Policy on Data Privacy

INTRODUCTION

This 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, including issuances of the National Privacy Commission.

ALTERNERGY respects and values data privacy rights, and makes sure that all personal data collected from our employees, our stakeholders and other third parties, are processed adherent to the general principles of transparency, legitimate purpose, and proportionality.

This Manual outlines the data protection and security measures adopted by the organization, and shall serve as a guide in the exercise of rights under the DPA.

DEFINITION OF TERMS

"Data Privacy Act or DPA" refers to the Republic Act No. 10173 or the Data Privacy Act of 2012 and its implementing rules and regulations.

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

"Company" refers to the ALTERNERGY organization, including but not limited to its affiliates and subsidiaries, including but not limited to: *Alternergy Holdings Corporation, Alternergy Tanay Wind Corporation, Pililla AVPC Corporation, Alternergy Mini Hydro Holdings Corporation.*

"Personal Data" collectively refers to the Personal Information, Sensitive Personal information, and Privileged Information.

"Personal Information" refers to any information, recorded in a material form of otherwise, from which the identity of an individual is apparent or can be reasonably or directly ascertained by the entity holding the information, or when put together with other information directly and certainly enables identification of an individual.

"Processing" refers to any operation or set of operations performed upon Personal Data including but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data are contained or an intended to be contained in a filing system.

"Privileged Information" refers to any and all forms of Personal Data, which under the Rules of Courts and other pertinent laws constitute privileged communication.

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

"Sensitive Personal Information" refers to Personal Data:

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

SCOPE AND LIMITATIONS

This Manual applies to all departments of the Company, all personnel of the Company, regardless of the type of employment or contractual arrangement, officers and third parties whose information are required to be kept and secured by the Company. The data covered by this Manual is limited to Personal Information collected and processed by the Company.

PROCESSING OF PERSONAL DATA

A. COLLECTION

The collection of both Personal Information and Sensitive Personal Information is done by lawful means and for a lawful purpose and is directly related and necessary in carrying out the purpose of the Company. Where Personal Data is publicly available, collection may be made from such public sources, including any online presence that the Data Subject may have.

Personal Information that is collected and processed by the Company would be the Data Subject's full name, address, email address, telephone number, age, marital status, information issued by government agencies and other information that may be used to enter into or help perform a contract or transaction that the Company has with a Data Subject.

Similarly, Personal Data of the Company's officials, employees and stakeholders, applicants to vacant positions and other third persons are obtained through the accomplishment of forms essential in employment, training and other developmental interventions.

B. USE

Personal Data collected shall be used by the Company generally for documentation purposes and for the purposes: (i) for which the Data Subject has provided the data or made it otherwise available to the Company or to the public, and to enable us to fully and efficiently achieve those purposes; and (ii) as allowed by applicable law.

C. STORAGE, RETENTION AND DESTRUCTION

This Company 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. The Company will implement appropriate security measures in storing collected Personal Information, depending on the nature of the information.

The Company will store and retain Personal Data for such period as may be required by applicable law or as may be needed to enable the Company to fully and efficiently achieve the purposes for which the Personal Data was collected and processed. After the purposes for data collection has been sufficiently achieved, which in no case shall be more than ten (10) years from the time the data was collected, all hard and soft copies of Personal Information shall be disposed of and destroyed through secure means.

D. ACCESS

Access to Personal Data of officials and employees of the Company and applicants to vacancies shall be limited to the Data Protection Officer (DPO), the pertinent Administration and Human Resources Officer and their designated Assistant, and the Data Subject to whom the Personal Data pertains. At no time should anyone be given access to the personal files of other employees, for any purpose, except for those contrary to law, public policy, public order or morals.

For Personal Data of stakeholders and other relevant third persons, only the DPO, the Management and their specifically designated personnel, depending on the nature of the Personal Data and the purpose for which it was collected, shall have access to the same.

