



2026

RESEARCH SECURITY REPORT



ARIZONA BOARD OF
REGENTS
ASU ♦ NAU ♦ U of A



ABOUT THIS REPORT

A.R.S. § 15-1626(A)(24) requires the Board, on or before October 1 of each year, to submit a report to the Governor, the President of the Senate and the Speaker of the House of Representatives, with a copy to the Secretary of State, that includes:

1. Information and details on each university's research security policy adopted pursuant to paragraph 23 of this subsection and related practices, protocols and strategies.
2. Information that demonstrates how each university is complying with applicable state and federal laws to promote a safe and secure research environment and to protect national security and intellectual property and to defend against any foreign adversary nation as defined in section 33-443.
3. The total number of grants, gifts, or donations that each university received from a foreign country in the preceding year that exceeded \$250,000.

ABOUT THE ARIZONA BOARD OF REGENTS

The Arizona Board of Regents is committed to ensuring access for qualified residents of Arizona to undergraduate and graduate institutions; promoting the discovery, application, and dissemination of new knowledge; extending the benefits of university activities to Arizona's citizens outside the university; and maximizing the benefits derived from the state's investment in education.

MEMBERS

Doug Goodyear, Chair
Jessica Pacheco, Chair Elect
Gregg Brewster, Secretary
Cecilia Mata, Treasurer
Michele Halyard, M.D.
James McCain
Steve Peru
Lee Stein
Felipe Garcia, Student Regent
Aydin-Kane Vo, Student Regent
Gov. Katie Hobbs, Ex-Officio
Superintendent Tom Horne, Ex-Officio

ABOR EXECUTIVE DIRECTOR

Chad Sampson

October 1, 2026



TABLE OF CONTENTS

4	EXECUTIVE SUMMARY
5	RESEARCH SECURITY POLICIES AND RELATED PRACTICES
13	COMPLIANCE WITH STATE AND FEDERAL LAW
17	FOREIGN GRANTS, GIFTS, DONATIONS AND CONTRACTS
18	<i>APPENDIX A: PUBLISHED RESEARCH SECURITY POLICIES</i>
19	<i>APPENDIX B: SUPPORTING DOCUMENTS</i>
67	<i>APPENDIX C: PUBLISHED RESOURCES</i>

EXECUTIVE SUMMARY

Each university has adopted and posted a research security policy under A.R.S. § 15-1626(A) (23). Each university reports that its policy safeguards research, promotes a security culture, furthers national security interests, mitigates threats from foreign adversary nations, and complies with applicable legal, regulatory, and contractual requirements. Each also reports that its policy supports federal funding eligibility and establishes processes to update the policy and to identify and address compliance concerns.

In practice, each university’s program covers:

- researcher disclosures and conflict review
- cybersecurity
- foreign travel security
- insider threat awareness
- export controls
- research security training
- identification and resolution of compliance concerns
- review of activities involving foreign adversary nations
-

Each university builds these requirements into its research processes and certifies compliance with federal research security requirements when it applies for federal funding.

UNIVERSITY	RESEARCH SECURITY POLICY	EFFECTIVE DATE	FOREIGN GRANTS, GIFTS, DONATIONS AND CONTRACTS EXCEEDING \$250,000, CY 2025
Arizona State University	Research Security Policy (RSP 216)	September 12, 2026	46
Northern Arizona University	Research Security (Interim) Policy	September 11, 2026	4
University of Arizona	Research Security Policy	February 4, 2026	21



RESEARCH SECURITY POLICIES AND RELATED PRACTICES

This section describes each university's research security policy and the practices, protocols, and strategies that support it, as reported by each university.

ARIZONA STATE UNIVERSITY

Policy: ASU's Research Security Policy (RSP 216), effective September 12, 2026, establishes a framework to safeguard ASU's research activities from risks posed by foreign adversarial influence, unauthorized access, theft, and misuse. The policy emphasizes protecting academic freedom while ensuring compliance with federal, state, sponsor, and institutional requirements. It requires all covered individuals involved in research to disclose foreign and domestic affiliations, financial interests, and external commitments. It addresses national security considerations through risk mitigation strategies related to foreign influence, malign foreign talent recruitment, export controls, cybersecurity, insider threats, and foreign travel security.

The policy requires mandatory training to promote a security-conscious research culture and annual policy reviews to adapt to evolving legal and regulatory requirements. It provides ongoing compliance monitoring, including advanced screening tools, proposal and travel reviews, and mechanisms for confidential reporting of suspensions, violations, or security incidents. Failure to comply results in corrective action consistent with university and federal requirements. The policy is published at public.powerdms.com/ASU/documents/2905017 and on ASU's Research Security Program webpage, researchcompliance.asu.edu/research-security. ASU reports that the policy is aligned with the requirements of A.R.S. § 15-1626 and that no policy gaps were identified.

Program: ASU's Research Security Program is administered by the Knowledge Enterprise Office of Research Compliance, which coordinates governance, risk assessments, training, and oversight activities across the university. The program includes institutional oversight, policy frameworks, mandatory training, proactive risk assessments, compliance monitoring and incident response mechanisms, and uses a suite of compliance screening and monitoring tools to identify and mitigate risk related to foreign influence and restricted parties. ASU reports that it has strengthened this infrastructure by streamlining operations, launching new training initiatives, expanding cybersecurity and export control resources, and improving oversight of international collaborations and foreign travel. ASU cites increased training completion rates, effective foreign travel review protocols, and strengthened oversight of research involving export-controlled technologies and sensitive research data.

Researcher disclosures and conflict review: Researchers and covered personnel disclose domestic and foreign affiliations, financial interests, and external activities through the ERA MyDisclosures system. Researchers also disclose appointments, affiliations, research support, in-kind resources, and external activities in federally required documents such as biographical sketches and current and pending (other) support submissions. The Office of Research Compliance reviews disclosures for completeness and accuracy and follows up as needed to ensure compliance with sponsor, ASU, and federal requirements. Disclosed consulting and outside activities are also reviewed for conflicts of commitment. When a

conflict of interest is identified, the Office of Research Compliance works with the researcher to create and implement a management plan.

Cybersecurity: ASU has established protocols for the timely reporting, investigation, and remediation of research security incidents. Suspicious activity potentially involving criminal conduct is reported to the ASU Police Department and, when appropriate, to federal agencies such as the Federal Bureau of Investigation. Incident response procedures comply with sponsor-specific reporting obligations, including DFARS 252.204-7012 and NIST SP 800-171, and ASU documents investigations, corrective actions, and escalations. ASU maintains capabilities to protect sensitive and regulated research, including Controlled Unclassified Information (CUI), export-controlled information, and classified research, through secure research environments, access controls, cybersecurity monitoring, and incident response.

Insider threat: ASU maintains an enterprise-wide cybersecurity program and insider threat awareness program to protect university information, technology, research, and data. Its Insider Threat Program is consistent with applicable National Industrial Security Program Operating Manual (NISPOM) requirements. It includes policies and procedures to detect, deter, and mitigate insider threats; security education and awareness; reporting requirements; access controls; and coordination among cybersecurity, research security, and other university functions. ASU's Security Operations Center provides continuous monitoring and supports the identification, investigation, and response to suspicious activity, with additional protections and oversight for secure research environments.

Foreign travel security: ASU conducts quarterly reviews of foreign travel to countries of concern, including China, Russia, Iran, and North Korea, using internal travel data. Researchers receive training and guidance on safeguarding intellectual property and complying with export control requirements while traveling. ASU's international travel guidance addresses handling of university information and technology, including using approved university devices, minimizing access to sensitive or regulated data while traveling, and protecting devices and accounts. It also addresses interactions with foreign institutions, organizations, or individuals that may warrant consultation with the Office of Research Compliance.

Export controls: ASU's Export Control team provides researchers with guidance, training, and tools, including the Export Control Wizard, to determine licensing requirements and compliance obligations. Technology Control Plans are developed and monitored for research involving export-controlled technologies, and personnel on those plans receive annual export compliance training. ASU manages export-controlled information, equipment, and services under the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Skysong Innovations, ASU's intellectual property management company, maintains internal controls to comply with export regulations and evaluates license requests for risks involving restricted parties, sanctioned entities, and export-controlled technologies.

Research security training: Covered individuals at ASU complete research security training as applicable and as federal requirements direct. That training includes the Collaborative Institutional Training Initiative (CITI) Research Security module, Export Compliance Training,

Insider Threat Awareness training, and Department of Defense (DoD) training on Controlled Unclassified Information (CUI). ASU also holds annual town hall sessions for researchers in high-risk programs. These include projects funded by the Advanced Research Projects Agency–Energy (ARPA-E), the Defense Advanced Research Projects Agency (DARPA), and DoD applied research (budget activity 6.2) programs. ASU updates its training content regularly to reflect changing federal requirements and emerging risks.

Identification and resolution of concerns: ASU provides pathways for reporting suspected research security concerns, policy violations, or unauthorized disclosures, including the confidential ASU Ethics Hotline and supervisory channels. ASU uses established processes and tools to identify, assess, and address research security and foreign influence concerns, and to screen foreign collaborators, faculty hires, visiting scholars, visa applicants, and entities involved in international academic initiatives. ASU evaluates concerns based on the evidence collected and relevant risk factors, which inform outreach, reporting, and risk mitigation. They are addressed through established compliance processes and escalated for further review when appropriate.

Review of activities involving foreign adversary nations: ASU reviews proposed research and other university activities involving foreign adversary nations to identify research security, foreign influence, export control, and other compliance risks. Each review considers the nature of the activity, the individuals and entities involved, applicable sponsor and regulatory requirements, and the sensitivity of the research or information. Where concerns are identified, ASU provides guidance and mitigation before the activity can proceed.

Published resources: ASU publishes the policies, procedures, and tools that support its program. These include its Export Control Policy (RSP 214), Foreign Malign Talent Programs Policy (RSP 215), Objectivity in Research policy on financial interests and conflicts of interest (RSP 206), and outside business activities policy (ACD 510-01). They also include guidance on NSPM-33 implementation, foreign talent recruitment programs, foreign ownership, control or influence (FOCI), international research and global collaborations, international travel, CUI handling, IT security standards and physical security.

NORTHERN ARIZONA UNIVERSITY

Policy: NAU approved its Research Security (Interim) Policy and published it in the University Policy Library on September 11, 2026, at in.nau.edu/university-policy-library/research-security. The policy commits NAU to protecting the integrity, security, and openness of its research enterprise. It establishes NAU's framework for research security, promotes a culture of security and compliance, supports national security interests, and safeguards research from threats to research activities, personnel, data, intellectual property, and other research assets. It applies to all university employees, students, affiliates, visiting scholars, and others engaged in research, sponsored activities, or activities supporting the research enterprise.

Implementation measures must address research security training, disclosure and transparency, cybersecurity, foreign travel security, insider threat awareness, export controls, international collaborations, and research risk management. The Office of Research Compliance must review the policy and related procedures at least annually and revise them

as needed to address changes in law, regulation, sponsor requirements, emerging threats or institutional needs. Noncompliance may result in corrective or disciplinary action. NAU reports that the policy addresses the elements of A.R.S. § 15-1626(A)(23). NAU is strengthening implementation in two areas: formalizing procedures for the Research Security Program and the Comptroller's Office to flag high-risk international travel, and documenting active research security practices as standard operating procedures. It expects to complete both by April 1, 2027.

Program: NAU has long maintained a risk-based framework of policies and procedures across multiple units, designed to safeguard the integrity, security, and openness of its research enterprise. The framework has evolved with new federal laws and regulations, state statutes, and industry best practices. It prioritizes protecting research activities, personnel, data, technology, intellectual property, facilities, and other institutional assets from undue foreign influence and theft. It also preserves academic freedom, facilitates international collaboration based on openness and reciprocity, and maintains NAU's eligibility for federal funding. NAU is now moving to a centralized Research Security Program, administered by the Office of Research Compliance under the authority of the Vice President for Research. The program coordinates with the Office of Sponsored Projects, Information Technology Services, the Office of General Counsel, the Comptroller's Office, the Center for International Education, and Human Resources. During FY 2026, NAU approved and published its policy and implemented mandatory research security training for all senior and key personnel applying for federal funding. It also added new disclosure and certification requirements to proposal review, continued conflict of interest, foreign-affiliation, export control, and restricted-party reviews, and advanced a new Secure Research Enclave. NAU also continued its use of Technology Control Plans and provided targeted compliance support to higher-risk research initiatives.

Researcher disclosures and conflict review: Researchers disclose financial interests, outside employment, and commitments through NAU's eCERT platform, at least annually and after any change. Participation in foreign talent recruitment programs must be disclosed prior to proposal submission through a form internal to the Office of Sponsored Projects. When applying for funding, all senior and key personnel must complete an updated conflict of interest disclosure and certify that they are not party to a malign foreign talent recruitment program before the proposal is submitted. These internal requirements supplement the federal disclosures and certifications on biographical sketch and current and pending (other) support forms. Pre-award administrators in the Office of Sponsored Projects verify that all required disclosures and certifications have been submitted and reviewed before any proposal goes to a federal agency.

When a disclosure may create a conflict of interest, conflict of commitment, or security concern, it is escalated to the Office of Research Compliance. That office decides whether the conflict can be mitigated and managed and the research adequately safeguarded, after a risk-benefit analysis, a review of applicable laws, regulations, and agency guidelines, and consultation with university leadership as appropriate. If the concern can be managed, the chair of the department where the activity takes place implements and oversees a management plan. If it cannot, the Office of Research Compliance and the Office of the Vice President for Research disallow the activity. The Office of Sponsored Projects also requires

research security disclosures and certifications from institutions collaborating with NAU as subrecipients.

Cybersecurity: NAU applies cybersecurity measures across its cloud-based and on-premises infrastructure. Its Data Classification and Handling Policy and related procedures require heightened cybersecurity and access controls for research data with higher sensitivity and risk. For research involving CUI, NAU is developing a Secure Research Enclave designed to comply with NIST SP 800-171. The enclave's security documentation provides security-control assessments, system security plans, plans of action, continuous monitoring, vulnerability review, access authorization, and protection against unauthorized disclosure. Until the enclave is complete, NAU has contracted with ASU for a NIST SP 800-171-compliant environment to support its current CUI project.

Foreign travel security: NAU's travel policies require that all international travel for university business be registered and approved in advance. Project-specific controls may limit the equipment or information taken abroad, require security briefings, or impose additional protection and reporting requirements, with special attention to researchers conducting export-controlled research. NAU's annual Information Security Awareness Training, required of all employees and others authorized to access university information or technology, includes a module on traveling internationally with university equipment. Information Technology Services maintains a loaner laptop program that makes clean laptops available for travel abroad, and the Office of Research Compliance strongly encourages their use for travel to countries of concern.

Insider threat: NAU mitigates insider risk through background screening, least-privilege access, continuous system monitoring, reporting systems, and refined incident response procedures. Information Technology Services teaches insider threat awareness and breach reporting through mandatory Information Security Awareness Training. The Office of Research Compliance and the Center for International Education screen foreign scholars and visitors before they arrive.

