Ranger College Research Security Program/Procedures Plan

Introduction

In accordance with Ranger College Policy CU(LOCAL), which mandates the development and maintenance of a comprehensive research security program, this Research Security Procedures Plan provides the official framework for protecting the College District's research activities. Ranger College (RC) is committed to fostering an open and collaborative environment for research and workforce development while ensuring the integrity, compliance, and security of all research-related efforts.

These procedures establish clear roles, responsibilities, and processes for faculty, staff, and administrators engaged in research, grant management, international collaborations, ***travel outside the United States****, and the handling of sensitive or controlled information. The plan ensures institutional compliance with applicable federal and state laws—including requirements under NSPM-33 and the CHIPS Act—while supporting ethical research and data stewardship.*

All RC personnel involved in externally funded projects or international collaborations are required to follow these procedures to mitigate risk, safeguard against foreign interference or data breaches, and maintain eligibility for federal funding.

---

1. Research Security Risk Assessment Procedures

Purpose

To evaluate and mitigate security risks associated with research projects, collaborations, grants, and international partnerships.

Procedure

- **Initial Review:** All proposed research projects, grants, and collaborations (especially those with international components) will be reviewed by the **Research Security Officer (RSO)** prior to approval.
- **Risk Factors Considered:**
    - Data Sensitivity (personal data, intellectual property, export-controlled information)
    - Foreign Involvement (partners, funders, collaborators from foreign entities)
    - National Security Implications
    - Funding Source (domestic, international, governmental, private sector)
- **Risk Classification:** Projects will be classified as **Low, Moderate, or High Risk** based on:
    - Country of collaboration (extra scrutiny on **Countries of Concern**)
    - Technology sector (AI, biotechnology, semiconductors, etc.)
    - Data security requirements
- **Mitigation Plans:** For moderate and high-risk projects, the RSO will work with faculty, IT, and administrators to develop tailored mitigation plans.

In accordance with state law and **TASB policy CS(Local)** Information Security, at least every two years, Ranger College shall submit the results of its information security assessment to **DIR** and, if requested, to the office of the governor, lieutenant governor, and speaker of the house of representatives. This information security assessment is completed by the **RC IT Department**.

The **Texas Risk and Authorization Management Program (TX-RAMP)** provides a standardized approach for security assessment, certification, and continuous monitoring of cloud computing services that process the data of Texas state agencies. An institution of higher education contracting for cloud computing services that store, process, or transmit data of the institution of higher education shall:

- Confirm that vendors contracting with the institution to provide cloud computing services are **certified through TX-RAMP** prior to entering or renewing a cloud computing services contract.
- Require vendors to maintain **TX-RAMP compliance and certification** throughout the term of the contract.

Ranger College complies with the **Gramm-Leach-Bliley Act (GLBA)**, which requires institutions handling student financial aid data to implement safeguards to protect **nonpublic personal information (NPI)**. While GLBA focuses on financial data, its principles of risk assessment, data protection, vendor oversight, and incident response align closely with the College's broader research security and data governance efforts. The **Research Security Officer (RSO)** and **IT Department** work together to ensure that research projects involving sensitive data or third-party service providers meet both GLBA Safeguards Rule requirements and state-level security standards, including **TX-RAMP** for cloud services.

---

2. Research Security Training Procedures

Purpose

To ensure faculty, staff, and student researchers understand research security risks and their compliance responsibilities.

Procedure

- **Training Requirement:** All new research-involved personnel must complete **Research Security Awareness Training** within 30 days of assignment.
- **Ongoing Training:** Annual cybersecurity training is required for all personnel.
- **Training Topics:**
  - Foreign influence and improper data requests
  - Handling sensitive data
  - Export control basics
  - Disclosure and reporting obligations
- **Documentation:** All training completions will be recorded and maintained by the IT Department.

---

3. Foreign Collaboration and Funding Disclosure Procedures

Purpose

To ensure compliance with **NSPM-33** and the **CHIPS Act** regarding foreign funding and collaborations.

