The Support Technician addresses client problems through phone, email, or live chat. They aid and all necessary coordination in the installation of client computer software products, the modification, and repair of hardware and the resolution of client technical problems.

7. Data Handling and Storage

Institutional data is information that supports the mission of Huston-Tillotson University. It is a vital asset and is owned by the university. Institutional data is considered essential, and its quality and security must be ensured to comply with legal, regulatory, and administrative requirements. Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). This administrative policy sets forth the university's standards regarding the handling of sensitive institutional data.

To establish policy for the safeguarding of restricted and sensitive data relating to students and HT personnel that is created, received, maintained, or transmitted by the university. This policy is intended to ensure that the information is uniformly used and disclosed in accordance with all university policies and applicable state and federal laws. A combination of physical security, personnel security, and system security mechanisms are used to achieve this standard.

7.1 Data Collection

a. Users should collect only the minimum necessary institutional/sensitive information required to perform university business.

b. Department heads must ensure that all decisions regarding the collection and use of institutional data are in compliance with the law and with university policy and procedure.

7.2 Data Access

a. Only authorized users may access, or attempt to access, sensitive information.

b. Authorization for access to sensitive data comes from the department head and is typically made in conjunction with an acknowledgement or authorization from the requestor's department head, supervisor, or other official authority.

c. Where access to sensitive data has been authorized, use of such data shall be limited to the purpose required to perform university business.

d. Users will respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies with respect to accessing, using, or disclosing information.

e. Notification of a user's termination or removal of authorized access to sensitive information must be conveyed immediately to the Office of Information Technology.

7.3 Data Handling and Data Transfer

a. Sensitive information must not be transferred by any method to persons who are not authorized to access that information. Users must ensure that adequate security measures are in place at each destination when sensitive data is transferred from one location to another.

b. Sensitive data must be protected from unintended access by unauthorized users. Users must guard against unauthorized viewing of such information which is displayed on the user's computer screen. Users must not leave sensitive information unattended and accessible.

c. Sensitive information must not be taken off-campus unless the user is authorized to do so, and only if encryption or other approved security precautions have been applied to protect that information.

d. Sensitive data should not be transmitted through electronic messaging even to other authorized users unless security methods, such as encryption, are employed.

e. Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a phone or laptop.

7.4 Storage of Sensitive Data

a. Physical protection must be employed for all devices storing sensitive data. This shall include physical access controls that limit physical access and viewing, if open to public view. When not directly in use, office, lab, and suite doors must be locked and any easily transportable devices should be secured in locked cabinets or drawers.

b. Users of laptop and other mobile computing devices always need to be particularly vigilant and take appropriate steps to ensure the physical security of mobile devices, but particularly when traveling or working away from the University.

c. Information Technology managed servers storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up.

d. Systems (hardware and software) designed to store and transfer confidential records require enhanced security protections and must be closely monitored.

e. It is strongly recommended that institutional data not be stored on PCs or other systems in offices or laboratories. Institutional data (including word documents, spreadsheets, and Access databases) that is created on a PC or similar system should be stored on a network drive hosted on an Information Technology managed server or SharePoint.

7.5 Data Retention and Disposal

7.5.1 Archiving

Institutional records, including sensitive information records, which are not being used for active university business, may be archived until retention requirements have been met.

a. Departments determine the criteria for inactive record status in their areas, based on need for the records and available storage space and public records law.

b. Storage areas for inactive records must be physically secure and environmentally controlled, to protect the records from unauthorized access and damage or loss from temperature fluctuations, fire, water damage, pests, and other hazards.

c. When appropriate, only primary student records should be archived. The contents of true "Shadow" record should be destroyed after it has been determined that they contain only duplicates of records maintained elsewhere, and do not contain any original materials.

d. Off-site storage facilities or locations for sensitive records must be approved by the Office of Information Technology

7.5.2 Record Disposal

The proper destruction of public records is essential to creating a credible records management program. Records containing restricted/sensitive data shall only be destroyed in the ordinary course of business; no records that are currently involved in, or have open investigations, audits, or litigation pending shall be destroyed or otherwise discarded.

a. No primary records of any type belonging to Huston-Tillotson University may be destroyed until they have met retention requirements established by HT policies and public records law.
b. When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction later.

c. The authorized methods of destruction for non-electronic records are shredding where authorized. The authorized methods of destruction for electronic records are wiping or physical destruction of the electronic media, and where possible.

