

Sam Houston State University
A Member of The Texas State University System

Finance and Operations-FO - 71

Transactions Involving Foreign-Adversary Countries

1. PURPOSE

The purpose of this policy is to detail Sam Houston State University's (SHSU or the University) institutional and employee compliance obligations when interacting with foreign adversaries and to safeguard state information resources and U.S.-developed technologies against intellectual property theft and other uses adverse to U.S. national security by foreign adversary countries or governments. To the extent that any provision of this policy is determined to be inconsistent with the Texas State University System Rules & Regulations, or state or federal law, those authorities shall control.

2. DEFINITIONS

2.01 Foreign-Adversary Nation. A foreign adversary is a country or government on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4. As of the effective date of this policy, foreign adversaries include the People's Republic of China, including the Hong Kong Special Administrative Region (China); the Republic of Cuba (Cuba); the Islamic Republic of Iran (Iran); the Democratic People's Republic of Korea (North Korea); the Russian Federation (Russia); and Venezuelan politician Nicolás Maduro (Maduro Regime).

2.02 Employee Applicability. This policy is applicable to University faculty and staff personnel.

2.03 Critical Infrastructure. Critical infrastructure means a communication infrastructure system, cybersecurity system, electric grid, hazardous waste treatment system, or water treatment facility.

2.04 Critical Infrastructure Employee. A critical infrastructure employee is University personnel, or similarly situated state contractors, who research, work on, or have access to University critical infrastructure which may include information technology, cybersecurity, and working on an electric grid. The designation as a critical infrastructure employee will be included in an employee's job classification description.

3. CONTRACTS

3.01 The University Procurement Department shall require any company that submits a bid or proposal to provide a contract for goods or services to certify that the company, and any of its holding companies or subsidiaries are not

- (a) Listed in Section 889 of the 2019 National Defense Authorization Act (NDAA);
- (b) Listed in Section 1260H of the 2021 NDAA;
- (c) Owned by the government of a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4; or
- (d) Controlled by any governing or regulatory body located in a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4.

3.02 The University may not enter into a new contract, contract extension, or contract renewal for goods or services with any company that meets the criteria in 3.01(a)-(d) above.

Sam Houston State University
A Member of The Texas State University System

4. PROHIBITION AND REPORTING OF GIFTS AND TRAVEL

4.01 Gifts.

- (a) No employee shall accept any gift, regardless of the value, from a country on the U.S. Department of Commerce's foreign adversaries list. Gifts include, but are not limited to, grants or funds provided for research or travel. Doing so violates an employee's ethical obligations to the State of Texas (see also HR-01, [Conflicts of Interest Policy](#)). Any employee approached with an offer of a gift, to include travel, or other suspected violation of this policy from a group or individual representing a foreign adversary must report such interaction to the SHSU Compliance Officer. The Compliance Officer shall maintain a record of the date of contact, name of the approaching individual or group, and employee contacted for a period aligning with SHSU's [Record Retention Schedule](#).
- (b) The University shall submit foreign gift and contract disclosure as required by the U.S. Department of Education (DOE). When such is reported to the DOE, the University will also submit a report of foreign gifts and contracts to the Texas Higher Education Coordinating Board.

4.02 Professional Travel. No employee shall travel for professional purposes to a country on the U.S. Department of Commerce's foreign adversaries list.

4.03 Personal Travel. Employees planning personal travel to foreign-adversary nations must submit a Foreign Travel Disclosure Form to the University Travel Office and the SHSU Compliance Officer not later than thirty days prior to their departure. Within three (3) business days of submission of the required form, the SHSU Compliance Officer will notify the traveling employee of the requirement to complete and submit the return portion of the Foreign Travel Disclosure form to the SHSU Compliance Officer within ten (10) days of returning from travel. The Compliance Officer shall maintain a record of personal travel brief for a period aligning with SHSU's [Record Retention Schedule](#).

- (a) Employees may not bring university-issued devices, non-public university information in any form, or personal devices containing university information, including devices containing passwords or access to university information resources, to a foreign adversary country. Further, any employee sending, shipping, or traveling with university electronic devices, research, or other export controlled items must comply with the SHSU [Export Control Policy](#) and all U.S. Export Control laws.

- (b) Employees may not log into or access any SHSU information resources while traveling in a foreign adversary country.

- (c) Employees may not provide access to non-public university information, including research conducted at or sponsored by SHSU or other U.S.-based entities, to any person or entity while traveling in a foreign adversary country.

- (d) Employees must immediately report to the SHSU Compliance officer any intentional or inadvertent disclosure of non-public university information or sensitive or proprietary technologies associated with the employee's work for SHSU, to a person or entity associated with a foreign adversary country or government.

Sam Houston State University
A Member of The Texas State University System

5. REQUIREMENTS OF CRITICAL INFRASTRUCTURE EMPLOYEES

- 5.01 The job classification descriptions for and any posting of a critical infrastructure position must include the critical infrastructure designation and a statement that the position requires the employee to have the ability to maintain the security and integrity of the infrastructure.
- 5.02 Critical Infrastructure Employees are required to undergo a periodic review of their criminal history and foreign adversary connections as required and conducted by the Texas Department of Public Services (DPS) or a third-party organization approved by DPS.

6. FOREIGN RECRUITMENT PROGRAMS

Employees are prohibited from participating in foreign recruitment programs sponsored or otherwise facilitated by a foreign-adversary country. An example of such recruitment would be the PRC's Thousand Talents Program.

7. CERTIFICATION

The Compliance Officer shall prepare a response for the University certifying compliance with this policy as required by the Texas Governor's Executive Order No. GA-48.

Approved by: President's Cabinet
Date: March 25, 2025

Reviewed by: Amanda Withers, Chief Financial Officer and Senior Vice President for Operations
Date: March 25, 2025