1 CISP PRIVACY POLICY

Contents

I. Introduction

The 1 Cooperative Insurance System of the Philippines Life and General Insurance *hereinafter referred to as ("1CISP" or "Cooperative")* hereby adopts this Privacy Policy to ensure that all personal data processed by it is secured at all times and that the data subject rights are respected in compliance to the principles and standards prescribed by Republic Act no. 10173, otherwise known as the "Data Privacy Act", its implementing rules and regulations as well as other issuances of the National Privacy Commission (NPC).

This Privacy Policy sets out the basic privacy principles that 1CISP, its employees and all other personnel must follow when processing personal data including how it seeks to protect personal data and ensure that all personnel understand the rules governing the processing of personal data to which they have access in the course of their work.

Therefore, all personnel should carefully read this Privacy Policy to learn what is expected from them by 1CISP when processing personal data in the course of their employment with or assignment for 1CISP and how their personal data is processed by the Cooperative within its operations.

Please note that this Privacy Policy requires all personnel to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant data protection compliance steps are properly addressed, and if applicable that a Privacy Impact Assessment (PIA) is undertaken.

II. Applicability

This Privacy Policy applies to all employees of 1CISP and personnel of personal information processors (PIPs) that the Cooperative has contracted with (collectively referred to as "personnel").

All personnel are enjoined to read, understand and comply with this Privacy Policy when processing Personal Data on behalf of the Cooperative. Compliance by all personnel with this Privacy Policy is mandatory.

III. Definition of Terms

The following terms which are used herein are defined, as follows:

A. Availability Breach - breach resulting from loss, accidental or unlawful destruction of personal data;

B. Compliance Officer for Privacy (COP) - refers to an individual that performs some of the functions of a DPO, as provided herein pursuant to NPC Advisory

No. 17-01. These are the personnel designated per LC Memorandum No. 005, series of 2020.

C. Confidentiality Breach – breach resulting from the unauthorized disclosure of or access to personal data;

D. Data Subject - refers to an individual whose personal, sensitive personal, or privileged information is processed. This includes all employees, member-owners, representatives of institutional customers, consultants or suppliers of 1CISP as well as the general public (e.g. visitors of the Cooperatives websites or social media).

E. Integrity Breach – breach resulting from alteration of personal data;

F. Personal Data – collective term referring to personal information, sensitive personal information and privilege information;

G. 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. A personal data breach may be in the nature of a confidentiality, integrity or availability breach;

H. 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. This includes the full name, contact information, and address of an individual, gender, place of birth, citizenship, type of employment, employment history, industry and other information not considered as Sensitive Personal Information or Privileged information as defined herein;

I. Privacy Impact Assessment (PIA) - is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology. The identification of risks and the use of a control framework for risk management should consider existing laws, regulations, and issuances relevant to privacy and data protection, as well as the rights of data subjects. The most appropriate standard recognized by the sector or industry of the PIC or PIP, as well as that of the information and communications technology industry shall also be considered;

J. Privileged Information - refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

K. Processing – any operation or any 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;

L. 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 shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place. This may include cyber-attacks through the following means: denial of service, phishing, spoofing, man-in-the-middle, spoofing, improper usage by employees, loss or theft of equipment;

M. Security Incident Management Policy (SIMP) - refer to policies and procedures, implemented by a personal information controller or personal information processor to govern the actions to be taken in case of a security incident or personal data breach; and

N. Sensitive Personal Information - refers to personal information:

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 of a person, 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;

4. Specifically established by an executive order or an act of Congress to be kept classified;

5. Data about the financial or economic situation including salary and insurance coverage;

6. Usernames, passwords and other login data;

7. Biometric data (e.g. signatures, thumbprints)

8. Other similar information, which may be made the basis of decisions concerning its personnel, including the grant of rights or benefits.

IV. Responsibilities and Accountabilities

The Cooperative shall implement, comply with and apply this Privacy Policy. Further, it shall carry out the training, monitoring, auditing and other compliance activities related to the areas of data privacy, as described in this Privacy Policy.

To this end, the following officers, employees and/or units shall have the following responsibilities:

A. Data Protection Officer[1] (DPO) – The DPO shall be responsible for implementation of this Privacy Policy. In addition, he or she shall be responsible for the following:

    1. Monitor the Cooperative's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

        a. collect information to identify the Cooperative's processing operations, activities, measures, projects, programs, or systems, and maintain a record thereof;

        b. analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by its third-party service providers;

        c. inform, advise, and issue recommendations to the Cooperative's Board of Directors or President, as applicable;

        d. ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and

        e. give advice to the Board and/or the President of the Cooperative as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law.