7.6 Responsibility

7.6.1 Supervisory Personnel:

Every HT employee who has supervisory responsibilities and whose job responsibilities include the maintenance of or use of sensitive data is responsible for implementing and ensuring compliance with this policy and initiating corrective action if needed. In implementing this policy, each supervisor is responsible for the following:

a. Communicating this policy to personnel under their supervision.

b. Ensuring that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

c. Providing education and training in data management principles to employees under their supervision.

7.6.2 User Responsibilities:

Users who are authorized to obtain data must ensure that it is protected to the extent required by law or policy after they obtain it. All data users are expected to:

a. Access institutional/sensitive data only in their conduct of university business.

b. Request only the minimum necessary confidential/sensitive information necessary to perform university business.

c. Respect the confidentiality and privacy of individuals whose records they may access.

d. Observe any ethical restrictions that apply to data to which they have access.

e. Know and abide by applicable laws or policies with respect to access, use, or disclosure of information.

7.7 Compliance

The compliance with this data protection policy is the responsibility of all members of the Huston-Tillotson University community. Violations of this policy are dealt with seriously and include sanctions up to and including termination of employment. Users suspected of violating these policies may be temporarily denied access to HT's information technology resources during investigation of an alleged abuse. Violations can also be subject to prosecution by state and federal authorities.

8. Back Up and Disaster Recovery

The Office of Information Technology maintains standard backup policies and guidelines for university mission critical technology-based systems. These backup standards are designed to help recover and restore digital data in the event of a malicious security breach, computer virus/malware attack, hardware/software failure or physical disaster, and to provide a measure of protection against human error, such as the deletion of important files.

It should be noted that this policy for system backups is not intended to serve as an archival copy or to meet records retention requirements.

8.1 Desktop Backups

Files stored on desktop equipment are the responsibility of the user. Users must backup critical work files on a regular basis. Information Technology will provide training and assistance to users and departments requiring assistance in backing up critical work files and other University mission critical digital data.

8.2 Frequency

The Office of Information Technology will adhere to information technology best practices that call for daily, weekly, monthly, and yearly system backups. In case of a disaster, this method will allow systems to be restored with the most current data available (minimum of one day of missing data).

8.3 Off-site (Cloud) Integrity and Recovery Testing:

Off-site integrity and recovery testing for all system backups will be conducted (and documented) quarterly (January, April, July, and October) by the contracted vendor to determine if the files and data can be restored. The results of these tests will be reported to the Vice President/Chief Operating Officer.

9. Security

Computers, networks, and electronic information systems are essential resources for accomplishing the Huston-Tillotson University mission. The university grants users **shared access** to these resources to support the accomplishment of its mission. Such access is a **privilege**, not a right, and users should be aware of the responsibilities associated with this privilege.

9.1 Network

All network resources including university information systems will be protected against unauthorized access, modifications, malicious and non-malicious intrusion, breaches, information theft, copying and distribution.

a. All employees of Huston-Tillotson University are provided with logon authentication credentials for access to networks, systems, computers, email and other HT managed accounts.

b. All Huston-Tillotson University students are provided with logon authentication credentials for access to appropriate networks, systems, computers, email and My.HTU accounts.

c. In a file-sharing environment, every file shall be associated with an owner. The owner of each file is responsible for specifying whether the file is sensitive and/or confidential and which users should be allowed to access it with specific read/write privileges (shared folder).

d. The division head or his/her designee has the authority to determine levels of access to information they manage or use.

e. The Office of Information Technology, in collaboration with the Office of the Vice President/COO, has the authority to schedule appropriate security audits based upon various information management and protection requirements.

9.2 Physical

Only Huston-Tillotson University authorized personnel will be granted access to technology resources located in secure technology physical spaces, i.e., server rooms, wiring closets, etc. All information technology resources will be reasonably protected against fire, water, physical damage, and theft. The appropriate protection will be selected from among physical barriers, environmental detection/protection, electronic monitoring systems, insurance, and other risk management techniques.

Individual users are responsible for safeguarding the equipment entrusted to them by the University. This includes reasonable protection of equipment from damage and theft.

