Information Security Training and Awareness Policy

Statement of Policy
Washington University in St. Louis (WashU) is committed to conducting all university activities in compliance with all applicable laws, regulations and university policies. WashU has adopted this policy to outline the security measures required to protect electronic information systems and related equipment from unauthorized use.

Objective
The policy and associated guidance provide an organized security awareness and training program that will inform WashU of relevant and recent security topics.

Applicability
This policy is applicable to all WashU systems, networks and campus locations.

Audience
The audience for this policy is all WashU faculty, staff and students. It also applies for all other agents of the university with access to WashU information and network for contracted services. This includes, but not limited to partners, affiliates, contractors, temporary employees, trainees, guests, and volunteers. The titles will be referred collectively hereafter as “WashU community”.

Roles & Responsibilities

Policy
Technical controls alone will not protect the WashU environment from risk. Securing systems and information is a shared responsibility. Training will provide the motivation, tools, and best practices needed at WashU to comply with policies, secure, and classify the information they will access, store, and transmit. Awareness will be a continuous process to reinforce training and inform the WashU community of new requirements and risks.

The Information Security Office (ISO) will provide an Information Security Awareness Program for WashU workforce members and students. Training will be developed to ensure WashU community members receive training on information security policies, requirements, and methods to protect the confidentiality, integrity, and availability of WashU information and resources. Information security training that has been provided by an affiliate or third party for
a contractor or temporary workforce member may meet this training requirement. If there is a status change training requirements will be revisited.

Departments and schools are responsible for ensuring WashU community members have the appropriate level of security training to prepare anyone that may access, receive, transmit, or otherwise use protected (i.e. PHI, PCI, FERPA) or confidential information; that may set up, manage, or maintain systems and workstations which access, receive, transmit, or store protected or confidential information are familiar with the WashU security policies and Area Specific Compliance Offices (ASCOs) policies regarding such policies and procedures.

Information Security Training Process

The ISO will work with Human Resources, departments, and schools to provide information security training:

- Training will be provided during orientation sessions for workforce members and students.
- Training will be classroom-based or web-based.
- Security training records will be maintained in Learn@Work, a central training system, or in department/school systems.
- The ISO will develop general awareness training to re-enforce awareness of security best practices for all computer users.
- The ISO will provide security awareness presentations and training opportunities for technical support and management with elevated permissions and administrative responsibilities.

Training Development

- Third party services may be used by ISO to assist with training and awareness
- Basic training will be provided to individuals prior to any protected information access
- Targeted training and awareness sessions will be developed and presented for users that will need more than the basic understanding of information security based on department, school, industry or regulatory updates.
  - Role based training
    - Those with access to protected information
    - Those with assigned security roles and responsibilities
    - When required by regulation
  - Department, IT, or school specific with special information protection requirements
  - Regulatory specific such as PCI, FERPA, HIPAA, NRC, etc.

Training will consist of, but is not limited to, the following areas:
• Information Security Policies, Standards, Controls, and Guidance
• Confidentiality, integrity, and availability of information
• Security practitioner responsibilities and practices for IT staff and system custodians
• Practical information security safeguards for faculty, staff and students
• User response to suspected security incidents
• Common security threats and vulnerabilities
• Information Security best practices
• Secure use of WashU networks and information systems
• Legal and department/school requirements

Information Security Awareness
• ISO website will be the resource for the WashU community – policy, guidance, how-to information, and training.
• ISO will produce communication – articles, posts, newsletters, and digital images – covering changes in policy, compliance efforts, legal mandates, and best practices.
• Special notices will be issued addressing incidents, known threats, and methods to reduce their risk.
• Digital Signage will be used to target specific awareness areas.

Awareness topics will focus on the application of security best practices outlined by NIST, ISO, CIS, and regulatory agencies.

Policy Compliance
The ISO will measure the compliance to this policy through various methods, including, but not limited to – reports, internal/external audits, and feedback to the policy owner. Exceptions to the policy must be approved by the ISO in advance. Non-compliance will be addressed with management, Area Specific Compliance Office, Human Resources, or the Office of Student Conduct.

Related Policies
None

Reference
NIST 800-53 Rev 4
SP800-50 Building an IT Security Awareness and Training Program
ISO 27000

Policy Review
This policy will be reviewed at a minimum every three years.