UNIVERSITY OF ALBERTA

VP RESEARCH AND INNOVATION

Safeguarding Research Office

Responsible Open Source Due Diligence Protocol

Responsible Open Source Due Diligence Protocol

Preamble

As part of a continuing commitment to transparency, the University of Alberta's Safeguarding Research Office (SRO) is making this Responsible Open Source Due Diligence Protocol publicly available. This protocol was developed to proactively address possible issues relating to the conduct of open source due diligence work in an academic context in support of research security, and to outline the provisions in place to ensure that these activities are undertaken in a manner which meets legal, policy, and ethical requirements and community expectations.

Table of Contents

I. Executive Summary
II. Introduction
III. Guiding Principles and Parameters
IV. Processes: Requesting Due Diligence and Collecting Information
V. Review
VI. Contact

Appendices

- Appendix A: Due Diligence for Safeguarding Research Program
- Appendix B: Request for Safeguarding Research Office (SRO) Conduct of Open Source Due Diligence Form[1]

[1] Available upon request from safegrd@ualberta.ca.

I. Executive Summary

The University of Alberta (hereafter "U of A")'s Safeguarding Research Office (hereafter "SRO") provides support to the institution and to its researchers with activities that aim to secure the University's research and innovation ecosystem from research security risks.[2] These actions are taken in accordance with direction from, and funding provided by, the Government of Canada. SRO ensures that the University community understands and adheres to relevant policy requirements at the individual and institutional level. These requirements include the following policies: the National Security Guidelines for Research Partnerships, the Policy on Sensitive Technology Research and Affiliations of Concern, the Government of Alberta's direction with regard to partnerships with China, and supporting guidance materials found on the Safeguarding Your Research portal. As authorized by the U of A's Due Diligence for Safeguarding Research Program (hereafter "the Program") (see Appendix A), an essential part of the SRO's activities is the conduct of open source due diligence reviews.[3]

The Program provides for the identification, assessment and mitigation of research security risks through the application of open source due diligence activities. Open source due diligence methods bring structure, focus, and intent to online research and discovery. Collected information is used to mitigate risk and ensure compliance, supporting informed decision-making.

SRO due diligence activities contribute to positioning the U of A as a trusted ecosystem for sensitive research and innovation by:

- Identifying and mitigating risk in support of the institution's Enterprise Risk Management Framework[4];
- Aligning with government (federal and provincial) requirements aimed at addressing research security vulnerabilities within the postsecondary environment; and
- Contributing to the institution's commitments to safe and responsible research, commercialization, and technology transfer collaborations.

[2] Research security risks include but aren't limited to unwanted transfer of knowledge, data, technology, research and intellectual property, misappropriation of research, compromise of the integrity of the research ecosystem – including through interference in merit-based and peer-review processes, and conflicts of interest and commitment that could pose a threat to national security.
[3] The purpose of due diligence is to identify factors that may put the institution or its employees at risk, including legally or reputationally, and to anticipate future developments which could jeopardize academic integrity, the security of the research ecosystem, or the viability of an agreement or partnership.
[4] The aim of the Enterprise Risk Management Framework is to protect the University's value by managing uncertainties that could influence achieving the University's mission, vision, strategic and operational objectives.

As part of the U of A's commitment to the highest standards of institutional integrity, transparency, and accountability, a Responsible Open Source Due Diligence Protocol (hereafter "the Protocol") has been developed to ensure that these activities are conducted transparently, consistently, and fairly, with due regard to legal and privacy considerations, and in line with U of A policies, procedures, and foundational principles.

The Protocol also provides detailed information on the categories of open source due diligence conducted by SRO; the authorities for the collection, use, disclosure, and retention of information; and the safeguards in place to ensure that these activities are fully compliant with legal and ethical requirements, reflect privacy and human rights considerations, and adhere to applicable policies and legislation.

II. Introduction

Program Rationale

The U of A is governed by the *Alberta Freedom of Information and Protection of Privacy Act* (hereafter "the *Act"*) and Regulations and other provincial and federal privacy legislation.[5]

- Section 33 of the *Act* states that no personal information may be collected by or for a public body unless … (c) that information relates directly to and is necessary for an operating program or activity of the public body.

