University of Dallas	Information Technology Policy	**POLICY ITS** Responsible Executive: Executive Vice President Responsible Office: Information Technology Issued: 7.22.21 Revised: 10.05.22

1. PURPOSE

This Policy provides guidance to the University community regarding the appropriate use of University Information Technology systems and the transmission and storage of information on those systems. It is the responsibility of every systems user to know these guidelines, and to conduct their activities accordingly.

2. UNIVERSITY INFORMATION TECHNOLOGY SYSTEMS

2.1. **Ownership.** Except as set forth in University Policy APC – Copyright Ownership and Infringement Policy or pursuant to written agreement with the University, the University owns all information created or stored on University sponsored systems.

2.1.1. Retention of ownership. The University retains ownership of data created or stored by a University employee, and an employee may not remove such data from a University system, upon termination or conclusion of employment.

2.1.2. Information contained in any University sponsored systems is the property of the University and is subject to review at any time by a member of the authorized University staff; as authorized by the IT office, Office of the General Counsel or the Office of Human Resources.

2.2. **Right of control and review.** The University retains a right of control and review as to all University sponsored systems and the information stored in or on those systems. This right of control and review includes, but is not limited to, the following rights:

2.2.1. **Right to remove.** The University retains the right to remove any information or type of information on its University sponsored systems.

2.2.2. **Right to prohibit use.** The University retains the right to prohibit the creation or storage on any information or type of information on its University sponsored systems.

2.2.3. **Right to audit and review.** The University retains the right to audit the use of University sponsored systems, including so as to determine whether any individual has committed a violation of law or violated University policy.

2.2.3.1. The IT Office or its designee may, on a periodic or random test basis, attempt to predict, guess or breach the password of one or more authorized users. If the authorized user shares a password assigned to an individual, the authorized user will be required to change the password immediately and may be subject to disciplinary action.

2.2.4. **Right to restrict access.** The University retains the right to restrict the access of any person to some or all of University sponsored systems.

3. ACCEPTABLE USE

The University has information technology systems for use by different members of the University community as well as, in some cases, members of the public.

3.1. **Authorized users.** Authorized users are responsible for the proper use of their user accounts.

3.2. **University Sponsored Systems use**. All users of University sponsored systems, including, but not limited to, faculty, staff, and students, are expected to practice prudence in their use of University sponsored systems so as to protect the integrity and purpose of University sponsored systems, as well as the privacy and rights of others.

3.2.1. **Use of VPN software**. It is the responsibility of employees with virtual private network (VPN) privileges to ensure that unauthorized users are not allowed access to the University's internal networks. Only pre-approved software programs may be used to connect to the University's VPN. An individual who connects to the University's VPN with an unapproved software program is violating this Policy and subject to revocation of VPN privileges, disciplinary action, or other appropriate restrictions on access to University sponsored systems.

3.2.2. **No unauthorized use.** Use of restricted portions of the University's information technology systems without authorization from University IT personnel is prohibited.

3.2.3. **No commercial use.** Except for the development or storage of Scholarly, Professional and Creative Work or Instructional Materials by faculty (see University Policy APC – Copyright Ownership and Infringement Policy), University sponsored systems may not be utilized for commercial use, product advertisement, or any other form of revenue generating activities.

3.2.4. **No illegal or other improper use purposes.** University sponsored systems may not be used for any activity that is illegal under local, state, federal or international law. The following is a non-exhaustive list of prohibited activities:

3.2.4.1. University sponsored systems may not be used to violate copyright or other intellectual property rights;

3.2.4.2. University sponsored systems may not be used to download and/or install any software not related to job functions or not authorized by the IT Office;

3.2.4.3. University sponsored systems may not be used to introduce computer viruses into the University sponsored systems or into any other computing environment;

3.2.4.4. University sponsored systems may not be used to access or copy another person's electronic mail, data, programs, or other files without authorization;

3.2.4.5. University sponsored systems may not be used to bully or harass other individuals; and

3.2.4.6. University sponsored systems may not be used to violate any state or federal laws, or any University Policy.

3.2.5. **Disciplinary action.** Any violation of Sections 3. of this Policy is a violation of University policy and the applicable code of conduct (e.g., student, employee or faculty member). Individuals committing such violations may be subject to disciplinary action, as well as restrictions in their ability to use some or all of the University sponsored systems.

4. STORAGE AND TRANSMISSION OF INFORMATION

All authorized users are required to comply with the following requirements for the storage and transmission of information.

4.1. **Highly sensitive information.**

4.1.1. **Transmission.** Highly sensitive information, if transmitted, must be password protected and the password must be sent independently of the highly sensitive information.

4.1.2. **Storage.** Sensitive information should only be stored on University sponsored systems.

4.1.3. **Authority to review.** Sensitive information should not be made available or accessible to persons who do not have a legitimate University purpose to review it or who are not authorized to review it under applicable law.

