

DATA PRIVACY MANUAL

CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect the fundamental human right of privacy and communication.

While the government recognizes the vital role of information and communications technology in nation-building, it also acknowledges its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

The Act serves the following purposes:

1. Protect the privacy of individuals while ensuring free flow of information to promote innovation and growth;
2. Regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and
3. Ensures that the Philippines complies with international standards set for data protection through the National Privacy Commission.

Approved into law last August 15, 2012, the DPA created the National Privacy Commission (NPC) which is tasked to monitor its implementation.

It ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding an individual's data privacy rights.

Introduction

CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE Data Privacy Manual is hereby adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations, and other relevant policies that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects, including issuances of the NPC which are relevant to the insurance industry and the cooperative sector where CLIMBS belong, as well as the transactions it regularly carries out.

Definition of Terms

For purposes of this Manual the following terms are defined as follows:

1. Data Subject – refers to an individual whose personal, sensitive personal or privileged information is processed by CLIMBS. It may refer to officers, employees, consultants, and clients of this cooperative insurance.
2. 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.
3. Processing - refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.

4. Personal Information Controller (PIC) - refers to a natural or juridical person, or any other body who controls the processing, of personal data, or instructs another to process personal data on his behalf. It is the organization processing the data or CLIMBS.
5. Personal Information Processor (PIP) - refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject (e.g. CoopAssurance Center, BPO, telemarketing).
6. Data Protection Officer (DPO) – the DPO is a full-time employee of the PIC. He is accountable for insuring compliance with applicable laws and regulations for the protection of data privacy and security. His designation, postal address, dedicated contact number, and email address is found in the website and data privacy forms.
7. Compliance Officer for Privacy (COP) – the COP is a full-time employee of the PIC and refers to the individual that performs some of the functions of a DPO, as provided on this manual.
8. Personal data breach – is a breach of security resulting to accidental or unlawful destruction, loss, or alteration of personal data, including its unauthorized disclosure. There are three types of personal data breach: availability, integrity and confidentiality.
9. Security incident – is an event or situation that affects or will likely affect data protection or compromise the availability, integrity, and confidentiality of personal data.
10. Availability breach – loss, accidental or unlawful destruction of personal data.
11. Integrity breach – alteration of or unauthorized changes to personal data.
12. Confidentiality breach – unauthorized disclosure of or access to personal data.
13. Data sharing - is the disclosure or transfer to a third party of personal data under the control or custody of a PIC. It is different from and excludes the outsourcing or subcontracting of the processing of personal data.

Scope and Limitations

This Data Privacy Manual applies to all personnel of CLIMBS, regardless of the type of employment or contractual arrangement.

It is noted that it is useful to develop a separate Privacy Manual meant for external use or for persons who deal with CLIMBS where certain information is omitted particularly those that relate to internal policies or process that are relevant only to personnel of CLIMBS.

Processing of Personal Data

This section lays out the various data processing systems in existence within CLIMBS—from the collection of personal data, to their actual use, storage or retention, and destruction.

1. Collection

CLIMBS collects the basic contact information required both by AMLA, MID, CIC and NPC of its clients and customers, including their full name, address, email address, contact number, birthdate, source of income together with the insurance products that they would like to purchase.

These are obtained openly and straightforwardly without any hidden motive through the clients' filling up of official forms. These forms are essential in the provision of service to clients.



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.

Similarly, personal data of the CLIMBS officials and employees (including project and/or agency-based employees) and applicants to vacant positions are obtained through the requisite Personal Data Sheet (PDS) and by accomplishing forms essential in training and other developmental interventions.

2. Use

Personal data collected shall be used by CLIMBS for documentation purposes including the Know Your Client (KYC) in compliance with AMLA, for warranty tracking vis-à-vis purchased insurance policies and for the inventory of products.

3. Storage, Retention and Destruction

CLIMBS will 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. CLIMBS will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

All information gathered shall not be retained for a period longer than ten (10) years based on the BIR requirements. All hard copies after five (5) years and soft copies after ten (10) of personal information years shall be disposed and destroyed through secured means.

4. Access

Due to the sensitive and confidential nature of the personal data under the custody of CLIMBS, only the client and the authorized representative of CLIMBS shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

Any request for amendment of personal data shall require strict verification and approval to effect the change.

5. Disclosure and Sharing

All employees and personnel of CLIMBS 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 CLIMBS shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

Personal data of CLIMBS clients maintain in the personal laptop of separating employees shall be subject to verification and must be deleted.

Security Measure

As a PIC, CLIMBS must implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data.

Security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

In this section, a general description of those measures is enumerated.



1. Organization Security Measures

CLIMBS as PIC shall consider the human aspect of data protection. The provisions under this section include the following:

A. Data Protection Officer (DPO)

The designated Data Protection Officer and is appointed by the Board of Directors and shall serve a term of two (2) years which can be re-appointed or re-assigned.

Where applicable, a Compliance Officer for Privacy (COP) under the supervision of the DPO may be designated and shall serve a term of two (2) years which can be re-appointed or re-assigned.

