POLICY NAME	POLICY ON THE GOVERNANCE OF PERSONAL INFORMATION
Approving Body	Board of Governors
Initial Approval Date	Board of Governors: October 5, 2023
Date of last review	n/a
Date of next review	Fall 2028
Executive Sponsor	Secretary-General

Related Documents	**Key Provincial Legislation**
	• Act respecting Access to documents held by public bodies and the Protection of personal information, CQLR c A-2.1
	• Archives Act, A-21.1
	• Act to establish a legal framework for information technology, C-1.1
	
	Key McGill Document
	• Policy on the Responsible Use of McGill Information Technology Resources
	• McGill University Records Retention Schedule (MURRS)
	• Cloud Directive
	• Policy on Data Governance
	  ○ Standard on Enterprise Data Classification
	  ○ Standard on Enterprise Data Governance
	• Regulation on the Conduct of Research
	• Policy on the Ethical Conduct of Research Involving Human Participants

PART I – PURPOSE AND SCOPE

1. Purpose

Note: *Capitalized terms are defined in Section 4.*

(a) The purpose for this Policy is to inform **Persons Associated with the University** of:

(i) McGill University's (also referred to as the "University" or "McGill") principles and legal obligations surrounding the protection of Personal Information in the context of University activities and operations; and

(ii) their roles and responsibilities in upholding such principles and legal obligations pursuant to the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the "Access Act") and associated legislation which govern the University.

(b) At a high level, this Policy includes:

(i) roles and responsibilities for the protection of Personal Information at the University;

(ii) standards and requirements that various Persons Associated with the University must adhere to in order to assure Access-Act-compliant treatment of Personal Information (which includes Sensitive Personal Information) that is Processed for a University purpose;

(iii) a description of privacy training and awareness activities available at the University;

(iv) information on how to report a potential or actual Confidentiality Incident or potential or actual breach of the Access Act or this Policy.

(v) information on rights that Individuals Concerned may have in relation to their Personal Information and how to facilitate such rights fulfillment; and

(vi) a process for making complaints about how Personal Information is Processed at the University.

The companion document entitled "McGill Privacy Notice" is directed towards Individuals Concerned from whom Personal Information is collected. It explains to Individuals Concerned what the University does with Personal Information. The McGill Privacy Notice provides information regarding the categories of Personal Information Processed, the purpose(s) for Processing the Personal Information, and the Personal Information communicated to third parties.

2. Scope

(a) This Policy applies to all Processing of Personal Information carried out for a University purpose, whether the Personal Information is Processed within University or non-University equipment/facilities or by third parties.

(b) This Policy governs all Persons associated with the University that are involved in the Processing of Personal Information for a University purpose. While this Policy generally only refers to the Processing of "Personal Information", references to "Personal Information" in this Policy also apply to the Processing of "Sensitive Personal Information". However, there will be circumstances in which more stringent or particular obligations are made known to Persons Associated with the University involved in research or who Process Sensitive Personal Information for a University purpose, by way of specialized training or other applicable documentation and practices, in which case the more stringent or particular obligations concerning Sensitive Personal Information prevail. For research involving humans, the Policy on the Ethical Conduct of Research Involving Human Subjects may also augment compliance obligations and, in all cases, Research Ethics Board approval must be obtained prior the collection of Personal Information for Academic Research Purposes.

(c) This Policy should be read with referenced documentation, including notably (i) the McGill Privacy Notice, which provides disclosures to Individuals Concerned (i.e., data subjects); (ii) the University's Retention Schedule; and (iii) if applicable, any Research Ethics Board documentation.

(d) Should any of the University's policies conflict with applicable Québec and/or Canadian legislation, relevant provisions of such legislation shall prevail unless otherwise expressly provided for by law.

3. Guiding Principles

The University must comply with the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the "**Act**") and associated legislation. All persons involved in Processing Personal Information for a University purpose must protect the Personal Information throughout the life cycle of such Personal Information in accordance with this Policy, except as otherwise provided by the law. All such persons must respect these six (6) principles:

(a) Personal Information must be Processed fairly, lawfully and in a transparent manner;

(b) Personal information must only be used for limited, specified stated purposes and shall not be used or disclosed in any way incompatible with such purposes;

(c) Personal Information must be relevant and limited to what is necessary for these purposes;

(d) Personal Information must be accurate, and where necessary, up-to-date;

(e) Personal Information must not be kept for longer than is necessary; and

(f) Personal Information must be kept safe, confidential and secure.