The collection of personal information *may* be required in order for SRO to fulfill its responsibilities under the Program (see Appendix A).

Program Scope

SRO conducts open source due diligence under three predefined categories for the purpose of complying with relevant policy requirements and identifying, assessing, and mitigating risks:

- *Category A*: Due diligence conducted to identify research security risks related to partnerships and agreements;
- *Category B*: Due diligence to identify research security risks related to affiliations of concern from a national security perspective; and

[5] Note: the next version of this document will reflect the new *Protection of Privacy Act* and the *Access to Information Act* and regulations.

- *Category C*: Due diligence conducted at the request of the institution, for the purposes of supporting an inquiry or investigation relating to the responsible conduct of research.[6]

Personal Information Collected Under the Program

As per the *Act* and the U of A's Access to information and Protection of Privacy Procedure, personal information is defined as recorded information about an identifiable individual. Personal information includes information such as an individual's:

- Name and contact information, age, and gender
- Student or employee ID #, or other identifying number
- Application for employment, salary, employment evaluations, and other employment history
- Grades, assignments, and other educational history
- Health information or financial information
- Race, national or ethnic origin, or colour
- Religious or political beliefs or associations, marital status or family status
- Biometric information
- Criminal history[7]

With the exception of "name" and "educational and employment history," it is unlikely that the types of information listed above would be collected in the discharge of the Program.

It is anticipated that the types of information to be collected under the Program could include:

- Name of an individual or organization
- Organizational information (ownership, connections, leadership, activities)
- Research area, publication or patent information of an individual

[6] The primary source for understanding responsible conduct of research in Canada is the Tri-Agency Framework: Responsible Conduct of Research 2021. Given that U of A researchers also hold international research funding, similar documents from other jurisdictions (such as those outlined by the National Science Foundation in the United States) may also be relevant to the conduct of due diligence at the University. As such, this is intended to be a broadly defined reference to "responsible conduct of research."

[7] Comprehensively, the *Act* defines "Personal information" as recorded information about an identifiable individual, including (i) the individual's name, home or business address or home or business telephone number, (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations, (iii) the individual's age, sex, marital status or family status, (iv) an identifying number, symbol or other particular assigned to the individual, (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, (vi) information about the individual's health and health care history, including information about a physical or mental disability, (vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, (viii) anyone else's opinions about the individual, and (ix) the individual's personal views or opinions , except if they are about someone else.

- Funding information (individual or organization)
- Educational and employment history (individual)
- Information about professional affiliations (individual)
- Immigration status (individual)

This information would either be provided by the requester at the time that the due diligence request is received by SRO or collected from publicly available information[8]. Further, as defined by the U of A Institutional Data Management and Governance Procedure, information collected under the Program could be considered confidential.[9]

Protocol's Purpose

The purpose of the Protocol is to ensure that open source due diligence activities are conducted transparently, consistently, and fairly, with due regard to legal and privacy considerations, and in line with U of A policies, procedures, and foundational principles. In order to accomplish this purpose, the Protocol outlines:

- *Guiding Principles and Parameters* (Section 3) that support freedom of information and protection of privacy. These outline appropriate security measures to protect personal information from unauthorized access, use, or disclosure and also ensure a human rights-based approach to due diligence activities by integrating equity, diversity, and inclusion principles.
- *Processes* (Section 4) for requesting the conduct of due diligence by SRO and the corresponding collection of open source information.
- *Review* (Section 5) and *Contact* (Section 6) provisions for the Protocol.

Open Source Due Diligence Tools and Subscriptions

SRO currently has access to two subscription-based open source due diligence tools: Kharon Clearview and Dimensions Research Security. These tools assist with due diligence in aggregating relevant open source information into a tool which is searchable and provides useful reporting of results. Vendor selections were made with due consideration to privacy, security, and functionality. SRO also uses other publicly-available information such as sanctions, publications, patents, and corporate registry databases in conducting open source due

[8] Collection will be conducted in accordance with the Protocol's Guiding Principles and Parameters (see section 3 below), the Government of Canada's Guidance on Conducting Open Source Due Diligence for Safeguarding Research Partnerships.