B. Functions of the Data Privacy Officer (DPO)

Listed hereunder are the functions and responsibilities of the DPO and COP:

- b.1 Monitor the PIC or PIP compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies. As such he may:
 - Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
 - Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
 - Inform, advise, and issue recommendations to the PIC or PIP;
 - Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
 - Advise the PIP or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;
- b.2 Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- b.3 Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- b.4 Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- b.5 Inform and cultivate awareness on privacy and data protection within your organization, including all relevant laws, rules and regulations and issuances of the NPC;
- b.6 Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- b.7 Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;



- b.8 Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- b.9 Perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

C. Compliance Officer for Privacy (COP)

Except for items (1) to (3), a COP shall perform all other functions of a DPO. Where appropriate, he or she shall also assist the supervising DPO in the performance of the latter's functions.

The DPO or COP must have due regard for the risks associated with the processing operations of the PIC or PIP, taking into account the nature, scope, context and purpose of processing.

Accordingly, they must prioritize their activities and focus their efforts on issues that present higher data protection risks.

D. General Obligations of the PIC or PIP Relative to the DPO or COP

The PIC or PIP should:

- d.1 Effectively communicate to its personnel the designation of the DPO or COP and his functions;
- d.2 Allows the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection.
- d.3 Provide sufficient time and resources (financial, infrastructure, equipment, training and staff) necessary for the DPO or COP to keep himself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently.
- d.4 Grant the DPO or COP appropriate access to the personal data it is processing including the processing systems;
- d.5 Where applicable, invite the DPO or COP to participate in meetings of senior and middle management to present the interest of privacy and data protection;
- d.6 Promptly consult the DPO or COP in the event of a personal data breach or security incident and
- d.7 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 organization or with other organizations.

2. Conduct of Trainings or Seminars

CLIMBS 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, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.



3. Conduct of Privacy Impact Assessment (PIA)

CLIMBS shall conduct a PIA relative to all activities, projects and systems involving the processing of personal data.

The CLIMBS PIA team consist of Compliance Officer, Finance Officer, IT Manager, Legal Officer and CEO, however, CLIMBS may choose to outsource the conduct of PIA to a third party.

4. Documentation

Recording and documentation of activities carried out by the DPO, or CLIMBS itself, to ensure compliance with the DPA, its IRR and other relevant policies.

5. Duty of Confidentiality

All employees of CLIMBS will be asked to sign a Non-Disclosure Agreement. 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.

6. Review of Privacy Manual

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

Physical Security Measures

This portion shall feature the procedures intended to monitor and limit access to the facility containing the personal data, including the activities therein.

It provides for the actual design of the facility, the physical arrangement of equipment and furniture, the permissible modes of transfer, and the schedule and means of retention and disposal of data, among others.

To ensure that mechanical destruction, tampering and alteration of personal data under the custody of CLIMBS are protected from man-made disasters, power disturbances, external access, and other similar threats, the following provisions are included in this Manual:

1. Format of data to be collected

Personal data in the custody of CLIMBS may be in digital/electronic format and paper-based/physical format.

2. Storage type and location (e.g. filing cabinets, electronic storage system, personal data room/separate room or part of an existing room)

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

3. Access procedure of agency personnel

Only the DPO, COP and authorized personnel of each department/division shall be allowed inside the data storage/room. For this purpose, the DPO/CPO shall secure the master key and duplicate keys to the authorized personnel to the data room.



Other personnel may be granted access to the room upon filing of an access request form with the DPO/COP and the latter's approval thereof.

An official/employee who wishes to see documents on his/her personal file (201File) shall fill up a request form to be approved by the DPO or by the COP. The authorized HR personnel shall secure the requested document/s, have the same photocopied, and hand this/these over to the official/employee concerned.

An employee cannot invoke his/her right to access his/her 201 File under the law when the personal information is being processed for the purpose of investigation in relation to any criminal, administrative, or tax liabilities against him/her.

Directors and Top Management, other than those expressly mentioned in the preceding paragraphs, may have access to personal file information on a need-to-know basis.

To protect against inappropriate disclosure of confidential information, certain records including those containing confidential information about more than one individual and medical record shall not be allowed to be accessed.

At no time should authorized official/personnel bring gadgets or storage device of any form when accessing personal files of CLIMBS personnel, applicants and clients.

4. Monitoring and limitation of access to room or facility

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

5. 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.

6. Persons involved in processing, and their duties and responsibilities

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.

7. Modes of transfer of personal data within CLIMBS, or to third parties

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

8. Retention and disposal procedure

CLIMBS shall retain the personal data of a client for ten (10) year from the date of purchase. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.



Technical Security Measures

Each PIC implements technical security measures to make sure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access.

This includes the following, among others:

1. Monitoring for security breaches

CLIMBS shall procure and install anti-virus software, on an annual basis, to devices that regularly access the internet (desktop, laptop, apple and android devices).

The IT Department shall regularly read the firewall logs to monitor security breaches and alert the Board of any unauthorized attempt to access CLIMBS network.

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

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

The IT Administrator shall review and evaluate software applications before the deployment in the computer and devices of CLIMBS to ensure compatibility of security features with the data privacy policies.

On existing software applications, which involves processing of personal data of CLIMBS officers, employees, consultants, and clients the following shall be observed:

The end user, with the technical assistance of IT, shall evaluate and assess the security protocols of the system with regards to saving, backup, and data recovery. If such protocol runs counter with the data privacy principles stated in the Data Privacy Act of 2012, remedial steps should be made to correct such flaws.

The IT semestral maintenance activities shall check software applications installed in all IT hardware and devices for compliance with CLIMBS Data Privacy Policy.

If a software/application is found to be a security risk that it may disturb or interrupt the normal operations of CLIMBS, IT technical personnel shall notify the end user of the risk and the software/application shall immediately be uninstalled. The IT personnel shall thereafter prepare an incident report.