Export controls: The Office of Research Compliance is responsible for NAU's compliance with export control laws and regulations. It reviews proposed research activities, equipment, software, technology, technical data, international shipments, foreign-person access, and international collaborations for export control restrictions. The Office of Sponsored Projects screens every proposal before submission for activities or technology that may trigger export control risk. The Office of Research Compliance then reviews flagged proposals with the research team, secures any needed licenses, and implements Technology Control Plans. These plans document project-specific controls, including physical and information security, access restrictions, marking and storage, foreign travel safeguards, personnel rosters, training, self-evaluation, corrective action, and disposition of controlled materials.

Research security training: All senior and key personnel on federal proposals must complete research security training on the CITI platform within 12 months before submission, and Office of Sponsored Projects pre-award staff verify compliance. The CITI course uses research security training approved by the NSF SECURE Center and recognized by federal agencies as meeting the training requirement of the CHIPS and Science Act. The course expires after one

year, and CITI prompts annual renewal for those with active proposals or awards. During the reporting period, 170 NAU employees completed research security training through CITI.

Identification and resolution of concerns: Research security concerns may be reported to the Office of Research Compliance, the Chief Information Security Officer, the Office of General Counsel, the Vice President for Research, or the Provost. Concerns are assigned for assessment by subject matter. They may result in additional review, risk mitigation, corrective action, access restrictions, disclosure correction, sponsor notification, or other action required by law or policy.

UNIVERSITY OF ARIZONA

Policy: U of A implemented and published an interim Research Security Policy on June 10, 2025, and its final policy on February 4, 2026, at policy.arizona.edu/research-security-policy. The policy aims to protect research and development from foreign government interference and exploitation while maintaining an open research environment. It applies to employees, Designated Campus Colleagues, and researchers or contributors designated as covered individuals by a federal research agency. The policy sets several requirements:

- U of A must implement a cybersecurity program consistent with NSPM-33 and applicable federal regulations.
- Covered individuals must complete foreign travel security and research security training, and U of A must maintain a travel reporting program.
- Covered individuals working with export-controlled technologies must complete export control training.
- The Research Security Program must approve specified activities connected to a Country of Concern.
- Interactions with the Chinese universities identified as the “Seven Sons of National Defense” are prohibited.
- Employees and covered individuals must report known or suspected research security concerns and use a university-issued clean laptop when traveling to a Country of Concern.

U of A defines Countries of Concern as China (including Hong Kong and Macau, but excluding Taiwan), Cuba, Iran, North Korea, Russia, Venezuela, and other countries so designated under U.S. law. U of A reports that the policy establishes a comprehensive framework to safeguard its research enterprise in alignment with A.R.S. § 15-1626 and that no policy gaps were identified. Under U of A’s University Policy-Making Policy, the policy is reviewed at least every five years.

Program: U of A’s Research Security Program oversees compliance with the policy. It works with the Office for Responsible Outside Interests, Export Control, and the Office of Research Contracts & Agreements within the Office of Research & Partnerships.

Researcher disclosures and conflict review: Researchers disclose their own and their family members’ significant financial interests, significant personal interests, foreign interests, and outside activities, and certify whether they have any Foreign Affiliations. Foreign interests include participation in foreign talent or similar programs, all resources and other support for ongoing research, in-kind contributions from domestic and foreign

institutions or governments, and any payment or other compensation received from a foreign entity. Foreign Affiliations include research collaborations, appointments, consulting, talent programs, visiting scholar arrangements, laboratories outside the United States, and foreign-paid travel, among others. Researchers certify that their disclosures are truthful and complete. When a researcher discloses a foreign interest or Foreign Affiliation, the certification is sent to the Research Security Program for review.

Cybersecurity: U of A has adopted an enterprise approach to research cybersecurity, implementing minimum cybersecurity standards with NIST-aligned controls for all research data. U of A is pursuing Cybersecurity Maturity Model Certification (CMMC) to align with Department of Defense requirements. It is working toward Level 1 compliance across core enterprise applications, to be followed by a Level 2 self-assessment of its CUI enclave.

Foreign travel security: Travel to a Country of Concern requires approval from both the Research Security Program and Export Control. Researchers and employees must review a foreign travel security briefing and confirm completion before the Research Security Program approves travel to a Country of Concern, and must take a university-issued clean laptop. Export Control also reviews travel by anyone involved in export-controlled activities or traveling with specialized equipment or software, regardless of destination.

Insider threat: Insider threat awareness training is mandatory for individuals handling controlled or sensitive data and for cleared personnel, and covers what to report and how. As part of its facility clearance program, U of A operates an Insider Threat Awareness Program.

Export controls: U of A uses a third-party vendor to check persons and entities against restricted-party lists before approving certain engagements and activities. U of A recently added the Bureau of Industry and Security 50% (Affiliates) Rule list and the NDAA Section 889 list to that screening. U of A's published screening guide assigns responsibility for each activity, including foreign visiting scholars, employment candidates, international graduate students, Designated Campus Colleagues, international memoranda of understanding, proposals and contracts, vendors, and export-controlled projects. Potential matches must be cleared before an activity proceeds. Individuals conducting research with export-controlled technologies must complete export control training, and Export Control reviews compliance with Technology Control Plans.

Research security training: U of A implemented the NSF SECURE Center's consolidated training module and annual refresher module and requires researchers to complete training at least annually. Compliance is verified during proposal submission for federal awards.

Identification and resolution of concerns: U of A builds compliance checks into its research processes:

- Researchers are blocked from submitting a disclosure if their conflict of interest disclosure is not current.
- Proposals cannot be submitted to a federal agency until the Office for Responsible Outside Interests confirms that each researcher's training and conflict disclosure are current.

- Federal awards are placed on an “award hold,” which prevents spending, until conflict review is complete for each researcher.
- Research security and conflict requirements flow down to subrecipients, whose conflict policies must be reviewed and approved.

Offices within U of A's research security organization conduct periodic compliance reviews, and U of A maintains an Ethics Hotline for anonymous reporting. Noncompliance with conflict, export control, and research security requirements may result in administrative or employment sanctions, including suspension of research privileges and termination.

Review of activities involving foreign adversary nations: U of A uses a suite of tools to conduct research security reviews. The Research Security Program must approve the following activities when they involve an individual, entity, or component from a Country of Concern: research collaborations, proposals and subawards; contracts, agreements and memoranda of understanding; official university purchases; Designated Campus Colleague appointments or affiliations; employment offers; international travel; visa sponsorships and international scholars; material transfer and intellectual property licensing agreements; and other activities the program identifies. New research sponsors are vetted and approved for foreign ownership, control, or influence. Employees, Designated Campus Colleagues, and covered individuals may not interact with the Seven Sons of National Defense universities or their faculty, researchers, or students. Prohibited interactions include speaking engagements, visits, research collaborations, and appointments.

COMPLIANCE WITH STATE AND FEDERAL LAW

Each university has adopted and posted a research security policy as A.R.S. § 15-1626(A)(23) requires, and each builds research security requirements into its research processes so that compliance is checked before proposals are submitted and before awards are spent. This section summarizes how each university demonstrates compliance with applicable state and federal requirements, protects national security and intellectual property, and addresses risks from foreign adversary nations.

ARIZONA STATE UNIVERSITY

Federal compliance: ASU's program aligns with federal mandates, including National Security Presidential Memorandum-33 (NSPM-33), Department of Defense requirements, and other applicable federal, state, and sponsor requirements. ASU documents compliance through institutional research security certifications submitted to federal sponsors and through ASU-developed certifications that researchers complete. These include its ERA MyDisclosures disclosure certification, a covered individual certification for U.S. Department of Agriculture (USDA) awards, a National Aeronautics and Space Administration (NASA) Wolf Amendment certification, and a subrecipient commitment form with NASA and USDA addenda. Researchers also certify on the federal current and pending (other) support forms used by the Department of Energy, NASA, the National Institutes of Health, the National Science Foundation, and USDA. In FY 2026, 1,286 ASU faculty and staff completed the required annual CITI Research Security Training; covered individuals must complete it each year. ASU supports federally sponsored research with research security requirements, including CUI, export-controlled information, and classified research under a Defense Counterintelligence and Security Agency facility clearance.

State compliance: Under Arizona State law and ASU policy ACD 204-08, ASU employees must disclose substantial interests involving non-ASU organizations or entities, domestic or foreign, public, or private. The requirement also covers the substantial interests of an employee's relatives, and the reporting threshold is \$0. An employee with a substantial interest in any transaction involving ASU must disclose that interest and refrain from participating in the transaction.

Protecting national security and intellectual property: ASU protects sensitive and regulated research through secure research environments, access controls, cybersecurity monitoring, and incident response procedures that comply with DFARS 252.204-7012 and NIST SP 800-171. It manages export-controlled information, equipment, and services under ITAR and EAR, with Technology Control Plans for export-controlled projects. In coordination with university compliance functions, Skysong Innovations maintains internal controls to comply with export regulations. It evaluates license requests for risks involving restricted parties, sanctioned entities, and export-controlled technologies, which helps protect university intellectual property.

Foreign adversary nations: ASU reviews proposed research and other university activities involving foreign adversary nations before they proceed, and requires guidance and mitigation where concerns are identified. It conducts quarterly reviews of travel to China,

Russia, Iran, and North Korea. It screens foreign collaborators, faculty hires, visiting scholars, visa applicants, and entities involved in international academic initiatives. ASU's research security certifications define "foreign adversary" by reference to the U.S. Department of Commerce determination at 15 CFR 791.4, which currently lists China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia and the Maduro regime in Venezuela. Researchers on USDA awards certify that they are not subject to foreign ownership, control or influence and will not provide any benefit from the award to a foreign adversary or foreign country of concern.

National engagement: ASU takes part in the Council on Governmental Relations (COGR), the NSF SECURE Center, the Federal Demonstration Partnership (FDP) and the Association of University Export Control Officers (AUECO) to stay informed of evolving federal research security requirements, guidance and best practices.

NORTHERN ARIZONA UNIVERSITY

Federal compliance: NAU complies with federal research security requirements at both the employee and the institutional level. Every researcher applying for federal funding must:

- disclose outside employment, outside commitments, and participation in foreign talent recruitment programs, internally during proposal submission and to the funding agency on the common biographical sketch and current and pending (other) support forms.
- certify that they are not party to a malign foreign talent recruitment program;
- complete research security training at least annually through CITI;
- register with the Comptroller's Office and obtain advance institutional approval for international travel on university business; and
- complete export control training when conducting export-controlled research.

At the institutional level, NAU:

- files the annual Section 117 report with the U.S. Department of Education on foreign gifts, contracts and grants exceeding \$250,000 in cumulative value;
- files the annual Foreign Financial Disclosure Report with NSF, disclosing financial support of \$50,000 or more from or associated with a foreign country of concern;
- screens contracts and agreements with foreign entities for security risk before execution;
- screens foreign visiting scholars before arrival;
- conducts targeted outreach on research security to faculty in sensitive areas such as engineering, materials science, remote sensing and space exploration; and
- maintains the policies and procedures needed to assert compliance with federal regulations and agency terms and conditions.

NAU's proposal management system, Cayuse, presents these requirements and captures export control screening at proposal. NAU's Participation in Foreign Talent Recruitment Programs policy, in effect since August 8, 2024, prohibits participation in malign foreign talent recruitment programs. NAU submitted its policies, disclosure forms, subrecipient commitment form, and system screenshots as supporting exhibits.

Protecting national security and intellectual property: NAU safeguards sensitive research data through its Data Classification and Handling Policy and is developing a NIST SP 800-171-compliant Secure Research Enclave. It protects export-controlled technology and technical data through Technology Control Plans. NAU's Intellectual Property Policy governs university intellectual property.

Foreign adversary nations: NAU's policy directs its Research Security Program to address risks associated with foreign adversary nations and foreign entities. NAU prohibits participation in malign foreign talent recruitment programs, including those sponsored by a foreign country of concern and those on federal lists of restricted institutions and programs. It also screens foreign contracts before execution and foreign scholars and visitors before arrival.

National engagement: NAU maintains membership in COGR, AUECO, and the Association of Research Integrity Officers (ARIO) to keep pace with changes in federal requirements and incorporate current best practices.

UNIVERSITY OF ARIZONA

Federal compliance: U of A builds federal research security requirements into proposal and award processes. Proposals cannot be submitted to a federal agency until training and conflict disclosures are confirmed current, and federal awards are held until conflict review is complete. With federal proposals, U of A issues signed organizational compliance attestations from the Office of Research Contracts & Agreements. These certify the accuracy of current and pending (other) support disclosures under 42 U.S.C. § 6605, that researchers are not party to malign foreign talent recruitment programs, that researchers completed SECURE Center research security training, and that researchers are not collaborating on fundamental research with entities prohibited by Department of Defense research security policy. Researchers also sign disclosure certifications under penalty of perjury under Arizona law, acknowledging the federal penalties for false statements. U of A provided sample attestations and certifications as evidence.

Protecting national security and intellectual property: U of A applies NIST-aligned minimum cybersecurity standards to all research data and is pursuing CMMC. Material transfer and intellectual property licensing agreements involving a Country of Concern require Research Security Program approval. Technology Control Plans secure export-controlled technical data, materials, software, and hardware from unauthorized use, access, and observation.

Foreign adversary nations: U of A requires Research Security Program approval for activities involving an individual, entity, or component from a Country of Concern. It vets new sponsors for foreign ownership, control, or influence, screens people and entities against restricted-party lists, and prohibits interactions with the Seven Sons of National Defense universities.

National engagement: Members of U of A's Research Security Program have attended the Academic Security and Counter Exploitation program, hosted by the RISC Institute, since 2024. They are members of NCMS, the Society of Industrial Security Officers, and take

part in its educational events and annual meeting. U of A's Executive Director for Research Security & Responsible Outside Interests serves as an NSF SECURE Center mentor to other institutions and co-chairs the Federal Demonstration Partnership's Research Security & Subawards Working Group.

FOREIGN GRANTS, GIFTS, DONATIONS AND CONTRACTS

The table below reports, for each university, the number of foreign grants, gifts, donations and contracts exceeding \$250,000 received in calendar year 2025.

UNIVERSITY	FOREIGN GRANTS, GIFTS, DONATIONS AND CONTRACTS EXCEEDING \$250,000, CY 2025
Arizona State University	46
Northern Arizona University	4
University of Arizona	21

Methodology: The reporting period is January 1 through December 31, 2025. The count includes grants, gifts, donations, and contracts from any foreign source, including foreign governments, companies, universities, foundations, and individuals. An item is counted when that single grant, gift, donation, or contract exceeded \$250,000. Each university identified qualifying items from its own records:

- **ASU** counted items from its list of foreign grants, gifts, donations, and contracts received in calendar year 2025. For contracts, ASU's list shows the total contract amount, which may be received over more than one calendar year.
- **NAU** counted items from amounts received in calendar year 2025.
- **U of A** counted items from its federal Section 117 filings for July 1, 2025 through June 30, 2026. The count covers the 19 items over \$250,000 reported for July–December 2025. It adds two contracts that began before 2026 and first appear in the January–June 2026 filing: one began July 1, 2025, and the other December 11, 2024. A contract that appears in both filings is counted once. The filings report amounts by foreign source for every six months.