[9] The U of A Institutional Data Management and Governance Procedure defines confidential information as information that is sensitive within the University of Alberta and could cause serious loss of privacy, competitive advantage, loss of confidence in University programs, or damage to partnership, relationships and/or reputation. Confidential information includes highly sensitive personal information. Confidential information is available only to a specific function, group or role (e.g., personnel files, including personal salary data, and third party business information submitted in confidence).

diligence. The provisions outlined in this protocol will ensure that these tools are used responsibly and that steps are taken to validate results and minimize the impact of inaccurate or outdated information.

III. Guiding Principles and Parameters

All open source due diligence conducted by SRO under the Program will be authorized at the appropriate level, conducted in furtherance of Program objectives, and done in a manner consistent with the Government of Canada's guidance on Conducting Open Source Due Diligence for Safeguarding Research Partnerships. In addition, the principles and parameters below will be respected.

A. Legal and Policy Considerations

- Due diligence methods and processes comply with all relevant legislation and privacy requirements, as well as relevant U of A policies and procedures.
- In accordance with the U of A Access to Information and Protection of Privacy Procedure, SRO staff collecting personal information in the course of conducting due diligence acknowledge on an annual basis that they have read and understood the Procedure and all other procedures relevant to the privacy and security of personal information.

B. Authority for Collection

- The authority for the collection of any personal information under the Program is section 33(c) of the *Act*.
- The authority for the collection of other (non-personal) information under the Program is federal and provincial policies and guidance and institutional policy.

C. Manner of Collection

- SRO may collect personal information directly or indirectly. In most cases, information will be collected indirectly pursuant to section 34(1)[10] of the *Act*. The scenarios in which this indirect collection is anticipated can be found in the rationale of the Program (see Appendix A).
- In the event that information must be collected directly from an individual, that individual will be informed of the purpose for collection, the authority for collection, and contact details for further information.

[10] The *Act* provides for circumstances where personal information about an identifiable individual may be sought from sources other than the individual the information is about. If one of the provisions in section 34(1) applies, personal information may be obtained in verbal, written, electronic or other form (e.g., a file transfer).

D. Consistent Use and Disclosure

- In accordance with the *Act* and the U of A's Access to Information and Protection of Privacy Procedure, any personal information is only used for the purposes for which it was collected under the Program.
- If a scenario arises in which information collected directly is to be used for a purpose other than that for which it was originally collected, the individual that the information is about will be notified.
- Disclosures of information collected through the Program will only take place as authorized under section 40 of the *Act*[11].
- Personal information collected under the Program will only be disclosed to the relevant authority for the purpose for which it was collected or compiled. Collected information will be used in a way that is consistent with identified purposes as outlined in Categories *A-C* and as is relevant to governmental and/or institutional policies and procedures.

E. Secure Storage

- SRO's management of information under the Program adheres to the U of A Records Management Policy[12] and the University Records Office Electronic Documents Guide.
- In accordance with the U of A Privacy and Security Best Practices for Sharing Information, the information collected under the Program for *Category B* and *C* purposes is stored on an access-controlled network drive. All *Category A* information is stored on an access-controlled Google Drive.
- Safeguards are in place for the collection, use, access, disclosure, and disposal of information to protect sensitive information.

F. Access and Retention

- In accordance with the U of A Records Management Policy, access to personal information collected under the Program is limited to those requiring access to fulfill responsibilities further to a documented policy or program.
- All personal information collected is to be stored on the SRO network drive in an access-restricted folder and only used in relation to fulfilling Program requirements and in accordance with this Protocol.
- In accordance with the *Act* and the U of A Access to information and Protection of Privacy Policy, individuals have the right to access personal records about them collected under the Program.