PART II –POLICY PROVISIONS

4. Definitions

In this Policy, the terms below have the following meanings:

(a) **Access and Privacy Office** means the Secretariat, the administrative office that supports the Privacy Officer within the University's Secretariat.

(b) **Authorized Person** means a person that requires access to any Personal Information in order to perform their role/contract with(in) the University as determined by the Unit concerned and in compliance with this Policy.

(c) **Committee** means the University's Committee on Access to Information and the Protection of Personal Information, as referred to in Section 7 (b).

(d) **Consent means** any freely given, specific, informed and unambiguous indication of the Individual Concerned by which such individual signifies agreement to the Processing of Personal Information relating to them.

(e) **Confidentiality Incident** means an unauthorized access, use, release, loss, or any other breach of the protection of Personal Information.

(f) **Document** means information recorded in writing or print, on sound tape or film, in computerized form or otherwise, on any storage medium.

(g) **Express Consent** means consent obtained where the Individual Concerned demonstrates their intention in an apparent manner, in verbal or written form, in particular by signing a document or making a statement in public or in front of a witness, commonly done through positive and voluntary actions, such as filling out a form, answering affirmatively to a question or checking a box.

(h) **Individual Concerned** means a natural person to whom Personal Information relates (i.e., anyone from whom the University collects Personal Information for a University purpose).

(i) **McGill Privacy Notice** means a "Privacy Notice" from the University, which is addressed to Individuals Concerned and which discloses what the University does with Personal Information.

(j) **Personal Information,** which includes Sensitive Personal Information, means in any Document information concerning a natural person which directly or indirectly allows the person to be identified.

(k) **Personal Information Life Cycle** means all the steps involved in processing Personal Information (e.g., its collection, use, communication, storage/retention and destruction or anonymization, as the case may be).

(l) **Person Associated with the University** means a staff member, student, researcher, contractor, consultant, agent, volunteer or other person who is associated with the University by appointment, employment, contract, or agreement.

(m) **Privacy Manager** means the University staff member who provides support to the Privacy Officer and to Unit Heads and Unit liaisons, as described in Section 8 (a).

(n) **Privacy Notice** means a public statement addressed to Individuals Concerned outlining how the University Processes their Personal Information and adheres to legal requirements pertaining to privacy.

(o) **Privacy Officer** means the Secretary-General of the University who is responsible for monitoring internal compliance, advising on the University's privacy obligations, as described in Section 7 (a).

(p) **Procedures** means written procedures pertaining to this Policy.

(q) **Processing of Personal Information / Process** means the (handling of the) collection, use, storage, sharing, anonymization and/or final disposition/destruction of Personal Information.

(r) **Retention Schedule** means a document that identifies a series of groups of records and their use, sets out rules for the period for which they must be retained, and provides authority for the final disposition of the records, which will result in either the destruction or permanent retention of the records and their appropriate transfer to the archives. The current version of the McGill University Records Retention Schedule (MURRS), produced in compliance with the Archives Act, is available here: MURSS.

(s) **Sensitive Personal Information** means information the disclosure of which, because of its nature (e.g., medical, biometric or otherwise intimate information), or because of the context in which it is used or communicated, gives rise to an elevated expectation of privacy.

(t) **Serious Injury** means an act or event likely to cause harm to the Individual Concerned or such individual's property, and to prejudice such individual's interests in a significant way.

(u) **Unit** means a faculty, department, division, unit, centre, program, service or other office of the University, that collects Personal Information.

(v) **Unit Liaison** means a University staff member who has been designated to represent their Unit in matters relating to privacy, in consultation with the Privacy Manager.

5. Personal Information Life Cycle

5.1 Collection

(a) Data Minimization: The University will limit its collection of Personal Information to only what is strictly necessary to fulfill the purposes for which it is collected, in each case aligned with a University purpose.

(b) Consent: Where required by law, the University shall obtain Consent from an Individual Concerned when collecting Personal Information. Such Consent shall be clear, freely given, and given for a specific purpose (i.e., "purpose" or "purposes" disclosed by the University in relation to how the University will use the Personal Information).

