BENGUET ELECTRIC COOPERATIVE (BENECO)

DATA PRIVACY MANUAL

Approved by the Board of Directors (BOD)
through BOD Resolution No. ___, Series of 2022 dated _____

I.BACKGROUND

The Benguet Electric Cooperative (BENECO) is a duly organized electric distribution utility with the National Electrification Administration (NEA) with a franchise to exclusively operate in Baguio City and the thirteen municipalities of Benguet, namely Atok, Bakun, Bokod, Buguias, Kabayan, Kapangan, Kibungan, Itogon, La Trinidad, Mankayan, Sablan, Tuba and Tublay. It is also an electric cooperative registered with the Cooperative Development Authority (CDA).
The main business process of BENECO starts from the time a member consumer applies for an electric service connection until such time that his or her house, building or establishment is supplied with electricity following the installation of a kilowatt hour meter (kWh) meter. Along this process is a gamut of technical and support services the electric cooperative must hurdle to ensure customer satisfaction and compliance with regulatory requirements. The electric cooperative is also mandated to address the daily concerns of its member consumer owners through a continuous program of information, education and communication. BENECO also operates a 24/7 call center or consumer welfare desk to receive and reply to requests and complaints.

These tasks necessarily require BENECO to collect and process personal information and sensitive personal information.

II.AUTHORITY

Republic Act. No. 10173 or the Data Privacy Act and its Implementing Rules and Regulations (IRR)

III.BENECO AS A PERSONAL INFORMATION CONTROLLER (PIC)

The business of BENECO makes necessary the gathering and processing of personal information, sensitive personal information and privileged information. This makes the electric cooperative a Personal Information Controller (PIC) since it takes custody of the personal information or directs another, the Privacy Information Processor (PIP) to process personal data on behalf of the electric cooperative. The data is obtained from member consumer owners, contractors and suppliers and employees, referred to as Data Subjects, in the discharge of BENECO's legitimate functions and interests and other professional services

Being a PIC, BENECO is thus obligated to effect reasonable and appropriate measures to protect the personal data in its records and files and communication systems against

unlawful access, fraudulent misuse, unauthorized disclosure, alteration, contamination, loss and destruction.

III.STATEMENT OF PRINCIPLE

BENECO respects the privacy of its member consumer owners (MCOs) and values the confidentiality of all the personal information and sensitive personal information they furnish to BENECO in the course of the transactions that they will have with the electric cooperative. This is why BENECO has adopted and approved this Data Privacy Manual in its bid to formalize an official guide or handbook for ensuring BENECO's compliance with RA 10173 or the Data Privacy Act (DPA), its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). This Manual also encapsulates the privacy and data protection protocols that need to be observed and carried out within the electric cooperative to safeguard the privacy of its MCOs as data subjects.

Thus, to our MCOs, BENECO reiterates that as an electric cooperative, it respects and values your data privacy rights, and declares that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality. This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

IV.STATEMENT OF PURPOSE

This Data Privacy Manual has been adopted by BENECO for the following reasons: (1)To notify the BENECO Board of Directors, management, supervisors and the rank and file including the BENECO Employees Labor Union (BELU) and the BENECO Supervisors Association (BSA) that BENECO is tasked to implement the Data Privacy Act (RA 10173) and its IRR; (2)To inform all the heads of BENECO offices that gather and process personal data on their responsibilities and possible criminal civil and administrative sanctions should they commit a data breach pursuant to RA 10173; and (3)To give assurance to BENECO's Data Subjects on the security measures being implemented by BENECO to safeguard their personal data against unlawful access, fraudulent misuse, unauthorized disclosure, alteration, contamination, loss and destruction.

V.SCOPE AND LIMITATIONS

The scope of this Data Privacy Notice shall cover the personal information and sensitive personal information obtained by the electric cooperative or furnished by its Data Subjects, the Member Consumer Owners (MCOs), in the course dealing with the various business processes of BENECO.

All personnel of BENECO, regardless of the status of their employment or contractual arrangement have been directed to must comply with the terms set out in this Privacy Manual.

VI.DEFINITION OF TERMS

For consistency and uniformity, the following terms shall mean as follows:

