RESEARCH DATA RISK CLASSIFICATION FRAMEWORK AND GUIDELINES

DEVELOPED BY ANDRIANA VANEZI, INFORMATION SECURITY SERVICES, IST
PREAMBLE BY: IAN MILLIGAN, ASSOCIATE VICE-PRESIDENT, RESEARCH OVERSIGHT AND ANALYSIS
LAST UPDATED: MAY 20, 2025

PREAMBLE

The University of Waterloo, through its Research Data Management (RDM) Institutional Strategy, aims to support research excellence through the provision of excellent RDM services, tools, and supports. In Canada, the Tri-Agencies argue that research data collected using public funds should be responsibly and securely managed and be—where ethical, legal, and commercial obligations allow—available for reuse by others. To this end, the agencies support the FAIR (Findable, Accessible, Interoperable, and Reusable) guiding principles for research data management and stewardship, when appropriate.

Data management, the storage, access, and preservation of data produced from a given research project, is thus a critical component of research activities. Data management practices cover the entire lifecycle of the data, from planning the investigation to conducting it, and from backing up data as it is created and used to long-term preservation of data deliverables after the research investigation has concluded.

In the RDM strategy, the University notes that this strategy was "relevant to *all* research utilizing and producing research data in all forms (including, but not limited to, digital, analogue, paper, and physical materials)—whether funded or unfunded, published or unpublished, open or restricted."

Researchers may have questions about whether their data are "open or restricted," and how they should responsibly steward this information. Canadian research funders, and their institution, want to help researchers share their data (where appropriate) for the advancement of science; we hope this guide helps researchers navigate this landscape.

PURPOSE

The purpose of this document is to provide University of Waterloo (UW) researchers with a standardized framework to classify research data. While UW's Policy 46: Information Management outlines classifications based on the Freedom of Information and Protection of Privacy Act (FIPPA), it is important to note that research data falls outside the purview of this legislation. By standardizing the classification of research data, a mutual understanding of the associated risk levels is established. This shared framework facilitates effective communication and collaboration among impacted/interested parties, including researchers, faculty administration, the Library, Information Security Services (ISS)/Information Systems and Technology (IST), and the Office of Research (OR), with an institutionally accepted classification, these entities can provide meaningful and appropriate support tailored to the specific needs associated with the data risk classification. This collaborative and standardized approach enhances the overall data governance structure, promoting a cohesive effort in safeguarding research data and maintaining compliance with regulatory standards and contractual obligations to research sponsors, when applicable.

RESEARCH DATA

DEFINITION

For the purposes of this research data risk classification system the inclusive definition of the term "research data" provided by CASRAI (Canadian Association of Research Administrators and Institutions) and adopted by the Tri-Agency Research Data Management Policy and Digital Research Alliance of Canada.

Data that are used as primary sources to support technical or scientific enquiry, research, scholarship, or artistic activity, and that are used as evidence in the research process and/or are commonly accepted in the research community as necessary to validate research findings and results. All other digital and non-digital content have the potential of becoming research data. Research data may be experimental data, observational data, operational data, third party data, public sector data, monitoring data, processed data, or repurposed data.

THE VALUE OF RESEARCH DATA

The value of research data extends beyond its significance to the research community, encompassing a broad spectrum of applications. It serves as a cornerstone for scientific discovery, innovation, and evidence-based decision-making across diverse disciplines. Research data provides critical insights that drive breakthroughs in fields such as healthcare, technology, and the social sciences, enabling the development of novel treatments, product improvements, and informed public policy.

In addition to its academic and societal contributions, research data plays a pivotal role in fostering economic growth by stimulating innovation and enhancing competitiveness within industries. As organizations increasingly leverage data for strategic purposes, the insights derived from research efforts bolster operational efficiencies and deepen consumer understanding. The rising emphasis on data-driven decision-making within both public and private sectors further underscores the fundamental importance of research data in shaping the future and addressing complex societal challenges.

WHY UNIVERSITY RESEARCH DATA ARE A TARGET

Reflecting the attention paid to it by the University and funding agencies, research data are highly valuable and widely accessible.

In some cases, however, researchers may not want to share their research data – or it may not yet be ready to be shared. In those cases, there needs to be stewardship. Research data that is not yet public can pose an attractive target for attackers seeking to exploit it for financial gain, competitive advantage, or to compromise the integrity of scientific advancements. Universities generate vast amounts of intellectual property, collaborate with government agencies and private entities, and operate within an open academic culture, which introduce unique risks.

Many of these risks will be part of a researcher's approved research ethics application and study protocol or sponsored research agreement with a governmental or private-sector sponsor or may be considered as part of a researcher's commercialization strategy. For example:

- **Intellectual Property (IP)**: Universities often generate valuable research in fields such as pharmaceuticals, technology, and engineering.
- **Government-Funded Research**: Projects involving defense, health, and space exploration are of strategic interest to nation-states seeking an advantage.
- **Economic and Competitive Benefits:** Research institutions contribute directly to economic growth by driving innovation. Attackers can exploit this data to gain market advantages, accelerate product development, or sabotage competitors.
- **Collaborative Networks with Multiple Entry Points**: Universities work closely with government agencies, private companies, and other institutions, creating multiple entry points for attackers to infiltrate systems and/or access research data.
- **Monetizable Personal and Medical Data:** Research involving personally identifiable information (PII), and medical data are highly valuable for identity theft, financial fraud, or extortion. Health-related data are particularly attractive to attackers targeting healthcare systems.

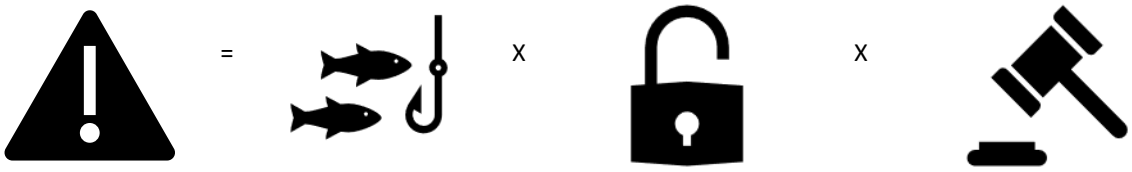
Acknowledging these factors, along with the potential for misuse, emphasizes the need to classify research data based on the specific risks and impacts associated with its type and use. Proper classification ensures that appropriate safeguards are in place to protect sensitive data, reinforcing academic integrity and supporting institutional security.

CALCULATING RISK

Considering the value of research data and its appeal to malicious actors, it is essential to align handling protocols, processes, and security controls with the assigned data classification. Researchers, with support from campus experts, must identify vulnerabilities and apply targeted cybersecurity measures to ensure data protection and reliable research outcomes. These efforts are critical to maintaining public trust and preserving the integrity of the research process.

Risk assessment involves evaluating threats to research and infrastructure, data exposure, and the impact of unauthorized disclosure, modification, or inaccessibility, forming the foundation for effective risk management.