APPENDIX A: PUBLISHED RESEARCH SECURITY POLICIES

UNIVERSITY	RESEARCH SECURITY POLICY	EFFECTIVE DATE	PUBLISHED AT
Arizona State University	Research Security Policy (RSP 216)	September 12, 2026	public.powerdms.com/ASU/documents/2905017
Northern Arizona University	Research Security (Interim) Policy	September 11, 2026	in.nau.edu/university-policy-library/research-security
University of Arizona	Research Security Policy	February 4, 2026	policy.arizona.edu/research-security-policy

APPENDIX B: SUPPORTING DOCUMENTS

The following policies, forms, and certifications were submitted by the universities and are attached to this report.

UNIVERSITY	DOCUMENT	DESCRIPTION
Arizona State University	B-1: ERA MyDisclosures Disclosure Profile: Instructions and Certification Language	Researcher disclosure requirements and certification
Arizona State University	B-2: Covered Individual Certification, USDA Federal Prime Award	Certification on foreign ownership, control or influence, malign foreign talent programs and training, with definitions
Arizona State University	B-3: NASA Wolf Amendment Certification	Certification of compliance with Wolf Amendment restrictions
Arizona State University	B-4: Subrecipient Commitment Form, with NASA and USDA addenda	Subrecipient certifications
Northern Arizona University	B-5: Exhibit 1: Research Security (Interim) Policy	Policy
Northern Arizona University	B-6: Exhibit 2: Participation in Foreign Talent Recruitment Programs	Policy
Northern Arizona University	B-7: Exhibit 3: Significant Financial Interest and Foreign Talent Recruitment Program Disclosure Form	Researcher disclosure and certification
Northern Arizona University	B-8: Exhibit 4: Federal Common Form Disclosure Instructions and Certification Language	Federal certification language
Northern Arizona University	B-9: Exhibit 5: NAU Subrecipient Commitment Form	Subrecipient certifications
Northern Arizona University	B-10: Exhibit 6: Data Classification and Handling	Policy
Northern Arizona University	B-11: Exhibit 7: International Travel (TRV 550)	Policy
Northern Arizona University	B-12: Exhibit 8: Travel Security Training Content	Training content
Northern Arizona University	B-13: Exhibit 9: Information Security Awareness Training	Policy
Northern Arizona University	B-14: Exhibit 10: Research Security Checks in Cayuse	System screenshots
Northern Arizona University	B-15: Exhibit 11: Enhanced Visitor Screening Form	Screening form
University of Arizona	B-16: Researcher Mandatory Disclosure Certification (redacted)	Researcher disclosure certification
University of Arizona	B-17: RPS Screening Responsibilities	Screening responsibilities by activity

APPENDIX B-1: ARIZONA STATE UNIVERSITY — ERA MyDisclosures Disclosure Profile: Instructions and Certification Language

ERA MyDisclosures - Disclosure Profile

Instructions and Policies

ASU Employees & Researchers:

State of Arizona regulations and ASU policy ([ACD 204-08](#)) require ASU employees to disclose [substantial interests](#) involving non-ASU organizations or entities that are domestic or foreign, public or private, which reasonably appears to be related to their institutional responsibilities and professional expertise. The disclosure requirement also includes substantial interests of the ASU employee's [relatives](#). If an ASU employee (or the employee's "relative") has a substantial interest in any transaction involving ASU, the employee must:

1. disclose that interest via the MyDisclosures module; and
2. refrain from participating in any manner in that transaction.

The threshold for reporting substantial interests under Arizona State procurement regulations is \$0.

For more information see the Office of General Counsel Conflicts of Interest website: <https://ogc.asu.edu/conflicts-interest>

ASU Researchers:

Note: All Pre-Approval Requests (i.e., Notification of Consulting or Other Outside Business Activities or Arrangements, Sponsored Foreign Travel) also need be added to your Disclosure Profile after it has been approved.

ASU researchers are also subject to ASU policy, [RSP 206](#). All research personnel responsible for the design, conduct, reporting or purpose of the research under a sponsored project are required to disclose all [significant financial interests](#) (SFI) which, due to their relationship to research or other scholarly activities, could give rise to a real or perceived conflict of interest. All disclosures must be made prior to proposal submission and updated at least annually or within 30 days whenever there is a change in a disclosed relationship, and, if necessary, prior to the expenditure of any funds upon receipt of an award. **NOTE:** Different sponsors may have different disclosure requirements.

What is an SFI in terms of research?

Anything of monetary value from a domestic and/or foreign source, including, but not limited to:

- Salary or other payments for services (e.g., consulting fees or honoraria),
- Equity interest (e.g., stocks, private equity, stock options, or other ownership interests),
- Venture or other capital financing, and
- Intellectual property rights (e.g., patents, copyrights and royalties from such rights)

Find definitions and explanations of reporting requirements for specific federal sponsors at <https://researchintegrity.asu.edu/coi/financial-conflicts-interest>.

Regarding board service, research personnel must disclose board service (U.S. or foreign) related to institutional responsibilities (ASU business/research), paid or unpaid.

Regarding travel, research personnel must disclose the occurrence of any reimbursed or sponsored travel (*i.e.*, that which is paid on behalf of the Investigator - contact COI@asu.edu with questions about Sponsored Travel), related to their institutional responsibilities. The disclosure requirement does not apply to travel that is reimbursed or sponsored by a Federal, state, or local government agency, an Institution of higher education as defined at [20 U.S.C. 1001\(a\)](#), an academic teaching hospital, a medical center, or a research institute that is affiliated with an Institution of higher education.

Regarding foreign interests, disclosures shall also include financial interests received from a foreign institution of higher education or the government of another country (which includes local, provincial, or equivalent). ASU faculty and staff who have international collaborations are required to be transparent and provide full disclosure of all **funded and unfunded** collaborations and affiliations as required by federal and state agencies, as well as ASU's policies.

Regarding required COI training, CITI "Conflict of Interest" training is required prior to engaging in sponsored project activities and at least every 4 years. If you haven't already completed this training in CITI, click [here](#) to access the training.

--

ERA MyDislosures - Disclosure Profile Update Completed Certification

By completing your disclosure profile update you are verifying that all disclosure information is accurate and current.

If funded by or applying for funding from any federal agency, I understand that this Disclosure is required to obtain funding from the U.S. Government. I certify to the best of my knowledge and belief that the information contained in this Disclosure Statement is true, complete, and accurate. I understand that any false, fictitious, or fraudulent information, misrepresentations, half-truths, or omissions of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims, or otherwise. (18 U.S.C. §§ 287, 1001, and 1031, and 31 U.S.C. §§ 3729-3733 and 3801-3812). I further understand and agree that (1) the statements and representations made herein are material to the U.S. Government's funding decision, and (2) I have a responsibility to update the disclosures during the period of performance of the Federal financial assistance award should circumstances change which impact the responses provided above.

I also certify that, at the time of submission, I am not a party to a malign foreign talent recruitment program. See Guidelines regarding Foreign Talent Recruitment Programs under "Additional Research Security Information" on the Research Compliance webpage.

FOR USDA COVERED INDIVIDUALS ONLY

I hereby certify that I am not currently subject to Foreign Ownership, Control, or Influence (FOCI) as defined herein. If I discover I am subject to FOCI, I will immediately report such discovery to the appropriate ASU Research Administration Offices for reporting to Federal awarding agency(ies) as may be required. I further agree, that during the period of any Federal Award, I will not enter into any subawards, contracts, or other agreements (including funded or unfunded foreign collaborations that may results in co-authorships) reasonably related to a Federal award, or otherwise provide any form of direct benefit (material or non-material) through work conducted under, in direct support of, or otherwise reasonably related to the Federal award, to any foreign adversary or foreign country of concern or any person or any person or entity known to be subject to FOCI.

"Foreign ownership, control, or influence (FOCI)" means a situation where the degree of ownership, control, or influence over the recipient or a covered individual by a foreign person or foreign entity that is a citizen or permanent resident of; representing; organized, chartered, or incorporated under the laws of; or otherwise substantially connected to a foreign adversary or

foreign country of concern such that a reasonable basis exists for concluding that compromise to that foreign person or foreign entity of non-public research, development, scientific, or technological information associated with the Federal award may result. "

See additional information regarding Foreign Ownership, Control, or Influence (FOCI) under "Additional Research Security Information" on the Research Compliance webpage.

APPENDIX B-2: ARIZONA STATE UNIVERSITY — Covered Individual Certification, USDA Federal Prime Award



COVERED INDIVIDUAL CERTIFICATION
USDA FEDERAL PRIME AWARD _____ (Federal Award)
DIRECT SPONSOR _____/Award No. _____

RE: USDA ASU Proposal FP _____/Award AWD _____

I, _____, hereby certify that by accepting this Federal Subaward, I am not currently subject to Foreign Ownership, Control, or Influence (FOCI) as defined herein. If I discover I am subject to FOCI during the period of the Federal Award, I will immediately report such discovery to the appropriate ASU Research Administration Offices for reporting to the USDA awarding agency.

I hereby agree, that during the period of the Federal Subaward, I will not enter into any subawards, contracts, or other agreements (including funded or unfunded foreign collaborations that may result in co-authorships) reasonably related to the Federal Subaward, or otherwise provide any form of direct benefit (material or non-material) through work conducted under, in direct support of, or otherwise reasonably related to the Federal Subaward, to any foreign adversary or foreign country of concern or any person or any person or entity known to be subject to FOCI.

I certify by accepting the Federal Subaward, that I am not currently participating, nor have I participated within the past 10 years, in a malign Foreign Talent Recruitment Program (FTRP) as defined in 42 U.S.C. § 19237. I further certify that I will not engage in any such malign FTRP for the duration of the Federal Subaward. I understand that if I have questions regarding malign FTRPs I will refer to ASU Office of Research Compliance online resources and/or contact them at export.control@asu.edu.

I further certify that I have completed required research security training at the time of applying for the award or within the 12-month period immediately preceding commencement of work on the award. I acknowledge that I must complete research security training each year during the award period and recertify that I have done so.

I further agree that I will comply with Arizona State University research security requirements, training, disclosure obligations, and applicable university policies related to research integrity, conflicts of interest, conflicts of commitment, and outside activities.

I understand that any questions regarding this attestation, ASU policies, or sponsor requirements should be directed to the appropriate university research administration offices.

Signature

Date: _____

Print Name: _____

For the purposes of these certifications, the following DEFINITIONS apply:

“Foreign adversary” means any foreign government or foreign non-government person as defined (see [15 CFR 791.2](#)) or determined (see [15 CFR 791.4](#)) by the Secretary of Commerce to have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons.

[15 CFR 791.4 Determination of foreign adversaries](#)

Currently –

- (1) The People's Republic of China, including the Hong Kong Special Administrative Region and the Macau Special Administrative Region (China);
- (2) Republic of Cuba (Cuba);
- (3) Islamic Republic of Iran (Iran);
- (4) Democratic People's Republic of Korea (North Korea);
- (5) Russian Federation (Russia); and
- (6) Venezuelan politician Nicolás Maduro (Maduro Regime).

“Foreign country of concern” means the People’s Republic of China, the Democratic People’s Republic of Korea, the Russian Federation, the Islamic Republic of Iran, or any other country determined to be a country of concern by the Secretary of State.

“Foreign entity” means a foreign government, foreign non-government entity (e.g. foreign corporation, business association, partnership, trust, society), foreign government instrumentality, or multilateral organization whose members are primarily foreign governments or non-government entities (e.g., Group of Twenty (G20)).

“Foreign person” means any natural person who is not a citizen, national, or lawful permanent resident of the United States.

“Foreign interest” means a foreign person or foreign entity.

“Foreign ownership, control, or influence (FOCI)” means a situation where the degree of ownership, control, or influence over the recipient or a covered individual by a foreign person or foreign entity that is a citizen or permanent resident of; representing; organized, chartered, or incorporated under the laws of; or otherwise substantially connected to a foreign adversary or foreign country of concern such that a reasonable basis exists for concluding that compromise to that foreign person or foreign entity of non-public research, development, scientific, or technological information associated with the Federal award may result.”

“Foreign talent recruitment program” means any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non *de minimis* value, honorific titles, career advancement opportunities, or other types of remuneration or consideration



directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.

APPENDIX B-3: ARIZONA STATE UNIVERSITY — NASA Wolf Amendment Certification

**Foreign Affiliations / Relationships
to Foreign Countries
Certification**

ASU Reference No. [FP or SPA Number]
Federal Agency: National Aeronautics Space Administration
Sponsor: [Name of non NASA Sponsor if applicable]
Description of Purpose: Proposal/Project entitled [Name of Project]

This certification is to comply with restrictions related to use of federal funds for National Aeronautics Space Administration (“NASA”) policies, programs, orders or contracts under the Frank Wolf Space Security Act (“NASA Wolf Amendment”)

I certify compliance with NASA Wolf Amendment restrictions and confirm no prohibited bilateral collaboration with Chinese government entities or Chinese state-owned organizations will occur under this project.

By:

Name: Principal Investigator’s Name
Title: Principal Investigator – [Professor,
Associate Professor, etc.]
Date:

APPENDIX B-4: ARIZONA STATE UNIVERSITY — Subrecipient Commitment Form, with NASA and USDA Addenda



OFFICE FOR RESEARCH & SPONSORED PROJECTS ADMINISTRATION
PO BOX 876011 • TEMPE, AZ 85287-6011

PROPOSAL & NEGOTIATIONS TEAM – SUBAWARDS@ASU.EDU

SUBRECIPIENT COMMITMENT FORM

Completion of this form when submitting a proposal to ASU will expedite the subaward process by providing a checklist of documents and certifications required by sponsors, and by providing ASU with an authorized institutional representative signature

Today's Date (MM/DD/YY): _____

SUBRECIPIENT INFORMATION

SUBRECIPIENT LEGAL NAME (Must match name associated with UEI (number): _____

SUBRECIPIENT PRINCIPAL INVESTIGATOR (PI): _____

ASU PI: _____ PRIME SPONSOR: _____

ASU'S PROPOSAL ENTITLED: _____

SUBRECIPIENT'S TOTAL FUNDS REQUESTED: \$ _____

PERFORMANCE PERIOD: BEGIN: _____ END: _____

[SAM.GOV](https://sam.gov) UNIQUE ENTITY IDENTIFIER (UEI) # (required): _____

EIN No.: _____

Institution Type: Choose an item: _____

Small Business: ☐ Yes ☐ No

If Yes: Check all applicable federally-defined qualifications:

- ☐ 8(a) business (Small disadvantaged business)
- ☐ Veteran-Owned business
- ☐ Service-Disabled Veteran-Owned business
- ☐ Women Owned business
- ☐ HUBZone small business
- ☐ Minority Institution

Subrecipient currently registered in System for Award Management (SAM) database?