Procedure

- **Pre-Project Disclosure:** Faculty and staff must complete a **Foreign Collaboration & Funding Disclosure Form** prior to submitting research proposals, accepting external funding, or establishing foreign collaborations.
- **Annual Updates:** Faculty and staff must annually update their disclosures, including:
    - Foreign research appointments or affiliations
    - Participation in foreign talent recruitment programs
    - Foreign gifts or funding exceeding $50,000 from **Countries of Concern**
- **Agreement Review:** All research-related **MOUs with foreign entities** must be reviewed and approved by the RSO.

---

4. Handling Controlled Unclassified Information (CUI) and Export-Controlled Data

Purpose

To ensure proper protection and handling of **research data** subject to export controls and federal classification laws.

Procedure

- **Identification:** The RSO will review projects to determine whether they involve **Controlled Unclassified Information (CUI)** or export-controlled data (**ITAR/EAR**).
- **Access:** Only authorized personnel with necessary training and need-to-know approval may access CUI or export-controlled data.
- **Secure Storage:** Such data must be stored in **designated secure systems** approved by the **IT Department**.
- **Export Screening:** Prior to sharing data with foreign persons, the RSO and IT will conduct **export control screening**.

---

5. International Travel with Research Devices and Data

Purpose

To protect institutional data during international travel and ensure compliance with export control laws.

Procedure

- **Pre-Approval:** Faculty and staff must obtain **RSO/IT approval** before traveling internationally with:
    - College-owned devices
    - Research data
    - Export-controlled materials
- **Device Preparation:** Loaner laptops with only essential data will be provided where possible.
- **Post-Travel Review:** Upon return, IT will **scan devices for malware**, and faculty must update **foreign collaboration disclosures** if new contacts were made.

---

6. Incident Reporting and Response Procedures

Purpose

To ensure timely identification, reporting, and response to research security incidents.

Procedure

- **Reportable Incidents:**
  - Unauthorized data access
  - Suspicious foreign requests
  - Unreported foreign affiliations
  - Lost/stolen research devices
- **Reporting:** Incidents must be reported to the **IT Department** within 24 hours.
- **Response:** The IT Department will **investigate, coordinate with leadership, and implement corrective actions**.

---

7. Annual Program Review and Update Procedures

Purpose

To ensure the **Research Security Program Plan** remains current and effective.

Procedure

- **Annual Review:** The RSO will conduct an annual review to assess:
  - Training effectiveness
  - Regulatory changes
  - Lessons learned from incidents
- **Revisions:** Updated procedures will be submitted to the **President and Board of Regents** for review.

---

8. Executive Oversight and Leadership Engagement

The RSO will brief the **President and Cabinet** at least annually on **research security risks, incidents, and program updates**.

College leadership will actively endorse and communicate the importance of research security throughout the institution.

---

9. Foreign Talent Recruitment Program Disclosure

Faculty and staff must disclose participation in any **foreign talent recruitment programs** during the annual **foreign collaboration and funding disclosure process**.

Participation in certain programs from **Countries of Concern** may trigger further review.

---

10. Extension to Workforce Development Programs

These research security procedures apply to **workforce development programs** involving **critical technologies, sensitive data, or federally funded equipment**.

This includes programs in **cybersecurity, advanced manufacturing, artificial intelligence, biotechnology, and semiconductors**.

---

11. Use of Data Analytics and Emerging Tools

RC's IT Department along with the RSO will explore the use of **data analytics and AI tools** to enhance **research security screening, risk identification, and monitoring** of institutional collaborations.

---

12. Guiding Principle: Balancing Openness with Security
Ranger College is committed to fostering **open, collaborative research and educational partnerships** while protecting **sensitive data** and ensuring compliance with **federal regulations**.
The research security program plan will balance **openness with necessary safeguards**.

In accordance with CU(LOCAL), the RSO will attend the annual Academic Security and Counter Exploitation Program Seminar offered by Texas A&M University to remain current with evolving research security threats and compliance standards.

Contact Information
Debbie Karl
Research Security Officer (RSO)
Vice President of Accreditation and Institutional Effectiveness
Ranger College
Email: dkarl@rangercollege.edu
Phone: 325-829-8255