Social Engineering Education Policy

Version 2

02/24/2020
1. Overview

1.1. The Social Engineering Education Policy for the University of Dallas states that all staff members of the University of Dallas must defend the integrity and confidentiality of the university's resources.

2. Purpose

2.1. This policy raises awareness among the staff of the university that social engineering attacks targeting the university are a legitimate threat to university resources.
2.2. This policy further informs staff members of the guise of social engineering attacks is varied and can include a variety of mediums, from email messages to in-person encounters.

3. Scope

3.1. The scope for this policy includes all constituents of the University of Dallas, including staff, faculty, and students.

4. Policy

4.1. University staff members will make a good faith effort to avoid the trap of social engineering. They will protect all information owned by or entrusted to the university, including information regulated by law and sensitive personal information regarding the university and its constituents.
4.2. University staff members will diligently attend and listen to any training on social engineering that they are directed to attend by university administration or previously authorized third parties.
4.3. University staff members will note warning signs for social engineering attacks and report them to UD Technical Support by emailing support@udallas.edu. Examples of these warning signs include the following by unauthorized individuals:
   4.3.1. Any reference to a higher authority figure without documentation and confirmation from that authority figure;
   4.3.2. Any claims of urgency or emergency without contextual support;
4.3.3. Any requests for unauthorized, undocumented releases of information, particularly of passwords, sensitive personal information, and financial information;

4.3.4. Any communication from unknown individuals via phone, email, text, fax, or in person. Unknown individuals may include unverified reporters or alleged subcontractors of the university;

4.3.5. Any appeals for information made without proper documentation or approval.

5. **Policy Compliance**

5.1. The University administration will assess compliance through various methods, including but not limited to training attendance, internal and external reports, breach monitoring, compliance drills, and feedback. Non-compliance with this policy will be addressed at the discretion of the University administration, including up to termination based on the severity of the violation.

6. **Related Standards, Policies and Processes**

   *General Acceptable Use Policy*

7. **Definitions and Terms**

   Definitions of terms used in this policy can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

8. **References**

9. Revision History

<table>
<thead>
<tr>
<th>Date of Revision</th>
<th>Responsible</th>
<th>Summary of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/2/2020</td>
<td>UD Policy Team</td>
<td>Updated and converted to new format.</td>
</tr>
<tr>
<td>2/24/2020</td>
<td>Blake Palmer</td>
<td>Updated phrasing and policy guidelines.</td>
</tr>
</tbody>
</table>