I. Introduction

This Data Privacy Manual ("Manual") is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 ("DPA"), its Implementing Rules and Regulations ("IRR"), and other relevant policies, including issuances of the National Privacy Commission. This organization respects and values your data privacy rights, and makes sure that all personal data collected from our Members and Licensees, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

II. Definition of Terms

A. Data Subject refers to an individual whose Personal Information, Sensitive Personal Information, or Privileged Information is processed.

B. Personal Data collectively refers to Personal Information, Sensitive Personal Information, and Privileged Information.

C. Personal Information refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

    e.g. Full name, birthdate, residential address, contact numbers, civil status, birth date and place, etc.

D. Processing refers to any operation or set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or are intended to be contained in a filing system.
E. **Privileged Information** refers to any and all forms of Personal Data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

F. **Personal Data Breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

G. **Security Incident** is an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity and confidentiality of Personal Data. It includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.

H. **Privacy Impact Assessment** ("PIA") refers to the process of managing risks to data privacy caused by the processing of personal data.

I. **Sensitive Personal Information** refers to Personal Data:

1. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
2. About an individual’s health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings;
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
4. Specifically established by an executive order or an act of Congress to be kept classified.

III. **Scope and Limitations**

All employees, representatives and agents of FILSCAP, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Manual.

IV. **Processing of Personal Data**

A. Collection
1. Membership: FILSCAP collects personal data of its applicants or members, including their full name, pseudonym, address, phone number, email address, age, birthdate, birthplace, nationality, civil status, tax identification number, contact details of immediate family member (in case of emergency), competent evidence of identity (e.g. Driver’s License, Passport, or any other government issued ID), personal picture and signature. The foregoing data are collected by the Membership Department through accomplished Membership Application Form or Membership Data Form.

2. Licensing: FILSCAP also collects basic personal information of its licensees or prospective licensees, including their full name, address, email address, contact number, company name, designation, together with their establishment that uses copyrighted musical composition, signature, thumbprint, competent evidence of identity (e.g. Driver’s License, Passport, or any other government issued ID) and signature. The foregoing data are collected by the Licensing Department through accomplished Application Form.

B. Use

1. Membership: Personal data collected by Membership Department shall be used by FILSCAP for administering copyrights of members, documentation and distribution of royalties, and membership concerns, including sending notices to members regarding FILSCAP updates and events, and for other legitimate purposes necessary for the collection, processing and retention of personal data.

2. Licensing: Basic personal information collected by Licensing Department shall be used by FILSCAP for communicating with licensees or prospective licensees for issuance of the necessary licenses and licensing concerns, including sending notices to licensees regarding FILSCAP updates and events, and for other legitimate purposes necessary for the collection, processing and retention of personal data.

C. Storage, Retention and Destruction

1. FILSCAP shall ensure that personal data under its custody are protected against any accidental or unlawful destruction,
alteration and disclosure as well as against any other unlawful processing.

2. FILSCAP will implement appropriate measures in storing collected personal information, depending on the nature of the information. All information gathered shall be retained:

a. During the continuance of the member’s membership with FILSCAP and within five (5) years after cessation of such membership, except the tax certificates, reports, returns and other documents required by the Bureau of Internal Revenue (“BIR”) which shall be retained and preserved by FILSCAP for a maximum period of ten (10) years.

b. During the contract period of the licensee’s license agreement with FILSCAP, including its renewal, and within five (5) years after the expiration or termination of such license except the license agreements, billing statements and official receipts and tax certificates required by the BIR to be retained by FILSCAP and preserved for a maximum period of ten (10) years.

3. After the lapse of the period stated in Article IV (C)(2) of this Manual, all hard and soft copies of personal information shall be disposed and destroyed through secured means.

D. Access, Disclosure and Sharing

Due to the sensitive and confidential nature of the personal data under the custody of FILSCAP, only FILSCAP and its authorized employees, agents, representatives, affiliate societies abroad and distribution service providers shall be allowed to access such personal data to the extent necessary for the Use stated in Article IV (B) of this Manual.