DATA SUBJECT	Refers to an individual (MCOs, officers, employees, consultants) whose personal, sensitive personal or privileged information is processed by BENECO.
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.
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 person, 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 not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (4) Specifically established by an executive order or an act of Congress to be kept classified.
PRIVILEGED INFORMATION	Refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
DATA SUBJECT	Refers to BENECO's Member Consumer Owners, Suppliers and Contractors and Employees whose personal, sensitive personal and privileged information are gathered and process by BENECO.
CONSENT OF THE DATA SUBJECT	Refers to the freely given and indication of will or approval given by the Data Subject regarding the collection and processing of his or her personal, sensitive personal and privileged information.
DATA 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.
DATA PROCESSING SYSTEM	Refers to the procedure and structure BENECO collects and processes personal data which includes the filing,

	information and communication system of the data gathered.
INFORMATION AND COMMUNICATION SYSTEM	Refers to a system for gathering, sending, receiving, storing and processing personal information through electronic processing, computer data, electronic message or electronic document.
DATA SHARING	Refers to the disclosure or transfer to a third party of personal data, sensitive personal information and privileged information under the control and custody of BENECO. This includes any disclosure by the Personal Information Controller (PIC) to the Personal Information Processor (PIP).
DATA SHARING AGREEMENT	Refers to any contract or agreement entered into by BENECO and any third party containing the terms and conditions of sharing personal data.
PERSONAL INFORMATION CONTROLLER	Refers to any personnel of BENECO who controls the collection, holding, processing or use of personal information, including a person or officer of the organization who instructs a BENECO employee to collect, hold, process, use, transfer or disclose personal information on his or her behalf.
PERSONAL INFORMATION PROCESSOR	refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.
PERSONAL DATA BREACH	Refers to a breach of data security leading to any accidental or intentional destruction, loss, alteration, contamination, unauthorized access or disclosure of personal information.
DATA PRIVACY NOTICE	Refers to the statement or declaration of BENECO's adherence to the Data Privacy Act, how it collects personal data and the purpose of the collection, how personal data is processed, stored, protected and destroyed after an allowable period of retention.
SECUSITY MEASURES	Refers to BENECO's organization, physical and technical measures employed to protect personal data from natural and human breach of data.
SECURITY INCIDENT	Refers to an y natural or man made events that affects or compromises personal data, or may compromise the availability, integrity and confidentiality of personal data.
DATA PROTECTION OFFICER	Refers to the duly designated officer of BENEO who shall be accountable for the compliance to the Data Privacy Act, its IRR and issuances of the National Privacy Commission (NPC).
COMPLIANCE OFFICER FOR PRIVACY	Refers to the employees/officers of BENECO designated to assist, help and backstop the DPO.

DATA BREACH RESPONSE TEAM	Refers to the designated employees who are tasked to immediately act on any security incident or personal data breach.
DATA PROTECTION RECORDS OFFICER	Refers to the employee designated by the electric cooperative to take custody of all records of meetings, minutes and proceedings, documents, communications, bard resolutions and directives of the NPC and management relative to the implementation of the Data Privacy Act in BENECO.

VII.THE NEED TO COLLECT AND SHARE PERSONAL DATA

TYPE OF FORM	PERSONAL INFO GATHERED	TO WHOM THE DATA IS SHARED	PURPOSE
1.Membership Form	a. Name of Applicant b. Address c. Civil Status d. Date of Birth e. Name of Spouse f. Contact Number g. Profession h. Nature of Business i. TIN j. Email address k. Signature of the applicant	a. CDA b. CWO	Membership Records
2. Application for Change Name form	a. Name of the existing member b. Name of the applicant c. Account Number/s d. Signature of the applicant e. Contact Number	a. CWO	Billing and membership records
3. Application for Burial Assistance Form	a. Name of the deceased member b. Members ID No. c. Name of the applicant d. Account Number/s e. Signature of the applicant f. Contact Number g. Relationship to the deceased member	a. CWO b. IAO c. OGM d. Accounting e. Collection	For recording and disbursement purpose
4.Application for Senior Discount	a. Account name b. Name of spouse c. Address d. Date of birth e. Place of birth f. Account number g. Meter No.	a. CWO b. MRBCD	Billing and records

	h. BENECO Id No. i. Signature of the applicant j. Contact Number k. OSCA id #		
5.Application for Correction of Data Entry form	a. Name of the Applicant b. Membership No c. Signature of the applicant d. Contact Number	a. CWO	Billing and records
6.Application for Long Time Disconnected Accounts	a. Name of the Applicant b. Address c. Account Number/s d. Signature of the applicant e. Contact Number	a. CWO b. SEMO	Billing and records
7. Job orders generated on CWMS	a. Name b. Address c. Contact Number d. Account Number/s	a. CWO b. MRBCD c. SEMO d. SPDO e. CMO	
8. Job Orders generated on OMS	a. Name b. Contact Number c. Address d. Landmark e. Account Number/s	a. CWO b. SCADA c. CMO	

DATA SUBJECT	PURPOSE
Member Consumer Owners (MCOs)	For the processing of applications for service connection, change of account name, educational, senior citizen, death burial assistance, assistance through BENECO's Corporate Social Responsibility Fund, and consumer complaints and requests.
Contractors and Suppliers	For accreditation and eligibility in project works and job orders; For accreditation and eligibility in procurement and bidding and contracts for supply of materials or services
Employees	For 201 files, loan applications and regulatory compliances. The 201 file, which is the personal file of the employees is a folder containing records about an employee's personal and sensitive personal information in document and electronic form.

