

Information Security Awareness and Training Policy

Current Version	Compliance Date	Approved Date
3.1	12/31/2019	1/29/2019

1. Purpose

This policy defines information security awareness and training requirements for users who are granted access to University Information Systems (IS). Information security awareness and training are necessary for users to understand how they should protect the confidentiality, integrity, and availability of IS and data.

2. Policy

All students, residents, faculty, staff, affiliates, volunteers and other persons ("Users") granted access to University IS are required to receive awareness and training on information security matters. Awareness and training will be commensurate with the classification of the IS, level of access granted to the User, and other relevant risk factors.

Minimum Awareness and Training Requirements

All Users must complete an online IT Security Awareness course within thirty (30) days of accessing their University Active Directory account.

All Users granted access to University IS must complete an annual online IT Security Awareness and Training Program defined by Information Security.

Information Security will provide awareness and training content that includes, but is not limited to:

- University Information Security policies, procedures and standards and/or significant revisions to them.
- The secure use of University information systems.
- Significant risks to University information systems and data and/or new threats as they are identified.
- The University's legal and business responsibilities for protecting its information systems and data and/or any significant changes to these responsibilities.
- Security best practices (e.g., how to construct a good password, what a security incident is and how to report a security incident) and/or changes to these practices.
- Security controls in place, any changes to these controls, and/or new controls being implemented.

Key Study Personnel (KSP) involved in human subjects research must complete initial and continuing education as required by the University HRPP SOPs regarding human participant protection training.

Additional security training will generally be required in response to security threats and incidents in compliance with industry standards and regulations where awareness is necessary, and may be required by a supervisor/manager/department head in response to an employee's action/inaction related to Information Security.

During the OUHSC account provisioning process all users must acknowledge they have read and agree to comply with the Acceptable Use of Information Systems Policy.

It is the responsibility of each University department or affiliate organization to define and provide any additional awareness training needs for Users performing a function for the department or organization. This may include, but is not limited to, departmental operating procedures or departmental policies or standards.

Role-Based Awareness and Training Requirements

Information Security will provide role-based training and awareness to students, residents, faculty, staff, affiliates or volunteers with a defined role and responsibility in IT Security Policies that include a minimum frequency of:

- Before authorizing access to an Information System or performing assigned duties, and
- When required by Information System and/or Policy or Standard changes.

Information Security will:

- Document and monitor Information Security training activities including basic security awareness training, and
- Retain individual training records for a minimum of six (6) years.

All University information security policies and procedures must be made readily available for reference and review by all IS Users. Information security policies can be located at <https://it.ouhsc.edu/policies>.

Third Party User Awareness and Training Requirements

Third parties, such as suppliers, contractors, and partners, are required to understand their roles and responsibilities regarding OUHSC Information Security requirements. Depending upon the nature of the third-party relationship, the roles and responsibilities may vary greatly.

If a third party has access to University data, the third-party may be required to have in place a training program that meets the same level of requirements as the OUHSC Information Security training and awareness program.

In the event that a third party that has access to University data does not have an adequate Information Security awareness and training program, OUHSC Information Security may administer its training and awareness program for the third party. Third-parties may be responsible for covering the costs for security awareness content and training provided by OU.

Awareness and Training Content Delivery

Information security awareness and training content may be delivered by means including but not limited to:

- Learning Management System(s) (LMS)
- In-house hosted workshops (group and one-on-one)
- Posters, brochures, electronic bulletin boards
- Informational email messages to users
- Targeted video conference workshops
- College sponsored awareness and safety events

3. Scope

This policy applies to all OUHSC Users.

4. Regulatory References

- OUHSC Office of Human Research Participant Protection SOP 102B
- OUHSC Acceptable Use of Information Systems Policy
- HIPAA 45 CFR 164.
- Payment Card Industry Data Security Standard (PCI DSS)

5. Authorization

This policy is authorized and approved by the OUHSC Dean's Council and Senior Vice President and Provost, and enforced by the IT Chief Information Officer. Internal Audit and other authorized departments of the University may periodically assess Business Unit compliance with this policy and may report violations to the University Administration and Board of Regents.

6. Review Frequency

This policy is scheduled to be reviewed, updated and modified annually, and more often as needed.

7. Revision, Approval and Review

7.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	05/09/2007	OUHSC IT	Baseline Version
2.0	12/18/2015	Randy Moore	Changed scope to "Anyone granted access to University Information Systems" throughout the document. Revised Purpose
3.0	12/22/2016	Randy Moore	Updates for new account management process for AUP
3.0	05/08/2018	April Lee	Added role-based training requirements, third party training requirements, training and awareness content delivery mechanisms.
3.1	01/08/2018	ISRB	Added language about potential costs to third-parties provided training by OUHSC IT. Modified language for key student personnel.

7.2 Approval History

Version	Date	Approved By
1.0	05/09/2007	Deans 'Council
3.1	01/29/2019	OUHSC Information Security Review Board

7.3 Review History

Date	Reviewed By
11/19/2014	OUHSC IT

12/8/2016	OUHSC IT
11/14/2018	OUHSC IT Security Services Director
01/04/2019	OUHSC IT Security Services Director
01/08/2019	OUHSC ISRB