UNIVERSITY *of* DENVER	**UNIVERSITY OF DENVER** **POLICY MANUAL** **IT SECURITY AWARENESS AND TRAINING FOR FACULTY AND STAFF**

<u>Responsible Department</u>: Information Security Office **<u>Recommended By</u>:** VC Information Technology, Chief Information Security Officer **<u>Approved By</u>:** Chancellor	**<u>Policy Number</u>** IT 13.01.015	**<u>Effective Date</u>** 10/27/2021

I. INTRODUCTION

A strong security program requires faculty and staff to be trained on security policies, procedures, and technical security controls.

II. POLICY OVERVIEW

A. It is the policy of the University to implement a viable information security program with a strong awareness and training component.

B. The University’s Chief Information Security Officer (CISO) is responsible for implementing and maintaining an effective security program.

III. PROCESS OVERVIEW

A. The University’s CISO shall be responsible for developing, implementing, and maintaining a Security Awareness and Training Plan (Plan). This Plan shall document the process for faculty and staff security training, education, and awareness and ensure that University faculty and staff understand their role and responsibility in protecting the confidentiality, integrity, and availability of Information Resources.

B. The Plan shall ensure that faculty and staff are provided with regular training, reference materials, and reminders to enable them to appropriately protect University’s Information Resources. Training shall include, but is not limited to:

1. University's responsibilities for protecting Information Resources
2. Risks to Information Resources

3. How to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls
4. The secure use of Information Resources
5. Information security policies, procedures, and best practices

C. The Plan shall ensure:

1. All new users attend an approved security awareness training class prior to, or at least within 30 days of, being granted access to any Information Resources.
2. Faculty and staff receive training appropriate for specific job roles and responsibilities. After such training, each faculty or staff member must verify that he or she received the training, understood the material presented, and agrees to comply with it.
3. Faculty and staff are trained on how to identify, report, and prevent security incidents.
4. Faculty and staff are aware of the most common indicators of an incident.
5. Faculty and staff understand the importance of enabling and utilizing secure authentication.
6. Faculty and staff identify and properly store, transfer, archive, and destroy sensitive information.
7. Security policies, procedures, and manuals are readily available for reference and review by the appropriate faculty and staff.
8. Faculty and staff attend annual security awareness training.
9. Faculty and staff sign an acknowledgement stating they have read and understand University requirements regarding computer and information security policies and procedures.
10. Faculty and staff are provided with sufficient training and supporting reference materials to allow them to properly protect Information Resources.
11. The IT Department prepares and maintains one or more information security web pages that contain information security policies and procedures.
12. Faculty and staff are made aware of the risks and responsibilities related to “bring your own device and technologies” (BYODT).
13. Faculty and staff are made aware of causes of unintentional data exposures, such as losing their mobile devices or e-mailing the wrong person due to autocomplete in e-mail.

D. The CISO shall:

1. Develop and maintain an IT web presence to communicate security program updates, security items of interest, and periodic reminders.
2. Provide training in security best practices to faculty and staff responsible for implementing Information Resources safeguards.
3. Deliver periodic security reminders (flyers or posters, e-mails, verbal updates at meetings) keep faculty and staff up to date on new and emerging threats and security best practices.

IV. DEFINITIONS

None

Revision Effective Date	**Purpose**