# University of Dallas

| | |
|---|---|
| **Name:** | Acceptable Use and Security Awareness |
| **Description:** | The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. The University of Dallas (UD) is committed to protecting all users from illegal or damaging actions by individuals, either knowingly or unknowingly.<br><br>Internet/Intranet-related systems, including but not limited to computers, laptops, wireless systems, operating systems, applications, removable electronic media, network accounts providing electronic mail, Internet browsing, and remote access, are the property of UD. These resources are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.<br><br>Effective security is a team effort involving the participation and support of every user and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. |
| **Purpose:** | The purpose of this policy is to outline the acceptable use of computer equipment at UD. These rules are in place to protect all users. Inappropriate use exposes UD to risks including virus attacks, compromise of network systems and services, non-compliance fines and legal issues. |
| **Policy:** | **Scope -**<br><br>This policy applies to all users (employees, students, contractors, consultants, temporary employees, student workers, and all other workers, including all personnel affiliated with third parties) at UD, and to all equipment, networks, systems, software and other resources owned or leased by UD.<br><br>**General Use and Ownership -**<br><br>1. While the IT Department desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of UD. Because of the need to protect the network, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to UD.<br>2. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.<br>3. UD equipment, systems, email address, etc. are not to be used to pursue outside business activities not sanctioned by the University.<br>4. The IT Department recommends that any information that users consider sensitive or vulnerable be encrypted.<br>5. For security and network maintenance purposes, authorized individuals within UD may monitor equipment, systems and network traffic at any time.<br>6. UD reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy. |

**Security and Proprietary Information -**

1. Users should take all necessary steps to prevent unauthorized access to confidential information. Examples of confidential information include but are not limited to: credit card information, student information, corporate strategies, trade secrets, specifications, employee, vendor, and research data.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System and user level passwords should be changed according to the Password Policy.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Users should secure their workstations by logging off or locking them when the host will be unattended.
5. Use encryption of information when appropriate.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised.
7. Postings from a UD email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of UD, unless posting is in the course of business duties.
8. All hosts that are connected to the UD Internet/Intranet, whether owned by the individual or UD, should be continually executing approved virus-scanning software with a current virus database.
9. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses and/or other malware

**Unacceptable Use -**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UD-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

**System and Network Activities**

The following activities are strictly prohibited, with no exceptions

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UD.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted

music, and the installation of any copyrighted software for which UD or the end user does not have an active license is strictly prohibited.

3. Downloading and/or installing any type of software not related to job functions or not authorized by the IT Department.
4. Connecting network devices such as wireless access points or personal laptops into the UD network environment without proper authorization from the IT Department.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a UD computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any UD account.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless authorized by the IT Department.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
16. Providing information about, or lists of, UD employees or Students to parties outside UD except in the performance of authorized duties.

| | |
|---|---|
| | **Email and Communications Activities**<br>1. Sending, forwarding or requesting email with any type of confidential data such as credit card data. Any exceptions must be approved by the IT Department.<br>2. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).<br>3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.<br>4. Unauthorized use, or forging, of email header information.<br>5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.<br>6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.<br>7. Use of unsolicited email originating from within UD's networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by UD or connected via UD's network.<br>8. Sending or forwarding email that is likely to contain computer viruses.<br><br>**Enforcement -**<br>Any user found to have violated this policy may be subject to disciplinary actions, up to and including termination of employment for employees, or expulsion for students. |
| **Principal Owners:** | Director of IT, Director of IT User Support Services |
| **Procedures:** | |
| **Keywords:** | IT, Information Technology, Computer, Security, Acceptable, Prohibited |
| **History:** | Modified: 7/8/2019 |