4.2. **Sensitive information.**

4.2.1. **Storage.** Sensitive information should only be stored on University sponsored systems.

4.2.2. **Authority to review.** Sensitive information should not be made available or accessible to persons who do not have a legitimate University purpose to review it or who are not authorized to review it under applicable law.

4.3. **Internal information.**

4.3.1. **Storage.** Internal information should only be stored on University sponsored systems.

4.3.2. **For University purposes.** Internal information should not be disseminated or made available for a purpose adverse to the University.

4.4. **Public information.**

4.4.1. **For University purposes.** Public information should not be disseminated or made available for a purpose adverse to the University.

5. PASSWORD MANAGEMENT

All authorized users are required to update their password in accordance with the schedule set forth in this Policy and in accordance with password protection requirements instituted by the IT Office.

5.1. **Update schedule.** Password update schedule.

5.1.1. All system-level passwords must be changed on at least a quarterly basis.

5.1.2. All user-level passwords must be changed at least every six months (though quarterly is recommended).

5.1.3. **Password protection** Authorized users shall protect their password(s) from disclosure. Such protection of password(s) includes, but is not limited to, the following:

5.1.3.1. Passwords shall not be stored in a file on **any** computer system without encryption.

5.1.3.2. Passwords shall not be visible in public spaces. Those spaces include but are not limited to: workstations, desks, monitors, or whiteboards.

5.1.3.3. Passwords shall not be provided to other individuals unless the authorized user is granting permission to the other individual to utilize the user account. (The IT Office **never** needs nor will it ask~~s~~ authorized users to disclose their passwords.)

5.1.4. **Password requirements.** The IT Office may institute mandatory password protections (e.g., password standards) that are enforced when a person creates or updates a user account password on a University sponsored system. The IT Office may publish additional password protection standards that users are recommended to utilize in order to better increase security for University sponsored systems

5.1.5. **Sharing passwords of individually assigned accounts is prohibited.** Users are strongly discouraged from sharing their password(s) with other persons. An authorized user who shares his or her password(s) with one or more other persons is responsible for any violations of law or University policy that may occur due to password sharing.

5.2. **Compromised account disclosure requirement**: If an authorized user suspects an account or password has been compromised, the authorized user must notify the IT Office immediately, and change all passwords used for accounts to University sponsored systems.

6. UNIVERSITY ELECTRONIC MAIL (E-MAIL)

6.1. **Email creation.** A new University e-mail account will be created for every new University employee and access to the University e-mail account will be provided to a new University employee on or after the first day of the employee's University employment.

6.2. **Email use.** Authorized users with University e-mail accounts are to use and access their account(s) within the following guidelines:

6.2.1. Authorized users are required to access their e-mail accounts through University-approved methods. University-approved methods are browser-based Gmail or the Gmail mobile application. Other access must be specifically outlined and approved through the submission of a support ticket or written authorization/approval by an authorized IT representative.

6.2.2. Authorized users are required to follow cyber security guidelines including but not limited to spam and phishing reporting, use of the "Phish Alert Button (PAB)" and Gmail's "Mark as spam" functionality.

6.3. **Email right of control and review**. The University retains a right of control and review as to all University e-mail accounts, as defined by 2.2 (Right of control and review). The provisioning and access to accounts along with any associated permissions for e-mail accounts are managed at the discretion of an authorized IT representative.

6.4. **Email management**. University email accounts will be managed on a per-role basis; including but not limited to faculty and staff addresses. Upon departure or termination from one or both roles and at the discretion of an authorized IT representative, in collaboration with the supervisor overseeing the position being vacated, the University may maintain the corresponding e-mail account.

6.4.1. Upon the departure or termination of an employee (staff or faculty member) from his or her position at the University, access to University e-mail accounts and all links to managed devices will be removed. IT reserves the right to lock or terminate the e-mail account.

6.4.2. The following are guidelines for the maintenance of, and continued access to, an account by internal staff and designate the length of time certain internal staff may have access to a former employee's e-mail account following the employee's departure from the University:

6.4.2.1. Vice President, Executive Vice President, Provost or President: access for three months

6.4.2.2. Assistant Vice President, Senior Director, Executive Director, Director: access for one month

6.4.2.3. Manager: access for one week

6.4.2.4. Exceptions.

6.4.2.4.1. Good cause. On a case-by-case basis, for good cause, IT may shorten or extend an internal staff's access to a departing employee's e-mail account.

6.4.2.4.2. Retired Faculty. Faculty who retire from the University may retain access to a University e-mail account if the faculty member maintains continued association with the University and receives written authorization/approval from an authorized IT representative.

7. DEFINITIONS

7.1. **"Authorized user"** means an individual who has been granted permission by the University to use one or more University sponsored systems that require an individualized account access.

7.2. **"Authorized IT representative"** means a University employee with a position in the University of Dallas Office of Information Technology Services who is authorized to exercise oversight in a particular area of Information Technology Services.