9.3 Malware/Virus Protection

Huston-Tillotson University's network infrastructure and other information resources must be continuously protected from threats posed by Malware. To maintain security the following should be adhered to:

a. All computing devices owned, leased, or under the control of Huston-Tillotson University must, to the extent technology permits, execute and keep up to date all required protection software and adhere to any other protective measures as required by applicable Policies and Procedures.

b. Any personally owned Computing Device that contains Confidential University Data must be configured to comply with required University security controls while holding such Data.

c. Any system identified as a security risk due to a lack of virus protection may be disconnected from the network or the respective network account may be disabled until adequate protection is in place.

9.3.1 Reporting Procedure

If a virus is suspected, the user should contact the Help Desk (extension 3168) immediately and isolate all media formats which have been used recently on that computer. **Do not, under any circumstances, allow the isolated program or media source to be used on another computer until the virus has been identified and removed or destroyed.**

9.4 Data Breach

All University employees must know how to respond to potential data security incidents in accordance with the Data Breach Response Policy. If a data security incident is suspected, the IT Helpdesk or Director of Information Technology must be contacted immediately. Unless directed otherwise by the Director of Information Technology, employees may not make changes to the affected system to preserve valuable forensic evidence.

9.4.1 Data Breach Response and Procedure

a. Response Team

- Vice President and Chief Operating Officer

- IT Director
- Network and Server Administrator
- Systems Analyst
- Director of Campus Safety

b. Reporting a Breach and Alert

Any employee that is aware of a possible or known data breach must immediately inform and alert their immediate supervisor, IT Director and Vice President/Chief Operating Officer.

The information that should be provide (if known) at this point includes:

1. When the data breach occurred?

2. Description of the breach.

3. What was the cause of the breach?

4. How was it discovered?

5. What systems where affected?

6. What individuals or parties are involved?

c. Containing the Breach

The Response Team will work with departments and units immediately contain the breach by, for example, shutting down and removing breached systems from network, reset passwords, disable accounts, and any other required mitigating factor to ensure containment.

d. Assessment and Potential Impact

After the data breach has been reported and contained, the Data Breach Response Team will convene to determine:

1. The scope of the breach

2. The severity of the breach

3. The individuals or parties affected

4. The personal/private information involved

5. The foreseeable harm from the breach

6. The harm to the university as a result of breach

e. Notification

At this point the response team will provide written statement within 30 days from the date the team was aware of the breach. The team will notify all parties and individuals that were affected.

These items should be included in the notification:

1. Date of the breach

2. Description of the breach

3. Description of the information inappropriately accessed, collected, used or disclosed.

4. The steps taken to mitigate the harm.

5. Next steps planned and any long-term plans to prevent future breaches.

6. Steps the individual can take to further mitigate the risk of harm.

7. Contact information for the Vice President and Chief Operating Officer

9.5 Multi-Factor Authentication

MFA defines requirements for accessing Huston-Tillotson University network and information systems from off campus. These standards are designed to minimize the potential security exposure to the university from damages which may result from unauthorized use of Huston-Tillotson resources. Multi-factor authentication adds a layer of security which helps deter the use of compromised credentials.

9.5.1 User Requirements

a. Users must register a device or alternative contact to provide a secure method for Huston-Tillotson to contact you during the authentication (logon) process, such as a cellphone that can receive texts, a landline phone or a non-university email address. If you do not register, you will not be able to use MFA— if MFA is required for that system or service, you will not be able to use the system.

b. Users must reauthenticate their device every 30 days.

10. Access Management

Proper management and use of computer accounts are basic requirements for protecting the university's Information Resources. All offices that create access accounts for applications, networks, or systems are required to manage the accounts in accordance with the university's access management processes. Access to an Information Resource may not be granted by another user without the permission of the Owner or the Owner's delegated custodian of that Information Resource. All accounts are to be created and managed using the following required account management practices:

10.1 Access Management Requirements

a. All accounts that access non-public university Information Resources must follow an account creation process. This process shall document who is associated with the account, the purpose for which the account was created, and who approved the creation of the account at the earliest possible point of contact between the account holder and the university.

b. All accounts wishing to access the university's non-public Information Resources must have the approval of the Owner of those resources. These measures also apply to accounts created by/for use of outside vendors or contractors.

