MEGAWIDE

DATA PRIVACY MANUAL

TABLE OF CONTENTS

PREFACE

Megawide Construction Corporation (the "Company") hereby adopts this Data Privacy Manual (the "Manual") in compliance with Republic Act No. 10173 or *An Act Protecting Individual Personal Information in Information and Communication Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes* (the "Data Privacy Act"), its Implementing Rules and Regulations (the "IRR"), and other relevant policies and issuances of the National Privacy Commission (the "Commission").

The Data Privacy Act passed into law in 2012 consistent with the Philippines' policy of protecting the fundamental human right of privacy, while ensuring free flow of information. To promote such policy, the Act, along with its IRR, shall govern the processing of personal data by any natural or juridical person in the government or private sector, who must in turn establish policies and implement measures to guarantee the security of personal data under their control and/or custody.

With the Data Privacy Act, other pertinent laws, and the principles of transparency, legitimate purpose, and proportionality as its backdrop, the Company abides by this Manual in carrying out its principal business. This is so as to ensure that personal data under its control remain safe and secured while being processed in the course of its key operations and processes.

This Manual aims to inform clients, employees, partners, and stakeholders of the Company's data protection and security measures, and to guide them in the exercise of their rights under the Data Privacy Act and other relevant regulations and policies.

ARTICLE I
INTRODUCTION

SECTION 1. DEFINITIONS

"**Authorized Personnel**" refers to employee/s or officer/s of the Company authorized to collect and/or to process Personal Data either by the function of their office or position, or through specific authority given in accordance with the policies of the Company.

"**Commission**" or the "**NPC**" shall refer to the National Privacy Commission.

"**Compliance Officer for Privacy**" or "**COP**" refers to an individual duly authorized by the Company to perform some of the functions of the DPO for a branch, sub-office, or component unit, if any.

"**Consent of the Data Subject**" refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and Processing of his/her Personal, Sensitive Personal, or Privileged Information. It shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of a Data Subject by a lawful representative or an agent specifically authorized by the Data Subject to do so.

"**Data Privacy Response Team**" refers to the group of individuals designated by the Company to respond to inquiries and complaints relating to data privacy, and to assist in ensuring the Company's compliance with the Data Privacy Act, its IRR, and any other government-issued data privacy regulations and issuances, as well as in implementing this Manual.

"**Data Processing Systems**" refer to the structures and procedures by which Personal Data is collected and further processed by the Company in its Information and Communications System/s and/or relevant Filing System/s, including the purpose and intended output of the Processing, as specified in **Annex** "**A**" hereof.

"**Data Protection Officer**" or "**DPO**" refers to the officer duly designated by the Company to be accountable for the latter's compliance with the Data Privacy Act, its IRR, and any other government-issued data privacy regulations and issuances, as well as implementation of the Manual. The DPO shall also act as liaison between the Company and the National Privacy Commission for privacy-related compliance matters.

"**Data Sharing**" refers to the disclosure or transfer to a third party of Personal Data under the control or custody of the Company.

"**Data Sharing Agreement**" refers to any written contract or agreement that contains the terms and conditions of a Data Sharing arrangement entered into by the Company. Any Data Sharing Agreement entered into by the Company shall substantially contain the terms and conditions prescribed in Article IV, Section 4.5.2 of this Manual, and substantially be in the form prescribed in **Annex** "**B**" hereof.

"**Data Subject**" refers to an individual whose Personal, Sensitive Personal, and/or Privileged Information are processed. For purposes of this Manual, it refers to employees (whether probationary, regular, casual, or project), trainees, applicants, members of the board of directors, consultants, clients, stockholders, partners, suppliers, subcontractors, service providers, office visitors, and other persons whose Personal Data are collected and processed by the Company as an integral and necessary part of its business operations.

"**Filing System**" refers to any set of information relating to a natural or juridical person to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

"**Information and Communications System**" refers to a system for generating, sending, receiving, storing, or otherwise Processing electronic data messages, or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

"**Outsourcing**" refers to the disclosure or transfer of Personal Data by the Company to a Personal Information Processor (PIP) for the latter's Processing, which shall be done strictly in accordance with the instructions of the Company.

"**Outsourcing Agreement**" refers to any written contract entered into by the Company with a PIP, including its service providers. Any Outsourcing Agreement entered into by the Company shall substantially contain the terms and conditions prescribed in Article IV, Section 4.6.2 of this Manual, and be in the form prescribed in **Annex** "**C.**"

"**Personal Data**" refers to all types of Personal Information collected and processed by the Company. The term Personal Data includes, but is not limited to, the following:

(a) "**Confidential Personal Data**" pertains to all information to which access is restricted, and of which Processing requires the written consent of the Data Subject concerned, such as but not limited to Employee 201 files and information contained therein, device passwords and/or passcodes, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

(b) "**Public Personal Data**" pertains to Personal Information of a Data Subject which may be disclosed to the public by the Company due to, or as required by, its business operations, and for government regulatory compliance and company disclosures.

"**Personal Data Breach**" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data Breach may be in any of the following nature:

(a) "**Availability Breach**," which results from the loss of, or accidental or unlawful destruction of Personal Data;

(b) "**Confidentiality Breach**," which results from the unauthorized disclosure of, or access to Personal Data; and/or

(c) "**Integrity Breach**," which results from the alteration of Personal Data.

"**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.

"**Personal Information Controller**" or "**PIC**" refers to a natural or juridical person, or any other body, including the Company, who/which controls the Processing of Personal Data, or instructs another to process Personal Data on its behalf.

"**Personal Information Processor** or "**PIP**" refers to any natural or juridical person, or any other body, to whom a PIC, including the Company, outsources, or gives instructions as regards the Processing of Personal Data of a Data Subject or group of Data Subjects.

"**Privacy Impact Assessment**" is a process undertaken and used to evaluate and manage the impact on privacy of a particular program, project, process, measure, system, or technology product of the Company or its PIP/s. It takes into account the nature of the Personal Data to be protected, the Personal Data flow, the risks to privacy and security posed by the Processing, current data privacy best practices, and the cost of security implementation. The Company shall conduct a Privacy Impact Assessment annually through the joint accomplishment by key personnel of the Company of a Privacy Impact Assessment form, substantially in the format specified in **Annex "D"** of this Manual.

"**Privacy Policy**" refers to the internal statement that governs the Company's practices of handling Personal Data. It instructs the users of Personal Data (i.e., Authorized Personnel) on the processing of Personal Data and informs them of the rights of the Data Subjects. This Manual outlines the Privacy Policy of the Company.

"**Privacy Notice**" refers to the statement, substantially in the format specified under **Annex "E"** of this Manual, made to a Data Subject to inform him/her of how the Company processes his/her Personal Data.

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

"**Processing**" refers to any operation or set of operations performed upon Personal Data including, but not limited to, its collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction. Processing may be performed through automated means or by manual processing.

"**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 to a Personal Data Breach, if not for safeguards that have been put in place.

"**Security Measures**" refers to the physical, technical, and organizational measures employed by the Company to protect Personal Data from natural and human dangers.

"**Sensitive Personal Information**" refers to Personal Information:

(a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political 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 government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and

(d) specifically established by an executive order or an act of Congress to be kept classified.

SECTION 2. SCOPE AND LIMITATIONS

This Manual shall lay down the data protection and Security Measures of the Company. It shall govern the Processing of Personal Data of Data Subjects by the Company and the latter's PIP/s, if any. All employees of the Company, regardless of the type of employment, as well as all PIP/s, are enjoined to comply with the terms laid down in this Manual.

SECTION 3. DATA PRIVACY PRINCIPLES

In the Processing of Personal Data, the Company, its employees and PIP/s shall abide by the following principles:

(a) **Transparency.** The Data Subject shall be informed of the nature, purpose, and extent of the Processing of his/her Personal Data, including the risks and safeguards involved, the identity of the Company, his/her rights as a Data Subject, and how these rights may be exercised.

(b) **Legitimate Purpose.** The Processing of Personal Data shall only be for the purpose declared and specified to the Data Subject. No further Processing of Personal Data shall be done without the consent of the Data Subject.

(c) **Proportionality.** The Processing of Personal Data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal Data will be processed by the Company only if the purpose of the Processing could not be reasonably fulfilled by other means, and if required by the Company's business operations.

ARTICLE II
DATA PROTECTION OFFICER AND COMPLIANCE OFFICER FOR PRIVACY

SECTION 1. DATA PROTECTION OFFICER

The Company shall have a Data Protection Officer who shall be responsible for overseeing the compliance of the Company with the Data Privacy Act of 2012, its IRR, other pertinent laws and government issuances on data privacy, and this Manual.

Upon the request of a Data Subject, the name of the DPO shall be made available by the Company. The contact details of the DPO of the Company shall be provided in **Annex "F."**

SECTION 2. COMPLIANCE OFFICER FOR PRIVACY

Each branch, department, and/or component unit of the Company may appoint among its ranks a COP, who shall assist the DPO in ensuring that the branch, department, and/or component unit assigned to him/her complies with the Data Privacy Act, its IRR, other pertinent laws and government issuances on data privacy, and this Manual. An overall COP may also be appointed who shall coordinate with, and supervise the COP/s assigned per branch, department, and/or component unit, as well as assist the DPO in ensuring that the Company complies with the Data Privacy Act, its IRR, other pertinent laws and government issuances on data privacy, and this Manual.

Upon request of a Data Subject, the name of the pertinent COP, if any, shall be made available by the Company. The contact details of the COP/s of the Company, if any, shall be provided in **Annex "G."**

SECTION 3. GENERAL QUALIFICATIONS

The Company shall ensure that the DPO and the COP/s, if any, possess the knowledge and demonstrate the reliability necessary for the performance of their duties and responsibilities. The DPO and/or COP/s should have sufficient understanding of the Processing operations being carried out by the Company.

Section 4. Term

The DPO and/or the COP/s shall be regular or permanent positions in the Company. Where their employment is based on contract, the term or duration thereof shall be for at least two (2) years.

Section 5. Vacancy

Where the position of either the DPO or COP is left vacant, the Company shall appoint, reappoint, or hire a replacement within a reasonable period of time. The Company may require the incumbent DPO or COP/s, as the case may be, or any employee of the Company who demonstrates possession of the General Qualifications required by Article II, Section 3 hereof, to occupy the vacant position in a holdover capacity, until the appointment or hiring of the new DPO or COP.