Risk = Threat X Exposure X Impact (Harm)



- **Threat:** Any potential danger that could exploit a vulnerability to cause harm to an asset. This can include malicious actors, natural disasters, or system failures.
- **Exposure:** How exposed or available are the data to threats, or potential threats.
- **Impact:** The potential consequences or damage that could result from a successful exploit. This includes financial losses, reputational damage, legal implications, and operational disruptions.

RESEARCH DATA RISK CLASSIFICATION

The Research Data Classification System is based on two main factors: the type of data and the potential gravity of harm that could arise from a compromise to the Confidentiality, Integrity, and Availability triad which represents the three pillars of cybersecurity:

Confidentiality – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity — guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

Availability – ensuring timely and reliable access to and use of information.

The research data risk classification applies to all research data used/created while conducting research under the auspices of University of Waterloo. The data may be or has been collected and/or stored in paper or electronic form. This could include mobile devices, personal computers, portable media, and online storage. These can be privately- or university-owned and located on or off university premises.

While the research data risk classification encompasses several types of data and considers varied factors contributing to potential harm resulting to a compromise to the Confidentiality, Integrity, and Availability (CIA) than the confidentiality classification outlined in Policy 46 proposed data protection standards will align effectively with each other. This alignment will ensure a cohesive approach to safeguarding sensitive information across both frameworks. For more details about the classification of non-research information see Appendix A.

***NOTE:** *In cases of ambiguity in research data classification, the higher risk category should be applied. If uncertainty persists, please contact Information Security Services for guidance. For assistance with classifying human participant data, please contact the Office of Research Ethics.*

LOW

Research data are open or publicly available, a compromise to the integrity or availability of data would cause minimal harm to impacted/interested parties.

Examples (not exhaustive):

TYPE OF DATA	POTENTIAL HARM - MILD
○ Open data-available in an open repository ○ Public data sources (generally unstructured) ○ Open-source software source code. ○ **Anonymized information** – the information is irrevocably stripped of direct identifiers, ○ **Anonymous information** – the information never had identifiers associated	○ Temporary unavailability – inconvenience ○ Data corruption causing minor delays and/or small amount of rework ○ Minor reputational impact

○ Data not subject to agreement/contracts, sovereignty, regulations, or compliance standards ○ *Non-research data classified as Public as per* Policy 46	

MEDIUM

- **Research data are typically confidential, even if they are not specifically potentially governed by domestic or foreign laws or industry regulation; any compromise to the confidentiality, integrity or availability could lead to mild to moderate harm to** impacted/interested parties**.**
  Examples (not exhaustive):

TYPE OF DATA	POTENTIAL HARM - MILD TO MODERATE
○ Research data classified as confidential by external entities (i.e., funding agencies, corporate sponsors), agreements or contracts such as an NDA if higher-risk categories are not applicable ○ Data that is an active research stage and not yet ready for publication or sharing ○ Unpublished software source code ○ *Non-research data classified as Confidential as per* Policy 46	○ Data is unavailable causing delays in research that impact timelines ○ Data corruption causing moderate delays and/or moderate amount of rework ○ Legal consequences, injunctions, fines, or penalties ○ Harm to relationships ○ Moderate reputational damage ○ Loss of competitive advantage

HIGH

Research data are confidential and/or potentially governed by domestic or foreign laws or industry regulation; a compromise to the confidentiality, integrity or availability data would cause significant harm to impacted/interested parties**.**

Examples (not exhaustive):

TYPE OF DATA	POTENTIAL HARM – SIGNIFICANT
○ Human participant datasets that include: ▪ Personal Health Information (PHI) without any identifiers (direct or indirect) ▪ Personal Information that contains low-risk direct or indirect identifiers ▪ Data linkage that could re-identify participants ▪ Sensitive information: geolocation, private communications. ○ Research involving information/data classified by the Government of Canada as Protected A or B, per the Government of Canada's Contract Security Program (See Levels of security)	○ Data is unavailable causing major delays in research that impact timelines ○ Data corruption causing delays ○ Significant harm to study participants – discrimination, stigmatization, reputation, psychological harm, loss of autonomy ○ Ethics review and approval questioned ○ Mandatory reporting and public disclosure ○ Fines, legal liability, and compliance issues ○ Financial costs associated with a breach ○ Loss of potential future funding ○ Significant researcher and/or university reputational damage

○ Research involving critical infrastructure, as per the National Strategy for Critical Infrastructure ○ Research data involving critical minerals, as per the Canadian Critical Minerals Strategy. ○ Big data/large datasets that could be considered sensitive (depending on nature of data) and how they are used in the aggregate to reveal behavioral patterns/trends ○ *Non-research data classified as Restricted as per* Policy 46	○ University registration with the Contract Security Program or the Controlled Goods Program revoked ○ University disbarment from engaging in research involving protected government assets or information and technology subject to Canadian or U.S. export control regulations

VERY HIGH

Research data are confidential, and/or potentially governed by domestic or foreign laws or industry regulation, or Indigenous data sovereignty and any compromise to the confidentiality, integrity or availability of data could cause serious harm to impacted/interested parties.

Examples (not exhaustive):

TYPE OF DATA	POTENTIAL HARM - SERIOUS
○ Human participant datasets that include: ▪ Personal Health Information (PHI) with identifiers (direct or indirect) ▪ Personal Information that contains high-risk identifiers that can be used to perpetrate identity theft ○ Indigenous Data ○ Sensitive Technology Research Area data ○ Research involving information/data classified by the Government of Canada as Protected C or Secret, per the Government of Canada's Contract Security Program (See Levels of security) ○ Research data or information that is subject to Canadian or U.S. export control regulations ○ Research goods, including components and technical data that have military or national security significance, which are controlled by the Government of Canada's Controlled Goods Program ○ Research involving technology or data that is subject to specific international contract security requirements ○ Files including passwords and private encryption keys, biometrics ○ *Non-research data classified as Highly Restricted as per* Policy 46	○ Severe researcher and university reputational damage ○ Data is unavailable causing serious delays in research that would seriously impact timelines ○ Data corruption would cause serious delays ○ Ethics review and approval questioned ○ Mandatory reporting and public disclosure ○ Harm to study participants – identity theft, discrimination, stigmatization, reputation, psychological harm, loss of autonomy ○ Substantial financial costs associated with a breach and possible fines ○ Harm to Indigenous communities if the data are misappropriated or misused ○ Damage to the University's relationship-building with Indigenous communities and risks reputational damage re: breaking commitments to reconciliation, decolonization, and Indigenization ○ Future funding limitations to the university ○ University registration with the Contract Security Program or the Controlled Goods Program revoked ○ Fines to the individual or University from $25,000 to $2,000,000 per day of non-compliance. ○ Imprisonment for up to 10 years ○ Criminal and administrative penalties may also apply for violations of U.S. export laws and regulations

	○ University disbarment from engaging in research involving protected government assets or information and technology subject to Canadian or U.S. export control regulations ○ Threaten national security or public Safety ○ Ethical violations affecting national security

ROLES & RESPONSIBILITIES:

Policy 46 – Information Management outlines distinct roles and responsibilities for research team members. Under this policy, the Principal Investigator or Faculty Supervisor for research projects is the information steward for the research data while other research team members for the research project are information custodians. There may be times when this approach is different, for example in the context of when researchers are engaging with Indigenous communities.