VIII. PROCESSING OF PERSONAL DATA

Principles

BENECO shall process data in accordance with the Data Privacy Act of 2012 (RA 10173) and its IRR and other issuances of the National Privacy Commission (NPC) and such other laws, rules and regulations related to data processing. The processing of

data will strictly adhere to the generally accepted principles of TRANSPARENCY, LEGITIMATE PURPOSE and PROPORTIONALITY.

By TRANSPARENCY, it means that you, as Data Subject, must be made aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.

By LEGITIMATE PURPOSE, it means that the personal information that will be collected from you, as Data Subject, must be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy

By PROPORTIONALITY, it means that the collection and processing of information about you, as Data Subject, shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

General Guidelines

A. Access to Personal Data

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

B. Disclosure and Sharing

It is the policy of BENECCO that all employees and personnel 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 BENECO shall be disclosed only pursuant to a lawful purpose and only to authorized recipients of such data.

C. Storage, Retention and Destruction

BENECO ensures that all the personal data (stored in hard copies/ copies of documents and soft copy/e copy) under its custody shall be well protected against any accidental or unlawful destruction, alteration and disclosure as well as against any unlawful processing. BENECO has adopted security measures in storing collected personal information. All information gathered shall be retained pursuant to BENECO's ISO QMS Manual

Type of Data Gathered and Processed

TYPE OF FORM	PERSONAL INFO GATHERED	TO WHOM THE DATA IS SHARED	PURPOSE
1.Membership Form	a. Name of Applicant b. Address c. Civil Status d. Date of Birth e. Name of Spouse f. Contact Number g. Profession h. Nature of Business i. TIN j. Email address k. Signature of the applicant	a. CDA b. CWO	Membership Records
2. Application for Change Name form	a. Name of the existing member b. Name of the applicant c. Account Number/s d. Signature of the applicant e. Contact Number	a. CWO	Billing and membership records
3. Application for Burial Assistance Form	a. Name of the deceased member b. Members ID No. c. Name of the applicant d. Account Number/s e. Signature of the applicant f. Contact Number g. Relationship to the deceased member	a. CWO b. IAO c. OGM d. Accounting e. Collection	For recording and disbursement purpose
4.Application for Senior Discount	a. Account name b. Name of spouse c. Address d. Date of birth e. Place of birth f. Account number g. Meter No. h. BENECO Id No. i. Signature of the applicant j. Contact Number k. OSCA id #	a. CWO b. MRBCD	Billing and records
5.Application for Correction of Data Entry form	a. Name of the Applicant b. Membership No c. Signature of the applicant d. Contact Number	a. CWO	Billing and records
6.Application for Long Time Disconnected	a. Name of the Applicant b. Address c. Account Number/s	a. CWO b. SEMO	Billing and records

Accounts	d. Signature of the applicant e. Contact Number		
7. Job orders generated on CWMS	a. Name b. Address c. Contact Number d. Account Number/s	a. CWO b. MRBCD c. SEMO d. SPDO e. CMO	
8. Job Orders generated on OMS	a. Name b. Contact Number c. Address d. Landmark e. Account Number/s	a. CWO b. SCADA c. CMO	

Data Processing

BENECO has seven major offices with defined functions – Network Services Department (NSD), Institutional Services Department (ISD), Non-Network Services Department (NNSD) Power Generation and Operations Department (PGOD); Internal Audit Office (IAO) and the Office of the General Manager (OGM). BENECO'S IT Office, called the Management Information and Communication Services (MICS) is under the OGM. The personal data obtained will depend on the various processes each office is tasked to handle.

DEPT/ OFFICE	IDENTITY OF PROCESS	SCOPE OF DATA ACCESSED FROM CWO	INFO STORAGE OR SYSTEM USED	TO WHOM IS THE DATA SHARED OR LINKED WITH
OGM	Compliance reports	Personal information	File	none
	Employees' medical result	Personal Information and Sensitive Personal Information	File	none
OGM-MICS	Data back and recovery	Personal information and sensitive personal information	3rd party system	ASC, Billing, Collection, Accounting, Payroll, Warehouse
	Maintenance of computers, servers and data storage	Personal information and sensitive personal information	Job request	
IAO	Audit reports	Personal information	file	Accounting, Payroll, Warehouse
PGD	Preparation of contracts and agreements	Personal information		None
ISD	Consumer Education Information	Personal information	Zoom app	None
	Attendance/ registration for PMES (face to face)	Personal information	Attendance sheet	None
	External service providers	Personal information	file	Procurement system
	Recruitment and	Personal information	file	Payroll system