☐ Yes EXPIRATION DATE: _____ (update information if within 60 days of expiration)

☐ No Note: SAM registration is mandatory. Registration website: <http://www.sam.gov/>

SUBRECIPIENT "AWARD" ADDRESS:

Name: _____

Address: _____

City: _____ State: _____ Zip Code + 4: _____

Congressional District for Award Address (N/A for foreign subrecipients): _____

SUBRECIPIENT "PLACE OF PERFORMANCE" ADDRESS: ☐ Check box if same as AWARD Address above

(Complete if subrecipient "Place of Performance" address differs from subrecipient "Award" address.)

Name: _____

Address: _____

City: _____ State: _____ Zip Code + 4: _____

Congressional District for "Place of Performance Address" (N/A for foreign subrecipients): _____

SUBRECIPIENT "REMIT TO" ADDRESS: ☐ Check box if same as AWARD Address above

(Complete if subrecipient "Remit to" address differs from subrecipient "Award" address.)

Name: _____

Address: _____

City: _____ State: _____ Zip Code + 4: _____

Subrecipient Contacts	
Administrative Contact (responsible for Subaward processing)	
Name: _____	
Address: _____	
City: _____	State: _____ Zip Code + 4: _____
Telephone: _____	Fax: _____
Email: _____	
Project Director/Principal Investigator	
Name: _____	
Address: _____	
City: _____	State: _____ Zip Code + 4: _____
Telephone: _____	Fax: _____
Email: _____	
Financial Contact	
Name: _____	
Address: _____	
City: _____	State: _____ Zip Code + 4: _____
Telephone: _____	Fax: _____
Email: _____	
Authorized Official	
Name: _____	
Address: _____	
City: _____	State: _____ Zip Code + 4: _____
Telephone: _____	Fax: _____
Email: _____	
Single Audit Contact	
Name: _____	
Address: _____	
City: _____	State: _____ Zip Code + 4: _____
Telephone: _____	Fax: _____
Email: _____	

SECTION A – PROPOSAL DOCUMENTS

The following documents are included in subrecipient subaward proposal submission and covered by certifications in Section B:

☐ **STATEMENT OF WORK** (REQUIRED – Please attach to this form with submission)

Includes work to be performed, project description, PI, period of performance, deliverables, and milestones.

☐ **BUDGET and BUDGET JUSTIFICATION** (REQUIRED – Please attach to this form with submission)

Includes budget for entire length of project and broken down by budget period; and budget justification with reasonable level of detail.

Participant Support costs requested	☐ Yes	☐ No
Value Added Tax (VAT) costs requested	☐ Yes	☐ No
Short-term travel visa costs are requested	☐ Yes	☐ No
International and/or domestic travel costs requested	☐ Yes	☐ No
Administrative and/or clerical salaries costs requested	☐ Yes	☐ No
Computers and/or computing device costs requested	☐ Yes	☐ No

IMPORTANT: ASU will be reviewing the budget and budget justification in order to assess if costs are appropriately justified and seek agency prior approval, when prior approval is required.

- ☐ **COST PRICE ANALYSIS (REQUIRED FOR BUDGETS OR PROJECTS WITH TOTAL COSTS OF \$100,000 OR MORE)**
- ☐ This **SUBRECIPIENT COMMITMENT FORM** (REQUIRED) signed by Subrecipient Authorized Official.
- ☐ Small/ Disadvantaged Business Subcontracting Plan, in agency-required format.
(Required for proposals over \$700,000 stipulated by FAR 19.704(a)(9)).
- ☐ If new to working with ASU, Registration in our Financial Management System is needed. Ask your ASU research administration contact to send an invite link via PaymentWorks or email subawards@asu.edu.
- ☐ OTHER: _____

SECTION B – SPECIAL REVIEW AND CERTIFICATIONS

1. **Facilities and Administrative Rates** included in this proposal have been calculated based on (check as applicable):
- ☐ Our federally-negotiated F&A rates for this type of work is _____ (Enter F&A rate).
(If this box is checked, attach a copy of your F&A rate agreement or provide a URL link to the agreement below)
URL: _____
- IMPORTANT: If your organization is receiving funding under a federal award and you do not have a federally-negotiated F&A rate, your organization can only include the maximum de minimis rate allowed under [2 CFR 200.414](#).**
- ☐ My organization has used the Sponsor's published limited F&A cap.
- ☐ My organization is not requesting any F&A.
- ☐ My organization is not receiving any federal funds for this project and is requesting an F&A rate of _____.
(Please specify basis on which rate has been calculated in "Section C - Comments" at end of form.)
2. **Fringe Benefit Rates** included in this proposal have been calculated based on:
- ☐ Rates consistent with or lower than Subrecipient's federally-negotiated rates.
(If this box is checked, a copy of subrecipient's Fringe Benefit rate agreement must be furnished to ASU before a subaward will be issued, submit along with this Subrecipient Commitment Form.)
- ☐ Other rates
(Please specify basis on which rate has been calculated in "Section C - Comments" at end of form.)
- ☐ Not applicable (fringe benefits request for subrecipient)
3. **Committed Cost Sharing / Matching / In-Kind:** ☐ Yes ☐ No Amount: \$ _____
(Cost sharing, Matching, and/or In-Kind amounts must be included in subrecipient's budget and budget justification.)

REGULATORY APPROVALS (Questions 4-15)

PROJECT-SPECIFIC REQUIREMENTS

4. Human Subjects: ☐ Yes ☐ No

Check **Yes** if proposal includes surveys, interviews, observations, or secondary data.

(If **Yes**: Copies of the Institutional Review Board (IRB) or Ethics Committee approval and approved "Informed Consent" form must be provided before any subaward will be issued. If pending, obtain approval as required and forward these documents to ASU's Principal Investigator as soon as available.)

(If **Yes** and NIH funding is involved: Have all key personnel involved completed Human Subjects Training?)

☐ Yes ☐ No

Note: All key personnel engaged in human subject research must take the NIH human subjects training or human subjects research training (http://grants.nih.gov/grants/policy/hs_educ_faq.htm)

5. Animal Subjects: ☐ Yes ☐ No

(If **Yes**: A copy of the IACUC Committee approval must be provided before any subaward will be issued. If pending, obtain approval as required and forward these documents to ASU's PI as soon as available.)

6. Certification Regarding Debarment and Suspension

Is the entity, Principal Investigator, or any other employee or student participating in this project debarred, suspended, or otherwise excluded from or ineligible for participation in federal department, agency, assistance programs, or activities?

☐ Yes ☐ No (If **Yes**: Please explain in Section C – Comments below)

Subawards to any entity or individual included in the Federal Excluded Parties are prohibited.

7. Subrecipient Financial Conflict of Interest (FCOI) Policy (Applicable to PHS-funded research and other sponsors adopting the federal financial disclosure requirements)

- ☐ Not applicable, as this project is not funded by PHS or any other sponsor that has adopted these financial disclosure requirements.
- ☐ Subrecipient hereby certifies that it has an active and enforced PHS-compliant FCOI policy that is consistent with the provision of 42 CFR Part 50, Subpart F, "Responsibility of Applicants for Promoting Objectivity in Research." Subrecipient also certifies that, to the best of Institution's knowledge, (1) all financial disclosures have been made related to the activities that may be funded by or through a resulting agreement, and required by its conflict of interest policy; and (2) all identified conflicts of interest have or will have been satisfactorily managed, reduced, or eliminated in accordance with subrecipient's Conflict of Interest policy prior to the expenditures of any funds under any resultant agreement.
- ☐ As a Subrecipient, I have a **pending** FCOI policy established and will adopt and implement a policy prior to execution of the subaward agreement that is compliant with PHS policy using the [Federal Demonstration Partnership \(FDP\) Model Policy](#) as a guide.

8. NSF Responsible Conduct in Research (RCR)

- ☐ Not applicable. This project is not providing NSF funding to undergraduate students, graduate students, or postdoctoral researchers.
- ☐ Subrecipient certifies that it maintains an Institutional Plan to meet NSF's Educational Requirements for the Responsible Conduct of Research, as required under the "America COMPETES Act" PUBLIC LAW 110-69- August 9, 2007, and subrecipient has a training program in place and will train all NSF-funded undergraduate students, graduate students, and postdoctoral researchers in accordance with NSF's RCR training requirements.

9. NIH Responsible Conduct in Research (RCR)

- ☐ Not applicable. This project is not providing NIH support to **trainees, fellows, participants, or scholars through any NIH training, career development award, research education grant, or dissertation research grant.**
- ☐ Subrecipient certifies that it will monitor and maintain records for the individual training plans as proposed by subrecipient in accordance with NIH's RCR training requirements.

10. Telecommunications Equipment or Services: ☐ Yes

Subrecipient certifies that no funds will be used to acquire telecommunications equipment or services in accordance with 2 C.F.R. § 200.216, Prohibition on Certain Telecommunication and Video Surveillance Services or Equipment and Section 889 (a) (1) (A) (Part A) [Rule Effective 13 August 2020](#) and (a) (1) (B) (Part B) of the [Fiscal Year 2019 National Defense Authorization Act \(FY19 NDAA\)](#).

STANDARD REQUIREMENTS

11. Affirmative Action Compliance

In accordance with the rules and regulations of the Secretary of Labor (41 CFR 60-1 and 60-2), if your organization has more than 50 employees and subaward will be for \$50,000 or more, you are required to have a written affirmative action program. Indicate whether your organization has a written affirmative action program:

- ☐ Yes, we have a written affirmative action program developed and on file.
- ☐ No, we do not have a written affirmative action program.
- ☐ Not applicable, as we have less than 50 employees or anticipate subaward amount less than \$50,000.
- ☐ OTHER: _____

12. Conflict of Interest Policy (ASU requires that every Subrecipient have its own established and enforced Conflict of Interest policy)

- ☐ Subrecipient certifies it **will follow** the Conflict of Interest policy established and enforced by its compliance office or equivalent. Subrecipient also certifies that, to the best of Institution's knowledge, (1) all financial disclosures have been made related to the activities that may be funded by or through a resulting agreement, and required by its Conflict of Interest policy; and (2) all identified conflicts of interest have or will have been satisfactorily managed, reduced, or eliminated in accordance with subrecipient's Conflict of Interest policy prior to the expenditures of any funds under any resultant agreement.
- ☐ Subrecipient does not have an active and/or enforced Conflict of Interest policy and agrees to adopt and implement a policy prior to execution of the subaward agreement. The undersigned certifies that to the best of his/her knowledge there is no officer or employee of Arizona State University who has, or whose relative has, a substantial interest in any transaction resulting from this request.

13. Mandatory Disclosures

- ☐ Subrecipient certifies it has and will disclose to Arizona State University all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the federal award for disclosure to federal awarding agency or pass-through entity. See [§200.113](#) for more details.

14. Fiscal Responsibility

Subrecipient certifies that its financial system is in accordance with generally accepted accounting principles and:

- ☐ has the capability to identify, in its accounts, all federal awards received and expended and the federal programs under which they were received;
- ☐ maintains internal controls to assure that it is managing federal awards in compliance with applicable laws, regulations and the provision of contracts or grants;
- ☐ complies with applicable laws and regulations;
- ☐ can prepare appropriate financial statements, including the schedule of expenditures of federal awards;
- ☐ there are no outstanding audit findings which would impact contract costs. If there are findings, submit a copy of the most report that describes the finding and steps to be taken to correct the finding.

15. Single Audit and Financial Status

Single Audit Report Link: _____

- ☐ We have completed our Single Audit for fiscal year ending _____. The Single Audit Report disclosed no material weaknesses, no material instances of noncompliance with federal laws or regulations, no reportable conditions, no findings, and there are no unresolved prior year findings related to any subaward(s) from Arizona State University.
- ☐ We have completed our Single Audit for fiscal year ending _____. The Single Audit Report noted material weaknesses, material instances of noncompliance with federal laws or regulations, reportable conditions, findings, or unresolved prior year findings related to subaward(s) from Arizona State University. The corrective action plan is included in the audit link above. Page number(s) for relevant finding(s) are: _____

- ☐ Our Single Audit for fiscal year ending _____ is not anticipated to be complete until _____. Within thirty days of completion, we will provide written notification of the results along with any required documentation.
- ☐ We **are not subject** to the provisions of Uniform Guidance because our organization:
- ☐ Expends less than \$1,000,000 in federal awards annually
- ☐ Is a for-profit entity ☐ Other _____

IF YOU ARE NOT SUBJECT TO OMB CIRCULAR A-133, YOU MUST COMPLETE THE **ANNUAL SUBRECIPIENT SINGLE AUDIT CERTIFICATION FOUND [HERE](#) AND ATTACH TO THIS FORM.**

16. FFATA - ASU must comply with the Federal Funding Accountability and Transparency Act (FFATA), and to do so requires the following information (based upon Place of Performance information stated above):

The names and total compensation of the five most highly compensated officers of the entities must be listed if, in the preceding fiscal year, the entities received:

- (i) 80% or more of its annual gross revenues in federal awards (federal contracts, (and subcontracts), loans, grant (and subgrants) and cooperative agreements); AND
- (ii) \$25,000,000 or more in annual gross revenues from federal awards; AND
- (iii) the public does not have access to information about the compensation of the senior executives of the entity through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m(a), 78o(d)) or section 6104 of the Internal Revenue Code of 1986.

Is subaward entity exempt from reporting executive compensation? Yes ☐ No ☐ (If No: Complete this [form](#).)

SECTION C – COMMENTS

SUBRECIPIENT AUTHORIZED APPROVER:

THIS BOX MUST BE COMPLETED

The information, certifications, and representations above have been read, signed, and made by an authorized official of the subrecipient named herein. The appropriate programmatic and administrative personnel involved in this application are aware of agency policy in regard to subawards and are prepared to establish the necessary inter-institutional agreements consistent with those policies.

Any work begun and/or expenses incurred prior to execution of a subaward agreement are at the subrecipient's own risk.

Signature of Subrecipient's Authorized Official

Date

(Type or print name and title of Authorized Official)

(Phone)

(Email)

National Aeronautics and Space Administration (NASA)

Subrecipient Commitment Form Addendum

This addendum is applicable to all subrecipients receiving funds under a NASA prime award.

The Subrecipient certifies that it will comply with all applicable NASA award terms and conditions, including restrictions arising under Section 1340 of the FY2011 NASA appropriations act (commonly known as the Wolf Amendment), prohibiting bilateral activities, collaboration, or coordination with the Government of the People's Republic of China or any Chinese-owned company or entity. The Subrecipient acknowledges that

(1) it has reviewed its proposed activities, collaborations, or coordination and certifies that they are in compliance with the Wolf Amendment,

(2) it will not use subaward funds for activities, collaborations, or coordination prohibited by the Wolf Amendment, and

(3) it will promptly notify Arizona State University in writing upon becoming aware of any actual or potential activity that may be inconsistent with the Wolf Amendment in connection with this Subaward and will cooperate in any required review or reporting.