RESEARCH DATA CLASSIFICATION FRAMEWORK

This framework provides researchers with a structured approach to classify their research data by assessing the potential harm that could arise from compromises in Confidentiality, Integrity, and Availability (CIA).

To calculate risk effectively, researchers must assess the following key factors:

1. **Determine the Scope**: Identify the impacted/interested parties**,** data types, research data lifecycle, and compliance obligations.
2. **Identify Expertise and Resources**: Identify internal or external experts (e.g., IT teams, Security, Ethics, Indigenous Data Sovereignty, legal advisors) to support the risk assessment.
3. **Identify Potential Harms & Impacts**: Assess the consequences of data breaches or misuse on individuals, the institution, and society.
4. **Identify & Assess Threats (Actors & Attacks)**: Consider actors such as nation-states, competitors, and insiders, and the attacks they may use (e.g., phishing, ransomware, espionage).
5. **Identify & Analyze Exposures**: Assess the level of exposure of data to threat actors, or potential threat actors
6. **Develop Strategies Based on Classification:** Based on the assigned classification, implement tailored security measures and data management strategies to address the specific risks, ensuring appropriate levels of protection, access control, and compliance with relevant policies and regulations.

STEP 1: DETERMINE THE SCOPE

The first step in the risk assessment framework for correctly classifying research data is to define the scope. This involves several key activities: identifying impacted/interested parties**,** determining the types of data that will be collected and managed and mapping the data lifecycle to understand how the data will flow through various stages of the research process. Also, researchers should identify the tools and processes used for data collection and management, as well as any compliance requirements related to data protection, privacy, and ethical

considerations. This comprehensive scope definition sets the foundation for effective risk assessment and data classification.

IDENTIFY IMPACTED/INTERESTED PARTIES

List all individuals or groups who have a vested interest in the research data or could be harmed by a compromise to the confidentiality, integrity, or availability. Consider not only potential harm to those directly involved but also consider the broader implications for the research community, the university, the public, and national security. Groups to consider include but are not limited to:

- **Researchers**
    - Principal Investigators, Co-Investigators, Collaborators, Graduate Students, Undergraduate Research Assistants, Post-doctoral Fellows, Staff
- **Research Participants**
    - Data/records- identifies/de-identified/anonymous, surveys, questionnaires.
- **University of Waterloo**
    - Institution, Faculty, Administration – Office of Research, Research Centre/Institute, Lab
- **Research Partners**
    - Institutional, Private, International
- **Research Sponsors**
    - Private, Public (Tri-Agencies, Municipal, Provincial, Federal), International, Non-Profit
- **Canada & Allies (**National Security, Democracy, Population Health, Economy, Infrastructure)
- **General Public (**Health, Safety, Rights & Freedoms)
    - Canadian citizens & permanent residents
    - Foreign nationals
- **Indigenous Peoples**
    - First Nations, Inuit, and Métis
    - International Indigenous Peoples

***Note on International Research Collaborations/Sponsors**

International research collaborations and funding, while pivotal for advancing scientific knowledge and fostering global cooperation, introduce heightened risks to research data security. A heightened awareness of the geopolitical landscape is required to identify potential risks associated with international collaboration and funding. The Office of Research published resources regarding the Government of Canada's National Security Guidelines for Research Partnerships, which help researchers, research institutions and funders identify and mitigate potential national security risks. The following are additional resources that help to identify countries and/or entities that contribute to a higher risk profile:

- Research which requires an export permit issued by the Minister of Foreign Affairs due to collaborations with institutions and/or researchers located in a country listed on the Area Control List of Export and Import Permits Act (EIPA).
- Research involving entities regulated by Canadian sanctions legislation, specifically the Special Economic Measures Act or the United Nations Act.
- Research involving individuals and entities subject to specific sanction regulations as listed on the Consolidated Canadian Autonomous Sanctions List.
- Research conducted in collaboration or funded by an organization on the Named Research Organization list (NRO) included in the Policy on Sensitive Technology Research and Affiliations of Concern or may

otherwise be deemed to have close linkages with hostile foreign military, state security intelligence agencies.

- Countries listed by the Canadian Centre for Cyber Security in the National Cyber Threat Assessment 2023-2024, which possess state-sponsored cyber threat programs.

Identify Data

Research data can come from diverse sources and practices, which vary based on how the data was collected and its intended purpose. Different types of data require different management strategies. Specify the types of data being used e.g., personal data, sensitive data, government-regulated data).

- **Human participant data:** Data from or about humans that are collected, obtained, and/or used as part of the research processes and outputs and/or used to answer the research question(s). Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition (TCPS2) Chapter 5: Privacy and Confidentiality outlines the following categories provide guidance for assessing the extent to which information could be used to identify an individual:
    - **Directly identifying information** – the information identifies a specific individual through direct identifiers
    - **Indirectly identifying information** – the information can reasonably be expected to identify an individual through a combination of indirect identifiers
    - **Coded information** – direct identifiers are removed from the information and replaced with a code.
    - **Anonymized information** – the information is irrevocably stripped of direct identifiers,
    - **Anonymous information** – the information never had identifiers associated

> *For more information about Human Participant Data and ethical considerations in being respectful stewards of their data, please review the* **Guideline on securing human research participant information and data** **and** *contact the Research Ethics team (researchethics@uwaterloo.ca).*

- **Indigenous Data** including any data, information, and knowledge, in any format, that impacts Indigenous Peoples, Nations, and Communities at the collective and individual levels including:
    - Data about Indigenous **Resources and Environments** (land, water, geology, titles, air, soil, sacred sites, territories, plants, animals, etc.)
    - Data about Indigenous **Peoples as Individuals** (administrative, legal, health, social, commercial, corporate, services, demographics, etc.)
    - Data about Indigenous **Peoples as Collectives** – Nations, Peoples, and Communities (traditional and cultural information, archives, oral histories, literature, ancestral and clan knowledge, stories, belongings, etc.)

For more information about Indigenous Data Sovereignty and considerations in being respectful stewards of Indigenous data, please contact the Indigenous Research team (Indigenous.Research@uwaterloo.ca).

Definition

Indigenous Data Sovereignty: is the authority of Indigenous peoples, Nations and communities over their own data, how their data are framed, and how their data are managed. This includes sovereignty over the collection, use, control, access, possession, and sharing of these data. These rights are recognized and upheld by the United Nations Declaration on the Rights of Indigenous Peoples.