c. Each account having special privileges must adhere to the university's password requirements.

d. All accounts must be able to be associated with an identifiable individual or group of individuals that are authorized to use that account.

e. Accounts of individuals on extended leave (more than 120 days) or accounts that have not been accessed in more than 120 days must be disabled.

f. Account passwords shall be expired based on Risk.

g. Accounts of individuals who have had their status, roles, or affiliations with university change must be updated to reflect their current status.

h. Accounts must be reviewed at least annually to ensure their current state is correct.

i. Password aging and expiration dates must be enabled on all accounts created for outside vendors, external contractors, or those with contractually limited access to the university's information resources.

10.2 Data Access Control Requirements

All owners must control and monitor access to Data within their scope of responsibility based on Data sensitivity and Risk, and through use of appropriate administrative, physical, and technical safeguards including the following:

a. Owners must limit access to records containing Confidential Data to those employees who need access for the performance of the employees' job responsibilities. An employee may not access Confidential Data if it is not necessary and relevant to the employee’s job function.

b. Owner must monitor access to records containing Confidential Data using appropriate measures as determined by applicable Policies, Standards, Procedures, and regulatory requirements.

c. Owners must establish log capture and review processes based on Risk and applicable Policies, Standards, Procedures, and regulatory requirements. Such processes must define:

    1. the Data elements to be captured in logs.

    2. the time interval for custodial review of the logs

    3. appropriate retention period for logs.

d. Employees may not disclose confidential data to unauthorized persons or Institutions except:

    1. as required or permitted by law, and, if required, with the consent of the data owner

    2. where the third-party is the agent or contractor for the Huston-Tillotson University and the safeguards described in Part 9.5 are in place to prevent unauthorized distribution

10.3 Data Access Control for Third Parties.

If Huston-Tillotson intends to provide university data to a third-party acting as an agent of or otherwise on behalf of Huston-Tillotson (example: an application service provider) a written agreement with the third-party is required.

a. Such third-party agreements must specify:

1. the data authorized to be accessed

2. the circumstances under and purposes for which the data may be used

3. that all data must be returned to Huston-Tillotson University, or destroyed, in a manner specified by Huston-Tillotson upon end of the third-party engagement.

b. If Huston-Tillotson University determines that its provision of data to a third-party will result in significant risk to the confidentiality, integrity, or availability of such data, the agreement must specify terms and conditions, including appropriate administrative, physical, and technical safeguards for protecting the data.

11. Appropriate Use of E-mail

Emails sent or received by users in the course of conducting university business are considered university data that are subject to state records retention and security requirements. Huston-Tillotson University strongly recommends that e-mail not be used for confidential communication. E-mail is now considered a formal written record that carries the same legal weight as a paper memorandum. Users of e-mail should remember that e-mail messages become the possession of the receiver and can be easily duplicated and redistributed by recipients. Messages that have been deleted can be retained unintentionally on system backup files in a disaster case only (server outage, mass e-mail virus, catastrophe, etc.). In addition, even secure passwords are not completely confidential. When a private message needs to be conveyed between two individuals, a conversation is the best way to accomplish it; and messages that should not be preserved should be deleted immediately. E-mail is also governed by state and federal laws regarding copyrighted material, photographic images and libelous remarks.

The following email activities are prohibited when using a University provided email account:

a. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.

b. Accessing the content of another User's email account except:

1. as part of an authorized investigation

2. as part of an approved monitoring process

3. for other purposes specifically associated with the user's official duties on behalf of University.

c. Sending or forwarding any email that is suspected by the User to contain computer viruses.

d. Sending of forwarding pornographic, harassment, political campaigning, or commercial solicitation

e. Any Incidental Use prohibited by this policy.

f. Any use prohibited by applicable University or System policy.

12. User Accounts and Passwords

Only the person responsible for the assigned account should have access to the password. Access to user accounts may not be loaned and/or sold. Any suspected breach of password security should be reported immediately to the Office of Information Technology Help Desk (helpdesk@htu.edu or (512) 505-3168). Listed below are some common rules to follow in protecting one's password:

- Do not store passwords at any workstation that can be used to gain access to computing resources;
- Never share passwords; and never tape passwords to a wall or under a keyboard or write them down on paper.