E. DISCLOSURE AND SHARING

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

SECURITY MEASURES

The Company shall implement reasonable and appropriate physical, technical, and organizational measures for the protection of Personal Data. These 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.

A. ORGANIZATION SECURITY MEASURES

1) Data Protection Officer

   A Data Protection Officer shall be appointed by the Company.

2) Functions of the DPO

   The DPO is responsible for ensuring the Company's compliance with applicable laws and regulations for the protection of data privacy and security. The functions and responsibilities of the DPO shall particularly include, among others:

   a. Monitoring the Company's Personal Data Processing activities in order to ensure compliance with applicable Personal Data privacy laws and regulations, including the conduct of periodic internal audits and review to ensure that all the Company's data privacy policies are adequately implemented by its employees and authorized representatives and agents;
   b. Acting as liaison between the Company and the regulatory and accrediting bodies, including the applicable registration, notification, coordination and cooperation and filing of reportorial requirements mandated by the DPA, as well as any other applicable data privacy laws and regulations;
   c. Developing, establishing and reviewing policies and procedures for the Data Subject's exercise of their rights under the DPA and other applicable laws and regulations on data privacy;
   d. Acting as the primary point of contact with whom the Data Subject may coordinate and consult for all concerns relating to their Personal Information;
   e. Formulating capacity-building, orientation and training programs for employees, agents or representatives of the Company regarding data privacy and security policies to inform and cultivate awareness on privacy and data protection within the organization; and
   f. Performing other duties and tasks that may be assigned by the Company that will further the interest of data privacy and security and uphold the rights of the data Subjects.

3) Conduct of trainings or seminars to keep personnel, especially the DPO updated vis-à-vis developments in data privacy and security

   The Company 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.

4) Conduct of Privacy Impact Assessment (PIA)

   The Company shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. The Company may choose to outsource the conduct a PIA to a third party.

5) Duty of Confidentiality

All employees 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 Company shall be updated to remain consistent with current data privacy best practices.

B. PHYSICAL SECURITY MEASURES

1) Format of data to be collected

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

2) Storage type and location

All Personal Data of the Company's officials and staff including those of its project- and agency-based employees in paper-based documents shall be stored in locked filing cabinets in the Company's primary place of business.

Documents bearing any Personal Data of stakeholders or other relevant third persons shall be kept in secure filing cabinets and drawers in the Company's primary place of business.

Digital/electronic files are stored in computers provided and installed by the company, which are protected by passwords and can only be accessed by authorized personnel.

3) Access procedure of agency personnel

Only the DPO, the pertinent Administration and Human Resources Officer and their designated Assistant shall have access to the stored Personal Information of current and former Company officials, staff and applicants to vacant positions.

An official/employee who wishes to see documents on their personal file shall fill up a request form to be approved by the DPO or by the Administration and Human Resources Officer. The designated Administration and Human Resources Assistant shall secure the requested document/s, have the same photocopied, and hand the documents over to the official/employee concerned.

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

An employee cannot invoke their right to access their employee file under the law when the Personal Information is being processed for the purpose of any investigation relating to any criminal, administrative or tax liabilities against them.

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

Employee files of former Company employees as well as their service records, duplicate copies of Company clearances and forwarding addresses and telephone numbers retained at the office shall be treated in the same way as the employee files of current employees.

Stored Personal Data of stakeholders and other relevant third persons shall only be accessed by the DPO, the Management and their specifically designated personnel, depending on the nature of the personal data and the purpose for which it was collected.

At no time should any authorized personnel use gadgets or electronic storage devices of any form when accessing personal files of Company personnel, applicants, stakeholders and other relevant third persons.

4) Monitoring and limitation of access to room or facility

All authorized personnel who entered and accessed the stored personal data must fill out and register access details in a logbook, indicating the date, time, duration and purpose of each access.

5) Design of office space/work station

Computers are located at the work stations of employees such that no computers are placed closely beside other computers to ensure the protection of processing Personal Data.

6) Modes of transfer of Personal Data within the organization, 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.