- **Open data are available to the public so that anyone can view, use, modify, and share as permitted by the license.** See Creative Commons for license options. Open data are typically accompanied by a license that promotes openness and transparency. Characteristics include:
    - Accessible without barriers, such as paywalls or registration requirements.
    - Formatted in a way that is easy to use and analyze, such as CSV or JSON, and not locked into proprietary formats.
    - Use the data for any purpose, including commercial use, if they comply with the terms of the open data license.
    - Promotes transparency and accountability in government and organizations, allowing citizens to engage with and understand information.
- **Publicly available** can be accessed by the public but may not necessarily adhere to the principles of openness. It may be available for viewing but could have restrictions on use, modification, or redistribution. Characteristics include:
    - May be some barriers, such as the need to register or agree to terms of use.
    - Limitations on how the data can be used, such as prohibiting commercial use or requiring attribution.
    - Not always provided in a user-friendly format.
    - May require permission to access or have an associated fee.
- **Regulated Data:** information that is protected by local, national, or international statute or regulation mandating certain restrictions.
- **Administrative Data** collected from administrative systems (e.g., government or institutional databases) and is commonly used in fields like health and social sciences.
- **Online Services Data** encompasses a wide range of information from online activities (like search engines and e-commerce) and can be valuable for various research inquiries.
- **Aggregate Data**: Data presented in summary form, where individual responses are combined to provide overall trends or statistics, such as survey results showing the average response from a group without revealing individual data points.
- **Confidential Information**: where there is an expectation that such information will not be disclosed to anyone except those people requiring the information for a legitimate purpose. Confidential information must be protected against unauthorized use (as "use of information" is defined, above) or disclosure.
- **Sensitive research areas data** identified in Annex A of the National Security Guidelines for Research Partnerships
    - Research subject to the **Export Control List (ECL)** of the Export and Import Permits Act (EIPA). Examples include:
        - conventional weapons and dual-use goods

        - missile and rocket technology, space technology and chemical and biological weapons and agents
        - nuclear programs
    - Research in the area involving or applicable to **nuclear programs** that are subject to the Nuclear Non-proliferation Import and Export Control Regulations.
    - Research in areas related to goods or technology identified in the Schedule (section 35) of the Defense Production Act (known as the Controlled Goods List) are sensitive and subject to the **Controlled Goods Program**; and/or technical data as defined by Technical Data Control Regulations also under the authority of the Defense Production Act
    - **Sensitive Technology Research Areas or dual-use technologies** that have both civilian and military applications, See Canada's Policy on Sensitive Technology Research and Affiliations of Concern
    - Additional research areas data that can be considered sensitive:
        - Research involving the 31 **critical minerals** which are deemed critical in the Canadian Critical Minerals Strategy and play a vital role in economic security, national transition to a low-carbon economy, and strategic partnerships
        - Research involving the 10 **critical infrastructure** sectors outlined in Canada's National Strategy for Critical Infrastructure which are processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.
        - **Big data/large datasets:** Semi-structured and unstructured data in a wide variety of formats, in large volumes, and produced at high speed. "Big" data, by virtue of their volume, velocity, or variety cannot be easily stored or analyzed with traditional methods. Things like sensors, Internet of Things (IoT) devices, and social media all create "big" data. This data can be analyzed to reveal patterns, trends, and associations, particularly concerning human behavior and interactions. The sensitivity of these datasets depends on factors like the nature, type, and state of the information contained, as well as how the data might be utilized in the aggregate.
        - Research areas that use **sensitive personal data** that could be leveraged by hostile state actors to harm Canada's national and economic security through its exploitation. a list of examples of sensitive data.

For more information about **Sensitive research areas** *Data and considerations in being responsible and compliant stewards the data, please review Safeguarding Research* **and** *contact the Research Security team (*safeguardingresearch@uwaterloo.ca*).*

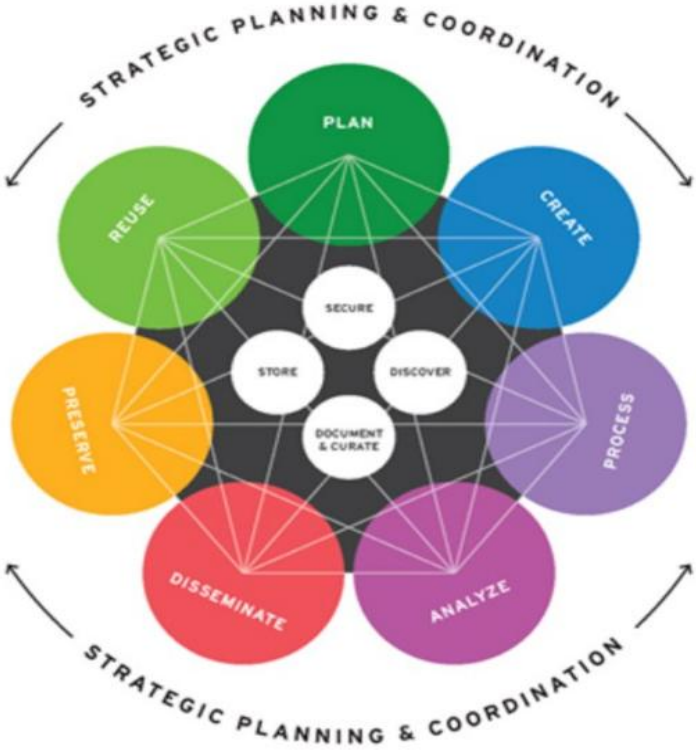
Map the Data Lifecycle:

The Research Data Lifecycle acts as a roadmap for researchers, outlining key considerations for Research Data Management (RDM) at each stage.

Researchers should also consider the extent to which the data are interconnected with other systems or datasets. This assessment helps identify the potential impact of data breach or exploit on other parts of the research

ecosystem and highlights key impacted/interested parties and their roles in managing and protecting the data throughout its lifecycle.

Summary of the Research Data Lifecycle Phases



Plan: organize research data for discovery, reuse, and archiving and creating a data management plan (DMP).

Create: identify, acquire, and generate research data and metadata.

Process: data are prepared for analysis through validation and cleaning.

Analyze: analyze prepared data.

Disseminate: share findings.

Preserve: transition data to an archival state.

Reuse: ensure data are discoverable and accessible for integration into new datasets.

The following elements need to be considered at each phase of the research data lifecycle and should be integrated into the DMP; the specific implementation of these elements will vary based on the assessed risk level classification of the data.

- **Store**: The active and archival storage of data, with an emphasis on accessibility and security.
- **Discover**: Ensuring data discoverability to facilitate accessibility and mobilization for future research use.
- **Document and Curate**: Providing rich descriptions of data context.

- **Secure**: Addressing consent, ethical considerations, and maintaining integrity while utilizing established security platforms and guidance from privacy and IT security services.