    2. Ensure the conduct of Privacy Impact Assessments (PIAs) relative to the Cooperative's activities, measures, projects, programs, or systems of the PIC or PIP;

    3. Give advice regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

    4. Ensure the proper data breach and security incident management, including the preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;

[1] NPC Advisory No. 2017-01 "DESIGNATION OF DATA PROTECTION OFFICERS", 14 MARCH 2017

5. Inform and cultivate awareness on privacy and data protection within the Cooperative including all relevant laws, rules and regulations and issuances of the NPC;

6. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs relating to privacy and data protection, by adopting a privacy by design approach;

7. Serve as the Cooperative's contact person vis-à-vis its data subjects, other PICs, third parties, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;

8. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

9. Perform other duties and tasks that the Cooperative may assign to him or her that will further the interest of data privacy and security and uphold the rights of the data subjects.

B. Compliance Officers for Privacy (COPs) – The COPs shall assist the DPO in the implementation of this Privacy Policy and his or her responsibilities as provided under the items 4 to 9 of the preceding paragraph.

C. Board of Directors (BOD) – The BOD shall perform the following:

1. Designate the Data Protection Officer of the Cooperative;

2. Effectively communicate to its personnel, the designation of the DPO or COP and his or her functions;

3. Allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;

4. Provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;

5. Grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;

6. Where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;

7. Promptly consult the DPO or COP in the event of a personal data breach or security incident;

8. Ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the Cooperative, or with other organizations; and

9. Delegate some of its authorities as provided herein to the President for the efficient and effective implementation of the data privacy-related policies.

D. President – The President shall perform the following:

1. Oversee the implementation of this Privacy Policy and other privacy-related policies of the Cooperative;

2. Direct the allocation of adequate resources in support of the privacy programs of the Cooperative;

3. Assign responsibilities that will ensure compliance with the requirements of the DPA, its IRR and other related issuances including the designation of Compliance Officers for Privacy (COPs); and

4. Perform other responsibilities that may be delegated to him by the Board of Directors.

E. Compliance Office – The Compliance Office shall ensure compliance with applicable rules and regulations, including all matters relating to Data Privacy.

F. Internal Audit – The Internal Audit shall perform audits on the privacy functions as deemed appropriate from time to time.

All personnel shall endeavour to read, understand and comply with this Privacy Policy and all other data privacy-related policies of the Cooperative.

V. General Principles

The Cooperative shall ensure that personal data is processed or shared pursuant to the principles of transparency, legitimate purpose and proportionality.

It shall uphold the data subject rights to information, access, object, rectify, remove/block, portability, complain or seek damages.

It shall institute organizational, physical and technical measures to protect personal data in accordance with the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), National Privacy Commission (NPC) Circular No. 2016-01 and other issuances of the NPC.

A. Privacy Notice

Data subjects of the Cooperative have the right to receive certain information before the processing activity is carried out. Such information shall include among others, the identity of the data controller, the purposes of the processing and the legal basis, any recipients of the personal data and intentions to transfer or share personal data outside the Cooperative.

As such, the Cooperative shall notify the data subjects through its Privacy Notice, the purpose and manner by which their personal data will be processed consistent with this Privacy Policy and in accordance with the Data Privacy Act and its Implementing Rules and Regulations. The Privacy Notice shall be posted in the website, conspicuous places in the business office or branches of the Cooperative and included in all forms and other documents whenever personal data is being requested by the Cooperative.

B. Collection of Personal Data

As part of the processing activities of the Cooperative, the following personal data may be collected from all personnel as well as from the Cooperative's customers, member-owners and third-parties:

Personal Information

1. Full Name
2. Address
3. Gender
4. Place of birth
5. Citizenship
6. Type of employment
7. Employment History
8. Industry
9. Contact Details including email address, phone numbers or any information that would allow 1CISP to contact the data subject and evaluate the insurance application of its customers.

