**IM Legal and Regulatory Framework Worksheet**

Populate this table with all relevant legislation, policies, procedures, regulations, contracts, and agreements (i.e. collective agreements) that contain IM requirements within which the University, or specifically your Unit, must comply. To get started, some sections of this table have been pre-populated with relevant legislation and policy that is applicable University-wide.

| **IM Legal and Regulatory Framework** |
| --- |
| **Reference - *Management of Information of Act*** |
| **IM Compliance Requirements** |
| 6. (1) A permanent head of a public body shall develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, disposal and transfer of public records.  6. (2) A system required under subsection (1) shall provide for retention periods and disposition by  (a) destruction, or  (b) transfer to the archives,  In accordance with the guidelines and schedules established by the Government Records Committee established under Section 5.1  6. (3) A permanent head of a public body shall ensure that the retention, disposal and removal of public records is carried out in accordance with this *Act*. |
| **Reference - *Access to Information and Protection of Privacy Act (ATIPPA)*** |
| **IM Compliance Requirements** |
| *ATIPPA* focuses on protection of privacy and access to information, not specifically on the management of information; however, mature IM practices enable compliance with ATIPPA. Examples of IM Compliance Requirements are as follows:  **Right to request correction of personal information**  **10.** (1) An individual who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.  **Protection of personal information**  **64.**  (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that  (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;  (b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and  (c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.  (3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is  (a) stolen;  (b) lost;  (c) disposed of, except as permitted by law; or  (d) disclosed to or accessed by an unauthorized person. |
| **Reference – *TRI-Agency Framework*** |
| **IM Compliance Requirements** |
| *TRI-Agency Framework* defines the responsibilities and corresponding policies for researchers, Institutions, and the Agencies. Examples of IM Compliance Requirements are as follows:  ***Responsible Conduct of Research***  **4.  Responsibilities of Institutions**  **4.3 Institutional Policy Requirements for Addressing Allegations of Policy Breaches**  The Institution shall develop and administer a policy(ies) to address allegations of policy breaches by researchers that meets the minimum requirements set out in the Framework.  ***Tri-Agency Financial Administration Guide***  Agreement on the Administration of Agency Grants and Awards by Research Institutions  **3.3 Financial Administration**   1. The Institution shall: 2. for each Grant and Award:    * 1. maintain a separate account;      2. ensure that each expenditure and charge made to the Grant or Award account is authorized by the Recipient, or by their delegate if the delegation is clearly documented; and      3. keep complete and accurate records on the use of Agency funding, including verifiable audit trails with complete supporting documentation for each transaction, for at least seven years; |

|  |
| --- |
| IM Legal and Regulatory Framework |
| **Reference – *Memorial University* *Information Management Policy*** |
| **IM Compliance Requirements** |
| *The purpose of the IM Policy is t*o manage and protect University Records created in the conduct of University activities in accordance with relevant legislation, University policy, standards, guidelines and procedures.   1. Information management is a shared responsibility:   a) Members of the University Community are responsible for the University Records they create or that are in their custody.  b) The OCIO is responsible for the Information Management and Protection Program of the University.  c) Each Unit Head shall be responsible to ensure adherence to this policy.  d) Each Unit Head shall designate an information management and protection lead to oversee operational matters and to liaise with the OCIO in matters related to implementation of and compliance with the policy.   1. University Records are the sole property of the University and must be managed throughout their Life Cycle by Members of the University Community who create or receive them.   a) University Records must be protected in accordance with the Security Measures section of the [Procedure for Administering Privacy Measures within a Unit](http://www.mun.ca/policy/site/procedure.php?id=486) and the[*Electronic Data Security*](http://www.mun.ca/policy/site/policy.php?id=248) policy. b) Official University Records must be created in a manner and format that is accessible and must be retained as required to support the University’s compliance with relevant legislation and policies.  c) Official University Records may not be removed from the control of the University, destroyed or otherwise disposed of except in accordance with a Retention and Disposal Schedule as outlined in the [Procedure for Retention and Disposal Schedules](http://www.mun.ca/policy/site/procedure.php?id=522).  d) Transitory University Records may not be removed from the control of the University, but when no longer required, must be securely disposed in accordance with the [Procedure for Secure Disposal of Transitory University Records](http://www.mun.ca/policy/site/procedure.php?id=523).   1. The University may use external services, such as commercial record storage and Cloud storage and services, in accordance with related University policy. When considering the use of such external services to store Official University Records, Information Risk Assessments must be completed. 2. In the event of any of the following circumstances, disposal of relevant University Records must be suspended: a) Notice of litigation or criminal investigation, b) Notice of an audit, c) Receipt of an ATIPP Request, d) When there is reasonable belief that litigation or criminal investigation may occur, and e) Initiation of a grievance or investigation pursuant to a University policy or collective agreement. 3. Members of the University Community leaving the University, changing positions within the University, or transitioning from one Unit to another shall manage all University Records in accordance with the [Procedure for Managing University Records of Exiting Employees](http://www.mun.ca/policy/site/procedure.php?id=524). 4. If, as a result of developing Retention and Disposal Schedules, records are identified as having archival value, they should be transferred to the University Archives. |
| **Reference – MUNFA Collective Agreement** |
| **IM Compliance Requirements** |
| The **MUNFA collective agreement** requires proper recordkeeping by the university, especially with respect to the management of academic human resource records. |
| **Reference –** |
| **IM Compliance Requirements** |
|  |
| **Reference –** |
| **IM Compliance Requirements** |
|  |
| **Reference –** |
| **IM Compliance Requirements** |
|  |