Section 6. Functions of the DPO and/or COP

The DPO and/or COP/s shall have the following functions:

(a) monitor the Company's compliance with this Manual, the Data Privacy Act, its IRR, issuances of the Commission, and other applicable laws and policies. For such purpose, the DPO and/or COP/s may:

(i) collect or cause the collection of information to identify the Processing operations, activities, measures, projects, programs, or systems of the Company, and maintain or cause the maintenance of records thereof;

(ii) analyze and check, or cause the analyzation and checking of, compliance of the Company's Processing activities, including the issuance of security clearances to, and compliance of service providers, with the applicable laws and contracts on data privacy;

(iii) inform, advise, and issue recommendations to the Company with regard to compliance with the applicable laws and contracts on data privacy, as well as the implementation of this Manual;

(iv) advice the Company as regards the necessity of executing Data Sharing Agreement/s and/or Outsourcing Agreement/s with third parties, and ensure its compliance with the law; and/or

(v) ascertain renewal of accreditations or certifications necessary to maintain the required standards in Personal Data Processing;

(b) ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the Company at least once a year;

(c) advise the Company regarding the exercise by Data Subjects of their Rights as specified in Article III hereof, as well as complaints made to the DPO and/or COP/s of the Company;

(d) ensure the Company's proper management of Security Incident/s, if any, including the latter's preparation and submission to the Commission of reports and other documentation concerning such Security Incident/s within the prescribed period;

(e) cultivate awareness of privacy and data protection regulations within the Company, including this Manual, the Data Privacy Act, its IRR, and other government issuances on data privacy;

(f) advocate for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the Company relating to privacy and data protection;

(g) serve as the contact person of the Company vis-à-vis Data Subjects, the Commission, and other authorities in all matters concerning data privacy or security issues or concerns and the Company;

(h) cooperate, coordinate, and seek the advice of the Commission regarding matters concerning privacy and data protection;

(i) lead the Data Privacy Response Team of the Company; and

(j) perform other duties and tasks that the Company may assign to further the interest of privacy and data protection and uphold the Rights of the Data Subjects, as specified in Article III hereof.

The COP/s of the Company, if any, may perform any of the functions of the DPO. Where appropriate, the COP/s shall assist the DPO in the performance of the latter's functions.

SECTION 7. OUTSOURCING THE FUNCTIONS OF THE DPO AND/OR COP/S

The Company may outsource any of the functions of the DPO and/or COP/s, if any, provided that the DPO and/or COP/s, if any, shall supervise the PIP/s.

ARTICLE III
RIGHTS OF THE DATA SUBJECT

As provided under the Data Privacy Act, a Data Subject shall have the following rights in connection with the Processing of his/her Personal Data. The Company's employees and PIP/s, as the case may be, shall respect the rights of all Data Subjects. To exercise said rights, the Data Subject may accomplish the Data Privacy Right Form prescribed in **Annex "H,"** indicating therein the right he/she wishes to exercise with respect to his/her Personal Data, and transmit the same to the Company through its Authorized Personnel, DPO or COP/s, if any.

SECTION 1. RIGHT TO BE INFORMED

The Data Subject has the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed. Before entry of his/her Personal Data into the Company's Information and Communications System/s and/or Filing System/s, or at the next practicable opportunity, the Data Subject shall be notified and furnished with the following information:

(a) description of the Personal Data to be entered into the Information and Communications System/s and/or Filing System/s of the Company;

(b) purpose/s for which Personal Data are being or will be processed;

(c) basis of Processing, in case Processing is not based on the Consent of the Data Subject;

(d) scope and method of the Processing of Personal Data;

(e) recipient/s or classes of recipient/s to whom the Personal Data are or may be disclosed or shared;

(f) in case of automated access, and where allowed by the Data Subject, the methods utilized therefor, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject;

(g) identity and contact details of the Company, its representative, and/or, upon request, the DPO and/or COP/s, if any;

(h) period for which the Personal Data will be stored; and

(i) existence of his/her rights as a Data Subject, including the right to lodge a complaint before the Commission.

SECTION 2. RIGHT TO OBJECT

The Data Subject shall have the right to object to the Processing of his/her Personal Data. The Data Subject shall also be notified and given an opportunity to withhold his/her consent to the Processing in case of changes or any amendment to the information supplied or declared to the Data Subject in the immediately preceding Section. When a Data Subject objects or withholds consent, the Company shall no longer Process the Personal Data, unless:

(a) the Personal Data is needed pursuant to a subpoena;

(b) the Processing is for obvious purposes, including, when it is necessary for the performance of, or in relation to a contract or service to which the Data Subject is a party, or when necessary or desirable in the context of an employer-employee relationship between the Company and the Data Subject (e.g., to assess the qualification of an applicant or the suitability of a current employee for promotion or transfer, the Company may require information as regards the person's educational attainment); or

(c) the Personal Data is being collected and processed pursuant to a legal obligation (e.g., to make the mandatory contributions to an employee's Social Security System, Pag-IBIG Home Development Mutual Fund, and PhilHealth accounts, the Company has to obtain the pertinent social security numbers of the employee).

SECTION 3. RIGHT TO ACCESS

The Data Subject has the right to demand reasonable access to the following:

(a) contents of his/her Personal Data that were processed;

(b) sources from which Personal Data were obtained;

(c) names and addresses of recipient/s of the Personal Data;

(d) manner by which his/her Personal Data were processed;

(e) reasons for the disclosure of the Personal Data to recipient/s, if any;

(f) information on automated processes where the Personal Data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the Data Subject;

(g) date when Personal Data concerning the Data Subject were last accessed and modified; and

(h) identity and address of the Company.

SECTION 4. RIGHT TO CORRECTION

The Data Subject has the right to dispute the inaccuracy or error in his/her Personal Data, and have the Company accordingly correct or cause the correction thereof, unless such is vexatious or unreasonable. If the Personal Data has been corrected, the Company shall ensure the accessibility of both the new and the retracted Personal Data, and the simultaneous receipt of the new and the retracted Personal Data by the intended recipient/s thereof. Recipients or third parties who have previously received such processed Personal Data shall be informed of its inaccuracy and its rectification, upon reasonable request of the Data Subject.

SECTION 5. RIGHT TO ERASURE OR BLOCKING

The Data Subject shall have the right to suspend, withdraw, or order the blocking, removal, or destruction of his/her Personal Data from the Company's Information and Communications System/s and/or Filing System/s, and may exercise such right, upon discovery and/or substantial proof of any of the following:

(a) the Personal Data is incomplete, outdated, false, or unlawfully obtained;

(b) the Personal Data is being used for purpose/s not authorized by the Data Subject;

(c) the Personal Data is no longer necessary for the purpose/s for which they were collected;

(d) the Data Subject withdraws consent or objects to the Processing, and there is no other legal ground or overriding legitimate interest for the Processing;

(e) the Personal Data concerns information prejudicial to the Data Subject, unless justified by the freedom of speech, of expression, or of the press, or otherwise authorized;

(f) the Processing is unlawful; or

(g) the Right/s of the Data Subjects has/have been violated.

Upon reasonable request of the Data Subject, the Company shall notify third parties who have previously received such processed Personal Data of the Data Subject's decision to exercise such right.

SECTION 6. RIGHT TO DATA PORTABILITY

Where his/her Personal Data is processed by electronic means and in a structured and commonly used format and upon his/her written request, the Data Subject shall have the right to obtain from the Company a copy of such Personal Data in an electronic or structured format that is commonly used and allows for further use by the Data Subject.

SECTION 7. RIGHT TO COMPLAIN BEFORE THE COMMISSION

The Data Subject shall have the right to complain before the Commission for any data privacy violation committed by the Company, if any.

SECTION 8. TRANSMISSIBILITY OF RIGHTS

Any lawful heir and/or assign of the Data Subject may invoke the Rights of the Data Subject to which he/she is an heir and/or assignee, at any time after the death of the Data Subject, or when the Data Subject is incapacitated or incapable of exercising his/her right.

ARTICLE IV
PROCESSING OF PERSONAL DATA

Whenever necessary, the Company may modify any of its Data Processing Systems as laid down in **Annex "A,"** but, under all circumstances, must respect the rights of the Data Subjects and observe compliance with this Article, among others, in Processing the Personal Data of Data Subjects.

SECTION 1. COLLECTION

1.1 **Conditions.** The Company shall only collect and process the Personal Data of a Data Subject upon the concurrence of the following conditions:

(a) Prior to collection, or as soon as practicable, the Company shall have informed the Data Subject of the following:

(i) the specific purpose for the collection and Processing of Personal Data;

(ii) the extent of Processing of Personal Data; and

(iii) the Rights of the Data Subject.

(b) The Company shall have obtained the Consent of the Data Subject to whom the Personal Data relates, unless the collection and Processing of the Personal Data are:

(i) pursuant to law and/or government issuances;

(ii) necessary to perform a contract to which the Data Subject is a party, or to take steps prior to entering into a contract;

(iii) necessary to protect the interest of the Data Subject;

(iv) necessary to perform a task in the interest of the public or in the exercise of official authority vested upon the Company; or

(v) necessary to protect the lawful rights and interests of the Company in court proceedings, or to establish, exercise, or defend a legal claim.

1.2 **Privacy Notice.** Information on collection and Processing of Personal Data of the Data Subject shall be relayed to the Data Subject through a Privacy Notice, which shall substantially be in the form prescribed in **Annex** "E." The Company's Authorized Personnel shall inform the Data Subject of the purpose/s for the collection and Processing of Personal Data, extent of Processing of Personal Data, and the Rights of the Data Subject with regard to privacy and data protection.

1.3 **Consent.** The Consent of the Data Subject shall be evidenced by written, electronic, or recorded means, substantially in the form prescribed in **Annex** "**I.**" Consent may also be given on behalf of a Data Subject by a lawful representative or an agent authorized by the Data Subject to do so.

SECTION 2. USE

2.1 **General.** The use of the Personal Data shall only be for the purpose/s specified and declared to the Data Subject, and with the Consent of the Data Subject.

2.2 **Purpose.** The Company's use of the Personal Data shall only be for the purpose of carrying out the business operation of the Company. The Processing of Personal Data of Data Subjects shall be for the following general purposes, among others:

(a) to document and manage the Company records;

(b) to conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract thereafter;

(c) to respond to queries, complaints, and requests;

(d) to provide information about Company services;

(e) to conduct research and analysis to improve customer experience;

(f) to maintain security; and

(g) to comply with legal, regulatory, and contractual requirements or obligations.

The use and processing of Personal Data also depends on the Company transactions involved.

If a Data Subject asks about, or avails him/herself of the Company services, the Company may collect, use, or process the Data Subject's Personal Data to:

(a) conduct appropriate credit investigation to assess the risk of transacting with the Data Subject;

(b) prepare and execute the necessary contract to cover the transaction;

(c) update the Company records and keep its contact details and billing address up-to-date; and

(d) communicate any advisories, changes, and other information relevant to the Data Subject's contract with the Company.

If the Data Subject is a vendor/supplier, a potential vendor/supplier, or a contractor, the Company may collect, use, or process the Data Subject's Personal Data to:

(a) conduct the appropriate due diligence checks;

(b) evaluate the Data Subject's proposal, including his/her technical, financial, and operational capacity;

(c) assess the viability of the Data Subject's proposal and process his/her accreditation;

(d) communicate any decision on such proposal; and

(e) perform any other action as may be necessary to implement the terms and conditions of the contract with the Data Subject, if any.