SUBRECIPIENT AUTHORIZED APPROVER:

THIS BOX MUST BE COMPLETED

The information, certifications, and representations above have been read, signed, and made by an authorized official of the subrecipient named herein. The appropriate programmatic and administrative personnel involved in this application are aware of agency policy in regard to subawards and are prepared to establish the necessary inter-institutional agreements consistent with those policies.

Any work begun and/or expenses incurred prior to execution of a subaward agreement are at the subrecipient's own risk.

Signature of Subrecipient's Authorized Official

Date

(Type or print name and title of Authorized Official)

(Phone)

(Email)

U.S. Department of Agriculture (USDA)
Subrecipient Commitment Form Addendum

This addendum is applicable to all subrecipients receiving funds under a USDA prime award.

By accepting this Federal award, I certify that I am not currently a party to any subaward, contract, or other agreement, or otherwise subject to Foreign Ownership, Control, or Influence (FOCI) by any country of concern or other foreign adversary, and I will not knowingly enter into any subaward, contract, collaboration, or other agreement, whether funded or unfunded, that would provide any material or non-material benefit to any foreign person, foreign entity, or U.S. person or entity that is subject to such FOCI by a foreign country of concern or another foreign adversary, as defined by applicable Federal requirements. I further certify that I will comply with all applicable requirements regarding FOCI for the duration of the award.

I certify that I am not currently participating in, nor have I participated within the past ten (10) years, in any Malign Foreign Talent Recruitment Program (FTRP) as defined in 42 U.S.C. § 19237.

I further certify that I will not engage in any such Malign Foreign Talent Recruitment Program (FTRP) for the duration of the Federal award.

SUBRECIPIENT AUTHORIZED APPROVER:

THIS BOX MUST BE COMPLETED

The information, certifications, and representations above have been read, signed, and made by an authorized official of the subrecipient named herein. The appropriate programmatic and administrative personnel involved in this application are aware of agency policy in regard to subawards and are prepared to establish the necessary inter-institutional agreements consistent with those policies.

Any work begun and/or expenses incurred prior to execution of a subaward agreement are at the subrecipient's own risk.

Signature of Subrecipient's Authorized Official

Date

(Type or print name and title of Authorized Official)

(Phone)

(Email)

APPENDIX B-5: NORTHERN ARIZONA UNIVERSITY — Exhibit 1: Research Security (Interim) Policy

9/24/26, 12:59 PM

Research Security - University Policy Library

Research

EXHIBIT 1

Research Security (Interim)

Northern Arizona University ("NAU" or the "University") is committed to protecting the integrity, security, and openness of its research enterprise. This policy establishes the University's framework for research security, promotes a culture of security and compliance, supports national security interests, and safeguards University research from threats that may compromise research activities, personnel, data, intellectual property, or other research assets.

Responsible Executive: Vice President for Research

Responsible Office: Office of Research Compliance

Origination Date: September 11, 2026

Last Revised: n/a

Scope

This policy applies to all University employees, students, affiliates, visiting scholars, and other individuals engaged in research, sponsored activities, or activities supporting the University's research enterprise.

Policy

1. Research Security Program

- NAU shall maintain a Research Security Program to protect the University's research enterprise and support compliance with applicable laws, regulations, sponsor requirements, contractual obligations, and University policies. The Research Security Program shall be administered by the Office of Research Compliance under the authority of the Vice President for Research.

2. Research Security Principles

- The University's Research Security Program shall:
 - a. Safeguard the University's research activities, personnel, data, intellectual property, facilities, and other research assets.
 - b. Promote a culture of research security, awareness, integrity, transparency, and compliance.
 - c. Support United States national security interests while preserving academic freedom and lawful international collaboration.
 - d. Identify, assess, and mitigate risks associated with foreign interference, undue foreign influence, unauthorized access, theft, diversion, misuse, or disclosure of research-related information or resources.
 - e. Address risks associated with foreign adversary nations, foreign entities, and other activities that may present research security concerns.
 - f. Support compliance with federal, state, sponsor, contractual, and institutional requirements related to research security.

3. Implementation

- The University shall establish procedures, standards, training requirements, review processes, disclosures, certifications, and other compliance measures necessary to implement this policy.

Implementation measures shall address:

- Research security training;
- Disclosure and transparency requirements;
- Cybersecurity;
- Foreign travel security;
- Insider threat awareness;
- Export controls;
- International collaborations;
- Research risk management; and
- Other research security requirements established by law, regulation, sponsors, or the University.

4. Reporting and Compliance

- The University shall maintain processes for reporting, reviewing, and addressing research security concerns and for monitoring compliance with this policy and related procedures.

University personnel are expected to comply with applicable research security requirements and to cooperate with reasonable institutional efforts to assess and manage research security risks.

5. Review and Continuous Improvement

- The Office of Research Compliance shall review this policy and related procedures at least once annually and make revisions as necessary to address changes in law, regulation, sponsor requirements, emerging threats, or institutional needs.

6. Noncompliance

- Failure to comply with this policy or related procedures may result in corrective or disciplinary action consistent with applicable University policies, sponsor requirements, and law.

Related Information*

[Conflict of Interest in Sponsored Projects \(https://in.nau.edu/university-policy-library/conflict-of-interest-sponsored-projects/\)](https://in.nau.edu/university-policy-library/conflict-of-interest-sponsored-projects/)

[Information Security Awareness Training Policy \(https://in.nau.edu/university-policy-library/information-security-awareness-training/\)](https://in.nau.edu/university-policy-library/information-security-awareness-training/)

[Intellectual Property Policy \(https://in.nau.edu/university-policy-library/intellectual-property/\)](https://in.nau.edu/university-policy-library/intellectual-property/)

[International Travel Policy \(https://in.nau.edu/university-policy-library/wp-content/uploads/sites/395/Travel-550.pdf\)](https://in.nau.edu/university-policy-library/wp-content/uploads/sites/395/Travel-550.pdf)

[Participation in Foreign Talent Recruitment Programs \(https://in.nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs/\)](https://in.nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs/)

[Export Control Program \(https://in.nau.edu/research/research-compliance/export-control/\)](https://in.nau.edu/research/research-compliance/export-control/)

Policy History*

09/11/2026: Interim policy approved.

*Related Information and Policy History are solely for the user's convenience and are not part of the official University policy.

APPENDIX B-6: NORTHERN ARIZONA UNIVERSITY — Exhibit 2: Participation in Foreign Talent Recruitment Programs

EXHIBIT 2

	Responsible Executive: Vice President for Research	
	Responsible Office: Office of Research Compliance	
	Effective Date: 08/08/2024	Last Revised: n/a
	Policy Title: Participation in Foreign Talent Recruitment Programs	

Purpose

Northern Arizona University encourages international collaborations that are mutually beneficial and characterized by academic freedom, open and reciprocal exchange of information, transparency, and integrity. To comply with federal law and regulations that require Covered Individuals to disclose participation in Foreign Talent Recruitment Programs (FTRP) and prohibit participation in Malign FTRPs, the University promulgates this policy.

Definitions

Covered Individual: Anyone, including faculty, staff, students, and subrecipient awardees, who a) contributes significantly to the design and/or execution of a research and development project that is, or if selected for award would be, funded by a Federal or non-federal sponsor, and b) is designated as key or senior personnel for the proposed research project.

Foreign Talent Recruitment Program (FTRP): Any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.¹

Malign Foreign Talent Recruitment Program:

- (A) Any program, position, or activity that includes compensation in the form of cash, in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration directly provided by a foreign country at any level

¹ For a list of permissible international collaboration activities that do not meet the definition of FTRP, and therefore do not require disclosure under this policy, please see the [FAQ section](#) on the policy website.

(national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to the targeted individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue, in exchange for the individual participating in any of the following activities:

1. engaging in the unauthorized transfer or intellectual property, materials, data products, or other nonpublic information owned by a United States entity or developed with a Federal research and development award to the government of a foreign country or an entity based in, funded by, or affiliated with a foreign country regardless of whether that government or entity provided support for the development of the intellectual property, materials, or data products;
2. being required to recruit trainees or researchers to enroll in such program, position, or activity;
3. establishing a laboratory or company, accepting a faculty position, or undertaking any other employment or appointment in a foreign country or with an entity based in, funded by, or affiliated with a foreign country if such activities are in violation of the standard terms and conditions of a Federal research and development award;
4. being unable to terminate the Foreign Talent Recruitment Program contract or agreement except in extraordinary circumstances;
5. through funding or effort related to the Foreign Talent Recruitment Program, being limited in the capacity to carry out a research and development award or required to engage in work that would result in substantial overlap or duplication with a federal research and development award;
6. being required to apply for and successfully receive funding from the sponsoring foreign government's funding agencies with the sponsoring foreign organization as the recipient;
7. being required to omit acknowledgment of the recipient institution with which the individual is affiliated, or the Federal research agency sponsoring the research and development award, contrary to the institutional policies or standard terms and conditions of the Federal research and development award;
8. being required to not disclose to the Federal research agency or employing institution the participation of such individual in such program, position, or activity; or
9. having a conflict of interest or conflict of commitment contrary to the standard terms and conditions of the Federal research and development award; and

(B) a program that is sponsored by:

1. a foreign country of concern or an entity based in a foreign country of concern, whether or not directly sponsored by the foreign country of concern;²
2. an academic institution on the list³ developed under section 1286(c)(8) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 4001 note: Public Law 115-232); or
3. a Foreign Talent Recruitment Program on the list⁴ developed under section 1286(c)(9) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. 4001 note: Public Law 115-232).

Policy

A. Foreign Talent Recruitment Program Participation and Disclosure

1. NAU employees must seek prior written approval from their supervisor, Chair, and/or Dean before participating in a FTRP to ensure participation in the FTRP does not interfere with the Covered Individual's University responsibilities.
2. All Covered Individuals, including non-employee Covered Individuals (e.g., non-employee students and sponsored project subrecipients), must disclose current participation in any FTRP in Cayuse prior to proposal submission. The Principal Investigator shall coordinate disclosure by all Covered Individuals on the project. The Office of Sponsored Projects shall review the disclosures to ensure compliance with this Policy and applicable sponsor regulations.
3. Covered Individuals must disclose all participation in FTRPs to any Federal sponsoring agency to which they submit a proposal for research and development funding, using the Biographical Sketch and Current and Pending Support (Other) Forms or other disclosure mechanism as specified by the Federal research agency in question.

B. Malign Foreign Talent Recruitment Program Prohibition

1. Covered Individuals are prohibited from participating in any Malign Foreign Talent Recruitment Program (MFTRP).
2. Covered Individuals applying for any research funding, regardless of sponsor, must certify in Cayuse at time of proposal that they are not participating in a MFTRP. When applying for or participating in Federally-funded research, Covered

² The term "foreign country of concern" means any country so designated by the Department of State under 42 US Code § 19221.

³ For the list of academic institutions and Foreign Talent Programs developed under this act, see: <https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/1286%20List.pdf>

⁴ Ibid.

Individuals must also certify in their Biographical Sketch and Current and Pending Support (Other) Forms at time of proposal, and annually for the duration of the award, that they are not participating in a MFTRP.

Compliance

All Covered Individuals must comply with this Policy. In the event of non-compliance, potential sanctions may include, but are not limited to:

- A. Additional training and/or oversight,
- B. Suspension of the Covered Individual's funding and/or research privileges, and
- C. Discipline, up to and including termination of employment or University affiliation.

Related Information*

[FY2023 List of academic institutions and Foreign Talent Recruitment Programs developed under paragraphs \(8\) and \(9\) of Section 1286\(c\) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 \(10 U.S.C. 4001 note: Public Law 115-232\)](#)

[China Defense Research Institutions Tracker](#)

[Creating Helpful Incentives to Produce Semiconductors \(CHIPS\) and Science Act of 2022](#)

[Office of Science and Technology Policy \(OSTP\) Guidance](#)

[Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education](#) (Department of Defense)

[Guidance for Implementing National Security Presidential Memorandum 33 \(NSPM-33\) on National Security Strategy for United States Government-Supported Research and Development](#)

[National Institutes of Health Dear Colleagues Letter, August 20, 2018](#)

Policy History*

8/8/2024: Policy adopted.

* Related Information and Policy History are solely for the user's convenience and are not part of the official university policy.

APPENDIX B-7: NORTHERN ARIZONA UNIVERSITY — Exhibit 3: Significant Financial Interest and Foreign Talent Recruitment Program Disclosure Form

EXHIBIT 3

NORTHERN
ARIZONA
UNIVERSITY

Office of
Sponsored
Projects

SIGNIFICANT FINANCIAL INTEREST AND FOREIGN TALENT RECRUITMENT PROGRAM DISCLOSURE FORM

Northern Arizona University is committed to promoting objectivity, openness, and transparency in research and ensuring institutional compliance with applicable federal regulations and non-federal agency guidelines. Accordingly, the Office of Sponsored Projects (OSP) requires all Investigators¹ to submit annually and prior to the submission of sponsored projects proposals the following: 1) a significant financial interest (SFI) disclosure,² 2) a Foreign Talent Recruitment Program (FTRP) disclosure, and 3) certification that they are not party to a Malign Foreign Talent Recruitment Program.³ Completion and submission of this form fulfills these disclosure and certification requirements. NAU's goal is to support Investigators in protecting the integrity of their research and ensuring the design, conduct, and reporting of sponsored projects activities will not be biased by an Investigator's SFIs or subject to undue influence by foreign entities.

Federal and other applicable agency proposals/applications **will not be submitted until all required disclosure certifications have been completed** by all Investigators and submitted to OSP. Compliance with this requirement is a prerequisite for acceptance by Northern Arizona University of a federal or other applicable agency sponsored grant or contract award.

DISCLOSURE INSTRUCTIONS

1. All Investigators must, at a minimum, complete and certify Section I of the disclosure form below.

Sections II and III must also be completed when the following criteria are met:

- a. If any answer to the questions in Section I.A regarding significant financial interests is "yes", then complete and certify Section II.
- b. If the answer to the question in Section I.B regarding participation in Foreign Talent Recruitment Programs is "yes," then complete and certify Section III.

2. Submit the completed disclosure certification to the assigned Pre-Award Research Administrator in OSP.

3. If there is a material change in an Investigator's previously disclosed significant financial interests or FTRP participation, a revised disclosure certification must be completed and filed with OSP **within thirty (30) days** of the change.

All disclosures will be reviewed and handled according to NAU's Conflicts of Interest in Sponsored Projects Policy and Participation in Foreign Talent Recruitment Programs Policy.

All NAU Investigators seeking external sponsored funding from a Federal agency and other applicable agencies are required to complete this form before a proposal can be submitted.