	Selection – 201 files	and sensitive personal information		
	Legal Communication	Personal information	file	none
NNSD	Collection of power bill and other payments	Personal information and sensitive personal information	Collection system	Meter Reading/COMS billing/Android app system
	Handling of membership records	Personal information	Membership system	ASC, CWMS
	Handling of consumer feedback	Personal information	Survey form	zimbra
	Printing of share capital certificates	Personal information	Tagging and printing of certificates	CWMS
	Handling of consumer requests	Personal information	SCD, CDE, COAN, Job order	CWMS/Billing
NSD	Electric pilferage	Personal information	Anti-pilferage form	none
	ASC processing	Personal information	ASC form/ASC system	Billings system/OMS
	Consumer requests related to billing and meter	Personal information	Billing system	ASC system
	Distribution system and planning design	Personal information	Contracts	GIS database
	Operations and Maintenance of Distribution system	Personal information	File	Billing system
	Accident report	Personal information	File	Zimbra/OMS

IX.DATA GATHERING AND PROCESSING PROTOCOL

COLLECTION. The employee assigned to collect and process the personal data must be have the authority to do so either by specific instruction of his or her superior or by virtue of the performance of his or her functions. In gathering the personal information, the following must be accomplished: (1)To inform the data subject of the purpose why such personal data is being collected; (2)To collect only the data that is needed and relevant to the process needed by the Data Subject; and (3)To inform the Data Subject that the personal information given will be processed or given to other offices of BENECO relative to his or her request, application or complaint.

1. Identify the Type of Personal Data that will be collected and processed. The personal data to be collected must be necessary, adequate, relevant and compatible for the specific purpose.

2. The consent of the Data Subject must be obtained prior to the processing of personal data subject to the exemptions provided by the Data Privacy Act and other applicable laws and regulations. A Data Consent Form must be accomplished by the Data Subject before any personal data can be processed.

3. The Data Subject must be provided with specific information in clear and plain language he or she understands regarding the purpose and extent of the data gathering ranging from profiling until data sharing to the department that has jurisdiction to supply or handle his or her complaint, application or request.

4. Personal data processing for research purposes shall be allowed provided the personal data required is publicly available or has the consent of the data subject provided the research is intended for a public benefit and that it complies with applicable laws, regulations or ethical standards and that the researcher complies with the code of ethics of research. BENECO reserves the right to reject or refuse the release of any personal information requested by any third party that intends to use the said personal information to promote wellness, insurance, loan and credit facility, products and other commercial promotions.

5. The rights of the Data Subject must be complied with such as the right to correct the personal data given, right to refuse the release of his or her personal data, right to withdraw his or her consent, object to provide personal data over which the Data Subject finds it irrelevant, unnecessary or highly offensive. Should the Data Subject refuse to divulge information which BENECO finds it necessary to eb acquired, the consequences thereof must be fully explained.

ACCURACY AND CORRECTION

The personal data collected must be accurate, complete and up to date before any allowed disclosure.

BENECO must establish measures to ensure that the personal data collected are accurate, complete and up to date. Inaccurate or incomplete personal data must be rectified, supplemented, destroyed or stopped from further processing. BENECO has a documented process for the correction or upgrading of personal data.

USE AND ACCESS

Personal data must only be used for the purposes they are being collected. Only the authorized officers and employees of BENECO whose tasks make necessary the access to such personal data must only be the parties authorized to have such access.

1.BENECO musty have an access policy that contains procedural, technical and physical measures to ensure that personal data will only be used for authorized purposes and only by authorized personnel.

2.The access to personal data must be restricted. Each department must identify a person responsible to protect the personal data for every department process. Access must have a control system that records what data was sought to be accessed, why the personal data is sought to be obtained, who is the party requesting the access, and who was the person who allowed the access.

3. The data collected for research shall be allowed if the data is publicly available or has the consent of the data subject and pursuant to existing BENECO policy on the disclosure of personal for research purposes. Adequate safeguards must be in place and no decision directly affecting the Data Subject shall be made on the basis of the data collected or processed. The rights of the Data Subject must be upheld without compromising the integrity of the research.

RETENTION

Only the needed and necessary personal data should be retained and stored and only for a period required by law Reference shall be made to BENECO's Quality Management System (QMS) in relation to its accreditation as ISO complaint.

1. The retention periods must be determined for the personal data in BENECO's custody considering the fulfillment of the declr4ed, specific and legitimate purpose for processing, defense of legal claims and legitimate business purposes which must be consistent with standards followed by the distribution business of electric cooperatives.
2. The documentation and destruction or disposal of personal data must follow an established and approved procedure. The disposal must be made in a secure manner that would prevent further processing, unauthorized access or unlawful disclosure to any other party or the public to the prejudice of the Data Subject.
3. Personal data originally collected for a declared specific and legitimate purpose mat be stored for longer periods if these are to be processed further for historical, statistical or scientific purposes and in cases allowed by law. This retention must be subject to the implementation of the proper organizational, physical and technical security measures required by the Data Privacy Act in order to protect the rights of the Data Subject.
4. No personal data must be retained perpetually in contemplation of a possible future use that is yet to be determined or speculated.