If the Data Subject is a prospective employee, the Company may collect, use, or process the Data Subject's Personal Data to:

(a) evaluate his/her suitability for employment and, with a written or expressed consent, retain his/her Personal Data for a maximum of five (5) years for future job opportunities that may be of interest to the Data Subject;

(b) communicate with the Data Subject about his/her employment application;

(c) if hired, process his/her Personal Data as may be necessary for purposes such as, but not limited to, payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand or require processing of his/her Personal Data (*e.g.*, to execute business transactions directly related and/or incidental to his/her job, business travels, socials, and so on);

(d) while employed, evaluate his/her performance and career development;

(e) upon separation, process his/her Personal Data for the exit interview and to prepare his/her final pay;

(f) provide assistance to, and account for, employees in case of emergency; and

(g) perform such other processing or disclosure that may be required in the course of the Company's business or under law or regulations.

If the Data Subject is a Company stockholder, the Company may use, collect, or process the Data Subject's Personal Data to:

(a) maintain and update the Data Subject's records with the Company;

(b) administer his/her stock transactions; and

(c) comply with legal, regulatory, and contractual requirements or obligations.

If the Data Subject is a visitor of the Company premises or any of the Company's project sites, the Company may use, collect, or process the Data Subject's Personal Data to:

(a) grant access to the premises and/or project site/s; and

(b) maintain the security within the premises and/or project site/s.

2.3 **Government-Mandated Use.** The Company may use and process the Personal Data of Data Subjects for government regulatory compliance, company disclosures, and reportorial requirements, and pursuant to a lawful order of any court or tribunal.

2.4 **Quality.** Personal Data processed by the Company must be accurate and, to the extent necessary, up-to-date. Personal Data that is inaccurate or incomplete shall be corrected, supplemented, and/or erased by the Company through its Authorized Personnel, upon receipt of a written request or an accomplished Data Privacy Right Form as provided in **Annex "H,"** from the Data Subject, provided that such request is not vexatious and/or unreasonable.

SECTION 3. RETENTION

3.1 **General.** Personal Data should only be stored for as long as necessary to carry out an aspect of the business operation the Company. The purpose/s for which it was collected and processed, as well as the applicable periods prescribed by law, if any, shall be considered in retaining the Personal Data.

The Retention Period for the Personal Data collected and processed shall be as specified in **Annex** "**A**" on Data Processing Systems.

3.2 **Storage.** The Personal Data of Data Subjects shall be stored in the pertinent Information and Communications System/s and Filing System/s of the Company, such as but not limited to, password-protected computer devices, secure filing cabinets, secure filing rooms, PeopleCore, SAP/NetSuite, MS SQL/Backup, LMS, SecureDocs system, and Archive Room. Where necessary to further its business and to keep its security software tools up-to-date, the Company reserves the right to change and/or update its Information and Communications System/s and Filing System/s.

SECTION 4. DISCLOSURE AND SHARING

4.1 **Confidentiality.** At every stage of the Data Processing Systems employed by the Company, and even after the termination of the relation of the Data Subject with the Company, the Company, its employees, particularly Authorized Personnel, and its PIP/s shall maintain the confidentiality and secrecy of Personal Data that come to their knowledge and possession.

4.2 **Access and Security Clearances.** Only Authorized Personnel and PIP/s contracted by the Company are allowed to access and process the Personal Data of the Data Subject. In accessing and Processing Personal Data, all Authorized Personnel and PIP/s, as well as employees who request to access Personal Data of Data Subjects are enjoined to comply with this Manual.

4.2.1 **Exercise of Data Privacy Right.** A Data Subject who seeks to access and/or modify his/her Personal Data with the Company shall accomplish the Data Privacy Right Form provided in **Annex "H."** The Data Privacy Right Form may be filed with the Authorized Personnel previously dealt with by the Data Subject as processor of his/her Personal Data. The Authorized Personnel shall then endorse the same to the COP for the branch, sub-office, component unit, or department concerned, or in the COP's absence, the head of such branch, sub-office, component unit, or department, who must in turn determine the reasonableness of the exercise of the right. If found reasonable, the COP, if any, or the head of such branch, sub-office, component unit, or department shall approve and transmit the same to the branch, sub-office, component unit, or department concerned for implementation.

4.2.2 **Access Request.** Any person, including an employee who is not an Authorized Personnel but wishes to access Personal Data of Data Subjects pursuant to his/her function in the Company, shall accomplish the Access Request Form provided in **Annex "J"** hereof. Verbal request for access shall not be allowed. The Access Request Form may be filed with the Authorized Personnel who has custody of the Personal Data to be accessed. The Authorized Personnel may either approve or reject the same, depending on the merits of the reasons provided for the requested access. In no case shall access be approved if no meritorious reason is provided in the Access Request Form. If approved, the Authorized Personnel shall endorse for final approval the Access Request Form to the COP for the branch, sub-office, component unit, or department concerned, or in the COP's absence, the head of such branch, sub-office, component unit, or department. Once approved, the Access Request Form shall be transmitted to the branch, sub-office, component unit, or department concerned for implementation.

4.2.3 **Monitoring.** The COP, if any, or the head of the branch, sub-office, component unit, or department concerned shall supervise and monitor the implementation of Article IV, Sections 4.2.1 and 4.2.2 hereof.

4.2.4 **Propriety of Exercise of Right and/or Access Request.** In case of doubt on the propriety of the exercise of right and/or access request, as the case may be, the COP, if any, or the head of the branch, sub-office, component unit, or department concerned shall consult and/or seek clearance from the DPO and/or the Office of the Chief Legal Officer of the Company.

4.2.5 **Security of Access.** Whenever Authorized Personnel, employees of the Company, whether Authorized Personnel or not, and PIP/s of the Company obtain access to Personal Data of Data Subjects in the course of their functions in the Company and/or contractual relations with the Company, they shall observe the Security Measures prescribed in this Manual. Anyone with access to Personal Data shall only process the same in accordance with the purpose of the Processing, and may not share, disclose, or distribute the Personal Data unless instructed by the Company, and with the consent of the Data Subject.

4.3 **Disclosure and Sharing.** Disclosure and sharing of Personal Data to third parties, such as other PIC/s and PIP/s shall be pursuant to a legitimate purpose only. Whether a Data Sharing Agreement or an Outsourcing Agreement shall be drawn up to cover an arrangement that the Company would like to enter into shall be determined by the head of the branch, sub-office, component unit, or department concerned, in consultation with the DPO, COP concerned, if any, and the Office of the Chief Legal Officer of the Company.

4.4 **Consent to Data Sharing.** Consent of the Data Subject shall be obtained prior to the disclosure and sharing of Personal Data and shall be evidenced by a Consent Form, substantially in the form prescribed in **Annex "I."** The Data Subject shall be provided with the following information prior to Data Sharing:

(a) identity of the PIC/s and/or PIP/s that will be given access to the Personal Data;

(b) purpose/s of the Data Sharing;

(c) categories of Personal Data concerned;

(d) intended recipient/s or categories of recipient/s of the Personal Data;

(e) existence of the Rights of the Data Subject; and

(f) such other information that would sufficiently notify the Data Subject of the nature and extent of Data Sharing and manner of Processing.

4.5 **Data Sharing Agreement.** Whenever the Company discloses or transfers Personal Data under its control to another PIC, it shall execute a Data Sharing Agreement, substantially containing the terms and conditions prescribed below, and in the form prescribed in **Annex "B"** hereof, to cover said arrangement.

4.5.1 **Form.** A Data Sharing Agreement shall be in writing.

4.5.2 **Content.** A Data Sharing Agreement shall contain substantially the following:

(a) its purpose/s;

(b) the identity of the PIC/s that are parties to it, including the Company, and for every party, the:

(i) type of Personal Data to be shared under the Agreement;

(ii) the PIP, if any, who will have access to or process the Personal Data, including the type of Processing that it may perform;

(iii) how the party may use or process the Personal Data;

(iv) remedies available to a Data Subject, in case the Processing of Personal Data violates his/her rights, and how such rights may be exercised; and

(v) the DPO and/or COP, if any;

(c) the term of the Data Sharing Agreement, which may be renewed, provided that such term or any extension thereof shall not exceed five (5) years;

(d) an overview of the operational details of the sharing or transfer of Personal Data under the Data Sharing Agreement;

(e) a general description of the Security Measures to be employed under the Data Sharing Agreement;

(f) the method through which a copy of the Data Sharing Agreement may be accessed by the Data Subject;

(g) the details of online access to Personal Data, if such would be granted;

(h) the PIC/s responsible for addressing any request or complaint filed by a Data Subject, and/or investigation by the Commission, if any;

(i) such other terms and conditions as agreed upon by the Company and the PIC/s.

4.6 **Outsourcing Agreement.** The Company may subcontract or outsource the Processing of Personal Data, as well as the functions of the DPO and/or COP/s, provided that such arrangement, if any, is covered by an Outsourcing Agreement substantially containing the terms and conditions prescribed below, and in the form prescribed in **Annex "C."**

4.6.1 **Form.** An Outsourcing Agreement shall be in writing.

4.6.2 **Content.** An Outsourcing Agreement shall contain substantially the following:

(a) its subject matter;

(b) its duration;

(c) its purpose/s;

(d) the type of Personal Data and categories of Data Subjects;

(e) the obligations and rights of the Company;

(f) the geographic location of the Processing;

(g) the obligations of the PIP/s.

SECTION 5. DISPOSAL

5.1 **Schedule.** Upon expiration of the Retention Period as specified in **Annex** "**A**" on Data Processing Systems, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure means that would render the Personal Data unreadable and irretrievable and prevent the occurrence of any Personal Data Breach and other Security Incidents.

5.2 **Procedure.** The disposal procedure per Data Processing System shall be as specified in **Annex** "**A**" on Data Processing Systems.

ARTICLE V
SECURITY MEASURES

The Company shall establish and implement reasonable and appropriate physical, technical, and organizational measures to ensure privacy and data protection. These Security Measures aim to protect Personal Data against natural dangers, such as accidental loss or destruction, and human dangers, such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

The DPO, with the assistance of the COP/s, if any, and the Data Privacy Response Team, shall monitor the Company's compliance with the Security Measures specified in this Article.

SECTION 1. PHYSICAL SECURITY MEASURES

1.1 **Format of Data.** The Personal Data in the custody of the Company may be in digital/electronic format and/or paper-based/physical format.

1.2 **Storage Type and Location.** All Personal Data being processed by the Company shall be stored in a secure facility, whether virtual or physical. Papers or physical documents bearing Personal Data shall be stored in locked filing cabinets, access keys to which shall be entrusted only to Authorized Personnel. Digital or electronic documents containing Personal Data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes. Computers, portable disks, and other devices used by the Company and its PIP/s in Processing Personal Data shall be encrypted with the most appropriate encryption standard.