Sensitive Personal Information:

1. Date of birth
2. Age
3. Civil Status
4. Medical status and other health records
5. Data about the data subject's financial or economic situation
6. Usernames, passwords and other login data
7. Biometric data (e.g. signatures, thumbprints)
8. Copies of identification documents including licenses or unique identifiers like Philhealth, SSS, GSIS, Tax Identification numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

C. Lawfulness of Processing

Each processing activity requires a legal basis. The Cooperative will only process and share personal data fairly and lawfully and for specified purposes. In general, the Cooperative shall process personal data only when it is necessary under the following circumstances:

1. To effectively serve customers of the Cooperative and carry out its business operations, which may include the following:

    a. To verify identity;
    b. To provide information about the Cooperative's services;
    c. To respond to queries, complaints, and requests, or otherwise communicate with the data subject;
    d. To conduct research and analysis to improve the Cooperative's products and services; or
    e. To grant access to the Cooperative's premises and maintain security

2. For the performance of contracts with the data subject or to fulfil a request from the data subject;

3. Consent is given by data subject, or by the parties to the exchange of personal data, prior to the processing of the personal data, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;

4. To protect vitally important interests of the data subject, including his or her life and health. Sensitive personal information will be processed only when the data subject is not legally or physically able to express his or her consent prior to the processing;

5. To respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;

6. To pursue a legitimate interest, such as to maintain Cooperative's operational security and to manage risks;

7. To protect the lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate; or

8. To comply with a laws, rules or regulations.

Specifically, the Cooperative shall process personal data of the following data subjects and for the corresponding purposes:

A. For Member-Owners

1. To perform 1CISP's obligations under its engagement agreement with its member-owners;
2. To provide its members reliable insurance products with optimal benefits;
3. To update their records with us;
4. To assist beneficiary/ies by giving the insurance claim benefit; and
5. To assess the right applicant for vacant positions;

B. For Job Applicants

1. To evaluate their qualifications and other requirements for employment with us;
2. To conduct verification or background checks; and
3. To communicate with the job applicant regarding his/her application.

C. For Employees, Consultants, Maintenance and Other Personnel

1. To process their payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand or require processing of their Personal Data (e.g., to execute business transactions directly related and/or incidental to their job, business travels, socials, and so on);
2. To evaluate their performance and career development;
3. To process their Personal Data for the exit interview and to prepare their final pay upon separation;
4. To provide them with assistance and to account for them in case of emergency; and
5. To perform such other processing or disclosure that may be required in the course of the Cooperative's business or under law or regulations.

D. For suppliers and Other Third-Parties

1. To conduct the appropriate due diligence checks;
2. To evaluate their proposal, including their technical, financial, and operational capacity, assess the viability of their proposal and process their accreditation;
3. To communicate any decision on such proposal;
4. To enter in contract or agreements with suppliers and other third-parties; and
5. To perform any other action as may be necessary to implement the terms and conditions of the Cooperative's contract.

D. Purpose Limitation and Data Minimization, Quality and Accuracy

The Cooperative shall process personal data only for a specified, explicit and legitimate purpose as set forth in preceding section. Only personal data that are necessary for the specified purpose shall be processed.

Further, personal data shall be adequate, relevant, accurate, up to date and limited to what is necessary in relation to the purposes for which it is collected. It must not be processed further in a manner incompatible with those purposes.

The Cooperative shall ensure that it uses reliable sources when collecting the data and it will not collect excessive data. It will allow data subjects to correct or update his/ her own personal data. It shall pursue a privacy by design perspective to avoid that data is processed which is not relevant for the specified purpose.

E. Retention Limits

The Cooperative shall not process personal data for a longer period than necessary for the purposes for which the personal data was collected. Therefore, it has adopted the protocols set out in Section D (Disposal) hereof, specifying how personal data shall be erased when the purpose of the processing of the personal data has been fulfilled. It will maintain retention policies and ensure that data subjects are informed of the period for which data is stored and/or how that period is determined.

F. Integrity and Confidentiality, including Data Privacy by Design and default

To ensure appropriate integrity, confidentiality and security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, the Cooperative shall implement organizational, physical and technical security measures, including requirements on data protection by design and default.

Those security measures shall be applied in the procurement, development, production and maintenance as well as the sun-setting of systems (whether operated internally or procured as a service).

Also, the Cooperative shall implement protocols for notification to the supervisory authorities as set forth in the Security Incident Management Policy of the Cooperative and Section E (Handling Data Breach) hereof in case of data breaches as well as protocols for carrying out privacy impact assessments.

G. Data Transfers Within or Outside the Cooperative

In the course of delivering Cooperative's services and fulfilling its responsibilities, the Cooperative may engage the services of third-party service providers. It may also share personal data to third-party personal information controllers. In doing so, certain personal data is required to be disclosed or shared for legitimate business concerns and as may be necessary to provide its members with its services.