[11] Section 40 of the *Act* provides for specific situations where a public body, including postsecondary institutions, may disclose personal information without an access request. The *Act* restricts the disclosure of personal information to situations where, for example, there is no unreasonable invasion of personal privacy.

[12] As per the Records Management Policy, information collected under the Program is considered a University Record: recorded information in any format within the custody or under the control of the University relating to the operation and administration of the University.

- Formal requests for access to information and/or correction of personal information are to be processed through the Information and Privacy Office in accordance with the U of A Access to Information and Protection of Privacy Procedure.
- All information collected under the Program is retained for a minimum one-year period in order to allow individuals a reasonable opportunity to obtain access to personal records about them further to U of A Records Retention for Faculty or Departmental Information.
- Records are disposed of in accordance with the U of A Records Disposition Guideline.

G. Accuracy and Validation of Findings

- SRO makes every reasonable effort to ensure that information collected through the Program is accurate and complete.
- SRO utilizes best practices set out in the aforementioned federal government guidance document and other sector best practices to ensure results are accurate, complete, corroborated, reliable, and repeatable. Findings will never be based on a single source of information and any adverse information is always corroborated with additional sources.
- SRO takes all reasonable efforts to determine the original source of information obtained through due diligence and used to support a risk assessment.
- SRO assesses the integrity and quality of information accessed and collected including, where possible, by assessing whether the information reflects any underlying biases or inferences.

H. Limits and Prohibition on Due Diligence

- Due diligence conducted by SRO will be limited to the types of sources listed in the Government of Canada's guidance on Conducting Open Source Due Diligence for Safeguarding Research Partnerships. A full list of sources used will be made available by SRO upon request.
- Due diligence must only be conducted by SRO where a requirement under the Program exists and in accordance with the purpose and scenarios identified in Section 1 of the Protocol.
- As per the U of A's Discrimination, Harassment and Duty to Accommodate Policy, it is strictly prohibited to use or collect personal information with the intent to discriminate against any individual or group.
- Social media will not be included in due diligence conducted by SRO with the sole exception of LinkedIn which may be used due to its function as a repository of employment and educational history and professional affiliations.

I. Proportionality of Intrusiveness

- Personal information is only collected if credible[13] information demonstrates necessity.

[13] Credible in this document means information which is coherent, plausible, reasonable, and not counter to generally known facts.

- The level of due diligence undertaken by SRO is proportional to an initial assessment of overall risk. Higher-risk scenarios may require more intrusive due diligence activities and the use of a wider range of due diligence tools[14].
- Search queries are scoped as narrowly as possible while still fulfilling the requirements of the Program.
- In order to protect institutional and/or individual reputations, due diligence is conducted as discreetly as possible.

J. Consistency of Approach

- The Protocol is used by SRO to ensure consistent methods and processes in conducting due diligence.
- Consistent use of Protocol processes and methods and adherence to document procedures produces reliable and repeatable due diligence results.

K. Transparency

- Methods and processes for conducting due diligence contribute to a culture of safety, trust, and accountability in safeguarding research at the U of A.
- In describing the Program, and in associated documents, the possible collection of personal information (directly or indirectly), and the authority for the collection, will be identified.
- The Protocol is accessible to the public and to all members of the U of A's research and innovation ecosystem on the Safeguarding Research Office internal and external websites.
- SRO will share this Protocol and information relating to due diligence sources and methods in order to provide assurance to the U of A community and government officials. This transparency can also support the development of best practices and standards for the conduct of due diligence in support of research security.

L. Respect for Equity, Diversity, and Inclusion (EDI) and Non-discrimination

- Due diligence processes and methods are as fair and as equitable as possible; and will uphold the principles of equity, diversity and inclusion.
- The collection, use, and disclosure of information is conducted without bias or intent to discriminate based on identity, age, culture, ethnicity, gender expression, gender identity or any other personal characteristics.

