Technologies Prohibited by Regulation Policy

Purpose: The purpose of this policy is to define information security controls around systems, services, and technologies prohibited by regulation.

Scope: This policy applies to the Texas State University System (TSUS) and its component institutions. All users are responsible for understanding and observing these and all other applicable policies, regulations, and laws in connection with their use of the institution's information resources.

Application: The statements in this document establish the minimum requirements for each component institution. At the discretion of the component institution, more stringent, restrictive, or enhanced requirements may be established.

Management: This policy is managed by the TSUS Information Security Council and will be reviewed at minimum every five years, or more frequently as needed, by the chief information security officer and appropriate component institution information security officers.

Exceptions: Unlike certain security controls, policies, standards, and other requirements of TSUS components, the regulatory nature of the prohibitions described by this policy significantly limit or prevent exceptions from being granted by a component institution's information security officer, individual department heads, or other Personnel. Exception requirements for Prohibited Technologies are addressed in section 9 of this policy.

POLICY/PROCEDURE

1. Policy Statements

1.1 Prohibited Technologies controls implemented by component institutions must comply with applicable federal or state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

2. Definitions

2.1 Texas State University System defines technical policy terms in the information technology glossary.

2.2 DIR: Initialism for the Texas Department of Information Resources.

2.3 DPS: Initialism for the Texas Department of Public Safety.

2.4 Mobile Device: A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); and is powered on for extended periods of time with a self-contained power source. Mobile Devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or

determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include laptops, smart phones, tablets, smart watches, and e-readers.

2.5 Personnel: Employees or contractors of the TSUS or its components.

2.6 Prohibited Technologies: Any technologies prohibited by section 8 of this policy, including, but not limited to, certain software, hardware, companies, telecommunications devices, and equipment.

2.7 Sensitive Location: Any physical or logical (such as video conferencing or electronic meetings) location designated by the TSUS or a component institution that is routinely used by Personnel to discuss confidential or sensitive information, including information technology configurations, criminal justice information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

2.8 State Business: Employees or contractors accessing component-owned information resources including, but not limited to, data, information systems, email accounts, non-public facing communications, telecommunication systems, and video conferencing.

2.9 Unauthorized Devices: Devices not owned by the TSUS, its component institutions, or another state agency of Texas, including, but not limited to, personally owned Mobile Devices.

2.10 Visitor: A person who is not Personnel.

3. Procedures

Authority - Texas State University System (TSUS)

3.1 Component institutions must:

3.1.1 Develop procedures to facilitate the implementation of the Prohibited Technologies policy and associated controls;

3.1.2 Review and update Prohibited Technologies procedures at an institution-defined frequency; and

3.1.3 Designate an institution-defined individual as responsible for managing, developing, documenting, and disseminating institutional Prohibited Technologies procedures related to the controls in this policy.

4. Component-owned Devices

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Objective 1

4.1 Except where approved exceptions apply, the use or download of Prohibited Technologies are prohibited on all TSUS- or TSUS component-owned devices, including Mobile Devices, desktop computers, and other internet capable devices.

4.2 Component institutions must:

4.2.1 Identify, track, and control component-owned devices;

4.2.2 Implement the following controls on Mobile Devices to:

4.2.2.1 Restrict access to app stores or non-authorized software repositories to prevent the installation of Prohibited Technologies;

4.2.2.2 Maintain the ability to remotely wipe non-compliant or compromised Mobile Devices;

4.2.2.3 Maintain the ability to remotely uninstall Prohibited Technologies from Mobile Devices; and

4.2.2.4 Deploy secure baseline configurations for Mobile Devices.

4.2.3 Detect and remove Prohibited Technologies from component-owned devices unless an exception has been granted.

5. Personal Devices Used for State Business

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Objective 2

5.1 Employees and contractors shall not install or operate Prohibited Technologies on any personal device used to conduct State Business.

6. Identification of Sensitive Locations, Meetings, and Personnel

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Objective 3

6.1 Component institutions must:

6.1.1 Authorize an individual or role to designate Sensitive Locations and periodically review designations of Sensitive Locations;

6.1.2 Designate Sensitive Locations by identifying, cataloging, and labeling locations meeting the criteria prescribed by this policy;

6.1.3 Indicate when someone is entering a Sensitive Location using conspicuous and permanently affixed exterior signage for physical locations, labeling electronic meetings, or other institution-defined means of notification;

6.1.4 Not permit Unauthorized Devices to enter Sensitive Locations;

6.1.4.1 Devices excepted from this requirement are personal medical devices prescribed or authorized by a physician and medically necessary.

6.1.5 Subject Visitors granted access to Sensitive Locations to the same limitations on Unauthorized Devices as contractors and employees when entering secure locations.

6.1.5.1 Excepted from this requirement are meetings between Personnel and Visitors when the Visitor is the owner or subject of the sensitive or confidential information (e.g., a student speaking with their professor or guidance counselor).

6.2 Due to the nature of component institutions' communications and practices, as well as the various environments in which students interact with higher education Personnel, the potential exists for sensitive or confidential information to be disclosed incidentally in locations not designated as sensitive. This policy is not intended to impede higher education's customary and essential communications and practices and thus does not require that all risk of incidental use or disclosure be eliminated to satisfy this policy requirement. Rather, this policy permits certain incidental uses and disclosures of sensitive or confidential information to occur outside of designated Sensitive Locations when the component institution has in place reasonable safeguards and minimum necessary policies and procedures to protect sensitive and confidential information.

7. Network Restrictions

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Objective 4

7.1 Component institutions must:

7.1.1 Configure perimeter security systems to restrict access to Prohibited Technologies (e.g., network or endpoint firewalls, intrusion prevention systems).

7.1.2 Place Devices with authorized exceptions in physically or logically separate networks intended exclusively for access to Prohibited Technologies.

7.2 Personal devices with Prohibited Technologies are prohibited from connecting to component networks.

8. Prohibited Technologies

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Objective 5

8.1 Component institutions must:

8.1.1 Implement the removal and prohibition of any Prohibited Technologies included on:

8.1.1.1 The Department of Information Resources' Prohibited Technologies List.

8.1.2 Not use, acquire, or reimburse the purchase of any Prohibited Technologies.

9. Exceptions

Authority - DIR/DPS Model Security Plan for Prohibited Technologies, Exceptions

9.1 Exceptions to this policy may only be approved by each component institution's agency head to enable law-enforcement investigations and other legitimate business uses. This authority may not be delegated.

9.2 All approved exceptions of Prohibited Technologies on DIR's Prohibited Technologies List must be reported to DIR.

9.3 Devices granted an exception must be exclusively used for the purposes of accessing Prohibited Technologies.

10. Issuance of Institutional Standards

Authority - TSUS

10.1 Component institutions must develop and maintain one or more institution-level standards with regard to the technologies prohibited by regulation covered by this policy. The standard(s) must include the following items to a non-confidential level of detail:

10.1.1 Reference to the regulation(s) prohibiting subject technologies;

10.1.2 A summary of technical controls used to enforce the implementation of this policy;

10.1.3 A summary of administrative controls used to enforce the prohibition requirements of this policy;

10.1.4 Measures required to address existing instances of Prohibited Technologies if present within the institution;

10.1.5 A list or summary of authorized exceptions only if such a list has been determined to not present a risk to the institution's information resources;

10.1.6 The nature of permittable exceptions, such as intended circumstances, required justification, duration, and the process for requesting and facilitating exceptions;

10.1.7 The individual or role authorized to approve exceptions, including whether the exceptions must be approved within the institution or externally; and

10.1.8 The entity or entities to which exceptions must be reported.