The Library offers Research data management services (RDMS) to support researchers in developing research data management plans (DMPs). The DMP Assistant is a free online data management planning tool, developed by the Digital Research Alliance of Canada available for researchers.

Identify Compliance Requirements:

Certain research areas are subject to regulatory oversight, while others may not face such constraints. It is crucial to identify the applicable contractual, ethical, regulatory, legislative, and data sovereignty considerations relevant to the data being managed to ensure compliance.

- University of Waterloo Policies
  - **Intellectual property rights – Policy 73**
  - Policy 41 – Contract* Research at University of Waterloo
  - Policy 46 - Information Management
  - Policy 11 - University Risk Management
- Tri-Agency Open Access Policy on Publications, which requires making peer-reviewed journal publications freely accessible online within 12 months of publication through an institutional repository or publisher's website. This includes complying with any additional requirements for specific funding agencies (e.g., CIHR's data deposit requirements) and best practices for metadata creation and long-term preservation.
- Research Ethics Board (REB) review at Waterloo or an external REB.
- As outlined in the Tri-Agency Policy on Research Data Management, researchers must adhere to the distinct data governance frameworks, community protocols, and data stewardship practices that dictate how research data involving Indigenous knowledge, culture, or heritage should be collected, used, shared, and protected.
  - Indigenous data sovereignty U.S. Indigenous Data Sovereignty Network (usindigenousdatanetwork.org)
- Research Regulated by:
  - *Export Control List* (ECL) of the *Export and Import Permits Act* (EIPA).
  - Nuclear Non-proliferation Import and Export Control Regulations.
  - Schedule (section 35) of the Defense Production Act (known as the Controlled Goods List)
  - Controlled Goods Program
  - Technical Data Control Regulations
  - Defense Production Act
- Data may also be subject to the following Canadian legislations:
  - Canada Federal: The Privacy Act
  - Canada Federal: Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Ontario Provincial: Personal Health Information Protection Act (PHIPA) and those of other provinces
- Data may also be subject to the following international standards, regulations, or legislations:
  - European Union: General Data Protection Regulation (GDPR)
  - United States Federal: Federal Information Security Modernization Act (FISMA)
  - United States Federal: Controlled Unclassified Information (CUI)
  - United States Federal: International Traffic in Arms Regulations (ITAR)
  - United States Federal: Family Educational Rights and Privacy Act (FERPA)

- Data may also be subject to the following international security standards:
  - International: Payment Card Industry Data Security Standards (PCI-DSS)
  - National Institute of Standards and Technology (NIST) Special Publication 800 Series
  - International Organization for Standardization/International Electrotechnical Commission ISO/IEC 27001

STEP 2: IDENTIFY EXPERTISE AND RESOURCES

Engage Expertise: Identify individuals or teams within the University of Waterloo who can provide guidance on various aspects of the research project regarding data management (e.g., IT specialists, legal advisors, data management experts).

By understanding the vulnerabilities inherent in research data, with help from expertise across campus, researchers can implement targeted cybersecurity measures that fortify defenses against breaches, ensuring the protection of research data and the reliability of research outcomes. Such proactive strategies are essential in maintaining public trust and upholding the integrity of the research process.

Topic	UW Contact & Resources	External Resources (non-exhaustive)
Sensitive research areas identified on Annex A of the National Security Guidelines for Research Partnerships - Regulated Research Areas – Export Controls, Controlled Goods - Sensitive Dual Use Technology - Big Data/Large Data Sets - Critical Infrastructure - Critical Minerals	safeguardingresearch@uwaterloo.ca Safeguarding Research Team Safeguarding Research	National Security Guidelines for Research Partnerships The National Security Guidelines for Research Partnerships' Risk Assessment Form Sensitive research areas National Strategy for Critical Infrastructure The Canadian Critical Minerals Strategy A Guide to Canada's Export Control List The Export and Brokering Controls Handbook Research Security Safeguarding Your Research
Research involving Human Participants including Indigenous Research subject to Research Ethics Board (REB) review or an external REB review.	researchethics@uwaterloo.ca Research Ethics Team Office of Research Ethics Guideline on securing human research participant information and data Privacy and security research risk assessment tool Research with Indigenous Peoples	Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition (TCPS2).
Research Partnerships International research collaborations and sponsors	Safeguarding Research Team Connect with the Corporate Research Partnership Team Research Partnerships Contracts Team Non-profit/public sector research partnerships	National Security Guidelines for Research Partnerships

	Senior Manager, Knowledge Mobilization and Partnerships	
Indigenous Data	Senior Manager, Indigenous Research Resources and Guides for Indigenous Research	The First Nations Information Governance Centre: Home First Nations Principles of OCAP® CARE Principles Principles of Ethical Métis Research National Inuit Strategy on Research United Nations Declaration on the Rights of Indigenous Peoples U.S. Indigenous Data Sovereignty Network
Research Data Management	research data management services (RDMS) at the University of Waterloo Library	Digital Research Alliance of Canada
Security Controls	Information Security Services (ISS) Research Project Cybersecurity Planning Research Computing Services Directory Security policies, standards, and guidelines IST (Information Systems & Technology) Service Catalogue: Security Information security for research Guidelines for secure data exchange	Canadian Centre for Cyber Security: Top 10 IT security actions The top 18 CIS Critical Security Controls NIST SP 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations
Threats & Exposures	Information Security Services (ISS) Research Computing Services Directory Safeguarding Research Team Cyber Awareness training Cyber Awareness website	Canadian Centre for Cyber Security How to protect your organization from insider threats Who are you at risk from? Protect your research - Ontario National Cyber Threat Assessments
Research Computing	Research computing infrastructure Research Computing Services Directory	Digital Research Alliance of Canada: Advanced Research Computing

STEP 3: IDENTIFY POTENTIAL HARMS & IMPACTS

Assess Harm Scenarios: List the types of harms and the impacts that could occur because of a successful exploitation that caused:

- Loss of **Confidentiality:** Data breach, unauthorized access, or unauthorized disclosure that exposes personal information or other confidential information and non-compliance with regulations leading to privacy violations, identity theft, legal penalties, or reputational damage.
- Loss of **Integrity:** Manipulation or falsification of data can undermine research outcomes, compromise trust, and damage the credibility of the findings.
- Loss of a**vailability**: Inaccessibility of data during critical phases can disrupt research activities, delay results, and hinder decision-making.

The successful exploitation of research data can result in a variety of significant impacts that reverberate across multiple dimensions of academic and scientific endeavors. The following is a non-exhaustive list of examples of potential impacts:

- **Reputation:** Breaches of research data can inflict reputational damage on individual researchers, academic institutions, or research organizations, eroding trust, and credibility within the scientific community, among impacted/interested parties and the public.

- **Loss of Trust:** Compromised confidentiality can erode trust in Waterloo's abilities to produce and manage the data. If impacted/interested parties, including the public and decision-makers, believe UW's data are not secure, they may be less likely to engage or collaborate in future research or policy initiatives.