DISCLSOURE AND SHARING

Personal data under the custody of BENECO shall only be disclosed when allowed by law, pursuant to a lawful purpose and made to parties whose representations and purposes are clearly identified. The following must be in effect:

1. The various offices and departments must take custody and protection of the personal data they collect in relation to the processes the office or department has control over. The data should only be disclosed or shared to the other departments or offices when such sharing is necessary or indispensable to purpose for which the personal data is shared.

2. For data to be disclosed to other parties external to BENECO, the office of department must determine if it is the authorized office to make the disclosure.

3. If the office or department is the one authorized or was authorized to make the disclosure, only the personal data that is authorized to be released or only the personal data relevant to the request must be revealed.

4. Any request for personal data must be made pursuant to the Data Privacy Act and its IRR. The information must not be released unless the information clearly falls under any of the exceptions provided by law.

5. Any request for the disclosure of personal data by other paeties external to BENECO must be given due course subject to the following conditions: (a)The information requested falls under matters of public concern; (b)The party requesting for personal data has declared a specific and legitimate purpose of his or her request; and (c)The declared purpose must not be contrary to law, morals, good customs, public policy and public order.

6. The sharing of personal data with government offices and agencies must always be for the purpose of a public function or provision of a public service, consistent with the policies on data sharing adopted by BENECO and the mandate of the government agency seeking the personal information. Such sharing must be covered by a Data Sharing Agreement.

7. The sharing or disclosure of personal data which are aggregated and no data subjects are specifically identified, otherwise called by BENECO as corporate information, will no longer require a Data Sharing Agreement, but which must be processed pursuant to BENECO's policy on the sharing and disclosure of corporate information.

DELETION, DESTRUCTION AND DISPOSAL

The personal data, sensitive personal information and privileged information gathered and collected by BENECO are subject to BENECO's retention policy. The deletion or disposal of such information must ensure the irreversible removal or elimination of the personal data so that they will become completely unreadable, accessible and irretrievable. The measures of erasure or deletion must cover all the manner of storage, be it digital, electronic file or paper based or hare copies.
HARD COPIES. They shall be shredded. Recycling papers to be used for written notes or scrap papers is nit prohibited provided the hard copies do not contain personal data.

SOFT COPY. All offices and departments must properly organize the storing of their soft copies particularly those that contain personal data. This will facilitate the deletion of the data when required and when needed. The MICS of BENECO must keep abreast with developments in the storage and deletion of data to keep pace with electronic technology as to measures on how to conduct the complete destruction of information.

SPECIFIC GUIDELINES.

1. Any request for access to files, records or for other documents containing personal information, sensitive personal information and privileged information stored in either hard copy or electronic file must be filed directly with the Consumer Welfare Office (CWO) which is the central office task to receive communications, requests and consumer complaints.
2. The CWO must determine which office or department has control or primary custody over the personal information requested. The written request,must then be forwarded to the appropriate office or department for its consideration.
3. If the party requesting for the personal information is a walk in client to the CWO or any other office or department, or that the request was made through phone, facebook or the BENECO website, he or she must be asked to submit a written request (Request for Issuance of Document/Information) stating the following – name of requesting party, address, sex, age, personal information requested and purpose. The written request must be submitted to the CWO which will endorse the same to the proper office or department. The request made through BENECO's facebook or website shall be acted upon immediately should the request contain all the necessary information required of a party who submits a written request.
4. Request for personal information by Data Subjects who are parties to an administrative, civil or criminal proceeding shall be accepted provided the Data Subjects are parties to such proceedings. BENECO must disclose any personal information required by a judicial writ or court order.
5. Before the requested personal information is released to the requesting party, he or she must be required to sign a written undertaking that he or she shall not share or disclose the information BENECO released to him or her to any other person or entity or use the information disclosed to him or her in a manner and purpose other than the purpose for which the personal data was requested.
6. Facsimile technology, email, internet, web and wireless transmission shall not be used for transmitting documents containing personal data that are requested unless so required or by express instruction of the requesting party who shall be advised that BENECO shall not be liable for any damage or disclosure of any personal information caused by hacking or intrusion into the mode of transmission advised by the requesting party. The mode of transmittal adopted by government regulatory agencies (SSS, PhilHealth, BIR) shall remain.
7. When the mode of transmittal of the personal information is through mail or post, BENECO shall ensure the use of registered mail or where appropriate, guaranteed post service. For personal data transmitted between offices and departments of BENECO, the same must ensure that the document shall only be delivered to the person or persons who are allowed to access such information relative to his function.

