Information Security Awareness Policy

Policy Information

Policy Number
...
Date Adopted
...
Implementation Date
...
Revision Date
...
Next Review Date
...
Responsible Office
Information Technology

Policy Purpose:
The Information Security Awareness Policy specifies the UNIVERSITY OF MONTANA create and manage the UM Cybersecurity Awareness and Training Program to inform and assess all UM employees regarding their information security obligations.

Policy Statement:
Technical security controls are a vital part of our information security framework but are not in themselves sufficient to secure all information assets. Effective information security also requires the awareness and proactive support of all employees and students, supplementing and making full use of the technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems.

Without adequate information security awareness, UM employees are less likely to recognize or react appropriately to information security threats, and are more likely to place information assets at risk of compromise. In order to protect information assets, all employees must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations.

The policy applies throughout the organization as part of the IT governance framework. It applies regardless of whether employees use computer systems and networks, since all employees are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience.

In general, this program applies to all UNIVERSITY OF MONTANA employees with access to UNIVERSITY OF MONTANA systems, networks, University of Montana information, nonpublic personal information, personally identifiable information.
The policy will be updated and re-issued at least annually to reflect, among other things, changes to applicable law, update or changes to UNIVERSITY OF MONTANA requirements, technology, and the results or findings of any audit.

All awareness training must fulfill the requirements for the security awareness program as listed below:

• The information security awareness program should ensure that all employees achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

• Additional training is appropriate for employees with specific obligations towards information security that are not satisfied by basic security awareness, for example Financial Administrators, Client Experience, Information Security, Systems Administrators/Engineers, and Network/Telecommunications Operations personnel. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements.

• Security awareness and training activities should commence as soon as practicable after employees join the organization, generally through attending information security induction/orientation as part of the on boarding process. The awareness activities should continue on a continuous/rolling basis thereafter in order to maintain a reasonably consistent level of awareness.

• Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.

• The University of Montana will provide employees with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters.

Procedures:

UM Information Security Awareness and Training Program Procedures