1.3 **Access and Security Clearances.** Only Authorized Personnel and PIP/s may access the Personal Data stored by the Company, subject to the rules prescribed on access in Article IV, Section 4.2 hereof.

1.4 **Monitoring of Access.** Access of Personal Data by all Authorized Personnel and employees whose request to access Personal Data were approved pursuant to Article IV, Section 4.2 of this Manual shall be monitored by the COP concerned, if any, or the head of the branch, sub-office, component unit, or department concerned. All those who enter and access the Archive Room of the Company must fill out and register in the logbook, which shall indicate the date, time, duration, and purpose of each access.

1.5 **Design of Office Space and/or Work Station.** Computers shall be positioned with considerable spaces between them to maintain the privacy and protect the Processing of Personal Data. Authorized Personnel shall be assigned to office space and/or work stations with the least volume of foot traffic to minimize risk of Personal Data Breach and other Security Incident/s.

1.6 **Maintenance of Confidentiality.** Confidentiality shall be observed and maintained at every stage of the Data Processing Systems. Employees, whether Authorized Personnel or not, shall not be allowed to bring, connect, and/or use their own gadgets or storage devices of any form when Processing Personal Data.

1.7 **Modes of Transfer of Personal Data within the Company or to Other Parties.** Transfer of Personal Data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. As much as possible, facsimile technology shall not be used for transmitting documents containing Personal Data.

1.8 **Retention and Disposal Procedure.** The Company shall retain Personal Data in its custody following the Retention Period indicated in **Annex** "**A**" on Data Processing Systems.

SECTION 2. TECHNICAL SECURITY MEASURES

2.1 Monitoring for Security Breaches

2.1.1 The Company shall cause the monitoring of access to Personal Data so as to minimize the risk of Personal Data Breach and other Security Incident/s. For this purpose, the Company shall maintain and keep up-to-date its Data Privacy Tracker, which shall contain a log of all privacy-related incident/s, complaint/s and/or request/s from Data Subjects, access request/s, as well as a list of all Data Sharing Agreements and Outsourcing Agreements entered into by the Company. The Data Privacy Tracker shall substantially be in the form prescribed in **Annex** "**K**."

2.1.2 The Company shall cause the monitoring of its Information and Communications System/s through the employment of file integrity monitoring.

2.1.3 The Company shall run vulnerability scans periodically, to detect outdated versions of software and misconfigured networks, among others.

2.1.4 The Company shall use an intrusion detection system to monitor security breaches and to be alert of any attempt to interrupt or disturb its Information and Communications System/s.

2.1.5 The Company shall regularly read the firewall logs to monitor security breaches and alert itself of any unauthorized attempt to access the Company network.

2.2 Security Features of Software/s and Application/s Used

2.2.1 The Company shall procure and install an antivirus software for all Company devices where Personal Data are stored, including tablets and smartphones, that regularly access the Internet. The COP/s, if any, and/or the heads of branches, sub-offices, component units, and departments shall ensure that the antivirus software is updated and a system check is done periodically.

2.2.2 The Company shall use web application firewall to protect its servers and databases from malicious online attacks.

2.2.3 To ensure compatibility and data security, the COP/s, if any, and/or the heads of branches, sub-offices, component units, and departments shall first ensure that the software applications have been reviewed and evaluated by an Authorized Personnel or PIP/s concerned, if any, before the utilization thereof in Company computers and devices.

2.3 Regular Assessment and Evaluation of Effectiveness of Security Measures

2.3.1 The Company, through its Authorized Personnel or PIP/s concerned, shall conduct periodic penetration testing of the firewall appliance from outside the Company's premises and from within to conduct vulnerability assessment of the same.

2.3.2 If the use of any software application is found to be a security risk such that it may disturb or interrupt the normal operations of the Company's network, the Company, through its Authorized Personnel or PIP/s, shall notify the end user of such risk and the software application shall immediately be uninstalled. Such circumstance must be logged into the Data Privacy Tracker (see **Annex "K"**) as a privacy-related incident, and must be included in the Company's Annual Security Incident Report, which shall be in the form prescribed in **Annex "L."**

2.4 Encryption, Authentication, and Other Technical Security Measures

2.4.1 **Encryption.** As much as possible, Personal Data, most especially Sensitive Personal Data, processed by the Company shall be encoded into scrambled text using algorithms that render it unreadable unless a cryptographic key is used to convert it.

2.4.2 **Authentication.** Each employee with access to Personal Data shall verify his/her identity using a secure encrypted link and multi-level authentication. Passwords or passcodes used to access Personal Data should be of sufficient strength to deter password attacks.

2.4.3 **Other Technical Security Measures.** The Company shall use such other technical Security Measures to keep its software security tools up-to-date.

SECTION 3. ORGANIZATIONAL SECURITY MEASURES

3.1 **Key Personnel.** The Company shall appoint a DPO and/or COP/s, if any, in accordance with Article II, Sections 1 and 2 hereof, and shall constitute a Data Privacy Response Team in accordance with Article VI, Section 1 hereof.

3.2 **Inventory of Data Processing Systems.** The Data Processing Systems of the Company are as provided in **Annex "A."**

3.3 **Continuing Education on Data Privacy.** All Employees of the Company shall be required to read this Manual upon employment, and/or upon the effectivity of this Manual, whichever is applicable. All new employees shall be briefed of their obligations under the Data Privacy Act. The Company shall hold trainings on privacy and data protection at least once a year for employees handling Personal Data. Intra-office memoranda shall be distributed to inform employees of the most current government issuances on data privacy, as well as of any update of this Manual.

3.4 **Confidentiality and Data Privacy Protection Clauses and/or Non-Disclosure Agreements.** A confidentiality clause substantially in the form prescribed in Annex "M" hereof shall be incorporated into the employment contracts of employees, particularly Authorized Personnel. All employees with access to Personal Data shall operate and hold such Personal Data under strict confidentiality, unless the same qualifies as Public Personal Data. This obligation shall apply even after the employee has left the Company for whatever reasons. Alternatively, a non-disclosure agreement, substantially in the form prescribed in **Annex** "**N**" hereof, may be executed by the Company to protect confidential information and/or Personal Data given to an employee or any other party. Where the Company has to collect and process the Personal Data of a Data Subject under any contract with such Data Subject, it shall ensure that a Data Privacy Protection Clause substantially in the form prescribed in **Annex** "**O**" is contained in its contract with such Data Subject. Alternatively, the Company shall ask the Data Subject to fill out a Consent Form substantially in the form prescribed in **Annex** "**I**."

3.5 **Company Records.** Adequate records of the Company's Personal Data Processing activities shall be maintained at all times. The DPO, with the cooperation and assistance of all the concerned business and service units involved in the Processing of Personal Data, shall be responsible for ensuring that these records are kept up-to-date. These records shall include, at the minimum, general information about the Data Processing Systems of the Company.

3.6 **Review of Data Privacy Manual.** This Manual shall be reviewed and evaluated periodically. Privacy and security policies and practices within the Company shall be updated to remain consistent with current data privacy best practices.

ARTICLE VI
PERSONAL DATA BREACH AND SECURITY INCIDENTS

SECTION 1. DATA PRIVACY RESPONSE TEAM

A Data Privacy Response Team, consisting of the DPO, all COPs of the Company, if any, and representatives from the PIP contracted by the Company, if any, shall be constituted, which shall be responsible for ensuring immediate action in the event of a Security Incident or Personal Data Breach. The Company may also designate other key personnel of the Company to form part of the Data Privacy Response Team. The DPO shall lead the Data Privacy Response Team. The contact details of the members of the Company's Data Privacy Response Team shall be provided in **Annex** "**P**."

SECTION 2. DUTIES OF THE DATA PRIVACY RESPONSE TEAM

The Data Privacy Response Team shall, among others:

(a) ensure the implementation of this Manual;

(b) ensure the management of Security Incidents and Personal Data Breaches, if any;

(c) ensure the Company's compliance with relevant provisions of the Data Privacy Act, its IRR, and all related government issuances on personal data breach management;

(d) assess and evaluate the occurrence of a Security Incident or Personal Data Breach, if any;

(e) execute measures to mitigate the adverse effects of any Security Incident or Personal Data Breach, if any; and

(f) comply with reporting and notification requirements.

SECTION 3. PREVENTION OF SECURITY INCIDENTS AND PERSONAL DATA BREACH

The Data Privacy Response Team shall periodically conduct a Privacy Impact Assessment to identify risks in the Data Processing Systems. The Data Privacy Response Team shall likewise periodically review the existing policies and procedures of the Company with regard to data privacy, including this Data Privacy Manual and its implementation.

SECTION 4. 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 Personal Data Breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the Security Incident or Personal Data Breach.

SECTION 5. DOCUMENTATION AND REPORTING PROCEDURE FOR SECURITY INCIDENTS AND/OR PERSONAL DATA BREACH

Within twenty-four (24) hours from the Security Incident or Personal Data Breach, the Data Privacy Response Team shall log every Security Incident encountered into the Data Privacy Tracker, substantially in the form prescribed in **Annex "K,"** to be submitted to the Company's Management. The log shall contain the following:

(a) description of the nature of the Security Incident or Personal Data Breach, its root cause, chronology of events, estimate of the number of Data Subjects affected, and circumstances regarding its discovery;

(b) measures undertaken by the Data Privacy Response Team to address the breach and reduce the harm or its negative consequences;

(c) outcome of the breach or incident management, and difficulties encountered;

(d) compliance with notification requirements of the Company, if applicable;

(e) assistance provided or to be provided to the affected Data Subject;

(f) name of the Company, including contact details, from whom the Data Subject may obtain additional information about the Security Incident or Personal Data Breach.

SECTION 6. COMMISSION NOTIFICATION PROTOCOL

6.1 **Annual Security Incident Report.** The Annual Security Incident Report that must be submitted to the Commission annually shall be prepared by the Data Privacy Response Team.

6.2 **Mandatory Notification of the Commission.** Upon knowledge of, or reasonable belief that a Personal Data Breach has occurred, the Data Privacy Response Team shall notify the Company's management within twenty-four (24) hours, and the Commission within seventy-two (72) hours, of such occurrence. Notification to the affected Data Subjects should substantially contain the details in the form prescribed in **Annex "Q"**, while notification to the Commission shall substantially be in the same form as **Annex "R"**.

6.2.1 **Conditions.** A Personal Data Breach must be reported to the Commission when the following circumstances concur:

(a) there is a breach of Sensitive Personal Information or other Personal Data that may, under the circumstances, be used to enable identity fraud;

(b) the Personal Data is reasonably believed to have been acquired by an unauthorized person; and

(c) either the Company or the Commission believes that the Personal Data Breach is likely to give rise to a real risk of serious harm to the affected Data Subject.