X.SECURITY MEASURES

All personal information, sensitive personal information and privileged information in the custody of BENECO, be it in hard copies of soft copies, must be secured and protected, and as far as practicable, with the use of the most appropriate standard recognized in the information and communications technology industry subject to the provisions of the Data Privacy Act, IRR and issuance by the National Privacy Commission. BENECO thus ensures that measures are in place for all its process owners and data processors that guarantee security and compliance ith the requirements of the Data Privacy Act.
BENECO has installed security measures to maintain the availability, integrity and confidentiality of personal data to the human dangers of avoid any data breach, unlawful access and disclosure, fraudulent misuse, unlawful destruction, alteration and contamination; and against natural dangers such as accidental loss or destruction.

A.BENECO Organization Security Measures

DATA PROTECTION OFFICER (DPO)	
ATTY. DELMAR O. CARINO Corporate Legal Counsel and Department Manager Institutional Services Department (ISD)	Ensures the adoption and implementation of the Data Privacy Act in BENECO and the cascading of data privacy to the Board of Directors, Department Managers, Supervisors, Process Owners and other key officers of the electric cooperative. Serves as BENECO's spokesperson and focal person for DPA concerns and issues and oversees the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.
COMPLIANCE OFFICERS FOR PRIVACY (COPs)	
ENGR. RODOLFO BALAG-EY JR. Supervisor General Services Office Compliance Officer for Privacy (COP)	Oversees the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.
VIDAL BADIVAL JR., CPA Supervisor Meter Reading, Billing, Collection and Disconnection Office Non-Network Services Department	Oversees the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data

(NNSD)	breach protocol, and the inquiry and complaints procedure. CARINO, BALAG-EY and BADIVAL JR. have passed the examination of the DPA given by the NPC and are accredited as Data Compliance Officers
DPA RECORDS OFFICER AND DPA TRAINING OFFICER	
AILENE ALAFAG Human Resources Officer Institutional Services Department	She is BENECO's Document Controller for its QMS Manual for the ISO. She will also act as the DPA Records Officer. Part of her tasks as HRO is the preparation of an annual training plan (ATP) for the organization. She has included in the ATP trainings for the DPA.
TRAININGS AND SEMINARS	BENECO will conduct trainings or seminars to keep personnel, especially the DPO and the COPs, updated on the latest trends and developments in data privacy and security. Training of at least twice a year.
RECORDING AND DOCUMENTATION OF ACTIVITIES CARRIED OUT BY THE DPO OR THE ORGANIZATION ITSELF,	The recording will be led by the DPA Records Officer to ensure compliance with the DPA, its IRR and other relevant policies.
CONDUCT OF PRIVACY IMPACT ASSESSMENT (PIA)	BENECO already conducted is PIA on June 23-24, 2022.
PREPARATION OF A DATA PRIVACY MANUAL AND/OR DATA PRIVACY NOTICE	This document is BENECO's Data Privacy Manual/Data Privacy Manual which shall be reviewed from time to time including the revision and update of policies and practices to remain consistent with current data privacy best practices.
REVIEW OF PRIVACY POLICY	This Data Privacy Manual and the Data Privacy Notice must be reviewed once in two (2) years to remain consistent with latest developments and best practices in data protection.

ADHERENCE TO CONFIDENTIALITY

All employees who acquire, record, store and have access to personal information of BENECO's Data Subjects will be asked to sign a Non-Disclosure Agreement that will declare that they shall operate and hold personal data under strict confidentiality and that they will not allow public disclosure of such personal information subject to the electric cooperative's policy on disclosure.

B.Physical Security Measures

POLICY AND PROCEDURES. Policies and procedures must be instituted to monitor and limit access to activities in the various offices, rooms, workstation or any facility that have in their custody documents that contain personal information. The protection must cover all types of personal information in whatever form they are stored – physical, digital or electronic.

ACCESS BY BENECO PERSONNEL

Only authorized personnel of BENECO shall be allowed to access personal information. Requests for the 201 files of employees must be coursed through the authorized officer of the Institutional Services Department (ISD) after a written request or instruction shall have been issued by the requesting party. Should there be a need to share the hard copies of documents, the same must be duly receipted.

PHYSICAL MEDIA. Personal data stored in paper files, cabinets or any other physical media should be physically secured (lock and key), An office log must be maintained from which it can be ascertained which file was accessed, when, why and by whom.

INTEGRITY OF DATA. All BENECO employees involved in personal data processing shall always maintain the confidentiality and integrity of personal data in their custody.

MODE OF DATA TRANSFER WITHIN THE ORGANIZATION

Transfer 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 sued to transmit documents containing personal data.

