# UM Information Security Awareness Training Procedures

## Awareness and Training Campaigns

The UNIVERSITY OF MONTANA requires that each employee upon hire and at least annually thereafter successfully complete the assigned Security Awareness and Training Campaign. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Employees will be given a reasonable amount time to complete each course so as to not disrupt business operations. Generally, employees need to complete their assigned training campaign within one month of the assignment.

Onboarding Campaign assigned individually or as part of a unit

- Security Awareness Proficiency Assessment
- Security Awareness Fundamentals
- Password Security
- Phishing Fundamentals

Refresher Campaign assigned to all employees enrolled in the program in October of each year

- Security Awareness Proficiency Assessment
- TBD

Speciazlized Campaigns

- TBD

## Simulated Social Engineering Exercises

The UNIVERSITY OF MONTANA Information Security Office will conduct periodic simulated social engineering exercises. The UNIVERSITY OF MONTANA Information Security Office will conduct these tests at random throughout the year with no set schedule or frequency. The UNIVERSITY OF MONTANA Information Security Office may conduct targeted exercises against specific units or individuals based on a risk determination.

## Remedial Training Exercises

From time to time UNIVERSITY OF MONTANA employees may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the UNIVERSITY OF MONTANA Information Security Office as part of a risk-based assessment.

## Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all faculty and staff. The UNIVERSITY OF MONTANA Information Security Office will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises.

The Information Security Office is authorized to limit network access for individuals or Units not in compliance with all information security policies and related procedures. In cases where University resources are actively threatened, the Chief Information Security Officer (CISO) should act in the best interest of the University by securing the resources in a manner consistent with the Information Security Incident Response Policy. In an urgent situation requiring immediate action, the CISO is authorized to disconnect affected individuals or Units from the network. In cases of noncompliance with this policy, the University may apply appropriate employee sanctions or administrative actions, in accordance with relevant administrative, academic, and employment policies.

## Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program.

Chief Information Security Officer is accountable for running an effective information security awareness and training program that informs and motivates employees and students to help protect the organization's information assets.

Information Security Office is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other institutional functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Employees are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations at all times.

All Vice Presidents, Deans, Directors, and School/Department Chairs must take appropriate actions to comply with information technology and security policies. These individuals have ultimate responsibility for University resources, for the support and implementation of this policy within their respective Units, and, when requested, for reporting on policy compliance to the Information Security Office. While specific responsibilities and authorities noted herein may be delegated, this overall responsibility may not be delegated.