Questions concerning sponsored projects or research-related disclosures should be addressed to: Thomas Champagne, Associate Vice President for Research Thomas.Champagne@nau.edu

¹ "Investigator" means any individual who is responsible for the design, conduct, or reporting of a sponsored project, or a proposal for such funding. This definition is not limited to those titled or budgeted as Principal Investigator (PI), co-investigator, or key personnel, and may include postdoctoral fellows, senior scientists, or graduate students. This definition may also include collaborators or consultants when applicable.

² See COI in Sponsored Projects Policy: <https://nau.edu/university-policy-library/conflict-of-interest-sponsored-projects/>

³ See Participation in Foreign Talent Recruitment Programs Policy: <https://nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs/>

SECTION 1b: Foreign Talent Recruitment Programs

Yes ☐ No ☐

Are you currently participating in, or party to, a Foreign Talent Recruitment Program?

A Foreign Talent Recruitment Program (FTRP) is any program, position, or activity that involves compensation of any kind, including but not limited to:

- Cash,
- In-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration
- That is directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.

**Some common international collaboration activities do not qualify as an FTRP⁵ and therefore do not need to be disclosed here.*

**Participation in a FTRP may be acceptable as long as the arrangement is approved by the individual's supervisor, Chair and/or Dean and the FTRP does not meet the definition of a Malign FTRP.⁶*

If you answered "YES" to **any** question in Section 1.a above regarding SFIs, please complete **Section II** below for **every** organization with which you have a Significant Financial Interest.

If you answered "YES" to the question in Section 1.b above regarding FTRPs, please complete **Section III** below for each FTRP you are a party to.

Section 1c: Investigator Certification

I have read and understand Northern Arizona University's Conflict of Interest in Sponsored Projects policy and Participation in Foreign Talent Recruitment Programs policy.

I have read, understand, and completed all required sections of this Significant Financial Interest and Foreign Talent Recruitment Program Disclosure form and agree to file a new or updated form a) annually and within 30 days if answers to any question above have changed, b) when I have a new Significant Financial Interest related to the project title referenced above, and/or c) if I initiate participation in a previously undisclosed FTRP.

I certify that the answers to the declaration above are accurate and truthful to the best of my knowledge. I also certify that, at the time of submission of this form, I am not participating in, or party to, a Malign Foreign Talent Recruitment Program.⁷

Investigator Name: _____ **Date:** _____

Investigator Signature: _____

⁵ See Participation in Foreign Talent Recruitment Programs Policy FAQs <https://nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs>

⁶ For a definition of "Malign FTRP" see the Participation in Foreign Talent Recruitment Programs Policy. <https://nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs>

⁷ Ibid.

Section III: Disclosure of Participation in Foreign Talent Recruitment Programs

Complete this form only if you answered "YES" to any questions in Section I.B

Complete and submit one Section III form for each FTRP you have to disclose

NAU encourages international collaborations that are mutually beneficial and characterized by academic freedom, open and reciprocal exchange of information, transparency, and integrity. To comply with federal law and regulations, NAU requires⁸ all Senior/Key Personnel ("Covered Individuals") to disclose any participation in a FTRP⁹ and certify that they are not party to a Malign FTRP prior to proposal submission and annually thereafter for the duration of the award.

1. Investigator Name: _____

2. Name of Foreign Talent Recruitment Program (FTRP): _____

3. Name of Foreign Country Associated with the FTRP: _____

4. FTRP Contract/Participation Start Date: _____ Anticipated End Date: _____

5. Type of compensation received in exchange for participation in the FTRP (check all that apply)

☐ Cash/Salary

☐ In-Kind Compensation of any kind (including but not limited to: lab space, equipment, foreign travel, honorary degrees, research funding, promised future compensation or employment)

6. If you are receiving in-kind compensation for your participation in the FTRP, please describe the nature of the compensation:

7. Please describe the time commitment required for you to participate in the FTRP:

⁸ See Participation in Foreign Talent Recruitment Programs Policy: <https://nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs/>

⁹ For a list of international collaboration activities that do not qualify as an FTRP, and therefore do not need to be disclosed, see the Participation in Foreign Talent Recruitment Programs FAQ page. <https://nau.edu/wp-content/uploads/sites/26/FAQs-Participation-in-Foreign-Talent-Recruitment-Programs.pdf>

8. Are you required to engage in any particular activities or provide research results and/or Intellectual Property as a condition of your participation in the FTRP?

☐ Yes ☐ No

If yes, please describe:

9. Do you have written approval from your supervisor, Chair, and/or Dean to participate in the FTRP?

☐ Yes ☐ No

.....

I certify that the answers to the questions above are accurate and truthful to the best of my knowledge.

Investigator Signature: _____ **Date:** _____

Please forward the completed form to your assigned Pre-Award Research Administrator (PRA). Do not upload this form in Cayuse.

APPENDIX B-8: NORTHERN ARIZONA UNIVERSITY — Exhibit 4: Federal Common Form Disclosure Instructions and Certification Language

NAU 2026 Research Security Report to ABOR

EXHIBIT 4

Federal Common Form Disclosure Instructions and Certification Language

Screenshot of Common Biographical Sketch Form Disclosure Instructions

Consistent with NSPM-33, individuals are required to disclose contracts associated with participation in programs sponsored by foreign governments, instrumentalities, or entities, including [foreign government-sponsored talent recruitment programs](#). Further, if an individual receives direct or indirect support that is funded by a foreign government-sponsored talent recruitment program, even where the support is provided through an intermediary and does not require membership in the foreign government-sponsored talent recruitment program, that support must be disclosed. Individuals must also report other foreign government-sponsored or affiliated activities. In accordance with 42 U.S.C. § 19232, individuals are prohibited from being a party in a [malign foreign talent recruitment program](#).

A table entitled, *NSPM-33 Implementation Guidance Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support* ^[1] has been created to provide helpful reference information regarding pre-award and post-award disclosures. The table includes the types of activities to be reported, where such activities must be reported in the proposal, as well as when updates are required in the proposal and award lifecycle. A final column identifies activities that are not required to be reported.

Individuals are reminded not to submit any personal information in the biographical sketch. This includes items such as: home address; home telephone, fax, or cell phone numbers; home e-mail address; driver's license number; marital status; personal hobbies; and the like. Such personal information is not appropriate for the biographical sketch and is not relevant to the merits of the proposal. NSF is not responsible or in any way liable for the release of such material. See also Chapter III.H.

Screenshot of Common Biographical Sketch Form Certification Language

CertificationVIEW C

Each senior/key person is required to complete the following certifications regarding the information provided in their Biographical Sketch:

I certify that the information provided is current, accurate, and complete. This includes, but is not limited to, information related to current, pending, and other support (both foreign and domestic) as defined in 42 U.S.C. § 6605.

In accordance with Section 10632 of the CHIPS and Science Act of 2022 (42 U.S.C. § 19232), each individual identified as a senior/key person must certify that they are not a party to a malign foreign talent recruitment program.

Research Security Training Requirement for Federal Award Personnel: In accordance with Section 10634 of the CHIPS and Science Act of 2022 (42 U.S.C. § 19234), each individual identified as a senior/key person must certify that they have completed the requisite research security training that meets the requirements specified in Item 2 of Important Notice No. 149 within 12 months prior to proposal submission.

APPENDIX B-9: NORTHERN ARIZONA UNIVERSITY — Exhibit 5: NAU Subrecipient Commitment Form



EXHIBIT 5

7. Participation in Foreign Talent Recruitment Programs - Mandatory Certification (only check the box below most relevant to your institution)

- ☐ Subrecipient has an active and enforced policy addressing federal requirements to disclose participation in Foreign Talent Recruitment Programs (FTRP) and prohibiting participation in Malign FTRPs for covered individuals on federal awards.
- ☐ Subrecipient does not have an active or enforced FTRP policy and agrees to adopt NAU's policy "Participation in Foreign Talent Recruitment Programs."

If you do not have an active or enforced FTRP policy, answer the following:

Are any of the 'Key Personnel' listed on this project participating in, or party to, a FTRP?

A FTRP is any program, position, or activity that involves compensation of any kind, including but not limited to:

- cash;
- in-kind compensation, including research funding, promised future compensation, complimentary foreign travel, things of non de minimis value, honorific titles, career advancement opportunities, or other types of remuneration or consideration,
- that is directly provided by a foreign country at any level (national, provincial, or local) or their designee, or an entity based in, funded by, or affiliated with a foreign country, whether or not directly sponsored by the foreign country, to an individual, whether directly or indirectly stated in the arrangement, contract, or other documentation at issue.

*International collaboration activities that involve open and reciprocal exchange of scientific information are not generally considered FTRPs, and do not need to be disclosed. For the complete official definition of a FTRP and a list of common international collaboration activities that do not qualify as FTRPs, see page 3 of the OSTP Memo Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs.

Yes ☐ No ☐

Are any of the 'Key Personnel' listed on this project participating in, or party to, a Malign FTRP?

A Malign FTRP is any program that a) meets the definition of an FTRP, b) requires the individual participant to engage in activities that are antithetical to the principles of integrity, transparency, and open science, and c) is funded or supported by a foreign country of concern as designated by the U.S. Department of State. As of 2024 there are four countries of concern: the People's Republic of China, Russian Federation, the Democratic People's Republic of Korea (North Korea), and the Islamic Republic of Iran.

*For the complete official definition of "Malign FTRPs" and a list of activities that qualify as malign, see page 5 of the OSTP Memo Guidelines for Federal Research Agencies Regarding Foreign Talent Recruitment Programs.

Yes ☐ No ☐

APPENDIX B-10: NORTHERN ARIZONA UNIVERSITY — Exhibit 6: Data Classification and Handling

EXHIBIT 6



Policy Owner: Chief Information Officer
Responsible Office: Information Security Services
Origination Date: February 13, 2018
Last Revised: February 11, 2026

DATA CLASSIFICATION AND HANDLING

POLICY SUMMARY

Northern Arizona University owns or controls, and acts as custodian for, a broad array of information, including information protected by law. Because the unauthorized release of protected information can inflict substantial harm, maintaining the integrity of this data and the information systems where it is stored is a fundamental obligation. This policy establishes a data classification structure and data handling protocols to support this crucial task. All units and University Community Members that interact with data must comply with the requirements of this policy.

REASON FOR THIS POLICY

Clear standards, requirements, and protocols for the identification, classification, and internal handling of University information are an important contributor to the goal of maintaining its integrity and availability.

ENTITIES AFFECTED BY THIS POLICY

- All units that handle or interact with University information or data
- External Data Use Committee
- Information Security Committee
- Information Security Services
- NAU Communications

WHO SHOULD KNOW THIS POLICY

- All University Community Members who interact with University information or data
- Chief Information Officer ("CIO")
- Chief Institutional Data Officer
- Data Stewards
- Data Governance Trustees
- Director, Information Security Services

DEFINITIONS

Access: the means or ability and permission to connect to, view, alter, obtain or distribute IT Resources.

Authorization: a set of rules that determines what an authenticated Digital Identity has access to, or what actions it is approved to perform.

Data Cookbook: an electronic library housing data element metadata and other information.

Data Steward: an official charged with controlling access to and properly curating University information or data.

Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University,

used to conduct University business, or connected to the University's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as "IT Resources."

System Administrators: University employees responsible for configuring, architecting, engineering, administering and maintaining University IT Resources for use by Authorized Users for authorized purposes.

Technicians: University employees who configure, maintain, or repair University IT Resources.

Unit: A Northern Arizona University campus, center, college, department, division, research facility, extended program or other official University organizational unit, its divisions, programs, senates, or associations[.]

University Community Member: all University faculty, staff, student employees, students, alumni, affiliates, contractors, consultants, agents, and volunteers wherever located.

POLICY

A. Data Identification and Classification

All units and University Community Members shall identify and classify University information or data using the definitions described herein. Data identification must include the information systems used to handle and store the data, and special care must be given to data classified as Sensitive or Highly Sensitive. All University information or data generated, processed, transmitted, or otherwise handled, regardless of how the data is stored, the media or systems used to process it, or the systems or methods by which it is accessed or distributed, must comply with the [Data Handling Protocols](#). Questions regarding data types and how best to protect them should be directed to the appropriate Data Steward, the Chief Institutional Data Officer, or Information Security Services.

Level 1 Public Data – Very Low Risk

Level 1 Public Data is generally publicly available and intended for public use. This information may be freely distributed to the general public, all Units, and University Community Members, as there is no concern of unauthorized disclosure with Public Data. Access controls are necessary, however, to help protect Public Data integrity. See the [Data Type Examples](#) tool for examples of Level 1 Public Data.

Level 2 Internal Data – Low Risk

Level 2 Internal Data is not generally available to the public or to parties unaffiliated with the University. Risk of disclosure and harm to the University or University Community Members is low, however, as little or no adverse effects on the University's operations, assets, reputation, financial position, privacy obligations, or the personal privacy of individuals could result. See the [Data Type Examples](#) tool for examples of Level 2 Internal Data.

Level 3 Sensitive Data – High Risk

Level 3 Sensitive Data is private information intended for restricted use within the University. Access to Sensitive Data is limited to protect its integrity and confidentiality. A high level of risk is associated with these data types and they must be protected from unintended or unauthorized disclosure, loss, or destruction. Unauthorized release of Sensitive Data could have substantial and costly negative effects to the University or to University Community Members. Unauthorized exposure or loss of Sensitive Data could contribute to fraud, identity theft, legal violations, and substantial reputational, financial, or operational damage. See the [Data Type Examples](#) tool for examples of Level 3 Sensitive Data.

Level 4 Highly Sensitive Data – Very High Risk

Level 4 Highly Sensitive Data is the most confidential and sensitive data possessed or controlled by the University. Level 4 Highly Sensitive Data must be protected with the highest levels of security that are reasonably attainable. Highly Sensitive Data is intended for extremely limited use consistent with substantial legal requirements for its protection and stewardship. Any unauthorized access, disclosure, compromise, loss, modification, or destruction of Highly Sensitive Data could result in severely negative impacts or damage to the

University, to University Community Members, or to independent entities that may have provided the data. As with Sensitive Data, the unauthorized exposure or loss of Highly Sensitive Data could cause or contribute to fraud, identity theft, financial loss, substantial reputational damage, and even physical endangerment that creates safety risks for individuals. For these reasons, the University prohibits the transmission of this data via electronic mail. See the *Data Type Examples* tool for examples of Level 4 Highly Sensitive Data.

Please note: contact the Office of the Vice President for Research with any inquiry regarding the classification or handling requirements for information or data related to research or External Data Use Agreements.