13. Huston-Tillotson Acceptable Use Policy

This document defines a policy for acceptable use of Huston-Tillotson University's information technology. This policy applies to all users including faculty, staff, students and guest users of Huston-Tillotson University's computer networks, equipment, or connecting resources.

13.1 Use of Equipment

a. Only Huston-Tillotson University students, faculty, staff, alumni, and authorized users are allowed to use campus technology equipment.

b. Users shall adhere to the terms of software licenses and other contracts. Persons loading software on any University computer must adhere to all licensing requirements for the software. Except where allowed by University site licenses, copying software licensed for University use for personal use is a violation of this policy.

c. Users shall adhere to other University and campus policies, including the Collected Rules and Regulations of the University, Code of Conduct and Community Standards, and, if applicable, the University Business Policy

Manual, Human Resources Manual and policies established for a specific resource.

d. Users shall adhere to data access policies of the University or those established by law.

e. Users shall use University computer and network resources in a manner that is compliant with University policies and State and Federal law.

f. The use of University equipment by individuals or organizations for activities not directly connected with an approved Huston-Tillotson University activity is prohibited.

g. Users shall not use University technology equipment and network for unlawful purposes, including, but not limited to, illegal copying, installing or using of software, music, media or any copyrighted materials without a license.

The Information Technology Department reserves the right to inspect electronic information on University networks or equipment, including, but not limited to, electronic mail and personal information, which is subject to examination by the University where:

a. It is necessary to maintain or improve the functioning of University computing resources.

b. There is a suspicion of misconduct under University policies, or suspicion of violation of Federal or State laws

c. It is necessary to comply with or verify compliance with Federal or State law.

13.2 User Responsibilities

a. Users shall respect the intellectual property rights of authors, contributors, and publishers in all media.

b. Users may not divulge any personally identifiable information that they may have access to without permission or prior consent from a Huston-Tillotson University representative.

c. Users shall protect their user ID, password, and system from unauthorized use. Users shall comply with the following password security rules to protect their accounts.

1. Passwords must be at least 8 characters in length

    2. Passwords must include a letter, number and special character (i.e.: ( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? / , etc.

d. Users shall not use or try to discover another user’s password.

e. Users shall log-off of computers when they are not in use.

f. Users shall lock their personal workstations when away from their desk.

g. Users shall not deliberately use campus technology to annoy or harass others in any way.

h. Users shall not deliberately create or access any obscene, non-educational, images or other content that are profane or sexual in content. Users who receive profane content are required to delete the content and contact the Information Technology Helpdesk.

i. Users shall not intentionally damage any campus technology or electronic information belonging to others, or misuse campus technology resources, or allow others to misuse campus technology resources.

j. Users shall not remove any campus technology equipment from its assigned/designated location without prior approval by the appropriate manager.

13.3 Prohibited Uses of University Computer Resources

a. Unauthorized or excessive personal use. Use may be excessive if it overburdens a network, results in substantial use of system capacity, or otherwise subjects the institution to increased costs or risks (employees additionally may be subject to discipline for unauthorized or excessive personal use of computer resources.)

b. Uses that interfere with the proper functioning of the University's information technology resources.

c. Uses that unreasonably interfere with the ability of others to make use of University computer resources.

d. Attempting to gain or gaining unauthorized access to the computer system or files of another.

e. Use of University computer resources to infringe the intellectual property rights of others.

f. Use of University computer resources for personal profit, except as permitted under the University's conflict of interest policy.

g. Mass mailing of email by and to university personnel should be limited to relevant university business including the announcement of events, activities, policies, procedures, or emergency situations. Mass mailing should not be used for e-mails only meant to be inspirational, funny, religious, which support a particular religious or world view, or which attempt to sway the reader's beliefs.

h. Use of university computer resources to influence legislation or campaign for or against political candidates is prohibited.

13.4 Consequences of User Violations

Use of campus technology is a privilege. Violations of the policies and procedures of Huston-Tillotson University concerning the use of videos, computers, campus technology and networks will result in disciplinary actions under Huston-Tillotson University's Personnel Policies for Administrators and Staff Manual or University's Policy and Procedures Manual, Student Handbook.