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

CLIMBS shall review security policies, conduct vulnerability assessments and perform penetration testing within CLIMBS on regular schedule to be prescribed 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.

The IT Department shall submit a quarterly report to the DPO/COP of personnel with access to personal data.



Breach and Security Incidents

Every PIP develops and implements policies and procedures for the management of a personal data breach, including security incidents. This section adequately describes or outlines such policies and procedures, including the following:

1. 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 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.

As approved by the Board or Executive Committee, the team composed of the following: Compliance Officer, Finance Officer, IT Manager, Legal Officer and President and CEO. The team is headed by the DPO.

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

CLIMBS shall regularly conduct a PIA 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 insurance cooperative.

3. Procedure for recovery and restoration of personal data

CLIMBS 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.

4. 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 the period prescribed by law (not more than 72 hours). Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

5. 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.

- Description of the nature of the breach;
- Personal data possibly involved;
- Measures undertaken by the team to address the breach and reduce the harm or its negative consequences; and
- Names of the personal information controller, including contact details, from whom the data subject can obtain additional information about the breach and any assistance to be provided to the affected data subjects.



Rights of a Data Subject

The data subjects, under RA 10173 are accorded certain rights which they may invoke and enforce against personal information controllers or processors, and which the latter are duty-bound to observe and respect.

1. The right to be informed.

The data subject has a right to be informed whether personal data pertaining to him or her will be, are being, or were processed.

The data subject should be notified and furnished with the following information before the entry of his or her personal data into the processing system, or at the next practical opportunity.

2. The right to access.

The data subject have the right to obtain from the PIC a copy of any information relating to him that they have on their computer database and/or manual filing system. It should be provided in an easy-to-access format, accompanied with a full explanation executed in plain language.

3. The right to object.

The data subject has the right to object to the processing of his or her personal data, including processing for direct marketing, automated processing or profiling. He or she should be given an opportunity to withhold consent in case of any amendment to the information supplied to the data subject under the right to be informed.

4. The right to erasure or blocking.

The data subject has the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system. This right may be exercised upon discovery and substantial proof.

5. The right to damages.

The data subject have the right to be indemnified for any damages sustained due to such false, incomplete, outdated, unlawfully obtained or unauthorized use of personal data, considering any violation of his or her rights and freedoms as a data subject.

Inquiries and Complaints

Every data subject has the right to reasonable access to his or her personal data being processed by the CLIMBS as PIC. Other available rights include:

1. Right to dispute the inaccuracy or error in the personal data;
2. Right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and;
3. Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

Accordingly, there must be a procedure for inquiries and complaints that will specify the means through which concerns, documents, or forms submitted to CLIMBS shall be received and acted upon. Thus, this section shall feature such procedure.

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of CLIMBS, including the data privacy and security policies



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.

implemented to ensure the protection of their personal data. They may write to CLIMBS at inquiry@climbs.coop and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to complaints@climbs.coop. The concerned department or unit shall confirm with the complainant its receipt of the complaint within forty eight (48) hours.

All access requests for information will be responded within forty eight (48) hours.

All requests for correction and erasure will be responded not more than forty five (45) days upon receipt of request.

Effectivity

This section indicates the period of effectivity of this Manual, as well as any other document that CLIMBS may issue, and which has the effect of amending the provisions of this Manual.

The provisions of this Manual are effective this 18th day of February, 2018, until revoked or amended by the Board of Directors, through a Board Resolution.

Annexes

This section indicates the different types of form to be used and other related policies in the implementation of this Manual and DPA.

1. Privacy Notice and Consent Form
2. Access Request Form
3. Request for Correction or Erasure
4. Non-disclosure Agreement
5. Data Sharing Agreement
6. Data Breach Response Policy
7. Security Incident Management Policy
8. Board Resolution Approving the Policy



Annex 1

Data Privacy Notice and Consent Form
CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Dear _____,

CLIMBS shall protect the data you provided in compliance with the Data Privacy Law of 2012 and its implementing rules and regulations. CLIMBS will not collect, disclose or process personal data, including data that may be classified as personal information and/or sensitive personal information unless you voluntarily choose to provide us with it and give your consent thereto, or unless such disclosure is required by applicable laws and regulations. Personal or sensitive personal information is information pertaining to racial or ethnic origin, religious belief, political affiliations, education, health or information provided by government agencies which are peculiar to individuals and such other data declared to be sensitive.

CLIMBS shall keep the Data throughout the term of the engagement and for a period of ten (10) years thereafter. CLIMBS shall take appropriate and commercially reasonable technical and organizational measure to ensure the requisite data security to protect the Data against unauthorized disclosure or unauthorized access. CLIMBS shall require its affiliates, subsidiaries and third parties who process the Data to adhere to similar or comparable data protection standards as required by the Data Privacy Law of 2012.

You understand that you are given certain rights under the Data Privacy Act, including the right to object to processing of your data, the right to access your data, the right to correct any inaccurate data, and the right to erasure or blocking of data. For more information on these rights, and for requests to review the Data, to withdraw consent to the use of the Data for any of the purpose stated above, and/or to correct or update the Data, please contact our Data Privacy Officer at dpo@climbs.coop

Sincerely yours,

CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

In compliance with the Data Privacy Act (DPA) of 2012, and its Implementing Rules and Regulations (IRR) effective since September 8, 2016, I allow CLIMBS to provide me certain services declared in relation to the insurance policy/ies I purchased.