6.2.2 **Doubt as to Necessity of Notification.** If there is doubt as to whether the Commission has to be notified, the Data Privacy Response Team shall consider the following:

(a) the likelihood of harm or negative consequences on the affected Data Subjects;

(b) how notification, particularly of the Data Subjects, could reduce the risks arising from the Personal Data Breach reasonably believed to have occurred; and

(c) if the Personal Data involved:

(i) information that would likely affect national security, public safety, public order, or public health;

(ii) at least one hundred (100) individuals;

(iii) information required by all applicable laws or rules to be confidential; or

(iv) Personal Data of vulnerable groups.

ARTICLE VII
NOTIFICATIONS, REQUESTS, INQUIRIES, AND COMPLAINTS

SECTION 1. NOTIFICATION ON USE OF PERSONAL DATA FOR MARKETING AND PROFILING

A Data Subject must be notified within forty-eight (48) hours before entry of his/her Personal Data into the Information and Communications System/s of the Company, whenever such Personal Data shall be used for direct marketing, profiling, or historical or scientific purpose/s. Notification shall be made through electronic mail to the address of the Data Subject found in the Company Records.

SECTION 2. REQUESTS AND INQUIRIES PERTAINING TO DATA PRIVACY ISSUES

A Data Subject may access and recommend corrections to his/her Personal Data being processed by the Company by accomplishing the Data Privacy Right Form prescribed in **Annex** "**H.**" Any person, including an employee who is required by his/her functions within the Company to access Personal Data of Data Subjects, may request access thereto through the accomplishment of the Access Request Form prescribed in **Annex** "**J.**"

SECTION 3. PROCEDURE FOR COMPLAINTS

The procedure to be observed in case of complaints for data privacy violation shall be as follows:

(a) Any suspected or actual violation of this Manual, the Data Privacy Act, and/or other government issuances related to data privacy, or any breach, loss, or unauthorized access or disclosure of Personal Data in the possession or under the custody of the Company must be reported immediately to any member of the Data Privacy Response Team who shall reply within twenty-four (24) hours to acknowledge receipt of the complaint.

(b) In case of a complaint for violation of this Manual, the Data Privacy Act, and/or other government issuances related to data privacy, or any breach, loss, or unauthorized access or disclosure of Personal Data in the possession or under the custody of the Company, the DPO, the COP, if any, or any two (2) members of the Data Privacy Response Team shall:

(i) verify the allegations of the complaint;

(ii) if warranted, conduct an official investigation in case of serious security breach as provided under the Data Privacy Act and its IRR; and

(iii) report the Security Incident or Personal Data Breach to the Commission following the procedure laid down in Article VI, Section 6 of this Manual.

The Data Privacy Response Team may also convene as an investigation committee to recommend actions, particularly when the violation is serious, or causes or has the potential to cause material damage to the Company or any of its Data Subjects. Such recommendation shall be submitted to the management of the Company for approval.

ARTICLE VIII
EFFECTIVITY

This Manual was approved by the Board of Directors of the Company on 03 September 2018, and shall take effect immediately.

EDGAR B. SAAVEDRA
Chairman

RAYMUND JAY S. GOMEZ
Chief Legal Officer,
Compliance Officer and
Data Protection Officer

ANNEXES

ANNEX A. DATA PROCESSING SYSTEMS

The structure and procedure by which Personal Data is collected and further processed by the Company in its Information and Communications System/s and/or relevant Filing System/s are explained below.

HUMAN RESOURCES DATA PROCESSING SYSTEM	
Whether particular DPS is managed as PIC, PIP, or both:	PIC
Type of DPS:	Manual or paper-based and electronic

Purpose/Description of DPS:	The Recruitment Team collects the Personal Data from applicants and employees who fill out application forms and transmit their curricula vitae, birth certificates, school records, and other personal records to the Company. The Recruitment Team will then forward the Personal Data collected to Human Resources – Benefits and Compensation for encoding into the PeopleCore System. Said documents are kept in the Archive Room and in the PeopleCore System of the Company. The Processing of Personal Data from applicants and employees are for any of the following purposes:
	to assess the qualifications of the applicants and suitability for the job applied for;
	to create, update, and/or maintain the employment records of employees;
	to have readily accessible information on Data Subjects when requested or needed by different departments within the Company (e.g., payroll);
	to evaluate his/her physical fitness for the job; and/or
	to ensure his/her physical and psychological wellness.
	The following Personal Data are collected:
	Full Name;
	Address;
	Birthdate and Birthplace;
	Contact Number;
	Age;
	Gender;
	Height/Weight;
	Marital Status;
	Educational Attainment;
	Employee Record;
	Salary;
	Mandatory government contributions;
	Taxes;
	Government Exam/s Taken;
	Trainings and Seminars Attended; and
	Family Background.

HUMAN RESOURCES DATA PROCESSING SYSTEM	
Information on whether the Processing of Personal Data is subcontracted or outsourced:	Yes
Details of PIP/s, if any:	Cycore Technology Solutions Co., Inc. Is there a subcontracting or outsourcing agreement? Yes. PIP Name: Cycore Technology Solutions Co., Inc. PIP Email: jvfaura@cycoretech.com PIP Address: Unit A55 Liberty Avenue, Cubao, Quezon City PIP Contact Number/Extension Number: (02) 6340615 PIP Description/Purpose: To maintain a database of employee records for Processing by the Company's Authorized Personnel Maxicare Healthcare Corporation Is there a subcontracting or outsourcing agreement? Yes. PIP Name: Maxicare Healthcare Corporation PIP Email: dpo@maxicare.com.ph PIP Address: 203 Salcedo Street, Legaspi Village, Makati City PIP Contact Number/Extension Number: (02) 9086900 PIP Description/Purpose: To maintain a database of employees eligible for healthcare coverage
Information on whether Personal Data is shared outside of the Philippines:	No
Categories of Data Subjects:	Job applicants and employees

Information as to whom Personal Data will be disclosed (public/private organization, name of organization):	Authorized Personnel (i.e., Recruitment Team, HR-C&B, Payroll, and only upon a request duly made therefor (Private);
	Department of Labor and Employment (Public);
	Bureau of Internal Revenue (Public);
	Home Development Mutual Fund (Public);
	Philippine Health Insurance Corporation (Public); and
	Social Security System (Public).

Retention Period:	5 years

ACCOUNTING DATA PROCESSING SYSTEM (FOR SUPPLIERS/SUBCONTRACTORS)	
Whether particular DPS is managed as PIC, PIP, or both:	PIC
Type of DPS:	Manual or paper-based and electronic
Purpose/Description of DPS:	The Purchasing Department collects and processes the Personal Data of key personnel of prospective, current, and previous suppliers and subcontractors through application forms duly filled

ACCOUNTING DATA PROCESSING SYSTEM (FOR SUPPLIERS/SUBCONTRACTORS)	
	out by the latter, identification cards, etc. for any of the following purposes: (1) to provide information for purchasing and accounting transactions; and (2) for billing purposes; and (3) for records management. The following Personal Data are collected: (1) Full Name; (2) Group; (3) TIN; (4) Contact Number; (5) E-mail; (6) Name of Contact Person; (7) Position; and (8) Address.
Information on whether the Processing of Personal Data is subcontracted or outsourced:	No
Details of PIP, if any:	(1) **Is there a subcontracting or outsourcing agreement?** N/A (2) **PIP Name:** N/A (3) **PIP Email:** N/A (4) **PIP Address:** N/A (5) **PIP Contact Number/Extension Number:** N/A (6) **PIP Description/Purpose:** N/A
Information on whether Personal Data is shared outside of the Philippines:	No
Categories of Data Subjects:	Key personnel of suppliers and subcontractors
Information as to whom Personal Data will be disclosed (public/private organization, name of organization):	(1) Authorized Personnel of the Company (Private); and (2) Department of Labor and Employment (Public).
Retention Period:	5 years

HEALTH SAFETY AND ENVIRONMENT DATA PROCESSING SYSTEM	
Whether particular DPS is managed as PIC, PIP, or both:	PIC
Type of DPS:	Manual or paper-based and electronic

HEALTH SAFETY AND ENVIRONMENT DATA PROCESSING SYSTEM	
Purpose/Description of DPS:	The Health Safety and Environment Department collects and processes Personal Data from the patient-employee for any of the following purposes: (1) to evaluate his/her physical fitness for the job; and/or (2) to ensure his/her physical and psychological wellness. The Personal Data are disclosed to Authorized Personnel only, and/or health professionals, when necessary. The following Personal Data are collected: (1) Full Name; (2) Address; (3) Birthdate/Birthplace; (4) Contact Number; (5) Marital Status; (6) Department; (7) Position; and (8) Medical History.
Information on whether the Processing of Personal Data is subcontracted or outsourced:	No
Details of PIP, if any:	(1) **Is there a subcontracting or outsourcing agreement?** N/A (2) **PIP Name:** N/A (3) **PIP Email:** N/A (4) **PIP Address:** N/A (5) **PIP Contact Number/Extension Number:** N/A (6) **PIP Description/Purpose:** N/A
Information on whether Personal Data is shared outside of the Philippines:	No
Categories of Data Subjects:	Employees
Information as to whom Personal Data will be disclosed (public/private organization, name of organization):	Authorized Personnel and health professionals, if necessary (Private)
Retention Period:	5 years

OFFICE SECURITY SYSTEM	
Whether particular DPS is managed as PIC, PIP, or both:	PIC
Type of DPS:	Manual or paper-based and electronic
Purpose/Description of DPS:	The following Personal Data are collected: (1) Full Name; (2) E-mail Address; (3) Company; (4) Contact Number; and (5) CCTV Footages. The office administration collects and processes above Personal Data from any Data Subject who visits the premises of the Company for any of the following purposes: (1) to monitor the number of visitors per day; and (2) to maintain the security in the Company premises.
Information on whether the Processing of Personal Data is subcontracted or outsourced:	No
Details of PIP, if any:	(1) **Is there a subcontracting or outsourcing agreement?** N/A (2) **PIP Name:** N/A (3) **PIP Email:** N/A (4) **PIP Address:** N/A (5) **PIP Contact Number/Extension Number:** N/A (6) **PIP Description/Purpose:** N/A
Information on whether Personal Data is shared outside of the Philippines:	No
Categories of Data Subjects:	Employees and Company visitors
Information as to whom Personal Data will be disclosed (public/private organization, name of organization):	The Personal Data are disclosed to government agencies, in case of any security incident, whether related to data privacy or not.
Retention Period:	5 years

ANNEX B. DATA SHARING AGREEMENT TEMPLATE

DATA SHARING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This Data Sharing Agreement (this "Agreement") is made and executed this ____________ in ____________ by and between:

Megawide Construction Corporation, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at 20 N. Domingo Street, Barangay Valencia, Quezon City 1112, represented herein by its ____________, ________________ (hereinafter referred to as "**MEGAWIDE**");

- and -

________________________, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at ___________________________, represented herein by its ____________, ________________ (hereinafter referred to as "**COMPANY B**");

(Each a "Party" and together, the "Parties")

WITNESSETH:

WHEREAS, MEGAWIDE desires to ______________________________________;

WHEREAS, COMPANY B desires to ______________________________________;

WHEREAS, the foregoing purposes will require MEGAWIDE and COMPANY B to share Personal Data of Data Subjects;

WHEREAS, adequate safeguards for data privacy and security must be observed by the Parties in the course of Data Sharing;

NOW, THEREFORE, for and in consideration of the foregoing premises and the terms and conditions hereinafter specified, the Parties hereby agree as follows:

ARTICLE I. TERM

This Agreement shall commence on the date of its execution and shall continue for a period of _ (_) years (the "Term"), unless sooner terminated under Article VII hereof on Termination. This Agreement is renewable upon the Parties' written agreement, provided that such Term or any extension thereof shall not exceed five (5) years.