> ***Note:*** *(1) Consent may be given through display of a Privacy Notice in many circumstances. (2) When collecting Sensitive Personal Information, the Consent obtained from the Individual Concerned must be an Express Consent.*

(c) Modification of Consent: Except as otherwise authorized by law, if the University wishes to use Personal Information for a purpose other than the original purpose for which it was collected from an Individual Concerned, the University shall obtain a new Consent from the Individual Concerned.

(d) Collection Through Technological Means: When collecting Personal Information from Individuals Concerned through technological means (e.g., its websites, mobile applications, point of sale in University-owned / operated stores, call centers, chats, etc.), the University must:

(i) provide a link to its McGill Privacy Notice;

(ii) disclose the purpose(s) for which Personal Information is being collected; and

(iii) provide Unit contact details for the Unit using the Personal Information, in the event of questions or concerns.

(e) Personal Information that is not Sensitive Personal Information – for "Non-Research Activities": Prior to the collection of such Personal Information, the relevant Unit Liaison will:

(i) identify and document the purposes for which Personal Information will be collected;

(ii) validate whether a Privacy Notice needs to be displayed at the time of collection, and if so, determine the correct means for display, and proceed with display and collection as follows:

(1) where the McGill Privacy Notice covers the intended collection: proceed with display and data collection;

(2) where the McGill Privacy Notice does not currently cover the intended collection: Consult the Privacy Manager to determine if (1) the McGill Privacy Notice needs to be modified or supplemented (possibly in the form of new separate Privacy Notice) or (2) if Express Consents will be collected; and then proceed with the relevant Privacy Notice or Express Consent, as the case may be, and data collection.

(f) Sensitive Personal Information for "Non-Research Activities": Prior to collection of Sensitive Personal Information (or mixed Sensitive Personal Information and regular Personal Information) for non-research activities, the Unit Liaison will review the proposed Express Consent to be used and confirm whether it is sufficient pursuant to Procedures, in consultation with the Privacy Manager if uncertain.

(g) Personal Information and Sensitive Personal Information for "Research Activities": All persons involved in research who plan to collect Personal Information (therefore including Sensitive Personal Information) must obtain review and approval from the relevant Research Ethics Board prior to any collection of Personal Information and must follow all requirements of the Research Ethics Board with respect to such data.

Note: *The "communication" of Personal Information to third parties for studies, research or production of statistics without the consent of the Individuals Concerned is treated under Section 5.3 below.*

(h) Collection from Third Parties: While the University usually collects Personal Information from the Individuals Concerned, the University may at times collect Personal Information from third parties, where authorized by law (e.g., other academic institutions, government bodies, etc.). In such cases, the University will ensure that the transfer from the third party is in conformance with this Policy and the Access Act.

(i) Collection from Minor Under 14 Years: The University may not collect Personal Information from a minor aged less than 14 years without the consent of the person having parental authority or of the tutor, except where authorized by law.

(j) Identification, Profiling and Localisation: If the University collects Personal Information by technological means which include functions allowing for the identification, localisation or profiling of individuals the University must:

(i) disclose the use of such technology; and

(ii) ensure that the functions allowing for the identification, localisation or profiling of individuals are disabled by default.

(k) The University will only use Personal Information for the purposes for which it was collected, unless otherwise authorized by law. The University must seek the Express Consent from the Individual Concerned before using the Sensitive Personal Information for purposes other than for which it was collected. (Section 65.1 Access Act)

(l) In some specific situations, the University can use Personal Information for purposes other than those for which it was collected without the consent of the Individual Concerned. The University must document these cases in its communication registry. (Section 65.1 Access Act)

(m) The University will ensure that Personal Information is up-to-date, accurate and complete, as necessary to serve the purposes for which it is Processed.

(n) The University will maintain a registry of the Personal Information it holds.

(o) Decision Based Exclusively on an Automated Processing of Personal Information: The University will disclose situations where Personal Information is used to make a decision rendered exclusively through an automated process. This disclosure will be made no later than at the time the individual is informed of the decision. Upon request by an individual, the University will also disclose:

(i) the Personal Information used to render the decision;

(ii) the reasons, the principal factors and parameters that led to the decision; and

(iii) the right of the Individual Concerned to have the Personal Information used to render the decision corrected.

The individual must be given the opportunity to submit observations to a University staff member who is in a position to review the decision.