Further, all employees, agents, representatives and personnel of FILSCAP shall maintain the confidentiality and secrecy of all Personal Data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal Data under the custody of FILSCAP shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.
V. Security Measures

A. Organization Security Measures

FILSCAP shall appoint or designate a Data Protection Officer (“DPO”) and a Compliance Officer.

The DPO shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a PIA, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

The Compliance Officer shall ensure the compliance of FILSCAP with the policies under this Data Privacy Manual, and assist the DPO in the conduct of PIA, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.

FILSCAP shall sponsor a mandatory training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, FILSCAP Management shall ensure the attendance and participation in relevant trainings and orientations, as often as possible.

FILSCAP shall conduct a PIA relative to all activities, projects and systems involving the processing of personal data. It may choose to outsource the conduct of a PIA to a third party.

FILSCAP shall require its employees, agents, representatives, affiliate societies abroad and distribution service providers to execute a non-disclosure agreement to ensure the confidentiality and protection of the personal data. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

1. Format of data to be collected
Personal data in the custody of FILSCAP may be in digital/electronic format and paper-based/physical format.

2. Storage type and location

All personal data being processed by FILSCAP shall be stored in a storage room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by FILSCAP with password and appropriate security measures.

3. Access procedure of authorized personnel and Monitoring and limitation of access

Only authorized personnel shall be allowed inside the storage room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the storage room upon filing of an access request form with the DPO and the latter’s approval thereof.

All personnel authorized to enter and access the data room or facility must fill out and register in a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

4. Design of office space / work station

The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.

Transfers of personal data via electronic email shall be made through FILSCAP office email, including any or all attachments. Personal email is now allowed. Facsimile technology shall not be used for transmitting documents containing personal data.

5. Retention and disposal procedure
For membership personal data, FILSCAP shall retain the personal data during the continuance of membership and for a period of five (5) years after cessation of membership except for the tax certificates, reports, returns and other documents required by the BIR to be retained and preserved for a maximum period of ten (10) years from the transaction. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

For licensing data, FILSCAP shall retain the personal data of a client during the continuance of the license with FILSCAP, including its renewal, and five (5) years after the expiration or termination of the license except for the license agreements, billing statements and official receipts and tax certificates required by the BIR to be retained and preserved for a maximum period of ten (10) years. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. Technical Security Measures

1. Monitoring for security breaches

   The organization shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used

   The organization shall first review and evaluate software applications before the installation thereof in computers and devices of FILSCAP to ensure the compatibility of security features with overall operations.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

   The organization shall review security policies, conduct, vulnerability assessments and perform penetration testing within the company on a regular schedule to be described by the appropriate department or unit.
4. Encryption, authentication process, and other technical security measures that control and limit access to personal data

Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication for data stored in database systems. While data in spreadsheets and doc files will be protected by file passwords.

VI. Breach and Security Incidents

A. Creation of a Data Breach Response Team

A Data Breach Response Team comprising of five (5) officers shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The Data Breach Response Team are as follows:

1. Data Protection Officer (Head)
2. Compliance Officer
3. In-House Counsel
4. I.T. Consultant or Personnel
5. Manager or Supervisor of the concerned department

The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

B. Measures to prevent and minimize occurrence of breach and security incidents

FILSCAP shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

C. Procedure for recovery and restoration of personal data

FILSCAP shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to
determine the presence of any inconsistencies or alterations resulting from the incident or breach.

D. Notification Protocol

The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal breach has occurred.

Generally, there shall be no delay in notification, however, the data breach notification may only be delayed to the extent necessary to determine:

- The scope of the breach;
- To prevent further disclosures; or
- To restore reasonable integrity to the information and communications system.

Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

E. Documentation and reporting procedure of security incidents or a personal data breach

The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period in Article VI (D). The following information must be included in any Data Breach notification:

a. Nature of the Breach;
b. Personal data involved;
c. Remedial measures;
d. Name and contact details of the Data Protection Officer or contact person designated by FILSCAP to provide additional information.

