University of Dallas	Information Technology Security Policy	**POLICY ITS** Responsible Executive: Chief Information Officer Responsible Office: Information Technology Issued: 7.22.21 Revised: n/a

1. PURPOSE

This Policy guidance to the University community regard the appropriate use of University sponsored systems and the transmission and storage of information on those systems.

2. UNIVERSITY INFORMATION TECHNOLOGY SYSTEMS

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.

2.1. **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:

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

2.1.2. **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.

2.1.3. **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.

2.1.3.1. The IT Office or its designee may, on a periodic or random basis, attempt to crack or guess the password of one or more authorized users. If the IT Office or its designee is able to crack or guess the password, the authorized user will be required to change the password immediately.

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

2.2. **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.

2.2.1. Information contained in University sponsored systems, including information in electronic mail stored or transmitted on University sponsored systems, is not private as to the University.

3. ACCEPTABLE 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.

3.1. **Use of University sponsored systems.**

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

3.1.1.1. **Use of VPN software.**

3.1.1.1.1. 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.

3.1.1.1.2. 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.

3.1.2. **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.

3.1.3. **No use for illegal or other improper purposes.** University sponsored systems may not be used for any illegal or other improper purpose. The following is a nonexhaustive list of prohibited activities:

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

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

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

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

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

3.1.4. **Disciplinary action.** Any violation of Sections 3.1.1, 3.1.2, or 3.1.3 of this Policy is a violation of University policy and the appropriate code of conduct (e.g., student or employee).

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.

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

3.2.1. **Sharing passwords discouraged.** Authorized 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 occur due to the sharing of the password(s).

3.2.2. **Protecting passwords.** Authorized users should protect their password(s) from disclosure to individuals who they have not authorized to access their user account. Such protection of password(s) includes, but is not limited to, the following:

3.2.2.1. Passwords should not be stored in a file on **any** computer system without encryption.

3.2.2.2. Passwords should 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 asks an authorized user to disclose his or her password.)

3.2.2.3. If an authorized user suspects that an account or password has been compromised, the authorized user must notify the IT Office and change all passwords used on accounts in University sponsored systems.

4. UPDATING OF PASSWORDS

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.

4.1. **Update schedule.** Password update schedule.

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

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

4.2. **Password protection requirements.** The IT Office may institute mandatory password protections (e.g., requirements as to passwords) that are enforced when a person creates or updates a User account password on a University sponsored system.

4.2.1. In addition, the IT Office may publish password protection standards that users are recommended to utilize in order to better increase security on University sponsored systems.

5. STORAGE AND TRANSMISSION OF INFORMATION

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

5.1. **Highly sensitive information.**

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

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

5.1.3. **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.

5.2. **Sensitive information.**

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

5.2.2. **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.

5.3. **Internal information.**

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

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

5.4. **Public information.**

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

5.5. **Determination of Category.**

5.5.1. The Director of the IT Office has primary responsibility for determining what security designation applies to information.

5.5.2. The President, or designee, has ultimate authority to determine what security designation applies to information.

6. DEFINITIONS

6.1. **"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.

6.2. **"Confidential information"** means information that

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

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

6.3. **"Highly sensitive information"** means information that meets the criteria for sensitive information and which, in the judgment of the University pursuant to Section 5.5 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,

6.3.1. Bank account numbers;

6.3.2. Driver's license numbers;

6.3.3. HIPAA data,

6.3.4. Social security numbers; and

6.3.5. Credit card numbers.

6.4. **"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.

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

6.6. **"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.

6.6.1. **"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.

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

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

6.8. **"Password protection standards"** means standards published by the IT Office as recommendations for maintaining security on University sponsored systems.

6.9. **"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.

6.10. **"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.

6.11. **"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).

6.12. **"Student"** means an individual who is enrolled at the University.

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

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

6.15. **"University sponsored systems"** means such 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.

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

7. 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 (or designee)	1. After a request has been considered by the IT Office and if further review is requested, review and make determinations on requests for clarification as to the appropriate security designation of information.

8. 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 or designee.

9. 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.

10. 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/

11. 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	