As such, the Cooperative shall enter into an outsourcing agreement or data sharing agreement with such service providers or third-party personal information controllers, as the case may be. These agreements shall contain all the terms and conditions as set forth by the Data Privacy Act of 2012 or its implementing rules and regulations. It shall ensure that personal data shared are likewise protected under law.

H. As Data Processor

Should the Cooperative act as personal information processor, i.e. process personal data on behalf of another entity, it shall:

1. Only act on the PIC's documented instructions.
2. Impose confidentiality obligations on all personnel who process the relevant data.
3. Ensure the security of the personal data that the Cooperative processes.
4. Follow the rules regarding appointment of sub-processors.
5. Implement measures to assist the PIC in complying with the rights of data subjects.
6. At the PIC's election, either return or destroy the personal data at the end of the relationship.
7. Provide the PIPC with all information necessary to demonstrate compliance with the DPA.

VI. Rights of the Data Subjects

The Cooperative shall protect the rights of its personnel. In the same manner, it shall protect the rights of the data subjects whose personal data may be processed in the course of their employment with the Cooperative through their compliance with this Privacy Policy and other data privacy-related policies. The data subject rights are as follows:

1. Right to be informed
2. Right to access
3. Right to object
4. Right to erase
5. Right to rectify/ correct
6. Right to data portability
7. Right to complain and damages
8. Right to transmissibility

All personnel may exercise their rights the same way that the Cooperative's other data subjects may exercise these rights.

The Cooperative shall as far as practicable, adopt policies and procedures that are consistent with NPC Advisory No. 2021 – 01 on the Rights of Data Subjects.[2]

Any personnel may reach the DPO or any of the COPs through the contact information provided herein for any data privacy related concerns.

For more information about these rights, kindly refer to the National Privacy Commission's webpage at https://www.privacy.gov.ph/know-your-rights/ and NPC Advisory No. 2021 – 01 on the Rights of Data Subjects.

VII. Security Measures

A. Organizational Measures

To implement organizational measures, the Cooperative shall:

1. Ensure that appropriate personnel are designated to ensure compliance with the DPA and its implementing rules and regulations. Data Protection Officer/s and Compliance Officers for Privacy shall be designated and provided the necessary support for their development and proper performance of their functions.

2. Implement this Privacy Policy and other appropriate data protection policies that provide for organizational, physical, and technical security measures, and, for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedoms of data subjects.

3. Maintain records that sufficiently describe the Cooperative's data processing system, and identify the duties and responsibilities of those individuals who will have access to personal data.

4. Be responsible for selecting and supervising its employees, agents, or representatives, particularly those who will have access to personal data.

5. All personnel are required to participate in the Cooperative's data privacy and information security trainings. To raise awareness of privacy issues, make data protection a part of the Cooperative's culture and improve the organisational security for the personal data processed, all employees and, as relevant, consultants, specifically the DPO and Compliance Officers for Privacy, shall be aware of the requirements set out in the Data Privacy Act and the adopted governing documents within the privacy field.

6. PIAs shall be conducted by all units as necessary. The DPO and designated personnel shall be responsible for performing PIAs on the data processing activities carried out on the unit level.

[2] Issued on 29 January 2021

B. Physical Measures

To implement physical measures, the Cooperative shall implement the following:

1. Establish policies and procedures to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media;

2. Design of office space and work stations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public;

3. The duties, responsibilities and schedule of individuals involved in the processing of personal data shall be clearly defined to ensure that only the individuals actually performing official duties shall be in the room or work station, at any given time;

4. Any natural or juridical person or other body involved in the processing of personal data shall implement policies and procedures regarding the transfer, removal, disposal, and reuse of electronic media, to ensure appropriate protection of personal data;

5. Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

C. Technical Measures

To implement technical measures, the Cooperative shall implement or have:

1. A security policy with respect to the processing of personal data;

2. Safeguards to protect the Cooperative's computer network against accidental, unlawful or unauthorized usage, any interference which will affect data integrity or hinder the functioning or availability of the system, and unauthorized access through an electronic network;

3. The ability to ensure and maintain the confidentiality, integrity, availability, and resilience of their processing systems and services;

4. Regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach;

5. The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

6. A process for regularly testing, assessing, and evaluating the effectiveness of security measures;

7. Encryption of personal data during storage and while in transit, authentication process, and other technical security measures that control and limit access.

