SUL ROSS STATE UNIVERSITY

MEMBER THE TEXAS STATE UNIVERSITY SYSTEM™

SRSU Policy: Transactions Involving Foreign Adversary Countries
SRSU Policy ID: APM 2.37
Policy Reviewed by: Executive Cabinet
Approval Authority: VP of Finance and Operations
Approval Date: June 13, 2025
Next Review Date: June 13, 2030

I. PURPOSE

A. The purpose of this policy is to detail Sul Ross State University's (SRSU 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.

II. SCOPE

A. This policy applies to all Sul Ross University employees.

III. DEFINITIONS

A. **Foreign Adversary.** 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).

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

C. **Critical Infrastructure Employee.** A critical infrastructure employee is University personnel, or similarly situated contractors, who research, work on, or have access to critical infrastructure as part of their work for Sul Ross University.

IV. CRITICAL INFRASTRUCTURE EMPLOYEES AND CONTRACTORS

A. The ability to maintain the security or integrity of critical infrastructure is an essential job function for employees and similarly situated contractors who research, work on, or access critical infrastructure as part of their work for Sul Ross University.

B. Administrative staff who meet the definition of a critical infrastructure employee will have this designation reflected in their job description.

C. Faculty and research staff, including student employees, who meet the definition of a critical infrastructure employee must disclose their critical infrastructure activities to Sul Ross University's Office of Research and Sponsored Programs Administration (ORSPA) upon initiation of the research or activity involving critical infrastructure and at least annually thereafter.

D. Critical infrastructure applicants, employees, or third-party contractors for such positions are subject to routine reviews to determine whether associations with foreign adversary governments, criminal history, or other conflicts of interest may compromise their ability to maintain the security or integrity of the critical infrastructure.

V. PROHIBITION ON GIFTS, CONTRACTS, AND PARTICIPATION IN FOREIGN TALENT RECRUITMENT PROGRAMS

A. Sul Ross University employees are prohibited from accepting any gift, regardless of value, from an entity associated with a foreign adversary country or government. Gifts include, but are not limited to, grants or funds provided for research or travel.

B. No Sul Ross University employee may enter into a contract, contract extension, or contract renewal for goods or services on behalf of the University with a person or entity
   a. Listed in Section 889 of the 2019 National Defense Authorization Act (NDAA); or
   b. Listed in Section 1260H of the 2021 NDAA; or
   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.

   Note. Any exception to this prohibition must be authorized by Sul Ross University's Chief Financial Officer (CFO) consistent with the exceptions set forth in Executive Order GA-48 (Nov. 19, 2024).

C. Sul Ross University employees are prohibited from taking part in talent recruitment programs sponsored by a foreign adversary country as defined by Section III, Paragraph A of this policy.

D. Any person may report being approached by groups representing foreign adversary countries or governments that offer gifts or travel or a suspected violation of this policy by a Sul Ross University employee to the Office of the University President.

VI. PROHIBITION ON PROFESSIONAL TRAVEL TO FOREIGN ADVERSARY COUNTRIES

A. Sul Ross University employees are prohibited from traveling to foreign adversary countries for professional purposes.

VII. PERSONAL TRAVEL TO FOREIGN ADVERSARY COUNTRIES

A. Employees traveling to foreign adversary countries for personal reasons must submit a Foreign Travel Disclosure Form to Sul Ross University's Travel Office at least ten (10) days prior to their departure.

B. Employees returning from travel to a foreign adversary country must complete the return portion of the Foreign Travel Disclosure Form within ten (10) days of returning to work.

C. Employees may not take 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.

D. Employees may not log into or access any Sul Ross University information resources while traveling in a foreign adversary country.

E. Employees may not provide access to non-public University information, including research conducted at or sponsored by Sul Ross University or other U.S.-based entities, to any person or entity while traveling in a foreign adversary country.

F. Employees must immediately report to Sul Ross University any intentional or inadvertent disclosure of non-public University information or sensitive or proprietary technologies associated with the employee's work for Sul Ross University, to a person or entity associated with a foreign adversary country or government.