- **Delayed Research**: A cyber-attack can disrupt research data availability, causing delays in the research process and hindering scientific advancement. Disruptions on critical resources, systems, and data within the research environment, including their impact on research operations, project timelines, and collaboration efforts.

- **Financial costs**: Costs associated with remediating data breaches, conducting forensic investigations, and implementing security measures can impose significant burdens on institutional budgets, research budgets, and organizational resources. This financial strain can hinder the ability of the University of Waterloo to allocate resources effectively, impairing the capacity to pursue innovative projects, attract top talent, and remain competitive in securing funding grants. Financial impacts extend beyond immediate remediation efforts, impacting the sustainability and growth of research initiatives and jeopardizing the advancement of scientific knowledge in critical areas.

- **Integrity and reliability:** Exploitation of research data compromises the integrity and reliability of findings, potentially leading to misinterpretations and undermining the credibility of scholarly work. Disruptions and delays stemming from compromised data integrity raise concerns about the reliability and reproducibility of research findings.

- **Misinformed Decision-Making:** If the integrity of the data are compromised, it may lead to incorrect conclusions, resulting in misguided policies, or flawed business strategies. This can exacerbate existing problems or create new challenges

- **Due diligence**: A successful attack can result in accusations of negligence in due diligence, non-compliance with regulatory requirements, ethical breaches, and violations of contractual agreements and obligations.

- **Debarment:** The University could be debarred from conducting research involving Canadian and/or U.S. controlled goods and government-controlled assets. Future funding limitations can be imposed on the University if our registration with the Contract Security Program or the Controlled Goods Program is revoked. No further federal funding would be permitted if access to protected government assets or if access to technology/goods subject to Canadian or U.S. export controls is required.

- **Loss of Potential Funding**: When sensitive research data are compromised, it raises concerns among funding bodies about the reliability and security of the research, leading to reduced confidence in the project's viability. This loss of trust can hinder researchers' ability to secure future financial support, limiting their capacity to pursue innovative projects, hire essential staff, and acquire necessary resources. Such funding setbacks can stifle scientific advancement and diminish the institution's credibility, making it increasingly challenging to attract future grants and partnerships.

- **Criminal:** Failure of a researcher to comply with Controlled Goods Regulations may lead to fines for the researcher and /or university of up to $2,000,000 and/or imprisonment for up to 10 years. Additional criminal and administrative penalties may also apply for violations of U.S. export laws and regulations.

- **Theft and illicit transfer of technology and know-how** can have significant consequences, particularly in the realm of IP and innovation. When proprietary technologies or trade secrets are unlawfully obtained or transferred, it jeopardizes the competitive advantage and market position of the affected entities. There is also a risk of reverse engineering, through which perpetrators dissect and analyze the stolen technology to replicate or modify it for their own purposes. This type of activity not only undermines the original creator's investment in research and development but also fosters unfair competition and erodes trust within industries.

- **Harm to Research Participants:** A compromise to the confidentiality of human participant research data or reidentification can significantly harm human participants by exposing their personal information, leading to risks such as identity theft, privacy violations, and reputational damage. Additionally, compromised data integrity may result in inaccurate conclusions about participants, or that of the community in which they reside or the group to which they are affiliated, which can affect them economically, socially, or psychologically, just to name a few.

- **Harm to Indigenous Communities & Reputational Risks:** There are many risks when it comes to Indigenous data being exploited, both to Indigenous Communities and to the University. Improper use, analysis, or misappropriation of Indigenous data can have detrimental impacts on the well-being of Indigenous Communities, with far-reaching implications such as the imposition of colonial policies, ongoing systemic discrimination, cultural exploitation, and loss of sovereignty and agency for the Communities themselves. A breach relating to Indigenous data may also harm the University's efforts in relationship-building, erode trust between researchers and the Communities, compromise commitments to Reconciliation, Decolonization, and Indigenization, and discourage Communities from partnering with other researchers in future projects.

- **Critical Minerals**: A data compromise related to these minerals could jeopardize the integrity of the Canadian Critical Minerals Strategy, which identifies 31 minerals deemed "critical" by the federal government. If research involves the extraction, processing, or use of these minerals, the implications of a data breach could be significant. Critical minerals are essential components in various technologies and industries, playing a vital role in economic security, the transition to a low-carbon economy, and strategic partnerships. Researchers may need to account for environmental, social, and economic factors associated with critical minerals.

- **National security:** The pursuit of advancing research can have implications for national security, as certain research domains have the potential to compromise national security foreign governments may seek to interfere with or exploit Canada's open research environment by employing a comprehensive approach to acquire pre-publication data, results, methods, knowledge, intellectual property, and talent. These infringements pose a significant threat to the security of Canada's research ecosystem.

- **Sensitive and dual-use research** and resulting technologies could have the capacity to enhance a foreign state's military, intelligence, or surveillance capabilities, posing a potential risk to Canada's national security interests and ability to identify and counteract threats or by causing disruptions to the economy, society, and critical infrastructure in the case of a breach.

- **Practices by Foreign Entities:** There is a potential risk that foreign militaries or governments could exploit research for purposes that compromise individual liberties or contribute to political and military oppression. The use of research findings by entities with differing political agendas raise concerns about the unintentional facilitation of activities such as internal surveillance, suppression of political dissent, or military operations that may violate human rights. This misuse of research could have serious implications for both individuals and communities.

- **Critical infrastructure:** Vulnerable critical infrastructure poses a significant national security threat due to the potential for malicious exploitation of vulnerabilities. A data compromise in this context could lead to disruptions in critical infrastructure, resulting in catastrophic loss of life, adverse economic impacts, and significant harm to public confidence. Investigating weaknesses or revealing sensitive information about these vital systems may inadvertently create a roadmap for malicious actors or adversaries. Such research could enable the development of cyber threats, attacks, or disruptive strategies targeting the essential services and operations that sustain a country. The Canadian Centre for Cyber Security has identified state-sponsored espionage and threats to critical infrastructure as pressing concerns.

- **Public Safety:** If research data related to critical infrastructure systems, such as energy grids or transportation networks, is compromised, it may lead to disruptions that pose risks to public safety and the provision of essential services**.** If research data related to infectious diseases or bioengineering is breached, it could facilitate the misuse of information for harmful purposes, potentially resulting in public health crises. Overall, compromised research data can undermine the safety and security of the public by enabling threats that disrupt vital services and create dangerous conditions.

- **Big Data/Large Datasets**: One such risk is the potential for poisoned datasets, wherein malicious actors intentionally manipulate or insert false information into the dataset. These actions can then lead to skewed research outcomes, misinformed decisions, and damage to the integrity of the dataset. Big data and large datasets can be analyzed to reveal patterns, trends, and associations, particularly concerning human behavior and interactions. The sensitivity of these datasets depends on factors like the nature, type, and state of the information contained, as well as how the data might be utilized in the aggregate. Identification of large datasets with ethical, commercial, or legal ramifications at various levels could designate them as a lucrative research area, entailing national security considerations.

