Athabasca University
HUMAN RESOURCES

Research Security Specialist Position Description

<div style="background-color:orange">Section I: Position Information</div>

Effective Date	Click or tap to enter a date.	☐ Update Only	☐ Classification Review

Position Title	Research Security Specialist
Position Number	TBD
Classification Level	TBD
Position Affiliation	☐ AUFA ☐ Excluded
Location	Virtual
Department	Research Office
Reports To	998636, Manager, Research Development

Position Summary
Briefly describe the main purpose(s) of the position.

The Research Security Specialist is the primary support, contact, and representative for AU for all matters related to research security. They will build institutional capacity of research security, risk mitigation, and compliance by applying expertise in the principles and practice of safeguarding research, policy analysis, and effective communications. They will also serve as a key network liaison in key provincial and national communities of practice and advising groups related to research security.

The Research Security Specialist will support the University's research mission by providing content and process expertise. They will also support and advise researchers across the University ecosystem with the design, implementation, and ongoing compliance of the research security risk mitigation plans that are quickly becoming required components of applications for external research funding. The incumbent will draw on existing resources and knowledge of safeguarding research, the Sensitive Technology Research and Affiliations of Concern (STRAC) policy, and the National Security Guidelines for Research Partnerships—familiarity with research security related best practices, and compliance with Institutional policies and procedures, will be critical to achieve success in this position. The Research Security Specialist will also build awareness of research security across the university, provide a variety of training opportunities related to research security, as well as provision advice and assistance to researchers with export controls, controlled goods, and sanctions regulations, to ensure compliance with all requirements.

Confidentiality and tactfulness will be necessary in dealing with faculty researchers and other members of the AU community. This position regularly deals with internal and externals stakeholders via email and online meetings and it's imperative that professional behaviour and good judgement is used.

The Research Security Specialist reports to the Manager, Research Development and is part of a growing Research Development team. This service-oriented position is driven by constant, multiple and simultaneous deadlines, continuous change and shifting priorities. The incumbent will work independently, possess very strong time management skills, and have superior research, organizational and communication skills.

The Research Security Specialist will also work closely with, and support, other internal and external teams in areas related to research integrity (e.g. research ethics, etc).

Duties and Responsibilities

Organize by key responsibility area and include % of time spent where possible.

The incumbent will:

- be responsible for developing educational and promotional material for the university to help ensure understanding of federal and provincial guidance and requirements regarding research security, particularly when applying to grant-funding agencies and seeking partnered research.
- be responsible for maintaining a high level of awareness regarding developments domestically and internationally that are relevant to the research security portfolio.
- use tools available to the university to conduct due diligence checks and create reports and/or briefings regarding research security issues of interest.
- work closely with Research Office colleagues to put forward competitive applications for research funding that are in compliance with research security expectations and requirements.
- assist researchers with the development and implementation of their research risk mitigation plan, conduct regular follow-up to ensure compliance, help monitor projects and partners, and identify and document new or evolving research security risks.
- maintain a record of all grant applications that required research security support.
- assist with the preparation of year end compliance reports.
- be the Institutional lead for sanctions and export controls and advise researchers accordingly. This includes tracking changes or developments related to export controls, controlled goods and sanctions and how they could impact the university research enterprise, as well as assist with the development and updating of an export controls and controlled goods framework and guide.
- be the institutional lead for fostering and providing compliance and risk mitigation support (including due diligence reviews and mitigation strategy development) and guidance for institutional research programs, projects, and grant applications.
- stay up to date on changes to risk mitigation measures that are required to secure government funding and update the compliance framework as necessary.
- drive an institutional-wide culture change regarding research security. This includes the promotion of an in-depth understanding of applicable guidelines, interpretations, best practices, and regulatory requirements related to safeguarding research.
- stay up to date on best practises both within Canada and internationally as to how to ensure compliance with ever changing national security requirements.
- develop and evergreen best practises, guidelines, SOPs, processes, and policies related to research security.
- participate in local, provincial, and national organizations, networks, and communities of practice associated with research security.
- as a member of the Research Development team, provide coverage and support, from time to time, for portfolios across the team and Research Development team activities, projects, and initiatives.
- Collaborate, consult, and advise on connections or shared considerations between research security and other key areas of research integrity, policy, and administration (i.e., research ethics, research data management, EDI, intellectual property) as well as organizational frameworks and compliance (i.e., compliance reporting, enterprise risk management, digital security).

Additional other duties as directed by the Manager, Research Development.

Occupational Health and Safety

Employees:
Responsible to participate in the AU OHS Program as required.

Supervisors:
Responsible for awareness of one's OHS Responsibilities as an AU employee and supervisor, for participating in the AU OHS Program as required, and for ensuring the participation of employees in the AU OHS Program as required.