5.2 Access within McGill

University authorization to access Personal Information is subject to the following conditions:

(i) the Authorized Person has signed a confidentiality undertaking; and
(ii) Such access is needed in order to carry out the Authorized Person's responsibilities (i.e., there is a "need to know").

5.3 Communication to Third Parties

(a) General: As a general principle, the University will not communicate Personal Information to any third party without the consent of the Individual Concerned unless otherwise authorized by law (e.g. where authorized by law with respect to: law enforcement, application of an Act in Québec; necessary to carry out a mandate or a contract for services; subject to written agreement; necessary to carry out collective agreement or conditions of employment). (Sections 66-68.1 Access Act).

(b) Written Agreement: When required by law, the University will ensure that third parties are bound by a written agreement that includes the contractual safeguards required to protect the Personal Information entrusted to them. (Sections 67.2, 68.1 Access Act).

(c) Registry: When required by law, the University will document communications of Personal Information to any person or body outside of the University made pursuant to an exception to consent in a registry to that effect. (Sections 66-67.3 Access Act).

(d) Communication of Personal Information outside the Province of Québec: The University cannot communicate Personal Information outside the Province of Québec without having completed a Privacy Impact Assessment and having put in place the appropriate security safeguards, including a written agreement with the receiving party.

(e) Communication of Personal Information for Studies, Research or Production of Statistics: The University may communicate Personal Information without consent of the Persons Concerned for studies or research purposes, or for the production of statistics, subject to the conditions below. Prior to doing so, it must conduct a Privacy Impact Assessment. The communication may only occur if the Privacy Impact Assessment concludes that:

(i) the objective of the study or research or of the production of statistics can be achieved only if the information is released in a form allowing the Persons Concerned to be identified;

(ii) it is unreasonable to require the University to obtain the consent of the persons concerned;

(iii) the objective of the study or research or of the production of statistics outweighs, with regard to the public interest, the impact of releasing and using the information on the privacy of the Persons Concerned;

(iv) the Personal Information is used in such a manner as to ensure confidentiality; and

(v) only the necessary information is released.

The University will only consider requests for such sharing of Personal Information for studies, research or production of statistics that comply with the criteria set out above in this paragraph 5.3(e)(i)-(v), and with the relevant provisions of the Access Act (Sections 67.2.1-67.2.3).

The University will enter into a written agreement with any applicant wishing to receive Personal Information in the manner described in this paragraph 5.3(d), detailing the parameters of the access to and use of the Personal Information, before it is disclosed. Such agreement must be filed with the *Commission de l'accès à l'information* (CAI) and comes into force 30 days after it is filed with the CAI.

5.4 Storage and Retention

(a) The University is responsible for protecting the Personal Information it holds.

(b) The University will retain Personal Information only for as long as required to fulfill the purposes for which it was collected, and in accordance with its Retention Schedule and applicable laws.

5.5 Disposition: Destruction, Archiving and Anonymization

Except as otherwise provided by applicable laws, when the purpose(s) for which Personal Information was collected have been achieved, the University will dispose of the Personal Information (e.g., by destroying, archiving or anonymizing) in accordance with its Retention Schedule and applicable laws.

6. Privacy Impact Assessment

(a) The University must proceed with a Privacy Impact Assessment ("**PIA**") in order to:

(i) assess the risks in connection with processing Personal Information;

(ii) deploy proper security safeguards to protect Personal Information; and

(iii) comply with its obligations pursuant to privacy laws.

(b) More specifically, the University must conduct a PIA for the below types of project where Personal Information (any Documents, including image of an Individual Concerned) is involved:

(i) a project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, release, keeping or destruction of Personal Information;

(ii) communication of Personal Information outside of the Province of Quebec;

(iii) new surveillance systems;

(iv) use of Artificial Intelligence (AI) Algorithms.

(c) The PIA must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information, and the medium on which it is stored.

(d) The University's Committee must be consulted at the outset of any project as described in section 6(b) above.

(e) As part of the PIA, the University must also ensure that any new IT project would allow computerized Personal Information collected to be communicated to the individual in a structured, commonly used technological format.

(f) The University has developed guidelines, including the McGill Cloud Acquisition Process, and PIA forms.