[14] Risk will initially be assessed and identified by the relevant due diligence approval authority (see Collection of Information Process - item iii). In cases that are assessed as higher risk, in order to ensure minimal intrusiveness to individual privacy, personal information will be collected as is necessary and in proportion to mitigating the identified level of legal, reputational and/or national security risks. Documentation of due diligence activities will demonstrate the necessity for more intrusive processes and the use of a wider range of due diligence tools as is proportionate to decision-making related to mitigating higher risk cases.

- Due diligence processes include the application of Gender-based Analysis Plus techniques to recognize and mitigate personal bias and unintended negative impacts on individuals or groups. SRO has also consulted EDI experts, and continues to refine internal processes to integrate EDI considerations.
- Safeguarding Research Specialists (SRS) in SRO conducting due diligence are trained to identify and mitigate bias to ensure objective and fair collection and analysis of information.

IV. Processes: Requesting Due Diligence and the Collection of Information

Request for Due Diligence Process

Requests for SRO open source due diligence support follow this process:

i. A requester must demonstrate, using the Request for Safeguarding Research Office (SRO) Conduct of Open Source Due Diligence form, that due diligence is necessary pursuant to a federal, provincial, or institutional policy requirement, that it is within scope of the Program, and that they have the authority to make the request.

ii. Necessity for due diligence will be assessed by the Director, Research Security in consultation with other University officials as appropriate and respecting the principles referenced above. The Director, Research Security will also consider the level of risk to the individuals involved, the University, and Canada's national security in determining whether and how to proceed with a request under the Program.

iii. In the event that a request for due diligence is rejected, a notice of rejection including rationale will be provided to the requester. A requester is permitted to submit a new request for due diligence.

iv. SRO will retain *approved* request forms and any supporting documents for a minimum one-year period. Rejected requests and any supporting documents will be destroyed and disposed of after notice of rejection is provided. A record of the rejection notification will be retained.

Collection of Information Process

Due diligence collection will follow this process:

i. Confirmation that the requester has followed the identified process, that the request is within scope of the Program, and that the requester has the authority to make the request.

ii. Confirmation of the Category of request (*A-C* as identified in the table below).

iii. Approval for collection will be obtained as follows:

Category	Description	Approval Authority
A	Due diligence to identify research security risks related to partnerships and agreements	Programmatic authority (no case-by-case approval required)
B	Due diligence to identify research security risks related to affiliations of concern from a national security perspective	Director, Research Security
C	Due diligence conducted at the request of the institution, for the purposes of supporting an inquiry or investigation relating to the responsible conduct of research	Associate Vice President, Research Integrity Support

iv. The relevant approval authority's assessment and approval of a due diligence request will be based on credible information signaling potential or existing reputational, legal, or research security risks to the institution, and its research community.

v. The relevant approval authority will assess privacy, legal, policy or reputational considerations associated with the request. If any particularly sensitive information or elevated risks are identified, consideration will be given to additional privacy-enhancing techniques, access restrictions or other mitigation measures.

vi. SRO will conduct the due diligence in accordance with this Protocol and documented internal procedures. These set out the queries to be searched, sources to be used, criteria to consider, process and format for documenting findings, and storage and access provisions. These procedures are available to the U of A community upon request.

vii. In the event that SRO identifies an instance of possible non-compliance with policy, legislation, or other binding requirements in the course of conducting due diligence for another purpose, this information will be documented digitally in an access-controlled

network drive and reported on a priority basis to the Director, Research Security in a standardized format. If the initial assessment of possible non-compliance is confirmed at the Director level, the matter will be escalated to the responsible senior executive through the Associate Vice-President Research Integrity Support.[15] Identified instances of non-compliance with any policy or other requirement will be communicated to implicated individual(s) within a timeframe and in a manner that allows for procedural fairness but does not impede any ongoing inquiry or investigation.

V. Review

This Protocol will be reviewed by SRO, at least annually, to ensure ongoing adherence to all applicable legislation, regulation, standards, and best practices.

VI. Contact

The contact responsible for this Protocol is the Director, Research Security.

Questions regarding the Protocol can be emailed to the University of Alberta's Safeguarding Research Office: safegrd@ualberta.ca.