As such, I agree and authorize CLIMBS to:

1. Continue to use my policies’ information to process insurance services and administer the benefits as stated in my policy(ies).
2. Retain my information for a period of ten years from the date of termination of my policy, or at such time that I submit to CLIMBS a written cancellation of this consent, whichever is earlier. I agree that my information will be deleted/ destroyed after this period.
3. Retain my information in the Medical Information Database shared with other life insurance companies in accordance with the Insurance Regulation.
4. Share my information to affiliates and necessary third parties for any legitimate business purpose. I am assured that security systems are employed to protect my information.
5. Inform me of future customer campaigns and base its offer using the personal information I shared with CLIMBS.

I also acknowledge and warrant that I have acquired the consent from all parties relevant to this consent and hold free and harmless and indemnify CLIMBS from any complaint, suit, or damages which any party may file or claim in relation to my consent.

Insured Signature over Printed Name

Policy Owner Signature over Printed Name

For more information, you may visit our Privacy Statement at www.climbs.coop

Further information on Data Protection:
The Data Privacy Officer / CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop



Annex 2

Access Request Form
CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Details of Person Making Request

Full Name _____
Address: _____
Telephone/Mobile No.: _____ Email Address: _____

Details of Request

Reason for Request

Verification of Identity

Please check and attach photocopy any of the following valid ID:

_____ Driver’s License
_____ SSS/TIN
_____ Passport

Part 4 – Declaration

I declare that all the details I have provided in this form are true and complete to the best of my knowledge.

All access requests for information will be responded within forty eight (48) hours.

Signature of Requester _____

Date _____

Verified by: _____ Name and signature	Approved by: _____ Data Protection Officer	Released by: _____ Name and signature	Received by: _____ Name and signature
Date:	Date:	Date:	Date:

Further information on Data Protection:

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop

Annex 3

Access Request Form
CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE
REQUEST FOR CORRECTION/ERASURE FORM

NAME :		POSITION :	
OFFICE :			
Request for <input type="radio"/> Correction <input type="radio"/> Erasure (Please Check): <input type="checkbox"/> Name <input type="checkbox"/> Birthday <input type="checkbox"/> Status <input type="checkbox"/> Address <input type="checkbox"/> Telephone Numbers <input type="checkbox"/> Others (Please specify) _____ _____ _____ _____ _____		Original Entry	Proposed Correction
Reason/s for Correction/Erasure (Please specify) : _____ _____ _____ _____ _____			
Requested by: _____ Signature over Printed Name	Approved by: _____ Signature over Printed Name Data Privacy Officer	Correction Made by: _____ Signature over Printed Name	Proof of Correction/Erasure: Received by: _____ Signature over Printed Name
Date :	Date :	Date :	Date :

All requests for correction and erasure will be responded not more than forty five (45) days upon receipt of request.

Further information on Data Protection:

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop

Annex 4

EMPLOYEE NON-DISCLOSURE AGREEMENT

This EMPLOYEE NON-DISCLOSURE AGREEMENT, hereinafter known as the “Agreement”, is entered into between _____ (“Employee”) and CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE (“Company”), collectively known as the “Parties” as of the ____ day of _____, 20____ (the “Effective Date”).

Scope of Agreement

This Agreement acknowledges that certain confidential information, trade secrets, and proprietary data of CLIMBS as may be discussed, shared and accessed by the Employee.

The provisions set forth in this Agreement define the circumstances in which the Employee can and cannot disclose Confidential Information, and include the remedies, penalties and lawful action that CLIMBS may take should such information be used or disclosed by Employee.

Both Parties agree that it is in their best interests to protect the CLIMBS Confidential Information, and that the terms of this Agreement create a bond of trust and confidentiality between them.

In consideration of Employee’s commencement of employment, or continued employment with CLIMBS, the Parties agree as follows:

Confidential Information

A. Definitions

Confidential Information is any material, knowledge, information and data (verbal, electronic, written or any other form) concerning the CLIMBS or its businesses not generally known to the public consisting of, but not limited to, inventions, discoveries, plans, concepts, designs, blueprints, drawings, models, devices, equipment, apparatus, products, prototypes, formulae, algorithms, techniques, research projects, computer programs, software, firmware, hardware, business, development and marketing plans, merchandising systems, financial and pricing data, information concerning investors, customers, suppliers, consultants and employees, and any other concepts, ideas or information involving or related to the business which, if misused or disclosed, could adversely affect CLIMBS business.

B. Exclusions

For the purposes of this Agreement, information shall not be deemed Confidential Information and the Employee shall have no obligation to keep it confidential if:

- (i) the information was publicly known;
- (ii) the information was received from a third party not subject to the restrictions of this Agreement and becomes available to Employee through no wrongful act or breach of Agreement on their part; or
- (iii) the information was approved for release by CLIMBS through written authorization.

C. Limitations

Employee shall limit access to Confidential Information to individuals on a strictly need-to-know basis, involving only those who are carrying out duties related to CLIMBS and its business.

Individuals under the Employee’s command (affiliates, agents, consultants, representatives and other employees) are bound by and shall comply with the terms of this Agreement.



D. Ownership

All repositories of information containing or in any way relating to Confidential Information is considered property of CLIMBS. The removal of Confidential Information from CLIMBS premises is prohibited unless prior written consent is provided by CLIMBS.

All such items made, compiled or used by the Employee shall be delivered to the Employer by Employee upon termination of employment or at any other time as per the Employer's request.