7) Retention and disposal procedure

The Company shall retain the Personal Data in its custody subject to the section on Storage, Retention and Destruction under Processing of Data in this Manual. Upon expiration of such period, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure technology.

C. TECHNICAL SECURITY MEASURES

1) Monitoring for security breaches

   The Company shall maintain a reliable anti-virus software, on an annual basis, for use in devices that regularly access the internet, which are also used to process Personal Data, such as desktop computers, laptops, handheld and mobile devices, tablets and smartphones.

   The Administration and Human Resources Officer and such other relevant personnel, with the assistance of the Company's IT provider which may be in – house or outsourced, shall regularly check and read the firewall logs to monitor security breaches and alert the Company of any unauthorized attempt to access the Company's network.

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

   The Company shall first review and evaluate software applications before the installation thereof in computers and devices of the Company to ensure the compatibility of security features with the Company's overall operations as well as data privacy policies.

   On existing software applications, which involves processing of Personal Data of officials, staff and applicants, the Company, with input from the end-user and the Company's IT Provider, in-house or outsourced, shall:

   a. Evaluate and assess the security protocols of the system relating to saving, back-up and data recovery. Remedial steps shall be taken should they be found lacking or counter to valid and existing data privacy laws and regulations.
   b. During the Company's IT scheduled maintenance activities, check software applications installed in all hardware and devices for compliance with this Manual and the Company's data privacy policies. In the event that a software/application is found to be a security risk that may disrupt or interrupt the normal operations of the Company's network, the end-user shall be notified of the risk and the software/application shall be immediately uninstalled, and the IT Provider shall prepare an incident report to that effect.

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

   The Company, with the assistance of the IT Provider, in-house or outsourced, as the case may be, shall regularly review security policies, conduct vulnerability assessments and perform penetration testing within the Company.

BREACH AND SECURITY INCIDENTS

A. CREATION OF A DATA BREACH RESPONSE TEAM

A Data Breach Response Team comprising of the DPO, the Administration and Human Resources Officer and the IT Provider under supervision of the Management 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.

B. MEASURES TO PREVENT AND MINIMIZE OCCURRENCE OF BREACH AND SECURITY INCIDENTS

The Company shall regularly conduct a Privacy Impact Assessment (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 shall attend trainings and seminars for capacity building. There shall be a periodic review of policies and procedures being implemented in the Company.

C. PROCEDURE FOR RECOVERY AND RESTORATION OF PERSONAL DATA

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

D. NOTIFICATION PROTOCOL

The Head of the Data Breach Response Team shall inform the Management of the need to notify the National Privacy Commission (NPC) and the Data Subjects affected by the incident or breach within seventy-two (72) hours from knowledge thereof. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

E. DOCUMENTATION AND REPORTING PROCEDURE OF SECURITY INCIDENTS OR A PERSONAL DATA BREACH

The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to Management and the NPC, within the prescribed period, containing the following:

1) Description of the nature of the breach;
2) Personal Data possibly involved;
3) Measures undertaken by the team to address the breach and reduce the harm or its negative consequences; and
4) Names of the personnel controlling the Personal Information, 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 DATA SUBJECTS

Every Data Subject has the right to:

1) Reasonable access to his or her Personal Data being processed by the Personal Information Controller or Personal Information Processor;
2) Dispute the inaccuracy or error in the Personal Data;
3) Request the suspension, withdrawal, blocking, removal or destruction of Personal Data; and
4) Complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data.

INQUIRIES AND COMPLAINTS

Data Subjects may inquire or request for information regarding any matter relating to the processing of their Personal Data under the custody of the Company, including the data privacy and security policies implemented to ensure the protection of their Personal Data. They may write to the Company at **contact@alternergy.com** and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) printed copies, or sent to **contact@alternergy.com**. Receipt of the complaint by the pertinent personnel shall be communicated to the complainant within a reasonable time.

EFFECTIVITY

This Manual takes effect on September 01, 2022 until revoked or amended.