13.4.1 Violations by Students of the Institution

a. First Offense:

Any student considered being in violation of the Acceptable Use Policy should be referred to the manager of the department or laboratory in which the offense occurs. The manager will counsel the student and advise the student of the offense, and may suspend the student's use of the computer or laboratory for twenty-four (24) hours.

a. Second Offense or Pattern of Abuse or Flagrant Violation:

Any student alleged of a second offense of the Acceptable Use Policy or who exhibits a pattern of flagrant violation of the Acceptable Use Policy, such as gross misconduct or destruction of property, or mischievous insult to others, should be referred to the manager of the department or laboratory in which the offense occurs. The manager may summarily suspend the student's use of the computer, network or laboratory for one week. Within twenty-four (24) hours, the manager shall submit a formal written complaint to the Dean of Student Affairs for referral to the conduct process for review and follow up.

Sanctions imposed by a Conduct Officer, or the University Conduct Council may include any combination of the following sanctions: monetary fine, suspension of the use of the campus technology for a specified amount of time not to exceed the balance of the semester, "campus work," suspension from school for the balance of the semester, or referral to legal authorities for prosecution under federal and state statutes.

13.4.1 Violations by Employees of the Institution

Any employee of Huston-Tillotson University who violates the Acceptable Use Policy should be referred immediately to the respective unit head. The unit head will counsel the employee and advise the employee of the offense and may recommend to the President the employee's appropriate sanction or termination from Huston-Tillotson University, and/or referral to legal authorities for prosecution under federal and state statues.

13.4.2 Violations by Employees of the Institution

Any student of Huston-Tillotson University who violates the Acceptable Use Policy should be referred immediately to the Dean of Student Affairs.

13.5 Changes to this Policy

Huston-Tillotson University reserves the right to change this Acceptable Use Policy at any time by posting a new Acceptable Use Policy on its website. You can send an email to Huston-Tillotson University with any question relating to the Acceptable Use Policy at itdepartment@htu.edu.

14. Disciplinary Actions

Violation of this Policy or other Huston Tillotson University Systems, Information Technology Policies and/or Standards by faculty, staff, and students who have access to HT Information Resources or Data for the purpose of providing services to or on behalf of an Institution, are subject to disciplinary action in accordance with the applicable institutional rules and policies.

For contractors and consultants, this may include termination of the work engagement and execution of penalties contained in the work contract. For interns and volunteers, this may include dismissal. Additionally, certain violations may result in civil action or referral for criminal prosecution.

15. Legal Compliance

All existing federal and state laws and the University's regulations and policies apply to the use of campus computing resources. Users of such resources are required to be in compliance with the laws, regulations and policies at all times. These are not limited only to laws and regulations that are specific to computer and network usage, but those that apply to personal conduct.

Individuals are responsible for ensuring that their activities comply with copyright laws. **Copyright laws apply to all materials published on the web unless the site specifically states otherwise.** Users must seek permission from owners to use materials, text or graphics, from any web site.

16. Indemnification of Huston-Tillotson University

Upon the granting of access to the University's computers and networking services, users agree to indemnify, defend, and hold harmless the University from any suits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the University’s computer resources and all other media services and facilities.

17. Privileges and Responsibilities

Prior to receiving the privileges associated with a network account, users must sign a statement that they also accept the responsibilities that accompany these privileges. Those using the University computer facilities are always responsible for using these facilities in a manner that is consistent with this policy and its intent. Users are responsible for obeying all official notices posted in local policy newsgroups by appropriate staff members or announced using electronic mail. They are also responsible for knowing and abiding by the policy set forth in this document, along with any changes announced by any of the means noted in this paragraph.

Users are also responsible for all activity initiated by their account. For this reason, as well as to protect their own data, users should always select a secure password for their account and keep that password secret. Users are responsible for protecting their own files and data from reading and/or writing by others, with whatever protection mechanics are provided by the operating system in use. They are also responsible for picking up their printer output in a timely fashion to avoid theft or disposal.

18. Conclusion

The Office of Information Technology is a vital resource for the fulfillment of academic and administrative purposes. Therefore, it is essential that all faculty, staff, and students exercise responsible and ethical behavior when utilizing this resource.

Technology is constantly changing and therefore this manual will need to be revised and updated periodically. Comments and corrections are welcomed and should be sent in writing to the IT Director.