See: https://ohs-pubstore.labour.alberta.ca/li008

Classification Factors

Communication

- Must be able to communicate in a clear, positive, and professional manner through both verbal and written communication.
- Must be able to prepare and deliver impactful, clear, high-quality presentations each designed to the specific target audience.
- Will need to contact various staff (support, professional, faculty, and management) throughout the university to provide support with research security.
- Provide high quality representation of AU in external networks and partners.
- Maintain a high degree of confidentiality with respect to personal and academic information. Some engagements will involve confidential or highly sensitive discussions that require discretion.
- Consults and uses a range of systems specific for the delivery of research security support (e.g. OSINT tools).
- Works with internal and external stakeholders collaboratively to create value-added advice.
- Establishes effective relationships with counterparts in other universities.
- Proactively collects feedback on areas of high interest and adjusts training/advisory material accordingly.
- Meet online (over MS Teams) with members of the AU community as necessary and do so in a professional manner. Handle all communications tactfully, whether verbally or written.

Supervision

The incumbent will not have any direct reports.

Impact of Service or Product

Due to the complexity of the tasks and the importance of accurate information, even minor errors or miscommunication could have serious repercussions. These consequences could significantly impact not only academic staff but also the entire university's operations and reputation.

The incumbent will have access to sensitive material and will be required to navigate through difficult conversations related to complex topics. In doing so, the incumbent will be required to uphold the utmost degree of confidentiality and, therefore, be required to be familiar with AU's regulations and the guidelines in order to conform with them.

Independence of Action

- Make well informed independent judgments and decisions related to research security matters and consult with the Manager, Research Development, where additional clarity and direction is required. In this space, the incumbent will, for instance:
  - Independently undertake due diligence reviews, reach determinations on research security risks and appropriate risk mitigation strategies, and then provide high quality and clear advice to AU team members (e.g. researchers, faculty leadership, etc.).
  - Spearhead the development of a Research Office led research security strategy which, once approved, the incumbent will have carriage over the execution of that strategy.
- Independently assess non-routine requests and queries to ensure complete and satisfactory processing and/or referral of same—this requires knowledge of other Athabasca University functions and how to triage out such requests or obtain the approval for any special action required by the appropriate staff member.
- Perform duties under minimal supervision with constant requirement for independent thought and will be responsible for ensuring the accuracy and completeness of all tasks performed.
- Independently organize, prioritize, and perform daily tasks as well as ensuring priorities and deadlines are being managed appropriately to ensure a smooth flow of requests and queries.
- Be able to tolerate disruption, manage time, cope with high volumes of work, set priorities, meet continuing changes in procedures, and institutional developments, and manage the unpredictability of dealing with a topic (i.e. research security) that will be new to many within AU.
- Serve as a key liaison and representative of AU in provincial and national networks of research security professionals.
- Function well as a team member and work cooperatively with others.
- Adjust daily workload to handle special tasks or assignments.

Complexity

- Provide advice and apply policy which will include complex conversations on sensitive issues which require tact to navigate.
- Provide advice on complex files and cases, impacted by new and emerging federal requirements, using open-source information techniques to allow senior university officials to make informed decisions.
- Develop a suite of educational and promotional materials for AU that are consistent with the institution's needs, culture and values.
- Research and curate an extensive library of educational tools and resources that can be used directly or which can inform research security-related training and awareness material.
- Perform research and create analysis (e.g., reports, briefings, memos) on research security-related topics on an as-needed basis.
- Maintain a high level of awareness and knowledge of geopolitical trends and their impact to the University.
- Develop and maintains subject matter expertise on research security-related government policies, and approaches adopted by other universities with regard to research security management.
- Deliver training and awareness-building sessions to relevant stakeholders.

Planning

- Assist researchers with the implementation of their research risk mitigation plan, conduct regular follow-up to ensure compliance, and monitor projects and partners and to identify and document new or evolving research security risks.
- Identify and develop new processes and services to administer a research security program.
- Evaluate and recommend program elements that should be publicly available vs. available only to the AU community.

Section II: Qualifications

Qualifications

Includes education, experience, skills, abilities and any other special qualifications required. The qualifications relate to the position not the incumbent.

- A University degree, either an undergraduate degree combined with 3+ years of relevant work experience, or a graduate degree with 1+ years of relevant work experience.
- Experience in a research environment at a university/college—preferably at a post-secondary institution setting that is governed by the Tri-Agency Framework for the Responsible Conduct of Research—or in a government office, or in the Canadian intelligence environment.
- Extensive knowledge of research security, regulations, and national security priorities, including an understanding of export controls and sanctions, National Security Guidelines for Research Partnerships, research data management, and cyber security.
- Demonstrable ability to consistently apply high level critical thinking, sound decision-making, and clear communication skills in a high volume, fast-paced environment is required.
- Excellent written and oral communication skills, as well as experience delivering presentations and briefings to both experts and lay audiences is an asset.
- Strong research skills with an ability to prepare detailed guidance resources for compliance and export control purposes is an asset.
- Demonstrable experience developing best practices, SOPs, processes, and policies as well as driving change.
- Demonstrable success navigating complicated, sensitive, and contentious issues with stakeholder groups who may have competing or conflicting priorities. And the ability to be comfortable in an ambiguous environment where diplomacy, discretion, and tact are paramount.
- Familiarity with risk management best practices.

- Familiarity with research ethics and integrity issues and best practices would be an asset.