Oklahoma State University Policy and Procedures

INFORMATION SECURITY POLICY	**3-0603** **ADMINISTRATION & FINANCE** **Information Technology** **October 2019**

PURPOSE

1.01 Oklahoma State University (OSU) is committed to protecting the integrity, availability, and confidentiality of sensitive information under University control, complying with legal requirements, and adhering to policies, procedures, standards, and guidelines set by federal and state laws, contractual obligations, the University and Oklahoma A&M System (A&M), or otherwise referenced in this document.

1.02 The purpose of this policy is to recognize OSU's responsibilities in, and establish mechanisms for, securing information electronically transmitted, stored, or processed in pursuit of the institution's mission.

SCOPE

2.01 This policy impacts all employees, staff and faculty of OSU and the Oklahoma A&M System, as well as vendors, contractors, partners, student, collaborators, and any others doing business or research with OSU/A&M.

2.02 This policy applies to certain members of Information Technology, the Oklahoma A&M Chief Information Officer, and identified Technology Coordinators or other personnel tasked with management of University information systems.

DEFINITIONS

3.01 Information Assets – any University-owned, -leased, -protected or otherwise authorized information or data.

3.02 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.

3.03 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.

3.04 Information systems – any resource or equipment used for accessing or for controlling access of information assets.

3.05 User – For the purposes of this document, a person, 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 Policies
Information Technology (IT) will work with users to adhere to applicable policies, procedures, standards, and guidelines associated with securing institutional information, including, but not limited to:

- 3-0601 Appropriate Use Policy
- 3-0604 Information & Resources: Access Control Policy
- 3-0605 Information Security: Security Awareness

4.02 Information Security Committee
Information Technology will establish and maintain an Information Security Committee (Committee) to address information security, compliance, and governance needs.

Committee Membership

Given the distributed nature of the University's technology services, the Committee will be comprised of, but not limited to, the following personnel:

- Chief Information Officer – Oklahoma State University
- Chief Information Officer – Agriculture and Mechanical Colleges
- Information Security Officer and Director of IT Security
- IT Manager designated for IT Governance, Risk and Compliance
- Technology Coordinators from each of the following OSU campuses or functional areas:
    - OSU-Center for Health Sciences (OSU-CHS)
    - OSU-Institute of Technology (OSUIT)
    - OSU-Oklahoma City (OSU-OKC)
    - Financial Information Management
    - Human Resources Information Management
    - Institutional Research and Information Management
    - Enrollment and Brand Management
    - Office of the Registrar
    - The Honors College
    - College of Arts and Sciences

    - College of Engineering, Architecture and Technology
    - College of Education and Human Sciences
    - College of Veterinary Medicine
    - Division of Agricultural Sciences and Natural Resources
    - Graduate College
    - Edmon Low Library
    - OSU Research
    - Spears School of Business
- OSU-Tulsa Administration Representative
- Additional members as required depending on the topic

Committee Operations

The Committee will meet each fall and spring semesters, or as needed depending on identified needs.

The Chief Information Officer – OSU will be responsible for scheduling and recording Committee meetings.

The Information Security Committee's responsibilities include:

- developing policies, general operational procedures, systems configuration or technological process standards, and other IT governance and administrative guidance as needs are identified within Committee discussions and activities.
- providing guidance to Committee members or the University regarding enforcement of information security policies.
- as needed or required, in the event of a compromise of information security assisting with and following applicable and appropriate procedures toward recovering information, mitigating losses, restoring and ensuring data security, and restoring technological services and business operations.

Duties of individual members of the Committee include:

- reporting to the Committee information security, compliance/regulatory, or governance needs for their campus/area

- communicating to students, faculty, staff, or authorized third-parties of policies set by the Committee.

- reporting to the Committee a need for or actions (which have been or are to be) taken regarding enforcement of information security policies.

4.03 Non-Compliance

Failure to adhere to the security measures referenced in this policy could result in hindered University operations, impaired organizational business, irreparable damage to institutional resources, persons associated with the institution and the community, and/or fines or other government sanctions.

In the event of non-compliance by individuals within the scope of this policy, the University may apply disciplinary procedures including, but not limited to, immediate revocation of user privileges to University information technology resources, revocation of access, required re-training on data security, notification of supervisors, loss of funding, lawsuits, suspension, and possible termination of employment. Further, violations of this policy may result in disciplinary actions 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