[15] An example of this kind of scenario could be an instance wherein a faculty member has not disclosed an appointment at another institution, is receiving funding from a talent plan without disclosure, or has an undisclosed, active affiliation with a Named Research Organization.

Appendix A – Due Diligence for Safeguarding Research Program

Purpose: To set out the rationale for the formal establishment of a Due Diligence for Safeguarding Research Program ("the Program").

Program's Rationale: In order to identify, assess, and mitigate risks to research security for the University of Alberta and to support related decision making, a due diligence program is required. The Program will provide for the conduct of due diligence to inform determinations about compliance with applicable federal and provincial policies and requirements and the terms and conditions of funding agreements. It will also support determinations of eligibility to participate in programs or to receive benefits (e.g., research grants and supports). Upon receipt of a request authorized at the appropriate level, due diligence could also be conducted for the purpose of supporting the institution in the context of an official inquiry or investigation[16].

The imperatives for the Program originate with the need to comply with direction and guidance from the federal and provincial governments, as well as institutional responsibility to identify and mitigate institutional risks stemming from threats to research security. This identification and mitigation of risks supports the Enterprise Risk Framework, and protects the University's value by managing uncertainties that could influence the achievement of the University's mission, vision, and strategic and operational objectives.

Purpose for Conducting Due Diligence Under the Program: The purpose of SRO's conduct of due diligence is to identify factors that may put the institution or its employees at risk, legally or reputationally, and to anticipate future developments which could jeopardize academic integrity, the security of the research ecosystem, or the viability of an agreement or partnership. Open source due diligence methods bring structure, focus, and intent to online research and discovery. Collected information is used to mitigate risk and ensure compliance, supporting informed decision-making.

Program's Aim: In order to identify, assess, and mitigate research security, reputational, or legal risks to the institution and its research community, the Program will provide the University and its research community with information collected via a structured and consistent method for conducting open source due diligence. The Program will be conducted in accordance with all

[16] The conduct of due diligence activities under the Program support institutional decision-making for mitigating reputational, legal, and national security risks. This includes the potential conduct of due diligence to support the institution with verifying cases of academic misconduct, employee misconduct, or to support a criminal investigation. **SRO does not conduct investigations**; due diligence is conducted in disciplinary cases as one option among many to gather credible and verifiable information using structured and documented methods that respect privacy and legal rights. This information can be a source of information for decision makers.

applicable legislative and privacy requirements. The Program will contribute to positioning the University as a trusted research ecosystem for sensitive technology research and innovation.

Federal Policy Drivers: In 2021, the Government of Canada first introduced policy measures to reduce research security risks associated with federally-funded research. These measures include the National Security Guidelines for Research Partnerships (NSGRP) and the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy). The conduct of due diligence by postsecondary institutions and individual researchers is an essential element of implementing these procedures as evidenced in the policies and the supporting documents found on the federal government's Safeguarding Your Research portal, including the Conducting Open Source Due Diligence for Safeguarding Research Partnerships guidance.

Specific references to the conduct of due diligence are included in:

March 24, 2021 - Policy Statement

- "These guidelines will better position researchers, research institutions, and government funders to undertake consistent, risk-targeted due diligence of potential risks to research security."
- "As the review is underway and the guidelines are under development, it is important that all interest-holders in Canada's research ecosystem work collaboratively to identify and mitigate risks in research partnerships by utilizing existing tools available through the Safeguarding Your Research portal, and Safeguarding Science's workshops. A critical piece of this effort includes carefully conducting due diligence - and seeking guidance from government partners when appropriate - on potential research partnerships to ensure an effective and integrated review of potential risks and mitigation measures."

National Security Guidelines for Research Partnerships

- "The Guidelines better position researchers, research organizations and Government funders to undertake consistent, risk-targeted due diligence of potential risks to research security."
- "The Guidelines will provide clear information on the specific national security considerations for research partnerships – including with whom researchers partner and what areas of research are at higher risk – to support researchers, research institutions, and government funders to undertake consistent, risk-targeted due diligence to identify and mitigate potential national security risks to research."
- "Therefore, the Government of Canada recommends that researchers undertake due diligence early in the development process, regardless of whether the partners know at the outset if they will eventually be applying for federal research funding."

