



LAKAN MUTUAL BENEFIT ASSOCIATION, INC. (LAKAN MBI)
Unit 704, 7/F Tower C, Regalia Park Towers, 150-P. Tuazon Avenue Cubao, Quezon City
Tel. No. (02)8643-5066 / Cell # 0917-1025221; TIN No.: 009-022-312-000; Email Address: pnpalakanmbai@gmail.com

☐ Membership
☐ Optional Coverage:
Please list [CL,YRT,ADB,TPD]

APPLICATION FOR MEMBERSHIP CERTIFICATE (MC) No.

Name	Last Name	First Name	Middle Name	Suffix
Address	Room/Unit/Floor/Building	House No/Lot/Block	Street	Subd. Barangay City/Municipality
Tax Identification No.	Civil Status	Gender	Cell. No.	
Place of Birth	Birth Date			
Branch of Service/ Employer Name	Class			
Rank/Occupation (state duties)	Email Address			
Source of Income				
Membership	[] Regular [] AffiliateAccount #:			
[] TIN [] SSS [] GSIS [] Other ID No.				
Name(s) of Beneficiary(ies)	Birth date	Relationship to Applicant		
Subject to Office Validation:				
Contribution				

I hereby declare that I am in good health and entirely free from any physical or mental impairment and that during the last 5 years, I have not consulted or been treated or examined by a doctor for any disease or injury for more than 2 weeks or been confined to a hospital for any length of time or had surgical operation before. I understand that any contribution due remaining unpaid at the end of the Grace Period shall automatically be paid as a loan against the Equity Value, if any.

I hereby allow LAKAN Mutual Benefit Association, Inc. (LAKANMBAI) to utilize the information I supplied in this application as basis for any subsequent application for insurance coverage. I signify my consent and agree that LAKANMBAI: (a) may collect, use, and disclose my personal data as provided in this document or obtained by LAKANMBAI as a result of being its member, for the purpose of processing this document and (b) may disclose and share the said information to its subsidiaries and/or affiliates, reinsurer or regulatory authorities. It is understood that I have a right to revise the information that I have provided including the deletion of the given information in accordance with the Data Privacy Act of 2012 and the data protection policy of LAKANMBAI.

Signature of Applicant

Date

For Office Use Only	Authorized Signatory/Date:
[] Approved [] Denied [] Others:	

AUTHORITY TO DEDUCT

I hereby declare that with my application with the Lakan Mutual Benefit Association, Inc., it is understood and agreed that this insurance coverage shall take effect on the first day of the month for which the payroll deduction is made, if the payment is made thru automatic salary deduction or the actual date of payment of first contribution, if directly paid to LAKAN MBI.

I hereby authorize LAKAN MBI, to secure from any government office such as the Philippine National Police (PNP) Bureau of Fire Protection (BFP), Bureau of Jail and Penology (BJMP) and the Philippine Statistic Authority (PSA), any or all information and documents relating to my membership such as but not limited to birth certificate (member and beneficiaries), Service Record (member) and advisory on marriage (member and spouse).

Signature _____
Printed Name _____ Contact No. _____
Date _____ Monthly Contribution ₱ _____

SUBSCRIBED AND SWORN to before me this _____ day of _____, 20__ at Quezon City, Metro Manila. Affiant exhibiting to me his _____ I.D. No. _____, issued on _____ at _____.

NOTARY PUBLIC

Doc. No. _____;
Page No. _____;
Book No. _____;
Series of 20_____.

DATA PRIVACY CONSENT FORM

PNP DATA PRIVACY NOTICE

The Philippine National Police (PNP) is committed to uphold, respect, and value the data privacy rights of its personnel in compliance with the Data Privacy Act of 2012 (Republic Act No. 10173) and its Implementing Rules and Regulations (IRR), in all aspects of handling personal information. This Privacy Notice outlines how we collect, use, maintain, and protect information obtained from individuals using or transacting in PNP services and platforms.