OFFICE SPACE AND WORK STATION. Employees involved with the processing of personal data must be provided with work stations that are with the least distraction of foot traffic to minimize risk of breach and other security incidents. Computers must be positions with considerable space from one another to maintain privacy and avoid unnecessary glances or look into open computers.

Format of Data Collected	Type of Storage	Procedure of Access	Security
Paper Based or Physical Document	Filing Cabinets	Only the authorized personnel who is in custody of the physical file shall be allowed access	CCTVs Permission to work overtime beyond 5PM or work on a Saturday, Sunday or holiday

Digital or Electronic Format	Electronic Storage System	Only authorized personnel shall be allowed access	CCTVs Permission to work overtime beyond 5PM or work on a Saturday, Sunday or holiday

C.Technical Security Measures

Digital or Electronic Format	Electronic Storage System	Only authorized personnel shall be allowed access	CCTVs Permission to work overtime beyond 5PM or work on a Saturday, Sunday or holiday
			(1)Regular Password Changes. Regular password changes to all of our servers ensures that a compromised server due to a leaked password will not affect all the other servers. Thus ensuring that only one server is compromised. (**2)Purchase of Firewall**.Firewalls are integral to any corporate networks. They manage said networks, as well as prevent hacking from outside our network and continuously protects users and data. Firewalls also restricts unnecessary traffic, such as torrents, which is the usual culprit in slow Internet connection. They also prevent users from visiting prohibited sites as defined in any Internet usage manuals. **(3)Monthly Systems Logs Audit**. Systems logs audit consists of reviewing two log files. A systems log which lists down all important events that has happened in an operating system. This is crucial in

			determining failing hardware and software so the system administrator could act on it as soon as possible. The second log file for review is the authorization log, which contains user logins and authentication mechanism that were used. They also consist of which commands were issued as administrator that affects the whole server.

NETWORK SECURITY. BENECO, through its Management Information and Communication Services (MICS) office must implement safeguards to protect the electric cooperative's computer network against accidental, unlawful of unauthorized usage or any interference that will compromise personal data integrity or hinder the functioning or availability of the system. The MICS shall include measures to enable the immediate restoration or availability of access to personal data in case of any physical or technical incident.

DATA BASE/SERVER SECURITY. BENECO employees handling personal data shall not be allowed to save files on their personal computer or desktops but instead, they must be ordered to save files only on their assigned network drive. The use computers, laptops and other devices to process personal data must be protected by passwords or passcodes. The said password or passcodes must be sufficiently strong on undetected to deter password attcks.

BACK UP. The MICS must provide a back up file for all personal data in the custody of BENECO so that in case of any security incident or data breach, the back up files can be used to compare the affected files and determine any inconsistencies or alterations arising form the security incident or breach.

ENCRYPTION AND AUTHNETICATION. BENECO, through the MICS, shall adopt means for the encryption of personal data through the most appropriate encryption standards during storage and while in transit, authentication process and other technical security measures.

SOFTWARE APPLICATION REVIEW. The MICS shall conduct a review of its software applications to be performed by an independent technical team. The review shall include a system audit to determine the effectiveness of the systems.

REVIEW OF SECURITY POLICES. BENECO should see to it that in conducting its review of organizational policies, it must include the review of security policies for the protection of personal information, conduct of vulnerability assessments and perform penetration testing on a regular schedule to be prescribed by the appropriate department.

XI.PROTOCOL FOR BREACH INCIDENTS

1. Creation of a Data Breach Response Team. BENECO has in place a data breach response team to ensure an immediate action to address the security incident or personal data breach. The team shall conduct the initial assessment of the incident or breach in order to ascertain the nature and extent thereof and agree on what measures to implement to mitigate the adverse effects of the security incident and avoid a similar incident in the future.
2. The Data Breach Response Team shall prepare and circularize detailed notification and reporting protocols for nay breach or security incident in accordance with the DPA, its IRR and other NPC issuances.
3. The Data Breach Response Team shall prepare a detailed documentation of every incident or breach experienced, as well as an annual report, to be submitted to the GM and the Board of Directors and the NPC within the prescribed period.

   The Data Breach Response Team shall be composed of the GM, MICS and the Department Managers.

(1)For Electronic Storage

The Management Information and Communications Services (NICS) under the Office of the OGM shall be BENECO's data breach response team for unlawful access into personal information stored electronically. The MICS 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.

The MICS 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.

The MICS 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. Management may decide to delegate the actual notification to the MICS or Data Protection Officer.

The MICS 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.

(2)For Physical Storage

The concerned department must immediately report to the Data Protection Officer (DPO) any breach on the physical files or documents that contain personal information

(theft, malicious mischief, lost records, damaged and destroyed records) for his/her appropriated action copy furnish the management.