Entire Agreement

A. Previous Agreements

This Agreement constitutes the entire agreement and the signing thereof by both Parties nullifies any and all previous agreements made between CLIMBS and Employee.

B. Modifications and Amendments

No modifications, amendments, changes or alterations can be made to the Agreement unless in writing and signed by authorized representatives of both Parties.

C. Successors and Assigns

This Agreement shall be binding upon the successors, subsidiaries, assigns and corporations controlling or controlled by the Parties.

CLIMBS may assign this Agreement to any party at any time, whereas the Employee is prohibited from assigning any of their rights or obligations in the Agreement without prior written consent from CLIMBS.

Immunity

Disclosing Confidential Information to an attorney, government representative or court official in confidence while assisting or taking part in a case involving a suspected violation of law is not considered a breach of this Agreement.

Should the Employee be required to disclose Confidential Information by law, the Employee shall provide CLIMBS with prompt notice of such request.

D. Breach of agreement

Indemnification

Employee understands and agrees that if the use or disclosure of Confidential Information by them or any affiliate, employee or representative of the Employee causes damage, loss, cost or expense to CLIMBS, the Employee shall be held responsible.

Employee shall indemnify CLIMBS and CLIMBS has the right to pursue legal action beyond remedies of a monetary nature in the form of injunctive or equitable relief. This may be in addition to any other remedy, penalty or claim the law can provide.

Notice of Unauthorized Use or Disclosure

Employee is bound by this Agreement to notify CLIMBS in the event of a breach of agreement involving the dissemination of Confidential Information, either by the Employee or a third party, and will do everything possible to help CLIMBS regain possession of the Confidential Information.



The failure to notify the NPC or the public may make you criminally liable for Concealment of Security Breaches Involving Sensitive Personal Information, which carries a penalty of imprisonment from one year and six months to five years, and a fine of Five Hundred Thousand Pesos (₱500,000.00) to One Million Pesos (₱1,000,000.00).

Prevailing party

In a dispute arising out of or in relation to this Agreement, the prevailing party shall have the right to collect from the other party its reasonable attorney fees, costs and necessary expenditures.

IN WITNESS WHEREOF, the Parties hereto agree to the terms of this Agreement and signed on the dates written below.

Employee Signature _____ **Date:** _____
Employee Printed Name: _____

Further information on Data Protection:
The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop



Annex 5

Data Sharing Agreement
CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

This agreement is entered into by and between _____ (“Company”) and _____ (“Partner”).

Duration of Agreement

This Data Sharing Agreement is effective from _____ through _____ to coincide with current MOU dates. This agreement may be amended in writing at any time with the concurrence of both parties.

Provided, that in no case shall such term or any subsequent extensions thereof exceed five (5) years, without prejudice to entering into a new data sharing agreement.

Description of Data

It shall specify, with due particularity, the purpose or purposes of the data sharing agreement, including if applicable, online access to personal data, or if access is open to the public or private entities, these shall also be clearly specified in the agreement.

Terms and Conditions

It shall identify all personal information controllers that are party to the agreement, and for every party, specify:

- 1. the type of personal data to be shared under the agreement;*
- 2. the partner that will have access to or process the personal data, including the types of processing it shall be allowed to perform;*
- 3. how the party may use or process the personal data, including, but not limited to, online access;*

Method of Data Access or Transfer

The transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing personal data.

Rights of Data Subject

The data subject has the right to reasonable access to his or her personal data being processed by CLIMBS and the Party:

1. Right to dispute the inaccuracy or error in the personal data;
2. Right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and;
3. Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

The data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of CLIMBS and Party, including the data privacy and security policies implemented to ensure the protection of their personal data.

They may write to CLIMBS at inquiry@climbs.coop and briefly discuss the inquiry, together with their contact details for reference.



Complaints shall be filed in three (3) printed copies, or sent to complaints@climbs.coop. The concerned department or unit shall confirm with the complainant its receipt of the complaint within forty eight (48) hours.

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop

Personal Data Online

If a personal information controller shall grant online access to personal data under its control or custody, it shall specify the following information:

1. *Justification for allowing online access;*
2. *Parties that shall be granted online access;*
3. *Types of personal data that shall be made accessible online;*
4. *Estimated frequency and volume of the proposed access; and*
5. *Program, middleware and encryption method that will be used.*

Return, Destruction, or Disposal of Transferred Personal Data

All personal data transferred to other parties by virtue of such agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement to CLIMBS.

Accountability for Cross-border Transfer of Personal Data

Each party to the data sharing agreement shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor.

Termination

A data sharing agreement may be terminated:

1. Upon the expiration of its term, or any valid extension thereof;
2. Upon the agreement by all parties;
3. Upon a breach of its provisions by any of the parties; or
4. Where there is disagreement, upon a finding by the Commission that its continued operation is no longer necessary, or is contrary to public interest or public policy.

Immunity

Disclosing Confidential Information to an attorney, government representative or court official in confidence while assisting or taking part in a case involving a suspected violation of law is not considered a breach of this Agreement.

Should the Party be required to disclose Confidential Information by law, the Party shall provide CLIMBS with prompt notice of such request.

Indemnification

Party understands and agrees that if the use or disclosure of Confidential Information by them or any affiliate, employee or representative of the Party causes damage, loss, cost or expense to CLIMBS, the Party shall be held responsible and shall indemnify CLIMBS and CLIMBS has the right to pursue legal action beyond remedies of a monetary nature in the form of injunctive or equitable relief.