7. Governance Roles and Responsibilities

(a) Secretary-General (Privacy Officer): The Secretary-General serves as the Privacy Officer under the Access Act, and is thus responsible for monitoring internal compliance and advising on the University's privacy obligations.

(b) Committee on Access to Information and the Protection of Personal Information: The Committee is responsible for supporting the University in carrying out responsibilities and obligations under the Access Act in respect of access to information and the protection of Personal Information. The Committee's specific responsibilities are set out in the Access Act. (Sections 8.1, 63.3, 63.5, 63.6 Access Act)

Subject to this Policy, the Committee shall be governed by Terms of Reference that set forth, among other things, its mandate, composition, and duties and responsibilities.

8. General Roles and Responsibilities

(a) Manager of Privacy and Protection of Personal Information: The Privacy Manager supports the Privacy Officer and serves as a resource person for Unit heads and Unit Liaisons for all matters relating to compliance with this Policy and applicable legislation. The Privacy Manager is the primary contact within the Access and Privacy Office for privacy-related matters, including for Individuals Concerned with complaints and comments relating to privacy at the University.

(b) Unit Heads/Unit Liaison: Unit heads are responsible for ensuring that the Processing of Personal Information in their Unit conforms to this Policy and applicable legislation. The Unit heads' more specific responsibilities are set out in Procedures. Each Unit head shall appoint a staff member to serve as Unit Liaison regarding privacy matters, in consultation with the Privacy Manager in order to confirm Unit coverage across the University and avoid duplication.

(c) General responsibilities and Obligations: All Persons Associated with the University who Process Personal Information for University purposes are responsible for complying with privacy legislation, this Policy and any other policy, guidance, procedures, and/or training introduced by the University to comply with the Access Act and applicable privacy legislation. For more detailed guidance, they

should contact their Unit Liaison. They must follow Procedures and any relevant Unit policies and procedures. In summary, but without limitation, they must ensure that they:

(i) only use Personal Information in ways Individuals Concerned would expect and for the purposes for which it was collected;

(ii) collect and use a minimum amount of Personal Information and only hold it for as long as is strictly necessary;

(iii) keep Personal Information up-to-date (where relevant);

(iv) keep Personal Information secure, in accordance with the University's current policies and procedures in this regard (See e.g., Secure Use of McGill Administrative Systems; https://www.mcgill.ca/it/it-policies);

(v) use additional vigilance when Processing Sensitive Personal Information;

(vi) do not disclose Personal Information to unauthorized persons, whether inside or outside the University;

(vii) complete relevant training as required;

(viii) report promptly any suspected or actual breaches of this Policy or the Access Act (including Confidentiality Incidents; see Section 16) to their Unit head or Unit Liaison or Access and Privacy Office; and

(ix) seek advice from their Unit head or Unit Liaison where they are unsure how to comply with this Policy or the Access Act when carrying out their role at/involving the University.

9. Training and Awareness

The University will offer the following training and awareness activities to staff and selected Persons Associated with the University:

(a) To all staff: Training on general privacy responsibilities and best practices when Processing Personal Information for a University Purpose; and

(b) By relevant teams: Training adapted to the level of contact with Personal Information and/or Sensitive Personal Information, according to role at the University.

10. Privacy by Default

When collecting Personal Information through technological means which include adjustable privacy settings, the University must ensure that those settings provide the highest level of confidentiality by default, without any intervention by the Individual Concerned.

11. Privacy Resource Toolkit

The University has developed a Privacy Resource Toolkit to provide additional information and guidelines on how to properly handle specific privacy-related situations. Unit Liaisons, in consultation with the Privacy Manager, shall make available access to the Privacy Resource Toolkit to selected staff and other Persons Associated with the University who need such information to carry out their role.

12. Security Measures

(a) The University follows industry security standards to protect the Personal Information it Processes. In particular, the University has put in place appropriate physical, technical, IT and administrative safeguards to protect the Personal Information against Confidentiality Incidents.

(b) Procedures contain additional security safeguards to be included in specific situations.

13. Personal Information Collected by Survey

This Policy applies to Personal Information collected through surveys, including notably Section 5. When conducting a survey, the University must also conduct an assessment of the necessity of conducting the survey and the ethical aspect of the survey, taking into account, in particular, the sensitivity of the Personal Information collected and the purposes for which it is to be used. (Section 63.3 Access Act).

