Oklahoma State University Policy and Procedures

INFORMATION SECURITY: SECURITY AWARENESS	3-0605 ADMINISTRATION & FINANCE Information Technology October 2019

PURPOSE

1.01 Oklahoma State University (OSU) is committed to educating the user base on cybersecurity threats having the potential to cause harm to the confidentiality, integrity, and availability of organizational data. This policy outlines expectations for an information security awareness program to be followed by faculty, staff, students, and in certain cases, affiliates.

SCOPE

2.01 This policy applies to all members of the OSU community who have been granted access to University data, whether students, faculty, staff, or affiliates.

DEFINITIONS

3.01 Data – For the purposes of this document, electronic information (e.g. databases, spreadsheets, email, etc.) or non-electronic (e.g., paper files, publications, hardcopy research, etc.). Information or knowledge concerning a particular fact or circumstance, gained via business operations, academic study, communications, research, instruction, or otherwise, within the pursuit of the University's mission.

3.02 Information technology resources – Technology and/or computer resources including, but not limited to, personal computers, workstations, mainframes, mobile devices (laptops, tablets, smart phones, etc.), printing equipment, and all associated peripherals and software, and electronic mail accounts, regardless of whether the resource is used for administration, research, teaching, or other purposes.

3.03 User – For the purposes of this document, a person, whether authorized or not, who makes use of, accesses, creates, or alters University information assets or technology resources from any location.

POLICY

4.01 Information Security Awareness Training – OSU will provide an Information Security Awareness training program covering common information security issues, which is designed to

educate all users within the scope of this policy who access the University's information technology resources.

4.02 Training Mandates – University employees will be required to complete the Information Security Awareness training program within thirty days of their effective start date. University employees will be required to complete this training program at least every three years. Students will be required to complete the Information Security Awareness training program during their first semester.

4.03 Administration Responsibilities for Mandates Compliance – Department heads are responsible for tracking employee participation.

On an annual basis, Information Technology (IT) will notify Human Resources and the Provost's Office with relevant employee and student training statuses.

Human Resources will be responsible for enforcing staff training mandates.

The Provost's Office will be responsible for enforcing student and faculty training mandates.

Training records will be retained for a period of no less than three years.

4.04 Training Content and Facilitation – It is the responsibility of IT to maintain relevant and up-to-date training material according to campus needs.

Campus communications will be used each fall and spring semesters to augment the standardized training.

Departments are not limited to security awareness training extended by IT and are encouraged to augment with training specific to their individual needs.

Regarding employee participation, the Human Resources standard delivery mechanism for employee training will be utilized.

Regarding student participation, the student online course management system will be utilized.

4.05 Non-Compliance – Failure to adhere to the training program as outlined in this policy may result in immediate revocation of privileges to use the University's information technology resources and/or disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, which may include referral for criminal investigation and/or prosecution.

Approved:
Staff Advisory Council, December 2019
Faculty Council, January 2020
Council of Deans, February 2020
E-Team, April 2020
Board of Regents, April 2020