February 14, 2023 - Policy Statement

- "This new action is one of many significant steps the Government of Canada is taking to protect our country, our institutions and our intellectual property. This includes guidelines developed in consultation with the Government of CanadaUniversities Working Group to support due diligence on potential risks to research security, and the establishment of a Research Security Centre to provide advice and guidance directly to research institutions."

Policy on Sensitive Technology Research and Affiliations of Concern

- "Canada recognizes that some research collaborations in Sensitive Technology Research Areas not involving connections to listed Named Research Organizations may still present risks, and, as such, researchers and institutions are encouraged to continue to exercise due diligence in all of their research partnerships, and to make full use of other research security tools available to them including those provided on the Safeguarding Your Research portal."
- "This new policy is focused on researcher affiliations and targets the highest risk collaborations with military and state security-related institutions. As part of this policy, researchers should keep in mind that institutions that are not included on the Named Research Organizations list at this point in time may still pose a risk to Canada's research. Researchers are encouraged to apply due diligence practices to mitigate risks that may be associated with any collaboration or partnership in a Sensitive Technology Research Area."

Tri-Agency FAQ on STRAC Policy

- "Where possible, institutions may support their grant recipients in following best practices when seeking to recruit new prospective research team members and/or to develop new collaborations and partnerships as part of a project or program funded by a grant that aims to advance a STRA. This may include the provision of support to researchers seeking to conduct open source due diligence to verify a prospective team member's affiliation(s) and sources of funding or in-kind support."

Tri-Agency Guidance on Research Security

- "All Canadian researchers are encouraged to consult these resources and to exercise due diligence when managing their research and establishing and/or continuing international partnerships and collaborations."

Provincial Policy Driver: In May 2021, the Government of Alberta announced a pause on the pursuit of any new or renewed partnerships with entities linked to the Government of China. Compliance with this provincial direction necessitates the use of due diligence to verify whether or not a proposed partnership involves an entity linked to the Government of China.

Program Description: Within SRO, a team of Safeguarding Research Specialists are responsible for conducting due diligence to support research security at the University of Alberta.

SRO has the capacity to conduct the following categories of due diligence for the purpose of identifying, assessing and mitigating risks:

- *Category A*: Due diligence to identify research security risks related to potential partnerships and agreements;
- *Category B*: Due diligence to identify research security risks related to affiliations of concern from a national security perspective; and
- *Category C*: Due diligence conducted at the request of the institution, for the purposes of supporting an inquiry or investigation relating to the responsible conduct of research.[17]

Training Requirements: All Safeguarding Research Specialists are required to successfully complete the following training (or equivalent):

- Government of Canada Research Security Training Courses
- SEC497 - Practical Open-Source Intelligence (OSINT)
- Government of Alberta Access to Information and Protection of Privacy course
- Government of Canada's Gender Based Analysis Plus

Other relevant courses completed by SRO employees include:

- First Nations Principles of OCAP
- Outsmarting Implicit Bias
- U of A Information Access and Protection of Privacy Foundations
- SEC587 - Advanced Open-Source Intelligence (OSINT)[18]

[17] The primary source for understanding responsible conduct of research in Canada is the Tri-Agency Framework: Responsible Conduct of Research 2021. Given that U of A researchers also hold international research funding, similar documents from other jurisdictions (such as those outlined by the National Science Foundation in the United States) may also be relevant to the conduct of due diligence at the University.

[18] Note: Although SRO Specialists complete this training, certain sources and methods are not used by the Safeguarding Research Office as they do not align with the aforementioned principles or are otherwise not appropriate to due diligence in a university context.

Office of Responsibility: The Safeguarding Research Office (SRO), formally established in 2023, is the Office of Responsibility for the Program.

Program Review: The operations of the Program will be reviewed annually to ensure adherence to all applicable legislation, policies, and protocols.