ARTICLE II. DEFINITIONS

1. "**Authorized Personnel**" refers to employee/s or officer/s of the Parties authorized to collect and/or to process Personal Data either by the function of their office or position, or through specific authority.

2. "**Compliance Officer for Privacy**" or "**COP**" refers to an individual duly authorized by the Company to perform some of the functions of the DPO for a branch, sub-office, or component unit, if any.

3. "**Consent of the Data Subject**" refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and Processing of his/her Personal, Sensitive Personal, or Privileged Information. It shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of a Data Subject by a lawful representative or an agent specifically authorized by the Data Subject to do so.

4. "**Data Protection Officer**" or "**DPO**" refers to the officer duly designated by each Party to be accountable for the latter's compliance with laws, regulations, and issuances on data privacy.

5. "**Data Sharing**" refers to the disclosure or transfer of Personal Data under the control or custody of MEGAWIDE to COMPANY B, and vice-versa.

6. "**Data Subject**" refers to any individual whose Personal, Sensitive Personal, and/or Privileged Information are processed by the Parties.

7. "**Outsourcing**" refers to the disclosure or transfer of Personal Data by the Parties to their respective Personal Information Processor/s (PIP/s), if any, for the Processing of Personal Data obtained or shared under this Agreement.

8. "**Outsourcing Agreement**" refers to any written contract entered into by the Parties with their respective PIP/s, if any.

9. "**Personal Data**" refers to all types of Personal Information collected and processed by the Company. Personal Data may be classified as follows:

   (a) "**Confidential Personal Data**" pertains to all other information to which access is restricted, and of which Processing requires the written consent of the Data Subject concerned, such as but not limited to Employee 201 files and information contained therein, device passwords and/or passcodes, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

   (b) "**Public Personal Data**" pertains to Personal Information of Data Subjects which may be disclosed to the public by the Parties due to, or as required by, their business operations, and for government regulatory compliance and company disclosures.

10. "**Personal Data Breach**" refers to an actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data Breach may be in any of the following nature:

   (a) "**Availability Breach,**" which results from the loss of, or accidental or unlawful destruction of Personal Data;

   (b) "**Confidentiality Breach,**" which results from the unauthorized disclosure of, or access to Personal Data; and/or

(c) "**Integrity Breach**," which results from the alteration of Personal Data.

11. "**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.

12. "**Personal Information Controller**" or "**PIC**" refers to a natural or juridical person, or any other body, who/which controls the processing of Personal Data, or instructs another to process Personal Data on its behalf. MEGAWIDE and COMPANY B are PICs.

13. "**Personal Information Processor** or "**PIP**" refers to any natural or juridical person, or any other body, to whom a PIC outsources, or gives instructions as regards, the Processing of Personal Data pertaining to a Data Subject. The Parties' service providers, if any, are PIPs.

14. "**Privileged Information**" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

15. "**Processing**" refers to any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction thereof. Processing may be performed through automated means or by manual processing.

16. "**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 to a Personal Data Breach, if not for safeguards that have been put in place.

17. "**Security Measures**" refers to the physical, technical, and organizational measures employed by the Parties to protect Personal Data shared under this Agreement from natural and human dangers.

18. "**Sensitive Personal Information**" refers to Personal Information:

(a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political 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 government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and

(d) specifically established by an executive order or an act of Congress to be kept classified.

ARTICLE III. PERSONAL DATA

1. **Personal Data Covered by Data Sharing.** To achieve the purposes laid down in this Agreement, MEGAWIDE may share or transfer Personal Information, Sensitive Personal

Information, and such other Personal Data to COMPANY B. COMPANY B may also share or transfer said information to MEGAWIDE.

2. **Operational Details of Data Sharing.** In sharing or transferring Personal Data to each other under this Agreement, the Parties shall observe the following:

(a) ***Information on Data Sharing.*** Prior to collecting Personal Data from a Data Subject and Data Sharing, either Party must provide the following information to the Data Subject:

(i) identity of the Parties and their PIP/s, if any, who will be given access to the Personal Data;

(ii) purpose/s of Data Sharing;

(iii) categories of Personal Data collected, shared, and further processed;

(iv) intended recipient/s or categories of recipient/s of the Personal Data;

(v) existence of the rights of the Data Subject; and

(vi) if requested by the Data Subject, other information that would sufficiently notify the Data Subject of the nature and extent of Data Sharing and the manner of Processing.

(b) ***Consent of the Data Subject.*** The Party collecting the Personal Information, Sensitive Personal Information, and such other Personal Data from a Data Subject shall ensure that the Data Subject gives his/her prior written consent to the Data Sharing and Processing.

(c) ***Data Sharing.*** The Parties may share the Personal Data collected to each other through paper-based/physical or digital/electronic means, provided that the Security Measures laid down in Article IV hereof are observed. Transfer of Personal Data via electronic mail shall be through a secure and encrypted e-mail facility.

(d) ***Processing of Personal Data.*** As soon as Personal Data is shared by one Party to the other, the latter may commence the Processing of Personal Data.

(e) ***Outsourcing of Personal Data.*** In the Processing of Personal Data, either Party may engage the services of any PIP, whose engagement must be covered by duly executed Outsourcing Agreement/s.

(i) *PIP of MEGAWIDE.* For the purpose of ________________, MEGAWIDE engaged the services of ________________ as PIP.

(ii) *PIP of COMPANY B.* For the purpose of ________________, COMPANY B engaged the services of ________________ as PIP.

ARTICLE IV. SECURITY MEASURES

1. **Security Measures.** The Parties undertake to observe and implement the following reasonable and appropriate physical, technical, and organizational measures to ensure privacy and data protection. These Security Measures aim to protect Personal Data against natural

dangers, such as accidental loss or destruction, and human dangers, such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

2. **Format of Data.** Personal Data shared by the Parties may be in digital/electronic format and paper-based/physical format.

3. **Storage Type and Location.** All Personal Data collected, shared, and processed by the Parties shall be stored in secure facilities, whether virtual or physical. Papers or physical documents bearing Personal Data shall be stored in locked filing cabinets, access keys to which shall be entrusted only to Authorized Personnel. Digital or electronic documents containing Personal Data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes.

4. **Access.** Only Authorized Personnel and the PIP/s named under Article III (2) (e) hereof, if any, may access the Personal Data shared by the Parties. Either Party shall ensure that any person acting under its authority, and who has access to the Personal Data collected under this Agreement, processes the Personal Data exclusively for the purpose/s identified in this Agreement.

5. **Monitoring of Access.** Access of Personal Data by all Authorized Personnel shall be monitored by the DPO and/or COP of the Party concerned, in accordance with its own data privacy policies.

6. **Retention and Disposal.** The Parties shall retain the Personal Data collected, shared, and processed for the Term of this Agreement, and for _ (_) years thereafter, or as long as may be necessary to accomplish the purpose of Data Sharing and Processing (the "Retention Period"). After the Retention Period or when the Data Subject requests in writing that his/her Personal Data be destroyed, the Parties shall dispose of the Personal Data in their custody, in accordance with their respective data privacy policies.

7. **Other Measures.** In the Processing of the Personal Data collected and shared under this Agreement, the Parties commit to observe the most appropriate Security Measures, whether physical, technical, or organizational, according to the requirements of data privacy laws, regulations, and government issuances, as well as their respective data privacy policies.

ARTICLE V. REPRESENTATIONS AND WARRANTIES

1. **Confidentiality.** The Parties shall treat the Personal Data shared under this Agreement with utmost confidentiality. Further, the Parties shall ensure that their respective personnel, employees, agents, and/or representatives, as well as PIP/s, if any, engaged in the Processing of Personal Data under this Agreement, understand and are fully informed of the confidential nature of the Personal Data being processed, and that their obligation to keep the same in confidence survives the termination of their engagement, employment, and/or any relationship with either Party.

2. **Data Sharing.** The Parties shall neither share the Personal Data received by virtue of this Agreement with any other party, nor process the same for any purpose other than those laid down in this Agreement, or incidental thereto, without the prior written consent of the concerned Data Subjects.

3. **Data Privacy Compliance.** The Parties hereby represent and warrant that in the Processing of Personal Data under this Agreement, they shall comply, and/or are compliant, with data privacy laws, regulations, and other relevant government issuances. The Parties further represent and warrant that they have in place appropriate Security Measures that endeavor to

protect the Personal Data they process under this Agreement from any Security Incident, including Personal Data Breach.

ARTICLE VI. REMEDIES AVAILABLE TO DATA SUBJECTS

1. **Rights of the Data Subjects.** In the Processing of Personal Data, the Parties commit to respect and uphold the following rights of the Data Subjects:

   (a) the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed;

   (b) the right to object to the Processing of his/her Personal Data;

   (c) the right to reasonable access, upon demand, to Personal Data;

   (d) the right to dispute the inaccuracy or error in his/her Personal Data, and have the Parties accordingly correct or cause the correction thereof, unless such is vexatious or unreasonable;

   (e) the right to suspend, withdraw, or order the blocking, removal, or destruction of his/her Personal Data from the Parties' data processing systems;

   (f) the right to obtain a copy of the Personal Data, where his/her Personal Data is processed by electronic means; and

   (g) the right to complain before government authorities of any data privacy violation committed by either Party in the Processing of Personal Data under this Agreement.

2. **Exercise of Rights.** The Parties shall ensure that it is made known to the Data Subjects that they may access and/or modify their Personal Data as processed by the Parties under this Agreement. A Data Subject who seeks to access and/or modify his/her Personal Data and/or exercise any of the rights under Article VI (1) hereof may address his/her request in writing to the DPO of the Party in custody of his/her Personal Data.

3. **Access to this Agreement.** Any Data Subject, whose Personal Data are being processed or shared under this Agreement, may request in writing a copy of this Agreement. Such request must be addressed to the DPO of either Party.

