SOUTH DAKOTA SCHOOL OF MINES & TECHNOLOGY
Policy Manual

SUBJECT: Research Security Program

NUMBER: Policy 9-2

REVISED:

PURPOSE

South Dakota Mines (SDM) recognizes that a strong research security posture is fundamental to protecting its people, discoveries, data and reputation. While SDM currently receives less than $50 million in federal science and engineering awards and is therefore not a "Covered Institution" under the National Security Presidential Memorandum-33 (NSPM-33) certification requirements, SDM still manages sensitive information, interacts with national laboratories, industry and government sponsors. This policy applies to all SDM faculty, staff, students, visiting scholars, and contractors involved in sponsored or unsponsored research. It establishes a Research Security Program that reflects SDM's size and risk while aligning with federal best practices and sponsor expectations.

Policy Statement. Research security involves protecting sensitive information and technologies from unauthorized access, theft or misuse. Sensitive information can include proprietary data, unpublished research results, personally identifiable information of research subjects, export-controlled technology (ITAR/EAR), and Controlled Unclassified Information (CUI) that, if compromised, could harm individuals, the institution or national security. SDM is committed to fundamental and national security research and understands that foreign government interference, intellectual property theft and cyber-enabled espionage pose real threats to university research. Therefore, SDM is implementing a research security program that integrates cybersecurity, foreign travel security, insider threat awareness and identification, export control compliance, and research integrity/ethics training. In developing this program, SDM has taken guidance from the CHIPS and Science Act and NIST's research security framework, which emphasize that even applicants receiving less than $50 million must provide a written research security plan addressing foreign talent programs, conflicts of interest and research integrity.

Program Elements. SDM's Research Security Program is structured around the following elements:

- **Risk Assessment:** SDM's Empowered Official (EO) and Export Control Officer (ECO) works with representatives from information technology (IT), export control, human resources, and facilities. This combined group will conduct periodic risk assessments to identify vulnerable research areas, emerging threats and compliance

obligations, and will maintain Technology Control Plans (TCPs) that details how SDM meets sponsor required information and physical security requirements.

- **Cybersecurity:** Working with the Chief Information Officer (CIO), the ECO will ensure that research information systems meet baseline security standards appropriate to the data they handle. Baselines may include National Institute of Standards and Technology (NIST) frameworks for Controlled Unclassified Information (CUI), multi-factor authentication (MFA), encryption of data at rest and in transit, secure storage of laboratory notebooks and backup procedures. For projects funded by agencies requiring specific cybersecurity standards (e.g., DoD or DOE), systems will meet sponsor-mandated requirements, such as Cybersecurity Maturity Model Certification (CMMC) level II certification.
- **Research Data Management and Physical Security:** The program will establish protocols for classifying research data (e.g., CUI, export-controlled (ITAR/EAR)), controlling access to labs and facilities, protecting technical data and prototypes, and managing laboratory visitors. Principal investigators (PIs) must maintain inventories of sensitive materials and ensure that research data is stored in authorized repositories as detailed in their TCPs.
- **Foreign Travel and Visitor Security:** All personnel traveling abroad on university business, attending international conferences or collaborating with foreign entities must complete foreign travel authorization. The ECO, in conjunction with the PI, must approve any foreign visitors who will access laboratories or information systems and will coordinate with export control to ensure compliance.
- **Export Control and CUI Safeguarding:** The Export Control Officer (ECO) in close collaboration with the Office of Sponsored Programs (OSP) will identify projects subject to export control (ITAR/EAR) and/or CUI controls. Personnel will receive training on export control fundamentals and CUI handling. Training will be documented in the project TCPs.
- **Training and Research Integrity:** Annual research security training will be mandatory for all covered individuals. SDM will track completion and may require refresher courses more frequently for projects with heightened risk.

Responsibilities. The ECO is responsible for program administration, risk assessment, coordination of training and reporting. Deans, department chairs and PIs must ensure compliance within their research projects, participate in training, disclose foreign affiliations and report potential security risks. The IT department will implement cybersecurity controls; the ECO will manage export control compliance; and Human Resources will support insider threat awareness.

Sanctions and Enforcement. Non-compliance with this policy may result in sanctions, including suspension of research activities, loss of research privileges and disciplinary action. Deliberate violations involving unauthorized disclosure of sensitive information or participation in malign foreign talent recruitment programs may result in referral to

federal authorities. The ECO will report significant violations to SDM leadership and in accordance with federal regulations.

Revision History: established January 2026

BOR Policy/Committee References: N/A