14. Rights of Individuals Concerned

Given the Access Act grants various rights to Individuals Concerned (i.e., data subjects) pertaining to their Personal Information held by the University, the University will adopt Procedures and practices which permit the following:

(a) Access: Subject to any exceptions prescribed by laws, the University shall provide access to the Personal Information it Processes about an Individual Concerned.

(b) Rectification: Each Individual Concerned may request the correction of their Personal Information held by the University if it is incomplete, inaccurate, or equivocal, or if the collection of it is not authorized by law; and the University will make any necessary corrections in compliance with the Access Act.

(c) Withdrawal of Consent: With respect to Personal Information that was disclosed to the University pursuant to an optional request, each Individual Concerned has the right to withdraw their consent to the University's use and communication of Personal Information.

(d) Automated Decisions: Each Individual Concerned has the right to present observations to the relevant University staff member who is in a position to review an automated decision. See Section 5.1(o) regarding "Decision based exclusively on an automated processing of Personal Information".

15. Privacy Complaints

The University will promptly treat complaints and comments made by Individuals Concerned regarding the implementation of this policy in accordance with the process outlined in this section.

(a) Informal Comments or Concerns: Individuals Concerned should first contact the Unit involved in processing their Personal Information, as applicable, if they have any concerns or comments on the University's privacy practices.

(b) Formal Complaints: Individuals Concerned wishing to lodge a complaint concerning the Processing of their Personal Information must contact the Access and Privacy Office using the procedure and form available for this purpose. The Access and Privacy Office shall:

  (i) investigate all complaints relating to the University's Personal Information management policies and practices diligently, promptly and confidentially;

  (ii) respond to all complaints within 30 days; and

  (iii) if a complaint is deemed to be well-founded, take appropriate measures to reduce the risk of harm to the Individual(s) Concerned and to prevent the recurrence of similar incidents.

16. Confidentiality Incidents

(a) Reporting of Possible or Actual Confidentiality Incident: Any Person Associated with the University who becomes aware of a possible or actual Confidentiality Incident, shall immediately report the possible or actual Confidentiality Incident to the Unit Head or the Unit Liaison.

(b) Reporting: The head of Unit or the Unit Liaison shall immediately report any possible or actual Privacy Incident to the Access and Privacy Office.

(c) Investigation: Unless otherwise indicated, Confidentiality Incidents will be investigated by the Access and Privacy Office, in consultation with the University's IT security Unit and other relevant Units, as applicable. Confidentiality Incidents investigated by any Unit other than the Access and Privacy Office must nevertheless be reported in accordance with section 16(b).

(d) Remedial Action: If it is determined that a Privacy Incident has occurred, appropriate remedial action shall be taken by the University. The Access and Privacy Office will act as a resource for all Persons

Associated with the University regarding appropriate remedial action to be taken following a Confidentiality Incident.

(e) Corrective Measures: When a Confidentiality Incident occurs, the Access and Privacy Office, in consultation with the University's IT security Unit as applicable, must take reasonable measures to reduce the risk of injury to privacy and to prevent new incidents of a similar nature.

(f) Notification of Individuals Concerned / CAI: If the Confidentiality Incident presents a risk of serious injury to the Individual(s) concerned, the University must notify the Individuals Concerned as well as the CAI. The authority to determine whether a Confidentiality Incident presents a risk of Serious Injury lies solely with the Privacy Officer, in consultation with other Units, as necessary.

(g) Register of Confidentiality Incidents/Notice to CAI: The University must document all Confidentiality Incidents in its register of Confidentiality Incidents.

17. Accountability

(a) Staff: All staff are responsible for complying with this Policy and Procedures. Staff must follow any mandatory training prescribed for them. Appropriate remedial action for any non-compliance may result in disciplinary action, which will be implemented pursuant to and in accordance with the relevant collective agreement, University policies and by-laws.

(b) All Persons Associated with the University (Other than Staff): All Persons Associated with the University are responsible for complying with this Policy and Procedures. Appropriate remedial action shall apply in the event of any non-compliance.

PART III – AUTHORITY TO APPROVE PROCEDURES

The Secretary-General is responsible for developing a procedure to implement and give effect to this Policy.

PART IV – REVIEW

This Policy shall be reviewed at least once every five years.

Legislative History:		
Approved:		
Board of Governors	October 5, 2023	Minute 6.2.3