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

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.p r i r

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 comy ng tems:10(s)(