B. Data Sharing Requirements

Data from a given classification may only be shared with University Community Members who have completed the training necessary to be granted appropriate Access and Authorization to that data. If it is necessary to provide data to an individual without the appropriate clearance, the Data Steward, Data Trustee, or Chief Institutional Data Officer may approve the data sharing in advance and in writing, provided that the receiving official displays the requisite awareness of, commitment to, and ability to comply with the applicable Data Handling Protocols. The transmittal of data to any non-University third-party must be approved in advance and in writing by an authorized University official. All data requests will be reviewed by the appropriate University Unit or official prior to approval and must include an evaluation of appropriate data security controls. Research and service projects often involve data owned/controlled by both NAU and external partners. The handling of external research or service data by University officials must take place in accordance with any applicable Material Transfer Agreement, Data Use Agreement, or other agreement as outlined further in the [External Data Use Agreements](#) policy.

C. Data Handling Protocols

The CIO, or their designee, with the concurrence of the Chief Institutional Data Officer, shall establish, update, revise, and republish, as necessary and appropriate, a comprehensive set of protocols designed to maintain the integrity, security, confidentiality, control, and availability of the University's data and information systems. These *Data Handling Protocols* shall be based on the sensitive data type classifications established herein and shall promote data handling best practices and compliance with all applicable laws, regulations, policies, and contractual or licensing requirements. Data element metadata, including the data element's sensitivity classification, shall be recorded and maintained in the [Data Cookbook](#) information system of record. These protocols shall cover, at a minimum, the following:

1. Access Controls
2. Backup/Disaster Recovery
3. Copying/Printing
4. Data Destruction and Disposal
5. Electronic Mail
6. Network Security
7. Physical Security
8. Remote Administration
9. Storage
10. System Security
11. Training
12. Transmission

D. Applicability and Implementation

This policy governs all information systems and devices utilized for accessing, reviewing, or storing University data. This policy applies to all campuses, Units, researchers, and University Community Members wherever located.

On an annual basis, all University data must be reviewed, classified, and have appropriate data classification handling protocols implemented by the Data Steward or responsible data owner. All Units, researchers, and University Community Members will use the sensitive data classifications established herein to determine the appropriate data handling requirements as outlined in the *Data Handling Protocols*.

E. Mandatory Reporting

All University Community Members are obligated to immediately report any IT security threat suspected or actual release or breach of Sensitive Data or Highly Sensitive Data. **Dial 928-523-3335 to make a report.** In collaboration with appropriate University stakeholders, Information Security Services is responsible for notifying all affected and responsible parties. The CIO, or their designee, will assemble an incident response team to investigate, preserve evidence, mitigate the situation, and analyze and report on the event. If health or safety may be a concern, the reporting party or Information Security Services shall immediately notify the Northern Arizona University Police Department and any other external entity or governmental agency as appropriate.

F. Public Records Requests

Data classification in accordance with this policy does not alter public information access requirements or the University's need to fulfil other legal obligations that may require the disclosure or release of information from any of the classification levels established under this policy. Questions regarding public records requests should be directed to NAU Communications or the Office of General Counsel.

G. Compliance and Enforcement

As outlined in the University's *Information Security* policy, when necessary to protect the integrity or security of its IT Resources or information systems and the University Information they contain, the University may suspend Access to its networks or devices and may examine any user account. At the discretion of the CIO, or their designee, enforcement of this and related IT policies may include the removal of devices or systems from the University's information networks until compliance with applicable requirements is achieved. Violations by a University Community Member of the duty and responsibility to protect the University's data, IT Resources, and information systems in accordance with this and other applicable policies, standards, or requirements may also result in denial of access to University Information and/or University IT Resources or the temporary or permanent revocation of Access privileges. Individuals who violate this policy are subject to disciplinary action under applicable Arizona Board of Regents and University conduct policies up to and including expulsion or termination and possible civil liability or criminal prosecution. In cases where full compliance with the requirements of this policy may not be immediately achievable, the Unit's leadership must consult with Information Security Services to develop a plan for achieving compliance as soon as possible.

RESPONSIBILITIES

Chief Institutional Data Officer: in collaboration with the Chief Information Officer, update as necessary and appropriate the University's *Data Handling Protocols* and train the University community in proper use of the Data Cookbook.

Chief Information Officer: in collaboration with the Chief Institutional Data Officer, update as necessary and appropriate and support the Director of Information Security Services with enforcement of this policy and the *Data Handling Protocols*.

Data Stewards: evaluate requests for data or information system access to determine if request is appropriate and justified based upon an employee's role and responsibilities.

Director, Information Security Services: develop and implement security policies, procedures, protocols, and standards in support of this policy and the Information Security Program; is the primary enforcer of this policy and the *Data Handling Protocols*; serve as chair of the Information Security Committee.

External Data Use Committee: assist all units and University Community Members—primarily faculty members and research administrators—in initiating, negotiating, and maintaining compliance with External Data Use Agreements as established in the *External Data Use Agreements* policy; work to ensure that the handling of external research or service data takes place in accordance with applicable Data Use Agreements, as outlined further in the *External Data Use Agreements* policy.

NAU Communications: coordinate the University's response to public information requests that implicate Level 2, 3, or 4 data with affected units as appropriate.

System Administrators and Technicians: maintain the privacy and confidentiality of sensitive information seen or obtained in the normal course of their work, and report suspected or actual violations of the University IT policies to the appropriate University authority.

University Community Members: ensure the effective implementation and enforcement of this policy within their respective areas of responsibility or jurisdiction.

PROCEDURES

There are no procedures associated with this policy.

RELATED INFORMATION

Forms or Tools

[Data Handling Protocols](#)

[Data Type Examples](#)

[Northern Arizona University Data Cookbook](#)

Cross-References

[Appropriate Use of Information Technology Resources](#)

[Electronic Mail](#)

[External Data Use Agreements](#)

[Information Security](#)

Sources

[Arizona Board of Regents Policy 9-201](#)

[Arizona Board of Regents Policy 9-202](#)

[Arizona Revised Statutes § 44-1373. Restricted use of personal identifying information](#)

[Arizona Revised Statutes §15-1823. Identification numbers; social security numbers](#)

[Family Educational Rights and Privacy Act \(20 U.S.C. § 1232g; 34 CFR Part 99\)](#)

[Health Insurance Portability and Accountability Act of 1996 \(Public Law 104-191\)](#)

[Gramm-Leach-Bliley Act \(Public Law 106-102\)](#)

APPENDIX

None.

EXHIBIT 7



Responsible Executive:	Senior Vice President of University Finance and Business Services
Responsible Office:	Comptroller
Effective Date:	07.01.2022
Last Revised:	08.22.2022

TRV: 550 – INTERNATIONAL TRAVEL

REASON FOR THIS POLICY

Clear standards for individuals traveling internationally on University business.

ENTITIES AFFECTED BY THIS POLICY

- All units and departments that may authorize University business travel.
- Comptroller's Office
- Reimbursement Processing Support Unit

WHO SHOULD KNOW THIS POLICY

- Individuals who travel for University business
- Supervisors of individuals who travel for University business
- Local Fiscal Oversight (LFO) designees of individuals who travel for University business

POLICY

A. Applicability

This policy applies to all University community members, including faculty, staff, students, agents, and Volunteers who travel for the purpose of conducting University business, which for purposes of this policy excludes normal or everyday personal transportation to and from the workplace.

For the purposes of travel policy, all references to "event" should be taken to include the following list: meeting, colloquium, convention, symposium, seminar, assembly, gathering, convocation, course, class, workshop, lecture, forum, event, training, summit, research travel or similar activity held by any association or organization involving discussion, research, or the exchange or dissemination of information.

B. General Requirements and Prohibitions

1. International, and any travel outside of the contiguous U.S., including Alaska and Hawaii, is to follow standard university travel policy with the exceptions and additional guidance that is outlined in this section.
2. All international student travel that is credit bearing, must be approved and registered through the Center for International Education's (CIE) approved portal, [Education Abroad](#).
3. A traveler may not claim reimbursement for more than three meals in any single calendar day or (24) consecutive hours.

Reimbursement for meals to destinations outside the contiguous U.S., including Alaska and Hawaii, may not exceed the Department of Defense (DoD) international rates.

- a. The exact reimbursement rate is determined by the country and city the traveler will spend the night, not necessarily where the meal was purchased or will be consumed. Exception is the day of return; meal rate is the location the traveler last stayed overnight.

- b. If a traveler's exact city is not listed, then the default rate for that country applies.
 - c. To determine the reimbursement limitations on meals and incidentals in Alaska, Hawaii, and out-of-country locations, add the DoD *Local Meal Rate* (not the Proportional Meal Rate) to the *Local Incidental Rate* and subtract ten dollars (\$10).
- 4. Partial day meal and incidental expense (M&IE) reimbursements are calculated by percentage of the total day's reimbursement for:
 - Breakfast 20%
 - Lunch 25%
 - Dinner 55%
- 5. Lodging costs for destinations outside the contiguous U.S., including Alaska and Hawaii, exclusive of taxes and other mandatory service charges, may not exceed the maximum lodging rate designated by the U.S. Department of Defense (DoD) International Rates. Exceeding maximum lodging rates when unavoidable, must be justified with a business purpose detailing why the accommodations were selected and a Justification for Exception to Policy must be submitted to the Comptroller's Office prior to booking travel. Normally, the individual booking the travel, the traveler, or someone else familiar with the reasons for the accommodation should submit the justification.
- 6. All travel claims will be submitted in U.S. dollars. If foreign currency conversion is required, use the actual days exchange rate listed on the purchase receipt or, calculate the exchange rate using one of the below online currency converters. The conversion rate must be calculated using the calendar date the purchase was made. A printout, .PDF version, of the currency conversion must be attached to the Expense Claim.
 - <http://www.xe.com/>
 - <http://www.oanda.com/converter>
- 7. Receipts for reimbursable travel expenses must be translated into English prior to submission for claim processing. All details of the transaction must be translated including vendor name, date, amount, etc. A printout, .PDF version, of the translated receipt must be attached to the Expense Claim.
<https://translate.google.com/>
- 8. Traveling to Countries with a Trade Sanction: For any person traveling to a country with a trade sanction, there is no coverage if the person conducts an illegal or sanctioned activity.

A list of sanctioned countries and summaries concerning travel can be viewed on the website of [The Office of Foreign Assets Control](#). The OFAC website includes the following introduction:
 - a. The Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations and international narcotics traffickers based on U.S. foreign policy and national security goals. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.
- 9. If a person plans travel to a trade sanctioned country, there is a high likelihood that country may also have other high travel risks, political or social unrest, or war. Such countries are subject to change, and a current list is maintained by [NAU Risk Management Services](#).

RESPONSIBILITIES

Traveler: agrees to and will adhere to all university travel policies, will always seek pre-trip authorization and approval from department leadership to expend funds for travel, and will provide all policy required and requested documentation to the travel specialist pre and post travel.

Departmental Supervisors: reviews business travel requests of direct report employees and Volunteers as required by travel policy and verifies business need.

Local Fiscal Oversight Designee: reviews all travel requests and verifies funding source (speedchart,

sub_dept, account codes) and determines and communicates any funding caps or limitations.

Departmental Leadership: ensure that only properly qualified and authorized individuals are allowed to travel on official University business for University programs and activities under their direction and control.

Reimbursement Processing Support Unit Staff: initiates and completes all travel expense claims and reimbursement via Expense Report or Check Request; and assists with booking travel upon request.

PROCEDURES

[Justification for Exception to Policy](#)

RELATED INFORMATION

Forms or Tools

[Annual Travel Certification \(ATC\)](#)

[Authorized Driver](#)

[Cost Comparison How-To](#)

[Currency Converters](#) - <http://www.xe.com/> OR <http://www.oanda.com/converter>

[Employee Service Center \(ESC\)](#)

[Enterprise Car Rental – NAU Contract](#)

[Google Translate – documents and receipts](#)

[Long-Term Travel Case Submission Business Process & Blanket Travel Approval Memo](#)

[Mobile Phone App: ServiceNow! – NAU Employee Service Center](#)

[NAU Mileage Log](#)

[Out-of-State Request for Multiple Representation](#)

[Current Arizona State Reimbursement Rates \(SAAM\) – Lodging & Meals Schedule](#)

[US Department of Defense \(DoD\) Reimbursement Rates – Lodging & Meals Schedule](#)

[Travel Case Submission How-To - transcript](#)

[Travel Case Submission Quick Reference](#)

[Travel Advance/Zelle Workbook](#)

[Traveler Itinerary - template](#)

Cross-References

[Comptroller's Office](#)

[NAU Risk Management](#)

[NAU Transit Services – Fleet Services](#)

[The Office of Foreign Assets Control \(OFAC\)](#)

Sources

[State of Arizona Travel Policy](#)

[Arizona Board of Regents Travel Policy](#)

[Arizona Revised Statutes § 38-621 – 38-627](#)

[Fly America Act](#)

APPENDIX

None.

APPENDIX B-12: NORTHERN ARIZONA UNIVERSITY — Exhibit 8: Travel Security Training Content

NAU 2026 Research Security Report to ABOR

EXHIBIT 8

Screenshot of International Travel Content within NAU’s Information Security & Awareness Training Course



International Travel with University Equipment

International travel with University equipment requires extra preparation.

Before traveling outside the United States, remember that devices, data, and software may be subject to export control laws and foreign regulations. In some countries, laptops and their contents may be searched or seized, and U.S. Customs may also inspect devices when you return.



[Video Transcript](#)

Reduce Risk Before and During Travel

If you are taking NAU-owned equipment abroad, reduce risk before and during travel.

Before you leave:

- Keep only the data and applications you need
- Make sure the device is fully updated
- Back up your information
- Store University data on secure network drives whenever possible instead of keeping it directly on the device
- Contact the ITS Service Desk if you are unsure how to prepare

While traveling:

- Keep devices with you
- Assume networks may be monitored
- Avoid accessing University systems without the NAU VPN
- Avoid unknown USB devices
- Avoid public charging stations
- Be aware of your surroundings when entering passwords

If a University device is lost or stolen, notify NAU immediately.

APPENDIX B-13: NORTHERN ARIZONA UNIVERSITY — Exhibit 9: Information Security Awareness Training

EXHIBIT 9



Policy Owner: Chief Information Officer
Responsible Office: Information Security Services
Origination Date: June 1, 2018
Last Revised: February 11, 2026

INFORMATION SECURITY AWARENESS TRAINING

POLICY SUMMARY

Northern Arizona University owns or controls, or acts as custodian for, a broad array of information, including Sensitive Information protected by law. To safeguard this University Information, this policy establishes information security awareness training requirements for all University employees (including student employees) and all other persons authorized to access this material.

REASON FOR THIS POLICY

All authorized users should gain a broad understanding of information security threats, risks, and best practices in order to assist the University in protecting the confidentiality, integrity, and availability of University Information and the University's Information Technology ("IT") Resources.

ENTITIES AFFECTED BY THIS POLICY

- All units that interact with University Information or IT Resources
- External entities authorized to access University Information or IT Resources
- Information Security Services

WHO SHOULD KNOW THIS POLICY

- All persons authorized to access University Information or IT Resources
- Chief Information Officer ("CIO")
- Director, Information Security Services

DEFINITIONS

Authorized User: a person who has truthfully identified themselves and their purposes and to whom the University has granted access credentials to permit their Authorized Use of the University's IT Resources, or a person accessing the University's public information services through a network connection open to the general public, for legitimate activity or purposes that further the University's mission.