PERSONAL INFORMATION COLLECTION

The PNP collects personal identification information from individuals in various ways, including but not limited to, visiting PNP offices, engagement in PNP services, completion of application/registration forms, or involvement in programs or activities. The following personal information may be collected:

- Full Name
- Address
- Other Relevant Details such as duty status, unit or office
- Birthdate
- Rank
- Account Number
- Date Entered into the Service
- Declared Legal Beneficiaries
- Service Record
- Date of Optional Retirement, if any
- Contact Number
- Email Address

In case of applications or requests for the use of the automatic salary deduction, the following:

- The personnel's salary taking into account the requirements of the existing General Appropriations Act (GAA) on the individual's Net Take-Home Pay
- In case the individual has a pending case, the following:
 - Office where the case is filed
 - Case or docket number
 - Nature of the offense
 - Case status

While your consent may be solicited to process your personal data, we may also process personal data without your consent, in cases when the processing is according to our mandate or when processing is allowed under Section 12 or Section 13 of the DPA.

USE OF PERSONAL INFORMATION

The PNP may use collected personal information for the following purposes:

- To authenticate and verify identity;
- To process and assess requests or applications;
- To communicate with Data Subjects;
- To provide relevant information or updates;
- To improve our services;
- To comply with legal requirements; and
- Other legitimate purpose

RETENTION AND DISPOSAL

Personal data will be retained for historical, audit and legal purposes. Once the lawful and legitimate purpose of processing is achieved, data will be securely disposed of in accordance with established policies and procedures.

SECURITY MEASURES

The PNP implements appropriate security measures to protect personal data against unauthorized access, alteration, disclosure or destruction. Only authorized personnel can access collected personal information, and all transactions are securely facilitated.

RISK INVOLVED

Risk refers to the potential of an incident to result in harm or danger to a data subject or organization. Risks may lead to the unauthorized collection, use, disclosure, or access to personal data. It includes risks involving the confidentiality, integrity, and availability of personal data or the risk that processing will violate the general data privacy principles and the rights of data subjects.

The PNP ensures that adequate physical, technical, and organizational security measures are in place to protect personal information's confidentiality, integrity, and availability. However, this does not guarantee absolute protection against certain risks involving the processing of personal data, such as when systems are exposed to targeted cyberattacks, malware, ransomware, and computer viruses or when manual records are accessed without authority. Relative to this, the PNP guarantees that adequate policies are in place to ensure appropriate security incident management in line with existing laws, policies, circulars, and other administrative issuances.

DATA PROTECTION AND SECURITY MEASURES

We safeguard the confidentiality, integrity, and availability of your personal information by maintaining a combination of organizational, physical, and technical security measures based on generally accepted data privacy and information security standards. Among the measures we implement are the following:

- Policies on access control in both digital and physical infrastructures to prevent unauthorized access to personal information.
- Acceptable use policies
- End-to-end encryption and data classification whenever suitable.
- Security measures against natural disasters, power disturbances, external access, and similar threats.
- Technical measures to protect our computers and databases against accidental, unlawful, or unauthorized usage, interference, or access.

RIGHTS OF DATA SUBJECTS

The PNP acknowledges and respects the privacy rights of data subjects. It also recognizes the following rights of its personnel:

- **Right to be informed** whether personal data shall be, are being, or have been collected or processed;
- **Right to Object** to the processing of personal data where such processing is based on consent or legitimate interest;
- **Right to Access** personal data;
- **Right to Rectification** dispute the inaccuracy or error in the personal data;
- **Right to Erasure or Blocking**, suspend, withdraw or order the blocking, removal or destruction of personal data;
- **Right to Damages** to be indemnified for any damages sustained due to such inaccurate, incomplete, outdated false, unlawfully obtained, or unauthorized use of personal data;
- **Right to Data Portability** to obtain personal data in an electronic or structured format; and
- **Right to File a Complaint** before the NPC if any data privacy rights have been violated.

CONSENT AND ACCEPTANCE OF TERMS

By clicking on this consent agreement, the personnel signify his/her acceptance of the terms outlined in this privacy notice. This includes consenting to the collection, use, disclosure, recording, processing, and sharing of all information necessary for transacting and availing of PNP services. Failure to click the consent agreement, will preclude the personnel from engaging in transactions or availing services.

CHANGES TO PRIVACY NOTICE

The PNP reserves the right to revise and amend this Privacy Notice as necessary. Individuals are advised to regularly monitor updates posted on PNP websites, Police Stations, and Offices. Continued engagement in transactions and service availed after any updates to this privacy notice shall be deemed acceptance of the revisions.

CONTACT INFORMATION

If you have any questions, or concerns regarding this Privacy Notice, suggestions, or feedback, you can contact the Compliance to Privacy Officer (CPO) or the PNP through the following:

☐ I have read and understood and consent to be bound by all the terms and conditions stated above.

✓

Signature over printed name of Personnel

Date Signed