4. **Security Incident/s and Personal Data Breach.**

   (a) ***Personal Data Breach.*** If either Party becomes aware of any Personal Data Breach, involving any of its personnel, premises, facilities, systems, and/or equipment, it shall, within a reasonable period and/or according to its data privacy policies:

      (i) inform the other Party of the Personal Data Breach;

      (ii) investigate the Personal Data Breach and inform the other Party of the results thereof;

      (iii) take all necessary and reasonable steps to mitigate the adverse effect of, as well as minimize any damage, if any, resulting from, the Personal Data Breach; and

(iv) inform the relevant government authorities of such event, if legally required to do so.

(b) **Security Incident/s.** Any Security Incident/s other than Personal Data Breach, and any unsuccessful or attempted Personal Data Breach shall not be subject to the foregoing Section. An unsuccessful or attempted Personal Data Breach is one that does not actually result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed under this Agreement.

(c) **No Fault or Liability.** The obligation of either Party to report or respond to a Personal Data Breach under Article VI (4) (a) hereof is not and will not be construed as an acknowledgment by either Party of any fault or liability for the Personal Data Breach.

5. **Other Request/s.** Any other request/s, including complaint/s, of Data Subjects with regard to the Processing of Personal Data may be communicated to either Party through its DPO, as follows:

(a) ***DPO of MEGAWIDE.*** The DPO of MEGAWIDE may be reached through the following:

Name:	Atty. Raymund Jay S. Gomez
Postal Address:	20 N. Domingo Street Barangay Valencia Quezon City 1112
Telephone Number:	+632 6551111
E-mail Address:	rgomez@megawide.com.ph

(b) ***DPO of COMPANY B.*** The DPO of COMPANY B may be reached through the following:

Name:	
Postal Address:	
Telephone Number:	
E-mail Address:	

ARTICLE VII. TERMINATION

Either Party may terminate this Agreement by giving the other Party three (3) months prior written notice.

ARTICLE VIII. GENERAL PROVISIONS

1. **Interpretation.** This Agreement and any other contract it supplements, if any, shall be interpreted and construed together so as to give harmonious effect to their respective provisions; provided that, in the event of irreconcilable conflict as regards data privacy, the provisions of this Agreement shall prevail.

2. **Severability.** If any provision in this Agreement or any document or instrument relevant, executed, or delivered pursuant hereto shall be held invalid, the remainder thereof shall not be affected thereby.

3. **Amendment.** This Agreement and the terms and conditions hereof may not be changed, discharged, amended, modified, or altered, unless in writing and duly signed by an authorized representative of each of the Parties.

4. **Venue of Action.** Any legal action, suit, or proceeding arising out of or relating to this Agreement shall be instituted exclusively in the courts of Quezon City.

5. **Governing Law.** This Agreement shall be governed by and construed in accordance with Philippine laws.

IN WITNESS WHEREOF, the Parties herein have hereunto set their hands on this ______ day of ________________ at ________________.

MEGAWIDE CONSTRUCTION CORPORATION	**COMPANY B**
By:	By:
______________________________	______________________________
[Position]	*[Position]*

SIGNED IN THE PRESENCE OF:

______________________________ ______________________________

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY OF ______________________) S.S.

BEFORE ME, a Notary Public, personally appeared the following:

Name	*Competent Evidence of Identity*	*Date and Place of Issuance*
Megawide Construction Corporation Represented by: ______________________________		
Company B Represented by: ______________________________		

known to me and to me known to be the same persons who executed the foregoing Agreement, and they acknowledged to me that the same is their free and voluntary act and deed, as well as the free and voluntary act and deed of the Corporations that they represent, for the uses, purposes, and considerations therein set forth.

This instrument refers to an Agreement consisting of ______ (_) pages, including this page on which the Acknowledgment is written, duly signed by the Parties and their witnesses on each and every page thereof, and sealed with my notarial seal.

WITNESS MY HAND and official seal at the place and on the date first above-written.

NOTARY PUBLIC

Doc. No. ______;
Page No. ______;
Book No. ______;
Series of 2018.

ANNEX C. OUTSOURCING AGREEMENT TEMPLATE

OUTSOURCING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This Outsourcing Agreement (this "Agreement") is made and executed this ____________ in ___________ by and between:

Megawide Construction Corporation, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at 20 N. Domingo Street, Barangay Valencia, Quezon City 1112, represented herein by its ____________, _________________ (hereinafter referred to as "**MEGAWIDE**");

- and -

_______________________, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at __________________________, represented herein by its ____________, _________________ (hereinafter referred to as the "**PROCESSOR**");

(Each a "Party" and together, the "Parties")

WITNESSETH:

WHEREAS, MEGAWIDE desires to ____________________________________, and for such purpose, has to collect and process Personal Data;

WHEREAS, the PROCESSOR is engaged in the business of ____________________;

WHEREAS, MEGAWIDE desires to contract the services of the PROCESSOR in the Processing the Personal Data of its Data Subjects;

WHEREAS, adequate safeguards for data privacy and security must be observed by the Parties in the course of Outsourcing (as defined below);

NOW, THEREFORE, for and in consideration of the foregoing premises and the terms and conditions hereinafter specified, the Parties hereby agree as follows:

ARTICLE I. TERM

This Agreement shall commence on the date of its execution and shall continue for a period of _ (_) years (the "Term"), unless sooner terminated under Article IX hereof on Termination. This Agreement is renewable upon the Parties' written agreement, provided that such Term or any extension thereof shall not exceed five (5) years.

ARTICLE II. DEFINITIONS

1. "**Authorized Personnel**" refers to employee/s or officer/s of the Parties authorized to collect and/or to process Personal Data either by the function of their office or position, through specific authority, or pursuant to this Agreement.

2. "**Compliance Officer for Privacy**" or "**COP**" refers to an individual duly authorized by the Company to perform some of the functions of the DPO for a branch, sub-office, or component unit, if any.

3. "**Consent of the Data Subject**" refers to any freely given, specific, informed indication of will, whereby the Data Subject agrees to the collection and Processing of his/her Personal, Sensitive Personal, or Privileged Information. It shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of a Data Subject by a lawful representative or an agent specifically authorized by the Data Subject to do so.

4. "**Data Protection Officer**" or "**DPO**" refers to the officer duly designated by each Party to be accountable for the latter's compliance with laws, regulations, and issuances on data privacy.

5. "**Data Subject**" refers to any individual whose Personal, Sensitive Personal, and/or Privileged Information are processed by the PROCESSOR, on behalf of MEGAWIDE, pursuant to this Agreement.

6. "**Outsourcing**" refers to the disclosure or transfer of Personal Data by MEGAWIDE to the PROCESSOR for the Processing of Personal Data under this Agreement.

7. "**Personal Data**" refers to all types of Personal Information collected and processed by the Parties. Personal Data may be classified as follows:

   (a) "**Confidential Personal Data**" pertains to all other information to which access is restricted, and of which Processing requires the written consent of the Data Subject concerned, such as but not limited to Employee 201 files and information contained therein, device passwords and/or passcodes, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

   (b) "**Public Personal Data**" pertains to Personal Information of Data Subjects which may be disclosed to the public by the Parties due to, or as required by, their business operations, and for government regulatory compliance and company disclosures.

8. "**Personal Data Breach**" refers to an actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. A Personal Data Breach may be in any of the following nature:

   (a) "**Availability Breach**," which results from the loss of, or accidental or unlawful destruction of Personal Data;

   (b) "**Confidentiality Breach**," which results from the unauthorized disclosure of, or access to Personal Data; and/or

   (c) "**Integrity Breach**," which results from the alteration of Personal Data.

9. **"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.

10. **"Privileged Information"** refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication.

11. **"Processing"** refers to any operation or any set of operations performed upon Personal Data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction thereof. Processing may be performed manually or through automated means.

12. **"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 to a Personal Data Breach, if not for safeguards that have been put in place.

13. **"Security Measures"** refers to the physical, technical, and organizational measures employed by the Parties to protect Personal Data shared under this Agreement from natural and human dangers.

14. **"Sensitive Personal Information"** refers to Personal Information:

(a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political 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 government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and

(d) specifically established by an executive order or an act of Congress to be kept classified.

ARTICLE III. PERSONAL DATA

1. **Personal Data covered by Outsourcing.** To achieve the purposes laid down in this Agreement, MEGAWIDE may share or transfer to the PROCESSOR, or instruct the PROCESSOR to collect and further process on its behalf, Personal Information, Sensitive Personal Information, and such other Personal Data of the Data Subjects.

2. **Further Outsourcing of Personal Data.** In the Processing of Personal Data, upon the prior written instruction of MEGAWIDE, the PROCESSOR may further engage the services of another PROCESSOR, provided that such engagement must be covered by duly executed Outsourcing Agreement/s.

ARTICLE IV. RIGHTS AND OBLIGATIONS OF MEGAWIDE

1. **Information on Processing of Personal Data.** Prior to collection or causing the collection of Personal Data from a Data Subject, MEGAWIDE must ensure that the following information are provided to the Data Subject:

(a) identity of MEGAWIDE as PIC;

(b) purpose/s of Processing;

(c) categories of Personal Data collected, shared, and further processed;

(d) intended recipient/s or categories of recipient/s of the Personal Data;

(e) existence of the rights of the Data Subject; and

(f) if requested by the Data Subject, other information that would sufficiently notify the Data Subject of the nature and extent of Processing and Outsourcing, and the manner of Processing.

2. **Consent of the Data Subject.** MEGAWIDE shall ensure that the Data Subject gives his/her prior written consent to the Processing of Personal Data.

3. **Control over Processing.** MEGAWIDE shall control the Processing of Personal Data pursuant to this Agreement, and for such purpose, may give instructions to the PROCESSOR.

ARTICLE V. OBLIGATIONS OF THE PROCESSOR

1. In the Processing of Personal Data pursuant to this Agreement, the PROCESSOR undertakes to:

(a) process the Personal Data only upon the documented instructions of MEGAWIDE, including transfers of Personal Data to another country or an international organization, unless such transfer is authorized by law;

(b) ensure that an obligation of confidentiality is imposed on Authorized Personnel and other persons authorized to process the Personal Data;

(c) implement appropriate security measures and comply with the data privacy laws, regulations, and relevant government issuances;

(d) not engage another processor without prior written approval from MEGAWIDE: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the Processing;

(e) assist MEGAWIDE, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by Data Subjects relative to the exercise of their rights;

(f) assist MEGAWIDE in ensuring compliance with the data privacy laws, regulations, and relevant government issuances, taking into account the nature of Processing and the information available to the PROCESSOR;

(g) at the choice of MEGAWIDE, delete or return all Personal Data to MEGAWIDE after the end of the provision of services relating to the Processing: Provided, that this includes deleting existing copies unless storage is authorized by law;

(h) make available to MEGAWIDE all information necessary to demonstrate compliance with the obligations laid down in data privacy laws, regulations, and relevant government issuances, and allow for and contribute to audits, including inspections, conducted by MEGAWIDE or an auditor mandated by the latter; and

(i) immediately inform MEGAWIDE if, in its opinion, an instruction infringes data privacy laws, regulations, and relevant government issuances.