Not all data breaches have to be reported to the NPC. Only when these are all present:

a. There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
b. The data is reasonably believed to have been acquired by an unauthorized person; and

c. Either the personal information controller or the NPC believes that the data breach is likely to give rise to a real risk of serious harm to the affected data subject.

If there is doubt as to whether notification is indeed necessary, consider:

- The likelihood of harm or negative consequences on the affected data subjects;
- How notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred; and
- If the data involves:
  - Information that would likely affect national security, public safety, public order, or public health;
  - At least one hundred (100) individuals;
  - Information required by all applicable laws or rules to be confidential; or
  - Personal data of vulnerable groups.

VII. RIGHTS OF THE DATA SUBJECT

As provided under the DPA, data subjects have the following rights in connection with the processing of their personal data: right to be informed, right to object, right to access, right to rectification, right to erasure or blocking, and right to damages. Employees and agents of FILSCAP are required to strictly respect and obey the rights of the data subjects. The DPO shall be responsible for monitoring such compliance and developing the appropriate disciplinary measures and mechanism.

a. Right to be Informed

i. The data subject has the right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed.

ii. The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the records of the Office, or at the next practical opportunity:
1. Description of the personal data to be entered into the system;
2. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
3. Basis of processing, when processing is not based on the consent of the data subject;
4. Scope and method of the personal data processing;
5. The recipients or classes of recipients to whom the personal data are or may be disclosed or shared;
6. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
7. The identity and contact details of the DPO;
8. The period for which the information will be stored; and
9. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the National Privacy Commission.

b. Right to Object

i. The data subject shall have the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. The data subject shall also be notified and given an opportunity to withhold consent to the processing in case of changes or any amendment to the information supplied or declared to the data subject in the preceding paragraph.

ii. When a data subject objects or withholds consent, FILSCAP shall no longer process the personal data, unless:

1. The personal data is needed pursuant to a subpoena;
2. The collection and processing are for obvious purposes, including, when it is necessary for the performance of or in relation to a contract or service to which the data subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Office and the data subject; or
3. The personal data is being collected and processed as a result of a legal obligation.

c. Right to Access

The data subject has the right to reasonable access to, upon demand, the following:

1. Contents of his or her personal data that were processed;
2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the DPO.

d. Right to Rectification

The data subject has the right to dispute the inaccuracy or error in the personal data, and the Office shall correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal data has been corrected, the Office shall ensure the accessibility of both the new and the retracted personal data and the simultaneous receipt of the new and the retracted personal data by the intended recipients thereof: Provided, That recipients or third parties who have previously received such processed personal data shall be informed of its inaccuracy and its rectification, upon reasonable request of the data subject.

e. Right to Erasure or Blocking

i. The data subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his or her personal data from the Office's filing system.

ii. This right may be exercised upon discovery and substantial proof of any of the following:
1. The personal data is incomplete, outdated, false, or unlawfully obtained;
2. The personal data is being used for purpose not authorized by the data subject;
3. The personal data is no longer necessary for the purposes for which they were collected;
4. The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing by the Office;
5. The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
6. The processing is unlawful; or
7. The data subject’s rights have been violated.

VIII. Inquiries and Complaints

A Member or Licensee may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of FILSCAP, including the data privacy and security policies implemented to ensure the protection of their personal data. They inquire with FILSCAP at privacy@filscap.com.ph and briefly discuss the inquiry, together with their contact details for reference.

In case a Member or Licensee suffered a data privacy violation or personal data breach relating to the Personal Data, said Member or Licensee may file a written complaint to FILSCAP via:

- Personal delivery or mail:

  Data Protection Officer  
  FILSCAP INC  
  140 Scout Rallos Street, Brgy. Sacred Heart, Diliman, Quezon City 1103, Philippines; or

- Email: privacy@filscap.com.ph.

The Data Protection Officer shall confirm with the complainant of his or her receipt of the complaint.
IX. Effectivity

The Manual shall take effect on 23 January 2020 until revoked or amended by FILSCAP through a resolution of the Executive Committee as delegated by the Board of Trustees.