STEP 4: IDENTIFY & ASSESS THREATS (ACTORS & ATTACKS)

- **Identify Potential Threats:** Determine who or what could cause harm, including:
  - Internal threats (e.g., employee error/negligence, malicious insiders)
  - External threats (e.g., cybercriminals, nation states)
- **Assess Threats:** Assess the threats based on skill, motivation, opportunity, and size
- **Attacks:** Identity potential attacks

THE THREAT AGENT

Threat agents are the entities or factors that pose a risk to the data and usually operate with malicious intent to exploit vulnerabilities. Research data can be targeted by various threat agents for a range of reasons. The Canadian Center for Cybersecurity has identified the following threat agents:

- **Advanced persistent threats (APT)** are sophisticated and well-funded threat actors who target specific organizations or entities over an extended period.

- **Cybercriminals** are individuals or a group who engage in criminal activities conducted over the internet or using computer technology to commit crimes such as extortion, identity theft, or fraud.
- **Hacktivists** are individuals or groups who engage in hacking activities for political or social causes, expose perceived injustices, challenge authority, or disrupt research projects that they oppose ideologically.
- **Insider Threats** are employees, contractors, collaborators, or sponsors who intentionally or unintentionally compromise research data through negligent or malicious actions.
- **Nation-states** are sovereign states (i.e., a country) that actively engages in cyber espionage, cyber warfare, or cyberattacks conducted by or on behalf of a government.
- **Terrorist groups** or organizations employ cyber capabilities as part of their tactics, strategies, or objectives to further its ideological, political, or social agenda through acts of terrorism. Knowledge or materials for the development of weapons of mass destruction are a prime target.
- **Thrill-seekers** are individuals who engage in hacking activities purely for the personal gratification or excitement of it, rather than for financial gain, ideological motives, or any specific agenda.

THREAT AGENT FACTORS:

Threat Agents should be assessed based upon the following factors:

- **Skills/capabilities** include technical expertise, knowledge of cyber tools and techniques, and proficiency in carrying out attacks.
- **Motive** determines the underlying reasons or objectives driving the actions of threat agents, whether financial gain, political motives, espionage, or other malicious intents
- **Opportunity** includes access to full resources or expensive tools necessary to execute sophisticated attacks effectively. This factor also encompasses the extent of access to vulnerable systems or networks.
- **Size** of the threat agent influences their capabilities, reach, and potential impact on research data security.

The threat agent	Skill	Motive	Opportunity	Size
Advanced persistent threats (APT)	**Highly Skilled** Sophisticated techniques, advanced tools, strategic objectives, and persistent targeting.	**Highly Motivated** Competitive advantage, stealing IP, or intelligence for espionage	**Significant** Capitalize on opportunities to infiltrate and compromise targeted systems or networks.	**Varies** Individual actors, small teams, larger organized entities, nation-state-sponsored cyber units, or well-funded criminal organizations.
Cybercriminal	**Varies** Basic to advanced knowledge of computer systems, networking, and cybersecurity.	**Highly Motivated** Financial profit, direct theft, fraud, extortion, sale of stolen data.	**Moderate** Accessibility of hacking tools, exploit kits, and dark web marketplaces allows them to launch attacks with minimal investment.	**Varies** Individuals or small groups, often collaborating via forums and communities.
Hacktivists	**Varies** Basic to advanced knowledge of	**Highly Motivated** Social or political causes and seek to	**Moderate** Take advantage of online forums, social	**Varies** Individuals, organized groups, collectives,

	computer systems, networking, and cybersecurity.	promote their ideologies, raise awareness about issues, or enact change through online activism.	media platforms, and communication channels.	networks, coalitions of diverse memberships/ affiliations.
Insider Threats	**Varies** Limited technical expertise to highly skilled with advanced knowledge of systems and security protocols.	**Highly Motivated** Financial gain, personal grievances, ideological beliefs, or coercion.	**Significant** Insider knowledge, extensive privileges/permissions, legitimate access to systems, networks, and data/sensitive information.	**Varies** Individual employees, contractors, or partners acting alone or in collusion with others.
Nation-states	**Highly Skilled** Advanced technical skills, knowledge, and resources.	**Highly Motivated** Geopolitical, military, economic, or ideological interests.	**Significant** Access to state-sponsored cyber infrastructure, resources, and support.	**Significant** Specialized cyber units, intelligence agencies, military branches, or government entities dedicated to cyber operations.
Terrorist Groups	**Varies** Rudimentary hacking skills to sophisticated cyber warfare capabilities.	**Highly Motivated** Ideological, political, or religious beliefs spread propaganda, instill fear, create chaos.	**Significant** Often have access to financial resources and have a global reach to recruit members, disseminate propaganda, and coordinate attacks.	**Varies** Small, decentralized cells or large groups. Collaborate with broader networks/alliances, other extremist organizations, or state sponsors.
Thrill-seekers	**Varies** Amateur enthusiasts with basic knowledge to hackers with advanced expertise in computer systems and networks.	**Motivated** Thrill, adrenaline rush, curiosity, a desire to learn, or a fascination with technology, push boundaries and test the limits of skills.	**Moderate** Participate in online communities, hacking tutorials, forums, and open-source hacking tools.	**Small** Individuals, small groups, hacking communities.

The attack.

Threat agents employ a diverse range of tools and techniques to execute their attacks. The Canadian Center for Cybersecurity provides a non-exhaustive list of common tools and techniques that are used by threat actors. MITRE ATT&CK® also provides a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. Researchers can consult with their respective Information Technology administrators and ISS/IST to identify applicable attacks. Below are a few examples of the types of attacks researchers should be concerned with:

- Credential and Authentication Attacks
- Social Engineering & Elicitation
- Malware Attacks (Ransomware)
- Network-Based Attacks
- Web Application Attacks
- Software Vulnerability Exploit Attacks
- Hardware and Supply Chain attacks

STEP 5: IDENTIFY & ANALYZE EXPOSURES

Assess the level of exposure of data to threat actors, or potential threat actors. Researchers should consider to whom the data will be available, what level of access is required by collaborators, and other special requirements or considerations for data storage (e.g., specialized data deposit repositories, code repositories). Factors to consider include:

- Proposed **storage location** for the data.
  - Physical, technical, and administrative security controls in place.
  - Volume of data/records
  - Backup frequency
  - Archival strategy for inactive data (e.g., cold storage, long-term preservation)
  - Compliance
- **Number of people** who can modify the data.
  - User profiles – researchers, student, staff
  - Role based access controls
  - Permissions granularity – read/write
  - Access frequency and volume - how much and how often is data accessed
- **Location from where** researchers access or modify the data.
  - Working from home
  - International or external domestic institutions or labs
- The **security of devices** used to access and/or modify the data.
  - Endpoint protection – e.g., Sentinel One
  - Vulnerability management and assessment – e.g., Qualys (to identify and mitigate device vulnerabilities)
  - Device authentication and access controls
  - Full-disk encryption
  - Device management policies
- **Level of collaboration** in performing the research referring to the extent and nature of teamwork involved in a research project. It can range from independent efforts to highly integrated, multi-institutional partnerships Factors to consider include:
  - Internal vs. External Partnerships