8. Data security is a high-priority for the Cooperative. It will at all times ensure that personal data are kept secure, both against external threats and internal threats.

D. Provisional Security Measures

The following security measures shall be implemented by all personnel in the various stages of processing of personal data pending issuance of the organizational, physical and technical measures mentioned in the preceding Sections.

Collection

1. Collection and processing of personal data shall be limited. Personal data that are "nice to have" shall not be collected but only personal data that is considered as "need to have" for the specific purpose.

2. Collection and processing of sensitive personal information such as information on health and ethnic origin shall be limited to those that are absolutely necessary for the specific purpose.

3. Only use social security numbers when it is necessary for a secure identification or another important reason (and necessary for the purpose of the processing).

4. All personnel shall make sure that:

    a. the persons whose data they process have been informed about the contemplated processing (see Section on Consent);

    b. there is a legal basis to process the personal data in the manner that is intended; and

    c. the personal data that they process is correct and up to date.

Storage

1. Personal data shall be stored in a centralized repository, which may be physical (e.g. file room) or virtual (e.g. data center or network drive), used for the storage, management, and dissemination of data.

2. Documents with sensitive personal information shall be clearly marked as "Confidential" on its face and on every page thereof.

3. Physical documents shall be properly kept in a similarly marked folder or envelope and stored in locked cabinets, drawers, vaults or safes, in the file room. Designated custodians shall adhere to policies or protocols that will ensure the confidentiality, integrity and availability of personal data.

4. All personnel shall maintain the information security for the personal data that they may use or are responsible for, e.g. by using complex passwords and locking their computer when they leave it unattended.

5. A "clean desk policy" shall be observed by all personnel to ensure that no document is left on desks when he/ she leaves his/her workstation. Similarly, personal computers, laptops and other devices should be turned off or logged off whenever the user leaves the workstation.

6. Personnel shall not keep physical documents in their workstations. Only physical documents being processed may be kept temporarily in locked drawers or cabinets located in their workstations.

7. Electronic documents must be password-protected and if possible, encrypted, whether at rest or in transit. Passwords shall be of sufficient strength, kept in a secure place and shall not be disclosed to unauthorized personnel. Electronic documents shall be saved in their allocated network drive in the data center.

8. Personnel using portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is password protected or encrypted. Personnel using their computers to store personal data must be password-protected.

9. Computers, USB drives and other storage devices to be used shall not contain any personal data that is not necessary or relevant to his/ her function.

Access

1. Access to file rooms or data centers shall be restricted to authorized personnel. Each file room or data center shall have a designated administrator that will control access and maintain a log that records when, where, and by whom the file rooms or data centers are accessed.

2. Documents shall be accessed or processed only by authorized personnel and only within designated workstations. Unauthorized personnel shall not be allowed in areas where documents are being processed.

3. Custodians of documents shall maintain a log from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. The Unit concerned shall regularly review the log records, including all applicable procedures.

4. Only programs developed or licensed by the Cooperative shall be used to access and modify databases containing the personal data under its control or custody. Units using programs or systems other than those developed or licensed by the Cooperative shall register the same with the IT unit.

5. All personnel shall agree to the Acceptable Use Policy (AUP)(or similar policy) maintained and kept up-to-date by the IT Unit. For this purpose, all personnel shall sign the appropriate agreement or document, before being allowed access to and use of the technology.

6. Use of cameras in areas where personal data is displayed or processed shall be prohibited. Scanners or other devices provided or authorized by the Cooperative for use in the processing of personal data shall be used.

7. Access by other entities to the personal data under the control or custody of the Cooperative shall be governed by data sharing or outsourcing/ subcontracting agreements.

Transfer

1. All computers or email accounts provided by the Cooperative to all personnel are the Cooperative's property and should be used only for their work. To a limited extent and within reason, such email addresses may be used for private purposes. However, if these email addresses are used for private purposes, the Cooperative will treat any such private files or emails as data belonging to the Cooperative and that data will be treated and deleted in the same manner as other data belonging to the Cooperative, as there is no reasonable manner in which the Cooperative can distinguish between the personnel's data and other data belonging to the Cooperative.

   Personnel may share personal data to their colleagues in the Cooperative through such email addresses provided that such personal data is authorized to be shared and personnel receiving the same are likewise authorized to receive the same.

2. Documents sent by email must be password-protected. Passwords should be sent directly to the recipient on a separate facility such as through phone or separate note. Employees of the Cooperative shall use their official email for official communications. Personnel using their personal email addresses shall register the same with the IT Unit.