This may be in addition to any other remedy, penalty or claim the law can provide.



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.

Notice of Unauthorized Use or Disclosure

Party is bound by this Agreement to notify CLIMBS in the event of a breach of agreement involving the dissemination of Confidential Information, either by the Party or a third party, and will do everything possible to help CLIMBS regain possession of the Confidential Information.

The failure to notify the NPC or the public may make you criminally liable for Concealment of Security Breaches Involving Sensitive Personal Information, which carries a penalty of imprisonment from one year and six months to five years, and a fine of Five Hundred Thousand Pesos (₱500,000.00) to One Million Pesos (₱1,000,000.00).

Prevailing party

In a dispute arising out of or in relation to this Agreement, the prevailing party shall have the right to collect from the other party its reasonable attorney fees, costs and necessary expenditures.

IN WITNESS WHEREOF, the Parties hereto agree to the terms of this Agreement and signed on the dates written below.

CLIMBS Life and General Insurance Cooperative

Party

Further information on Data Protection:

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop



Annex 6

Data Breach Response Policy CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

The Data Breach Response Policy is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization.

Incident Response Team

The Data Breach Response Team is established for the implementation of the Security Incident Management Policy and management of security incidents and personal data breaches ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.

The team composed of the following: Compliance Officer, Finance Officer, IT Manager, Legal Officer and President and CEO. The team is headed by the DPO.

Documentation

All actions taken by a PIC or PIP shall be properly documented. Reports should include:

1. Description of the personal data breach, its root cause and circumstances regarding its discovery;
2. Actions and decisions of the incident response team;
3. Outcome of the breach management, and difficulties encountered; and
4. Compliance with notification requirements and assistance provided to affected data subjects.

A procedure for post-breach review must be established for the purpose of improving the Security Incident Management Policy.

Notification

Notification shall be made by the PIC or PIP that a personal data breach has occurred:

1. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. The PIC or the NPC believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Public Information

A claim that the data involved in a breach is public information will not automatically exempt a PIC from the notification requirements. When the level of availability or publicity of the personal data is altered by a personal data breach, it shall be considered as a personal data breach requiring notification, subject to the preceding paragraphs.



Determination of the Need to Notify

The PIC shall take into account the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The PIC shall also consider if the personal data reasonably believed to have been compromised involves:

1. Information that would likely affect national security, public safety, public order, or public health;
2. At least one hundred (100) individuals;
3. Information required by applicable laws or rules to be confidential; or
4. Personal data of vulnerable groups.

Who Should Notify

The PIC through the DPO shall notify the NPC and the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the PIC even if the processing of information is outsourced or subcontracted to a personal information processor.

Notification to the NPC

The personal information controller shall notify the NPC of a personal data breach subject to the following procedures:

A. When Notification Should be Done

The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the PIC or PIP that a personal data breach has occurred.

B. Delay in Notification

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.

The PIC need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects.

Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

C. When delay is prohibited

There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject.

In both instances, NPC shall be notified within the 72-hour period based on available information.

The full report of the personal data breach must be submitted within five (5) days, unless the PIC is granted additional time by NPC to comply.



D. Content of Notification

The notification shall include, but not be limited to:

1. Nature of the Breach
 - a. Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
 - b. A chronology of the events leading up to the loss of control over the personal data;
 - c. Approximate number of data subjects or records involved;
 - d. Description or nature of the personal data breach;
 - e. Description of the likely consequences of the personal data breach; and
 - f. Name and contact details of the data protection officer or any other accountable persons.
2. Personal Data Possibly Involved
 - a. Description of sensitive personal information involved; and
 - b. Description of other information involved that may be used to enable identity fraud.
3. Measures Taken to Address the Breach
 - a. Description of the measures taken or proposed to be taken to address the breach;
 - b. Actions being taken to secure or recover the personal data that were compromised;
 - c. Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
 - d. Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
 - e. The measures being taken to prevent a recurrence of the incident.

E. Form

Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification including the name and contact details of the DPO and a designated representative of the personal information controller.

Upon receipt of the notification, NPC shall send a confirmation to the PIC.

Notification of Data Subjects

The PIC shall notify the data subjects affected by a personal data breach, subject to the following procedures:

A. When should notification be done

The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.

The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

B. Exemption or Postponement of Notification

If it is not reasonably possible to notify the data subjects within the prescribed period, the PIC shall request the NPC for an exemption from the notification requirement, or the postponement of the notification.

A PIC may be exempted from the notification requirement where NPC determines that such notification would not be in the public interest or in the interest of the affected data subjects.



The NPC may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.

C. Content of Notification. The notification shall include, but not be limited to:

1. Nature of the breach;
2. Personal data possibly involved;
3. Measures taken to address the breach;
4. Measures taken to reduce the harm or negative consequences of the breach;
5. Representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach; and
6. Any assistance to be provided to the affected data subjects.

D. Form

Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.

Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.

Exemption from Notification Requirements

The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:

1. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;
2. Subsequent measures that have been taken by the PIC or PIP to ensure that the risk of harm or negative consequence to the data subjects will not materialize;
3. Age or legal capacity of affected data subjects: Provided, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.

In evaluating if notification is unwarranted, the NPC may take into account the compliance by the PIC with the law and existence of good faith in the acquisition of personal data.