    - International collaboration
    - Interdisciplinary Engagement
    - Decision-Making and Resource Sharing
- Required/desired **interfaces** to access or modify the data (e.g., APIs)
    - Authentication and Authorization requirements (e.g., API keys, OAuth, SSO)
    - Data transfer protocols (e.g., HTTPS, TLS)
    - Logging and monitoring for API usage (e.g., access logs, activity monitoring
- **Data retention requirements** for the data.
    - Legal and regulatory requirements
    - Destruction protocols at end of lifecycle (e.g., secure deletion, certification)
    - Backup frequency and recovery to support retention
- **Software** required to access or modify the data.
    - Software licensing and compliance (e.g., open-source, proprietary)
    - Vendor security practices and risk assessment (for third-party tools)
    - Authentication requirements specific to software (e.g., multi-factor authentication)

STEP 6: DEVELOP STRATEGIES BASED ON CLASSIFICATION

Based on the previous steps, researchers should be able to confidently classify their research data according to the risk classification. With this classification in hand, researchers can engage with identified expertise on campus and work together to implement appropriate strategies to mitigate identified risks associated with potential harms, threats, and exposures.

This includes establishing policies and procedures for data protection, implementing security measures to safeguard data integrity and confidentiality, and ensuring availability through backup and recovery plans.

Also, researchers should prioritize training for personnel on best practices for data handling and security and establish clear protocols for responding to data breaches or incidents.

A thoughtful risk assessment, coupled with appropriate classification and security controls, ensures research data are properly safeguarded throughout the research data lifecycle and aligned with institutional policies and compliance requirements.

CONCLUSION:

In conclusion, this Research Data Risk Classification Framework provides a standardized approach for classifying research data based on the potential harm that could arise from compromises in Confidentiality, Integrity, and Availability. By implementing this framework, researchers at the University of Waterloo can ensure effective communication and collaboration among research impacted/interested partie**s**, including researchers, faculty administration, the Library, Information Security Services (ISS), Information Systems and Technology (IST), the Office of Research (OR), and the Office of Indigenous Relations.

The framework emphasizes the importance of safeguarding research data to maintain compliance with regulatory standards and protect sensitive information. It highlights the value of research data in driving scientific discovery, innovation, and evidence-based decision-making across various fields. Additionally, the framework addresses the unique risks associated with university research data, such as intellectual property, government-funded research, economic and competitive benefits, collaborative networks, and open academic culture.

By classifying research data in a standardized manner, researchers can identify vulnerabilities, apply targeted cybersecurity measures, and ensure data protection and reliable research outcomes. This collaborative and standardized approach enhances the overall data governance structure, promoting a cohesive effort in safeguarding research data and maintaining public trust in the research process.

APPENDIX A: INFORMATION NOT CONSIDERED RESEARCH DATA

Certain types of information are not classified as research data under the definition provided and are subject to the Freedom of Information and Protection of Privacy Act (FIPPA). This information should be classified according to Policy 46 Confidentiality Classifications. Examples of such information include:

- **Research Papers:** Scholarly articles presenting findings of research, including analyses and conclusions, but not classified as raw research data.
- **Administrative Records**: Documentation related to the planning and administration of research activities that do not involve the direct collection of data.
    - Cover Sheets
    - Grant Proposals
    - Data Management Plans (DMPs)
    - Cybersecurity plans
    - Equity, Diversity & Inclusion plans
- **Financial Data:** Budgetary and financial documents that do not pertain directly to specific research data.
- **Personnel Records:** Information related to staff and graduate students that does not involve research data collection or analysis.
- **Human participant information**: Personal information collected and used to run a research study such as contact information (names, phone numbers, email). This is not required to answer the research question(s).
- **Contractual Agreements:** Agreements with external collaborators or institutions that do not include research data.
- **Correspondence**: Communication related to the administration of research but not involving research data collection or analysis.
- **Policy Documents**: Institutional policies and guidelines not directly related to specific research projects.
- **Data about external partners or institutions** involved in the research project, including their expertise and contributions.
- **Intellectual Property (IP):** Creations of the mind (e.g., inventions, trademarks) resulting from research activities, but not considered research data. See Policy 73 for more details.

REFERENCES

Canada, Govenment of. (n.d.). *National Cyber Threat Assessments.* Retrieved from Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessments

Canadian Introduction to the cyber Threat Environment. (2022). *An introduction to the cyber threat environment.* Ottawa: Communications Security Establishment.

Govenmnert of Canada. (2009). *National Strategy for Critical Infrastructure.* Canada: Her Majesty the Queenin Right of Canada,.

Government of Canada . (2021). *Tri-Agency Research Data Management Policy.* Government of Canada .

Government of Canada . (n.d.). *State-sponsored espionage and threats to critical infrastructure.* Retrieved from Canadian Centre for Cyber Security: https://www.cyber.gc.ca/en/guidance/state-sponsored-espionage-and-threats-critical-infrastructure

Government of Canada. (2023). *Access to Information Review Indigenous-specific What We Heard Report.* Ottawa: Government of Canada.

Identity Defined Security Alliance. (2022). *2022 Trends in Securing Digital Identities.* Identity Defined Security Alliance.

Innovation, Science and Economic Development Canada . (2022). *Safeguarding Your Research.* Ottawa: Government of Canada.

Innovation, Science and Economic Development Canada . (2024). *National Security Guidelines for Research Partnerships.* Ottawa: Government of Canada.

Minister of Natural Resources. (2022). *The Canadian Critical Minerals Strategy.* His Majesty the King in Right of Canada, as represented by the Minister of Natural Resources.

National Cybersecurity Center of Excellence Information Technology Laboratory. (2018). *Privileged Account Management for the Financial Servies Sector.* National Institute of Standards and Technology.

Panel on Research Ethics. (2022). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022).* Government of Canada.

Portage Network Sensitive Data Expert Group on behalf of the Canadian Association of Research Libraries (CARL). (2020). *Sensitive Data Toolkit for Researchers.* Portage Network Sensitive Data Expert Group.

Portage Network Sensitive Data Expert Group on behalf of the Canadian Association of Research Libraries (CARL). (2020). *Sensitive Data Toolkit for Researchers: Part 1: Glossary of Terms for Sensitive Data used for Research Purposes.* Portage Network Sensitive Data Expert Group.

The Government of Canada. (n.d.). *National Cyber Threat Assessment 2023-2024.* Retrieved from Canadian Centre for Cyber Security : https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024