7.3. **"Confidential information"** means information that

7.3.1. would not generally be considered harmful or an invasion of privacy if disclosed, and

7.3.2. the University is not required to treat as confidential by law (e.g., FERPA).

7.4. "**Employee"** means all persons who receive wages, whether on a salaried or hourly basis, through the University payroll.

7.5. **"FERPA"** means Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

7.6. **"Highly sensitive information"** means information that meets the criteria for sensitive information and which, in the judgment of the University pursuant to Section 4.1. of this Policy, requires additional oversight and control due to the reputational, financial, or operational impact it may have on the University. Highly sensitive information includes, but is not limited to,

7.6.1. Bank account numbers;

7.6.2. Driver's license numbers;

7.6.3. HIPAA data,

7.6.4. Social security numbers; and

7.6.5. Credit card numbers.

7.7. **"HIPPA data"** means protected health information is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations.

7.8. **"Internal information"** means information that is intended for limited use within the University that, if disclosed, could have an adverse effect on the operations, assets, or reputation of the University. Information designated as internal would not generally compromise the University's obligations concerning information privacy and confidentiality.

7.9. **"IT Office"** means the University of Dallas Office of Information Technology.

7.10. **"Password"** means is a string of letters, numbers, and/or symbols used to provide security protection against unauthorized access of a user account or University sponsored system.

7.10.1. **"System-level password"** means a password for accessing the following types of user accounts on University sponsored systems: root, enable, NT admin, application administration accounts, etc.

7.10.2. **"User-level password"** means a password for accessing a user account.

7.11. **"Password protection requirements"** means standards that a user must use in order to create or update passwords on University sponsored systems.

7.12. **"Password protection standards"** means standards published by the IT Office as required or recommended for maintaining security on University sponsored systems.

7.13. **"Public information"** means information intended for broad use within the University community at large or for public use that, when used as intended, would have no adverse effect on the operations, assets, or reputation of the University, or the University's obligations concerning information privacy and confidentiality.

7.14. **"Security designation"** means the category for determining the level of security that should be maintained in the storage and transmission of University information. There are four security designations: public, internal, sensitive, and highly sensitive.

7.15. **"Sensitive information"** means information that is intended for limited use within the University that, if disclosed, could be expected to have a specific and serious adverse effect on the operations, assets, or reputation of the University, or to compromise the University's obligations concerning information privacy and confidentiality (e.g., under FERPA).

7.16. **"Student"** means an individual taking courses at the University, either full-time or part-time, in person, online or studying abroad, including on the Rome campus, and pursuing either undergraduate or graduate studies, including individuals who withdraw from the University during the conduct process; those who are not currently enrolled in courses but who have a continuing relationship with the University and those who have applied for readmission to the University.

7.17. **"University"** and **"the University"** mean the University of Dallas.

7.18. **"University information"** means information that is stored on University sponsored systems.

7.19. **"University sponsored systems"** means such property, leased or owned, in both hardware and software form to include servers, shared drives, learning management systems, and cloud service providers (e.g., Google Drive, Gmail) that are approved by University IT Office for storage or transmission of University information.

7.20. **"User account"** means a University sponsored system that requires an individualized account access (e.g., email, web-based access, desktop computer, etc.).

8. RESPONSIBILITIES

Responsible Party	List of Responsibilities
Office of Information Technology	1. Monitor compliance with this Policy. 2. Review and make determinations on requests for clarification as to the appropriate security designation of information. 3. Conduct security audits.

President	1. After a request has been considered by the IT Office, further review can be requested. 2. Following the request, the President may, following or in consultation with the IT Office, review and make determinations on requests for clarification as to the appropriate security designation of information.

9. PROCEDURES

Task	Procedure
Establish password requirements	1. The IT Office establishes password requirements for University sponsored systems and implements those requirements in such systems.
Audit security	1. The IT Office regularly reviews the security of University sponsored systems, including testing the security of individual passwords.
Determine security designations	1. The IT Office makes the primary determination as to the appropriate security designation for University information. 2. If there is a request for further review of the IT Office's primary determination, the final decision is made by the President or designee.

10. POLICY ENFORCEMENT

Enforcement	The Office of the General Counsel or the Office of Information Technology will investigate suspected violations of this Policy, and take appropriate action in accordance with University policy.
Reporting Violations	Report suspected violations of this Policy to the Office of the General Counsel or the Office of Information Technology.

11. RELATED DOCUMENTS

Policy or Document	Web Address
Policy APC – Copyright Ownership and Infringement Policy	https://udallas.edu/about/university-policies/index.php
SANS Glossary of Terms	https://www.sans.org/security-resources/glossary-of-terms/

12. CONTACTS

Subject	Office or Position	Telephone Number	Office Email or URL
Policy Clarification	Office of General Counsel	(972) 721-5363	hlachenauer@udallas.edu

Implementation	IT Office		support@udallas.edu
Web Address for this Policy		https://udallas.edu/about/university-policies/index.php	