Failure to Notify

In case the PIC fails to notify the NPC or data subjects, or there is unreasonable delay to the notification, the NPC shall determine if such failure or delay is justified. Failure to notify shall be presumed if the NPC does not receive notification from the PIC within five (5) days from knowledge of or upon a reasonable belief that a personal data breach occurred.

Investigation of a Breach or a Security Incident

Depending on the nature of the incident, or if there is failure or delay in the notification, the NPC may investigate the circumstances surrounding a personal data breach. Investigations may include on-site examination of systems and procedures and may require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects.



Reportorial requirements

All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements.

Any or all reports shall be made available when requested by the NPC: Provided, that a summary of all reports shall be submitted to the NPC annually, comprised of general information including the number of incidents and breach encountered, classified according to their impact on the availability, integrity, or confidentiality of personal data.

Notification and Reporting to the National Privacy Commission

The requirements pertaining to notification and the submission of reports shall be complied with through the appropriate submissions to the office of the National Privacy Commission or by electronic mail (complaints@privacy.gov.ph).

Regular Review

The Data Breach Response Policy shall be subject to regular revision and review, at least annually, by the DPO, or any other person designated by the Chief Executive Officer. The date of the last review and the schedule for the next succeeding review must always be indicated in the documentation of the incident response policy and procedure.

Further information on Data Protection:

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 local 120 Email address: dpo@climbs.coop



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.

Annex 7

Security Incident Management Policy CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

This policy is for managing security incidents, including data breaches.

This security incident management policy and personal data breach management procedure, the following shall be observed:

- Creation of a security incident response team, with members that have clearly defined responsibilities, to ensure timely action in the event of a security incident or personal data breach;
- Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident;
- Implementation of an incident response procedure intended to contain a security incident or personal data breach and restore integrity to the information and communications system;
- Mitigation of possible harm and negative consequences to a data subject in the event of a personal data breach; and
- Compliance with the Data Privacy Act, its IRR, and all related issuances by the NPC pertaining to personal data breach notification.

This Security Incident Management Policy also includes measures intended to prevent or minimize the occurrence of a personal data breach. These measures include:

- Conduct of a privacy impact assessment to identify attendant risks in the processing of personal data. It shall take into account the size and sensitivity of the personal data being processed, and impact and likely harm of a personal data breach;
- Data governance policy that ensures adherence to the principles of transparency, legitimate purpose, and proportionality;
- Implementation of appropriate security measures that protect the availability, integrity and confidentiality of personal data being processed;
- Regular monitoring for security breaches and vulnerability scanning of computer networks;
- Capacity building of personnel to ensure knowledge of data breach management principles, and internal procedures for responding to security incidents;
- Procedure for the regular review of policies and procedures, including the testing, assessment, and evaluation of the effectiveness of the security measures.

A. The Security Incident Response Team

The Security Incident Response Team is responsible for:

1. Implementing security incident management policy of the PIC;
2. Managing security incidents and personal data breaches; and
3. Compliance by the PIC with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

Although the functions of the Security Incident Response Team (SIRT) may be outsourced, and there is no precise formula for the composition of the SIRT, its members must, as a collective unit, be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements



B. Annual Reports

PIC are required to submit their Annual Report, where all security incidents and personal data breaches must be documented through written reports, including those not covered by the notification requirements.

In the event of a personal data breach, a report shall include: (a) the facts surrounding the incident; (b) the effects of such incident; and (c) the remedial action taken by the personal information controller. For other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation.

Any or all reports shall be made available when requested by the Commission: Provided, that a summary of all reports shall be submitted to the Commission annually, comprised of general information including the: (1) number of incidents and breach encountered; and (2) classified according to their impact on the availability, integrity, or confidentiality of personal data

C. Mandatory Notification

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

1. There is a breach of sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud;
2. The data is reasonably believed to have been acquired by an unauthorized person; and
3. 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:

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

The failure to notify the NPC or the public may make you criminally liable for Concealment of Security Breaches Involving Sensitive Personal Information, which carries a penalty of imprisonment from one year and six months to five years, and a fine of Five Hundred Thousand Pesos (₱500,000.00) to One Million Pesos (₱1,000,000.00).

This crime is committed by those, having knowledge of the security breach and with an obligation to inform the NPC of the fact of such a breach, either intentionally or by omission fails to inform the NPC that the breach has happened.

Aside from notifying the NPC, the PIC shall also notify the affected data subjects upon knowledge of, or when there is reasonable belief that a personal data breach has occurred. The obligation to notify remains with the PIC even if the processing of information is outsourced or subcontracted to a personal information processor (PIP).

The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the PIC that a personal data breach has occurred.

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



1. the scope of the breach;
2. to prevent further disclosures; or
3. to restore reasonable integrity to the information and communications system.

There can be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In either case, the Commission must be notified within the 72-hour period based on available information.

The full report of the personal data breach must be submitted within five (5) days from notification, unless the PIC is granted additional time by the Commission to comply.

The following information must be included in any Data Breach notification:

1. Nature of the Breach. – There must be, at the very least, a description of: (a) the nature of the breach; (b) a chronology of events, and (c) an estimate of the number of data subjects affected;
2. Personal data involved. – stating the description of sensitive personal information or other information involved.
3. Remedial Measures. – there must be: (a) Description of the measures taken or proposed to be taken to address the breach; (b) Actions being taken to secure or recover the personal data that were compromised; (c) Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident; (d) Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification; and (d) the measures being taken to prevent a recurrence of the incident.
4. Name and contact details. – of the DPO or contact person designated by the PIC to provide additional information.