The DPO shall inform or advise management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. The DPO shall immediately conduct an inspection and evaluation of the breach and should there be prima facie evidence of employee negligence or willful act, the report must be immediately forwarded to the Administrative Panel for appropriate action pursuant to the BENECO Employee Code of Ethics and Discipline.

BENECO adopts the policy of not outsourcing or subcontracting the collection and processing of personal information, sensitive personal information and privileged information of its Data Subjects.

RULES ON ACCOUNTABILITY

1. BENECO as an electric cooperative and its data processors shall be responsible for any personal data under their control and custody including information that may have been shared or processed to a PIP or third party in the performance of its functions as a distribution utility.
2. BENECO and its data processors shall also be accountable for complying with the requirements of the DPA, its IRRR and other issuances of the NPA.
3. The DATA PROTECTON OFFICER and the COMPLIANCE PRIVACY OFFICERS of BENECO shall be responsible in seeing to it that the electric cooperative complies with the DPA, its IRR and issuances of the NPC. They shall also be responsible in orienting or informing the management and the Board of Directors what the DPA is all about and how it can help BENECO. The DPO and the CPOs shall also cascade the DPA to all the other employees.
4. BENECO's data processors who fail to comply with this Data Privacy Manual, the DPA, its IRR and issuances of the NP shall be liable for such violation and shall be subject to any corresponding administrative action without prejudice t any civil or criminal action as may be applicable.

RIGHT TO INQUIRE, COMPLAINT OR ACCESS TO PERSONAL DATA.

Every Data Subject whose personal information is acquired and stored by BENECO has the following rights:

(1)R**ight to be informed.** This means that the data subject has the right to know when his or her personal data shall be, are being, or have been processed. Collection and processing of data without the data subject's knowledge and explicit consent is made unlawful, and entities in possession of personal data is obligated to inform the data subject of any breaches or compromises in their data.

(2)**R**igh**t to access.** This involves being able to compel any entity possessing any personal data to provide the data subject with a description of such data in its possession, as well as the purposes for which they are to be or are being processed. Furthermore, other details regarding the processing of their information may be

obtained, such as the period for which the information will be stored, and the recipients to whom the information may be disclosed. This must be complied with in an easy-to-access format, accompanied by a description in plain language.

(3)**Right to object.** This means that the consent of the data subject be secured in the collecting and processing of his or her data. It grants the data subject the choice of refusing to consent, as well as the choice to *withdraw* consent, as regards collection and processing. As earlier stated, any activity involving a data subject's personal data without his or her consent is deemed illegal.

(4)Right to erasure or blocking . This allows the data subject to suspend, withdraw or order the blocking, removal, destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected.

(5)R**ight to rectify.** This allows the data subject to dispute any inaccuracy or error in the personal information processed, and to have the personal information controller correct it immediately. In line with this, the personal information controller must ensure that the new and the retracted information will be accessible, and that third parties who received the erroneous data will be informed, upon the request of the data subject.

(6)**Right to Portability**. This enables the data subject to obtain and electronically move, copy, or transfer personal data for further use. This also carries out another policy behind the law–ensuring the free flow of personal information.

(7)R**ight to file a complaint.** The data subject can file a protest before the N**ational** Privacy Commission. This affords a remedy to any data subject who feels that his or her personal information has been misused, maliciously disclosed, or improperly disposedor in case of any violation of his or her data privacy rights.

(8)R**ight to damages.** This entitles the aggrieved data subject to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of his or her personal information.

INQUIRIES AND COMPLAINTS

Data subjects can write BENECO and personally deliver the same to the Consumer Welfare Office of BENECO at No. 4, Barangay South Drive, Baguio City

or email at ogmbeneco@gmail.com or isd@beneco.com.ph

XI.EFFECTIVITY

The provisions of this Manual are effective this 22nd day of September, 2022 until revoked or amended by BENECO through a Board Resolution.

Annexes

Document	Purpose
Board of Directors (BOD) Resolution No. 2022-150, Series of 2022 dated September 22, 2022.	Approval of (1) The implementation of the Data Privacy Act in BENECO; (b)Data Privacy Manual and Data Privacy Notice; (c)Designation of Atty. Delmar O. Carino as BENECO Data Protection Officer; and Engr. Rodolfo Balag-ey Jr and Vidal Badival Jr. as Compliance Officers for Privacy
BENECO Data Privacy Notice	This contains the electric cooperative's notice to all its clients, member consumers and Data Subjects to inform them that BENECO adheres to the Data Privacy Act.
Non- Disclosure Agreement (NDA)	Executed by BENECO PICs to ensure the confidentiality of the personal information they collect and gather
Conformity to Data Privacy	Signed by BENECO's member consumers to secure their consent in providing personal information
Data Privacy Statement	A general information posted in strategic locations of BENECO to inform its clients about BENECO's adherence to the Data Privacy Act