Information Technology ("IT") Resource: any computer, server, communication or mobile device, or electronic data, data storage, transmission or control device that is owned and/or operated by the University, used to conduct University business, or connected to the University's IT networking or communication systems regardless of ownership, location, or access method. These resources are referred to herein as "IT Resources."

Phishing: the fraudulent and malicious practice of sending electronic communications purporting to be from a reputable source in hopes of tricking or inducing the recipient to reveal sensitive or confidential personal information, such as passwords or credit card numbers.

Sensitive Information: all information that should remain private or confidential as designated by the University or as required by law, including, but not limited to, educational and student conduct records, social security numbers, credit card or banking information, regulated research data, and health care provider records.

Sensitive Information includes, but is not limited to, Level 3 – Sensitive Data and Level 4 – Highly Sensitive Data as defined in the University's *Data Handling and Classification* policy.

University Information: all written or verbal data or information that the University or its employees, students, or designated affiliates or agents collect, possess, or have access to regardless of the medium on which it is stored or its format.

POLICY

A. Information Security Awareness Training Program

Acting through the Director of Information Security Services, the CIO, or their designee, will establish and maintain an information security awareness training program that will include testing to assess and help ensure basic knowledge and comprehension of information security issues. To demonstrate basic competency in information security best practices, all faculty, staff, and other Authorized Users of University Information or IT Resources must complete this training as part of the onboarding process, annually thereafter, or as may be required by the CIO, or their designee. Information Security Services will:

- Develop or acquire appropriate information security training content and test materials
- Update and revise training content, test materials, and delivery methods annually to reflect current threats and emerging information security best practices
- Ensure a mechanism exists for feedback regarding the content and efficacy of the training program
- Track and record testing completion rates and other useful program statistics
- Report completion rates and follow-up with units not completing the mandatory training

B. Learning Objectives

The basic information security awareness training for all employees or agents will include:

- General information security awareness best practices
- Mobile device and wireless networking best practices
- Data confidentiality, integrity, and availability
- University IT Resource appropriate use and information security policies
- Individual employee information security roles and responsibilities
- Data classification and handling requirements, including the need to protect of Sensitive Information
- How to identify suspicious or risky activities
- Cybersecurity threat reporting requirements
- Insider threat detection and reporting
- IT security terms and definitions
- Authentication awareness and best practices

Additionally, role-based security training will be provided by subject-matter experts to employees and affiliates having unique, specific, or highly technical security responsibilities (such as roles involving financial transactions, health record processing, payment card transactions, and secure software development for web developers) as may be deemed appropriate for their roles or level of expertise. Students will have the option, but not the requirement, to complete the information security awareness training program.

C. Phishing

Employees whose accounts are found to be compromised by a successful Phishing attack may be required to retake and pass a specific Phishing security awareness training module.

Phishing simulations may be conducted up to 4 times per year or additionally at the direction of the CIO or their delegate.

D. Compliance

System access privileges may be revoked for employees or other Authorized Users (for whom training is required) who do not complete required information security awareness training within specified timelines, which shall not exceed thirty (30) days past onboarding, annually recurring, or other established training deadlines.

RESPONSIBILITIES

Chief Information Officer: ensure that appropriate and auditable information security awareness, training, and education controls are in place; has ultimate responsibility for the content of the security awareness program.

Information Security Services: determine the information security training content and enforce the training requirement with all units; annually review and update the training content as necessary or appropriate; maintain training statistics and report completion rates.

Director of Information Security Services: reporting to the Chief Information Officer, provide leadership in security awareness, training, and education, and develop and implement the University's information security awareness training program roles.

PROCEDURES

There are no procedures associated with this policy.

RELATED INFORMATION

Forms or Tools

[Security Essentials Online Training Modules](#)

Cross-References

[Appropriate Use of Information Technology Resources](#)

[Data Classification and Handling](#)

[Information Security](#)

Sources

[Arizona Board of Regents Policy 9-201](#)

[Arizona Board of Regents Policy 9-202](#)

APPENDIX

None.

APPENDIX B-14: NORTHERN ARIZONA UNIVERSITY — Exhibit 10: Research Security Checks in Cayuse

NAU 2026 Research Security Report to ABOR

EXHIBIT 10

Research Security Checks and Reminders in Cayuse
(NAU’s Proposal Management System)

Screenshot of Foreign Talent Recruitment Program notice:

****All investigators must complete, certify, and submit the [Foreign Talent Recruitment Programs Form](#) to OSP prior to proposal submission and annually for the duration of any sponsored project.****

Screenshot of Research Security Training requirement notice:

****All senior/key personnel must have completed the [Research Security Training \(Combined\) course](#) in CITI, no more than 12 months prior to submitting a proposal to any federal agency.****

Screenshot of Export Control screening questions:

>> Export Control

Export Control Laws regulate the distribution of controlled information and technology to foreign nationals and foreign countries for reasons of foreign policy and national security. Some types of research, including research that restricts publication rights, may have export control implications even if all the work is conducted within the United States. The following questions are intended to assure that any potential issues related to your project are addressed prior to issuance of an award. Please contact the [Export Control Office](#) if you have questions or would like more information about a particular situation.

* Indicates Required Fields

1. Will the proposed project involve:

* Participation, collaboration, or access to information, data, technology by foreign nationals residing abroad or within the U.S. (foreign nationals include individuals with foreign citizenship, foreign governments, foreign associations, corporations, or foreign political parties), OR the shipment of equipment, software, materials, funds, or other physical or electronic items or services of value outside of the United States?

☐ Yes

☒ No

2. Will the proposed project require issuance of a subcontract to a foreign entity or funding to a foreign entity?

☐ Yes

☒ No

Save

Reset

APPENDIX B-15: NORTHERN ARIZONA UNIVERSITY — Exhibit 11: Enhanced Visitor Screening Form

NAU 2026 Research Security Report to ABOR

EXHIBIT 11

Screenshot of Enhanced Visitor Screening Form

Enhanced Visitor Screening for New Scholars/ Employees

As part of the administrative process for hosting foreign national students, visitors and guests to NAU a technical review is required to determine if access or other controls are needed. This review is conducted by the Office of Research Compliance (ORC) and Center for International Education (CIE).

Please complete the following questions to the best of your ability. The answers will assist NAU in its review of potential licensing requirements under U.S. export control regulations or other considerations.

For more information about export control laws and regulations, please visit our website at <https://nau.edu/nau-research/research-safety-and-compliance/export-control/>

Section 1

1. NAU Host Faculty/Staff *

Enter your answer

2. NAU Host Department *

Enter your answer

APPENDIX B-16: UNIVERSITY OF ARIZONA — Researcher Mandatory Disclosure Certification (redacted)

Research Initiated Update for [REDACTED] [REDACTED]: Assurance and Certification

- I hereby acknowledge that I have read and understand the UArizona's Conflict of Interest and Commitment policies.
- I will provide any additional information as requested by the Conflict of Interest Office.
- I agree to cooperate in the development of any needed management plan as required by policy to manage, reduce, or eliminate existing conflicts of interest or commitment related to my research. I agree to comply with the terms and conditions contained in any management plan.
- These disclosure requirements apply to ALL foreign entities, including, but not limited to, employment and/or payments from any foreign entity.
- I certify under penalty of perjury under the laws of the State of Arizona that I have used all reasonable diligence in preparing this statement and the information provided is to the best of my knowledge true and complete and does not misstate any facts.

I understand that this Disclosure is required to obtain funding from the U.S. Government.

- I, [REDACTED], certify to the best of my knowledge and belief that the information contained in this Disclosure Statement is true, complete, and accurate.
- I understand that any false, fictitious, or fraudulent information, misrepresentations, half-truths, or omissions of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims, or otherwise. (18 U.S.C. §§ 1001 and 287, and 31 U.S.C. 3729 -3730 and 3801-3812).
- I further understand and agree that (1) the statements and representations made herein are material to U.S. Government's funding decision, and (2) I have a responsibility to update the disclosures during the period of performance of the award should circumstances change which impact the responses provided above.

1. My disclosures are up-to-date and accurate and I confirm that I understand and agree with the above statements. ☒

APPENDIX B-17: UNIVERSITY OF ARIZONA — RPS Screening Responsibilities

Screening Responsibilities		
Screening and subsequent match clearance should take place <i>before</i> further action or engagement		
UA Engagement or Activity	Who Should be Screened?	Screening Responsibility
Foreign Visiting Scholars	- Individual - Current and previous* institutions of study/employment	Department/College
Employment candidates	- Individual - Current and previous* institutions of study/employment	Department/College
Designated Campus Colleagues (DCCs)	Individual • Employer	Department/College
International Graduate Students	- Individual - Current and previous* institutions of study/employment	Department/College
International MOUs	Institutions • Companies • Individuals	Department/College, AZ International
Informal international research collaborations or partnerships	Associated Individuals • Institutions • Organizations	Department/College
Partnership/sponsorship of conferences	Foreign institutions or organizations	Department/College
Sending/sharing items, materials, or technology abroad	Institutions • Companies • Individuals	Department/College
Proposals/Contracts/Agreements	Sponsors	ORCA <i>and</i> Department
Subcontractors	Institutions • Companies • Individuals	ORCA <i>and</i> Department
Vendors	DV and PO vendors	FSO
Export-controlled activities and projects	Associated personnel	Export Control
*For candidates from sanctioned/restricted countries, screen previous institutions/organizations for the past 10 years. For non-sanctioned/restricted countries, screen for the past 6 years.		

Source: research.arizona.edu/sites/default/files/2025-12/RPS-Screening-Responsibilities.pdf

APPENDIX C: PUBLISHED RESOURCES

Each university identified the following published policies, procedures, guidance and tools that support its research security program.

UNIVERSITY	RESOURCE	LINK
Arizona State University	ASU Research Compliance Homepage	researchcompliance.asu.edu
Arizona State University	ASU Research Security Program Website	researchcompliance.asu.edu/research-security
Arizona State University	ASU Research Security Position	researchcompliance.asu.edu/wp-content/uploads/sites/50/2025/02/ASU-Research-Security-Position-02242025.pdf
Arizona State University	Research Security Policy (RSP 216)	public.powerdms.com/ASU/documents/2905017
Arizona State University	Conflict of Interest Disclosure Process	researchcompliance.asu.edu/coi/disclosure-process
Arizona State University	Controlled Unclassified Information Handling Procedures	researchcompliance.asu.edu/research-security/controlled-unclassified-information
Arizona State University	Enterprise Technology Get Protected IT Standards	getprotected.asu.edu
Arizona State University	Export Controls Guidance	researchcompliance.asu.edu/research-security/export-controls
Arizona State University	Export Control Wizard	researchcompliance.asu.edu/research-security/export-control-wizard
Arizona State University	Export Control Policy (RSP 214)	public.powerdms.com/ASU/documents/1559281
Arizona State University	Foreign Malign Talent Programs Policy (RSP 215)	public.powerdms.com/ASU/documents/2107993
Arizona State University	Foreign Talent Recruitment Program Guidance	researchcompliance.asu.edu/research-security/foreign-talent-recruitment-programs
Arizona State University	Foreign Ownership, Control or Influence (FOCI) Guidance	researchcompliance.asu.edu/research-security/foreign-ownership-control-or-influence
Arizona State University	Foreign Travel Checklist	researchcompliance.asu.edu/wp-content/uploads/sites/50/2025/10/International-Travel-Checklist-10-30-2025.pdf
Arizona State University	International Research and Global Collaborations Guidance	researchcompliance.asu.edu/research-security/international-research-and-global-collaborations
Arizona State University	International Research, Research Compliance and Security Checklist	https://researchcompliance.asu.edu/wp-content/uploads/sites/50/2025/04/International-Research-Compliance-and-Security-Checklist-final.pdf
Arizona State University	International Travel Guidance	researchcompliance.asu.edu/research-security/international-travel
Arizona State University	Notification of Consulting or Other Outside Business Activities or Arrangements (ACD 510-01)	public.powerdms.com/ASU/documents/1547043
Arizona State University	NSPM-33 Implementation Guidance	nsf.gov/policies/nspm-33
Arizona State University	Objectivity in Research: Disclosure of Financial Interests and Management of Conflicts of Interest (RSP 206)	public.powerdms.com/ASU/documents/1559274

UNIVERSITY	RESOURCE	LINK
Arizona State University	Physical Security Best Practices	researchcompliance.asu.edu/research-security/physical-security-best-practices
Arizona State University	Research Security Forms	researchcompliance.asu.edu/research-security/forms
Arizona State University	Research Security Training	researchcompliance.asu.edu/research-security/training
Northern Arizona University	Research Security (Interim) Policy	in.nau.edu/university-policy-library/research-security
Northern Arizona University	Conflict of Interest in Sponsored Projects	in.nau.edu/university-policy-library/conflict-of-interest-sponsored-projects
Northern Arizona University	Participation in Foreign Talent Recruitment Programs	in.nau.edu/university-policy-library/participation-in-foreign-talent-recruitment-programs
Northern Arizona University	Foreign Talent Recruitment Programs FAQ	https://in.nau.edu/university-policy-library/wp-content/uploads/sites/395/FAQs-Participation-in-Foreign-Talent-Recruitment-Programs.pdf
Northern Arizona University	Information Security Awareness Training Policy	in.nau.edu/university-policy-library/information-security-awareness-training
Northern Arizona University	Data Classification and Handling Policy	in.nau.edu/university-policy-library/data-classification-and-handling
Northern Arizona University	Data Handling Protocols	in.nau.edu/university-policy-library/wp-content/uploads/sites/26/Data-Handling-Protocols.pdf
Northern Arizona University	Intellectual Property Policy	in.nau.edu/university-policy-library/intellectual-property
Northern Arizona University	International Travel Policy (TRV 550)	in.nau.edu/university-policy-library/wp-content/uploads/sites/395/Travel-550.pdf
Northern Arizona University	Export Control Program	in.nau.edu/research/research-compliance/export-control
Northern Arizona University	Security Essentials Training Modules	in.nau.edu/its/infosecessentials
University of Arizona	Research Security Policy	policy.arizona.edu/research-security-policy
University of Arizona	RPS Screening Responsibilities	research.arizona.edu/sites/default/files/2025-12/RPS-Screening-Responsibilities.pdf
University of Arizona	Conflicts of Interest & Commitment Policy	policy.arizona.edu/ethics-and-conduct/conflicts-interest-commitment-policy
University of Arizona	Countries of Concern Webpage (Research & Partnerships)	research.arizona.edu/countries-concern
University of Arizona	Foreign Component Webpage (Research & Partnerships)	research.arizona.edu/foreign-component
University of Arizona	Research Security Program and Point of Contact	research.arizona.edu/compliance/research-security-program