Under the Data Privacy Act, The data subject has the right to be notified and in enforcement of such, the Personal data controller MUST:

1. Notify the data subject within seventy-two (72) hours upon knowledge of or reasonable belief that a personal data breach has occurred;
2. The notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects;
3. The notification shall have the same content as those made to the NPC, but shall include instructions on how data subjects will get further information; and
4. Recommendations regarding how to minimize risks resulting from breach and to secure any form of assistance.

The notification may be supplemented with additional information at a later stage on the basis of further investigation.

The notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. And whenever individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification.

The Notification requirement is not absolute; the NPC can allow the Postponement of notification when it may hinder the progress of a criminal investigation.

D. The Subsequent Investigation

The NPC will consider these factors in its investigation following the occurrence of a data breach:

1. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;



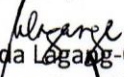
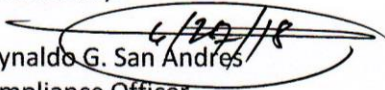

- 2. Subsequent measures that have been taken by the PIC to ensure that the risk of harm or negative consequence to the data subjects will not materialize;
- 3. Age or legal capacity of affected data subjects; Provided, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives; and
- 4. Compliance with the law and existence of good faith in the collection of personal information.

In investigation of a breach or a security incident, the Commission may investigate, depending on the nature of the incident, or in case of failure or delay in the notification. The investigation includes:

- 1. On-site examination of systems and procedures;
- 2. If necessary, the Commission shall require the cooperation of concerned parties, or compel appropriate action therefrom to protect the interests of data subjects; and
- 3. The investigation shall be governed by the Rules of Procedure of the Commission.

Further information on Data Protection:

The Data Privacy Officer
CLIMBS Life and General Insurance Cooperative
National Highway, Bulua, Cagayan de Oro City, Misamis Oriental, Philippines
Telephone No.: (088) 856 1355 Email address: dpo@climbs.coop

Prepared by:  Blesilda Legang-Cumba Assistant Compliance Officer	Reviewed by:  Reynaldo G. San Andres Compliance Officer
Attested by:  Noel D. Raboy President and CEO	Approved by: Board Resolution No. 8, series of 2018 January 31, 2018



REPUBLIC OF THE PHILIPPINES)
CAGAYAN DE ORO CITY) S.S.

SECRETARY CERTIFICATE

I, NIÑA FLOR B. BATARA, Filipino citizen, of legal age, and with office address at Bulua, Cagayan de Oro City after having been sworn to in accordance with law, hereby depose and say, that I am the Board Secretary of CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE (CLIMBS) a cooperative duly organized and existing in accordance with the laws of the Republic of the Philippines, and with principal address at Upper Zone 5, National Highway, Bulua, Cagayan de Oro City.

That in the meeting of the Regular Board of Directors on January 31, 2018 where a quorum exists, the Board approved and ratified the following Resolution to read as follows:

Board Resolution #8, series of 2018

“RESOLVE, AS IT IS HEREBY RESOLVED the appointment of **MR. REYANLDO G. SAN ANDRES**, as the Data Privacy Officer of CLIMBS Life and General Insurance Cooperative.”

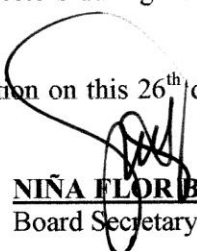
“ RESOLVE FURTHER, the appointment of the **Data Breach Response Team** composing of the following members: **CEO, Finance Officer, Legal Officer, and IT Manager.**

“FINALLY RESOLVED, approving CLIMBS Manual on Data Privacy.
Motion carried.”

SECRETARY’S CERTIFICATE

I hereby certify that the above is true and correct excerpt of Board Resolution No. 8, Series of 2018 as approved by the members of CLIMBS’ Board of Directors during its Regular Board Meeting held in Cebu City on January 31, 2018.

IN WITNESS WHEREOF, I have signed this certification on this 26th day of February 2018, at Cagayan de Oro City, Philippines.


NIÑA FLOR B. BATARA
Board Secretary

ACKNOWLEDGEMENT

Republic of the Philippines)
Cagayan de Oro City) S.S

BEFORE ME, personally appeared:

Name

SSS#/TIN#/DRIVER’S LICENSE #

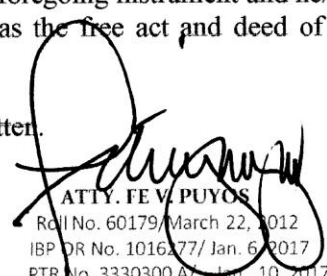
NIÑA FLOR B. BATARA

TIN# 935 430 937

Known to me and to me known to be the same persons who executed the foregoing instrument and he/she acknowledged the same to me to be his/her free act and deed as well as the free act and deed of the corporation which he/she represents.

WITNESS MY HAND AND SEAL, on the date and place first above written.

Doc. No. 202 ;
Page No. 41 ;
Book No. X ;
Series of 2018.


ATTY. FE V. PUYOS
Roll No. 60179/ March 22, 2012
IBP OR No. 101677/ Jan. 6, 2017
PTR No. 3330300 A/ Jan. 10, 2017
MCLE Compliance No. IV-0021008; issued on



CLIMBS LIFE AND GENERAL INSURANCE COOPERATIVE

Copyright © 2018 Data Privacy Manual. All Rights Reserved.

Do not copy, distribute or reproduce in whole or in part without prior written approval from CLIMBS.