

 <b>UNIVERSITY OF DENVER</b>	<b>UNIVERSITY OF DENVER POLICY MANUAL SECURITY AWARENESS AND TRAINING</b>	
<p><b><u>Responsible Department:</u></b> Information Security Office</p> <p><b><u>Recommended By:</u></b> VC Information Technology, Chief Information Security Officer</p> <p><b><u>Approved By:</u></b> Chancellor</p>	<p><b><u>Policy Number</u></b></p> <p>IT 13.10.015</p>	<p><b><u>Effective Date</u></b></p> <p>1/11/2023</p>

**I. INTRODUCTION**

The goal of the University’s information security awareness program is to educate University faculty, and staff on their roles and responsibilities in protecting the confidentiality, integrity, and availability of information resources.

**II. POLICY OVERVIEW**

The Chief Information Security Officer (CISO) will implement and maintain a robust University information security awareness and training program (“ISATP”) for all University faculty and staff.

**III. PROCESS OVERVIEW**

**A. General Requirements**

1. All University faculty and staff are required to complete annual security awareness training assigned by the University’s Information Security Office.
2. All new users shall complete mandatory security awareness training within thirty (30) days of being granted access to University Information Resources.
3. All University security awareness training shall be tracked and regularly reviewed by the Information Security Office.
4. The CISO will submit annual security awareness training reports to the senior leadership.

5. The University shall provide targeted training based on regulatory requirements (e.g. [HIPAA](#), [FERPA](#), [PCI-DSS](#), [GDPR](#), etc.) as determined by the University's CISO.

**B. Exceptions**

Exceptions to this Policy must be reviewed and approved by the Vice Chancellor for Information Technology.

**C. Violations**

The CISO may take reasonable measures to enforce this Policy, including but not limited to limiting a user's access to Information Resources.

**IV. DEFINITIONS**

- A. **“Information Resources”** means information owned or possessed by the University, or related to the business of the University, regardless of form or location, and the hardware and software resources used to electronically store, process, or transmit that information.

**V. RESOURCES**

- A. University Policy 1.10.080 – *Information Security*
- B. University Policy 2.30.070 – *PCI DSS Compliance*

<b>Revision Effective Date</b>	<b>Purpose</b>
12/___/2022	<i>Align policy with practice</i>