3. Personnel shall avoid photocopying, printing or otherwise, creating unnecessary duplicates of documents containing personal data. Only authorized personnel shall be allowed to photocopy or print personal data. Any printed or duplicate copy shall be disposed of immediately whenever such printed form is no longer necessary.

4. Manual transmission of personal data, such as through the use of removable physical media like compact discs or USBs shall not be allowed whenever such data can be accessed from the data center or otherwise, shared electronically. If transfer via such portable media is unavoidable or necessary, file-password protection shall be implemented.

5. Fax machines shall not be used for transmitting documents containing personal data.

6. Documents transmitted by mail or post shall make use of registered mail or courier services. Such documents or media shall be delivered only to the person to whom they are addressed, or his or her authorized representative.

7. Personnel tasked to physically transmit documents between units in the Cooperative shall not be allowed to open or browse documents, or discuss any personal data while in transit particularly in common areas such as in elevators and lobbies.

8. Documents containing sensitive personal information being transmitted from one Unit to the other within the Cooperative shall be placed in sealed envelopes, properly marked as "Confidential" and delivered directly to the addressee or his or her authorized representative.

9. Make sure personal data processing agreements (and data transfer agreements) are in place with service providers that have access to personal data when providing its services to the Cooperative.

10. When a data processor processes data on behalf of a data controller, a data processing agreement (DPA) shall be entered into between the data controller and the data processor. The DPO and the person responsible for the relevant procurement process shall ensure that a DPA is entered into with such processor.

Retention

1. In general, all personnel shall keep personal data only for as long as is necessary for the fulfilment of the declared, specified, and legitimate purposes state above.

2. All personnel may also retain personal data for the establishment, exercise or defense of legal claims or for other legitimate business purposes.

3. For member-owners and employees, their personal data may only be retained to the extent necessary for the fulfilment of the purpose/s for which it was obtained and for an additional period of ten (10) years thereafter. Thereafter, personal data will be anonymized and utilized solely for statistical purposes.

4. For job applicants, their personal data may be retained for a maximum of two (2) years for future job opportunities that may be of interest to the job applicant.

5. For visitors, suppliers and other third parties, their personal data may be retained for a maximum of one (1) year from end of the Cooperative's transaction with them.

Disposal

1. All personnel shall securely dispose of personal data when the processing relevant to the purpose has been terminated.

2. Personal data that have been stored in computer's which are no longer necessary to process taking into account the purpose for which they were collected shall be erased using effective tools that will prevent recovery thereof.

3. Units shall dispose their respective documents in accordance with the applicable retention periods as specified herein. Personal data records, as well as incoming and outgoing emails, of enduring value may be archived.

4. Designated custodians shall ensure that documents for disposal including copies thereof are disposed of or destroyed using secure methods such as shredding.

5. Personnel shall ensure that documents disposed of in trash bins or used as scratched paper do not contain any personal data.

E. Handling Data Breach

The Cooperative shall adopt a Security Incident Management Policy (SIMP) which shall define, among others, measures for the prevention of security incidents and personal data breach in the Cooperative. It shall establish procedures for breach response, notification to the NPC and affected data subjects and processes for personal data recovery and restoration.

The Cooperative shall designate and maintain a Security Incident Response Team who will be primarily responsible for implementing the measures and procedures set forth in the SIMP.

All personnel shall be responsible for reporting to the DPO or the Security Incident Response Team any security incident including any actual or possible breaches of confidentiality, integrity or availability of personal data.

VIII. Amendment and Review

This Privacy Policy and other privacy-related policies shall be reviewed at least annually by the DPO to make sure that the information contained therein is kept up to date.

The updated versions shall be subject to the approval of the Board of Directors or the President/CEO, as may be delegated by the Board.

IX. Communication

The DPO shall be responsible for communicating this Privacy Policy as well as any changes thereto to all personnel and affected data subjects.

X. Contact Information

For any questions about this Privacy Policy, any matter relating to Data Privacy or regarding the processing of personal data or for the exercise of data subjects, any personnel or data subject may contact the DPO or any COP of the Cooperative through the following:

Data Protection Officer: Sar C. Buksh
Mobile No.: +639175406992
Email: dataprotection@1cisp.coop

XI. Effectivity & Repealing Clause

This Privacy Policy shall be effective within 15 days from the approval hereof by the Board of Directors. Any other issuance or policy or provisions thereof that are inconsistent herewith are hereby superseded or amended accordingly.