7.5.16 Safeguarding Data

A. Purpose

The purpose of this Policy is to enhance approaches to cybersecurity consistent with our obligations as a state agency, to protect our patients, our business, our intellectual property assets and our ability to fulfill our mission, as required by UTS 165: Information Resources Use and Security Policy.

B. Persons Affected

This Policy applies to all individuals associated with or on the premises of the University, including without limitation Employees, faculty, students, patients, visitors, volunteers, contractors, or vendors.

C. Definitions

1. **Offshore data storage:** Hosting data in a location outside the physical borders of the United States.
2. **Servers:** A high-performance computer equipped with more memory, faster processors, and sometimes GPUs, to handle advanced computing needs such as storing larger-than-usual data sets, running complex applications, and/or allowing multiple users to connect and use its resources.Servers can be dedicated to a single task, multiple applications, or a specific client. Information Technology reserves final decision on what is considered a server.

D. Policy

D.1. Networks

1. **Secure network.**
    a. **University owned.** Only University-owned computers and IT-managed mobile devices will be permitted on the secure (internal) IT network.
    b. **Exceptions.** Any exceptions to devices allowed on the internal network must be approved by ISO.

2. **Guest network.** All non-University owned devices should use the guest network.

D.2. Networks

1. **University business on University devices.** All University business, including all research and IP-related work, must be conducted on University asset tagged and encrypted devices, IT-managed mobile devices, or University-managed applications.
2. **Ports may be disabled.** Ports on all University-owned computers, laptops and other equipment that connect storage devices (USB and external drives) to the network are a risk to the University. These risks will be evaluated and as a result, the use/availability of these ports and USB-enabled storage devices may be disabled.
3. **OneDrive.** OneDrive, an institutionally approved cloud-based storage solution, is available to all Employees.

D.3. International Travel

Information Technology-related international travel for the HSC campus and the Main campus varies slightly.

1. **HSC campus Employees:**
   a. **No assigned devices.** Employees traveling internationally will **NOT** be allowed to take their individually assigned University devices.
   b. **Loaned devices only.**
      i. **Before travel.** Employees must request and obtain loaned devices from the IT department before international travel to a restricted country.
      ii. **Upon return.** Upon return from international travel:
         i. Employees must **NOT** connect the loaned devices to the network; and

            ii. IT must be contacted immediately to collect and wipe the device(s).

    c. **Travel on personal time.** Devices must be requested if an Employee is travelling internationally on personal time and they plan to connect to University resources, e.g., network, email, Office365, SharePoint.

2. **Main campus Employees:**
    a. **Restriction on assigned devices.** Employees traveling internationally will **NOT** be allowed to take their individually assigned University devices to countries on the restricted country list **ONLY**. When travelling internationally to countries not found on the restricted country list, Employees are permitted to take their University-issued device.
    b. **Loaned devices only.**
        i. **Before travel.** Employees must request and obtain loaned devices from the IT department before international travel to a country on the restricted country list.
        ii. **Upon return.** Upon return from international travel:
            i. Employees must **NOT** connect the loaned devices to the network; and
            ii. IT must be contacted immediately to collect and wipe the device(s).
    c. **Travel on personal time.** Devices must be requested if an Employee is travelling internationally on personal time to a country on the restricted country list and they plan to connect to University resources (e.g., network, email, Office365, SharePoint). When travelling internationally to countries not found on the restricted country list, Employees are permitted to take their university issued device.

D.4. Data Storage Location

1. **Background.** Due to varying guidelines, local and international laws and regulations, offshore storage options may pose security risks compared to data

stored within the United States (U.S.). When data is stored offshore, it becomes more vulnerable to security incidents and there is an increased risk that it could be subject to the sovereign control of another country.

2. **Offshore storage prohibited.** All University data must remain within the boundaries of the U.S. and Employees shall follow the following guidelines:
    a. **U.S. vendors only.** University data should be hosted, stored, processed, transmitted, accessed, and disposed of only by approved vendors within the U.S.

    b. **No access outside U.S.** University data should not be accessible from outside the physical boundaries of the U.S., and students and Employees located outside of the physical U.S. territory should make prior arrangements with IT to gain access.

    c. **Exemptions.** Any requests for exemption from this Policy must be coordinated through the Chief Information Security Officer.

3. **Location of University servers.**
    a. **Physical location.** All server resources must be physically housed in the University's datacenter under the management of central IT.

    b. **Virtual server.** When possible, servers should be installed in the University's virtual server environment as opposed to acquiring additional physical hardware.

    c. **Dedicated hardware.** If dedicated server/hardware is required, the requestor must consult with IT before procurement.

    d. **Documentation.** Server documentation should include details such as backup procedures, elevated-privileged accounts, life-cycle replacement plans, and disaster recovery plans.

    e. **Exemption.** Any requests for exemption from this policy must be coordinated through the Chief Information Officer.

D.5. Penalties for Violations

Violation of this Policy may result in the following disciplinary actions:

1. termination (Employees and temporary Employees);
2. termination of employment relations (contractors or consultants);
3. dismissal (interns and volunteers);
4. suspension or expulsion (students); and
5. loss of University Information Resources access privileges, civil, and criminal prosecution (all persons).

E. Reference Sources and Authority

- Tex. Gov. Code, Title 10, Subchapter N-1: Cybersecurity
- UTS 165: Information Resources Use and Security Policy

F. Review Responsibilities and Dates

The Division Head for this Policy is the Chief Information Security Officer, and this Policy shall be reviewed every two (2) years or sooner, if necessary, by the Division Head or their designee.

APPROVED: 12/2021
AMENDED: 09/2023
AMENDED: 04/19/2024