ARTICLE VI. SECURITY MEASURES

1. **Security Measures.** The Parties undertake to observe and implement the following reasonable and appropriate physical, technical, and organizational measures to ensure privacy and data protection. These Security Measures aim to protect Personal Data against natural dangers, such as accidental loss or destruction, and human dangers, such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

2. **Format of Data.** Personal Data processed by the Parties may be in digital/electronic format and paper-based/physical format.

3. **Storage Type and Location.** All Personal Data processed by the Parties shall be stored in secure facilities, whether virtual or physical. Papers or physical documents bearing Personal Data shall be stored in locked filing cabinets, access keys to which shall be entrusted only to Authorized Personnel. Digital or electronic documents containing Personal Data shall be stored in computers, portable disks, and other devices, provided either the document or the device where it is stored is protected by passwords or passcodes.

4. **Access.** Only Authorized Personnel of MEGAWIDE and the PROCESSOR may access the Personal Data processed by the Parties. Either Party shall ensure that any person acting under its authority, and who has access to the Personal Data collected under this Agreement, processes the Personal Data exclusively for the purpose/s identified in this Agreement.

5. **Monitoring of Access.** Access of Personal Data by all Authorized Personnel shall be monitored by the DPO and/or COP of the Party concerned, in accordance with its own data privacy policies.

6. **Other Measures.** In the Processing of the Personal Data collected and shared under this Agreement, the Parties commit to observe the most appropriate Security Measures, whether physical, technical, or organizational, according to the requirements of data privacy laws, regulations, and government issuances, as well as their respective data privacy policies.

ARTICLE VII. REPRESENTATIONS AND WARRANTIES

1. **Confidentiality.** The Parties shall treat the Personal Data processed pursuant this Agreement with utmost confidentiality. Further, the Parties shall ensure that their respective personnel, employees, agents, and/or representatives, as well as PIP/s, if any, engaged in the Processing of Personal Data under this Agreement, understand and are fully informed of the confidential nature of the Personal Data being processed, and that their obligation to keep the same in confidence survives the termination of their engagement, employment, and/or any relationship with either Party.

2. **Data Sharing.** The Parties shall neither share the Personal Data received by virtue of this Agreement with any other party, nor process the same for any purpose other than those laid down in this Agreement, or incidental thereto, without the prior written consent of the concerned Data Subjects.

3. **Data Privacy Compliance.** The Parties hereby represent and warrant that in the Processing of Personal Data under this Agreement, they shall comply, and/or are compliant, with data privacy laws, regulations, and other relevant government issuances. The Parties further represent and warrant that they have in place appropriate Security Measures that endeavor to protect the Personal Data they process under this Agreement from any Security Incident, including Personal Data Breach.

ARTICLE VIII. REMEDIES AVAILABLE TO DATA SUBJECTS

1. **Rights of the Data Subjects.** In the Processing of Personal Data, the Parties commit to respect and uphold the following rights of the Data Subjects:

(a) the right to be informed whether Personal Data pertaining to him/her shall be, are being, or have been processed;

(b) the right to object to the Processing of his/her Personal Data;

(c) the right to reasonable access, upon demand, to Personal Data;

(d) the right to dispute the inaccuracy or error in his/her Personal Data, and have the Parties accordingly correct or cause the correction thereof, unless such is vexatious or unreasonable;

(e) the right to suspend, withdraw, or order the blocking, removal, or destruction of his/her Personal Data from the Parties' data processing systems;

(f) the right to obtain a copy of the Personal Data, where his/her Personal Data is processed by electronic means; and

(g) the right to complain before government authorities of any data privacy violation committed by either Party in the Processing of Personal Data under this Agreement.

2. **Exercise of Rights.** The Parties shall ensure that it is made known to the Data Subjects that they may access and/or modify their Personal Data as processed by the Parties under this Agreement. A Data Subject who seeks to access and/or modify his/her Personal Data and/or exercise any of the rights under Article VIII (1) hereof may address his/her request in writing to the DPO of MEGAWIDE.

3. **Access to this Agreement.** Any Data Subject, whose Personal Data are being processed under this Agreement, may request in writing a copy of this Agreement. Such request must be addressed to the DPO of MEGAWIDE.

4. **Security Incident/s and Personal Data Breach.**

(a) ***Personal Data Breach.*** If the PROCESSOR becomes aware of any Personal Data Breach, involving any of its personnel, premises, facilities, systems, and/or equipment, it shall, within a reasonable period and/or according to its data privacy policies:

(i) inform MEGAWIDE of the Personal Data Breach;

(ii) investigate the Personal Data Breach and inform MEGAWIDE of the results thereof;

(iii) take all necessary and reasonable steps to mitigate the adverse effect of, as well as minimize any damage, if any, resulting from, the Personal Data Breach; and

(iv) inform the relevant government authorities of such event, if legally required to do so.

(b) **Security Incident/s.** Any Security Incident/s other than Personal Data Breach, and any unsuccessful or attempted Personal Data Breach shall not be subject to the foregoing Section. An unsuccessful or attempted Personal Data Breach is one that does not actually result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed under this Agreement.

(c) **No Fault or Liability.** The obligation of the PROCESSOR to report or respond to a Personal Data Breach under Article VIII (4) (a) hereof is not and will not be construed as an acknowledgment by the Parties of any fault or liability for the Personal Data Breach.

5. **Other Request/s.** Any other request/s, including complaint/s, of Data Subjects with regard to the Processing of Personal Data may be communicated to either Party through its DPO, as follows:

(a) ***DPO of MEGAWIDE.*** The DPO of MEGAWIDE may be reached through the following:

Name:	Atty. Raymund Jay S. Gomez
Postal Address:	20 N. Domingo Street Barangay Valencia Quezon City 1112
Telephone Number:	+632 6551111
E-mail Address:	rgomez@megawide.com.ph

(b) ***DPO of the PROCESSOR.*** The DPO of the PROCESSOR may be reached through the following:

Name:	
Postal Address:	
Telephone Number:	
E-mail Address:	

ARTICLE IX. TERMINATION

MEGAWIDE may terminate this Agreement prior to the expiration of the Term thereof, by giving the PROCESSOR one (1) month prior written notice.

ARTICLE X. GENERAL PROVISIONS

1. **Interpretation.** This Agreement and any other contract it supplements, if any, shall be interpreted and construed together so as to give harmonious effect to their respective provisions; provided that, in the event of irreconcilable conflict as regards data privacy, the provisions of this Agreement shall prevail.

2. **Severability.** If any provision in this Agreement or any document or instrument relevant, executed, or delivered pursuant hereto shall be held invalid, the remainder thereof shall not be affected thereby.

3. **Amendment.** This Agreement and the terms and conditions hereof may not be changed, discharged, amended, modified, or altered, unless in writing and duly signed by an authorized representative of each of the Parties.

4. **Venue of Action.** Any legal action, suit, or proceeding arising out of or relating to this Agreement shall be instituted exclusively in the courts of Quezon City.

5. **Governing Law.** This Agreement shall be governed by and construed in accordance with Philippine laws.

IN WITNESS WHEREOF, the Parties herein have hereunto set their hands on this ______ day of __________________ at __________________.

MEGAWIDE CONSTRUCTION CORPORATION	**PROCESSOR**
By:	By:
______________________________	______________________________
[Position]	*[Position]*

SIGNED IN THE PRESENCE OF:

______________________________ ______________________________

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY OF ______________________________) S.S.

BEFORE ME, a Notary Public, personally appeared the following:

Name	***Competent Evidence of Identity***	***Date and Place of Issuance***
Megawide Construction Corporation Represented by: ______________________________		
Processor Represented by: ______________________________		

known to me and to me known to be the same persons who executed the foregoing Agreement, and they acknowledged to me that the same is their free and voluntary act and deed, as well as the free and voluntary act and deed of the Corporations that they represent, for the uses, purposes, and considerations therein set forth.

This instrument refers to an Agreement consisting of ________ (__) pages, including this page on which the Acknowledgment is written, duly signed by the Parties and their witnesses on each and every page thereof, and sealed with my notarial seal.

WITNESS MY HAND and official seal at the place and on the date first above-written.

NOTARY PUBLIC

Doc. No. _______;
Page No. _______;
Book No. _______;
Series of 2018.

ANNEX D. PRIVACY IMPACT ASSESSMENT

PRIVACY IMPACT ASSESSMENT

This Privacy Impact Assessment ("PIA") seeks to identify the specific information flows within a Department in Megawide Construction Corporation (the "Company") and to determine the overall importance of the information flow. This allows the Company to determine the reasonable measure of data security and privacy that should accordingly be adopted. A separate PIA may be necessary for projects and processes which are found to have a significant privacy impact.

To ensure that all information flows are identified, employees of varying positions and functions within the Department should be invited to participate in the PIA.

PART I – GENERAL INFORMATION

Name of Department:			
Date:			
PIA Leader:		**Position:**	
PIA Participants/Positions: **1.** **2.** **3.** **4.** **5.** **6.** **7.** **8.** **9.** **10.**			

Description of Department

Provide a brief description of the Department concerned and its functions.

Organizational Interaction

Provide a brief description of how this Department interacts with other Departments within the Company.

PART II – THRESHOLD ANALYSIS

The Threshold Analysis seeks to identify the existing information flows within a department. The first step is to determine if any personal or sensitive personal information is processed by the Department. When answering the Threshold Analysis, do not focus only on the main or primary function of the Department; all aspects of the Department, even minor functions, should be considered.

1. **Does the Department handle any of the following information pertaining to its employees, customers, or other persons interacting with the Department? Shade the appropriate choices.**

○ Name
○ Home Addresses
○ Email Addresses
○ Business Addresses
○ Telephone Numbers
○ Age
○ Birthdays
○ Marital Status
○ Photograph
○ Biometrics
○ Color, Race, or Ethnic Origin
○ Religious Beliefs or Affiliation
○ Political Orientation
○ Sexual Orientation
○ Education
○ Health
○ History of Misdemeanors/Violations
○ TIN/SSS/Passport No./ Government IDs

2. **Does the Department handle any other information aside from the above which may be used to specifically identify an employee, customer, or other person interacting with the Department?**

____
____
____
____
____
____

3. **List down the specific projects or processes which use any of the above information. Provide a brief description of the project or process, along with which of the above information it uses. Include processes which may originate from other departments.**
Also include secondary, minor, and informal processes which may not be part of the primary purpose of the Department. All processes should be included if they handle personal information.

PART III – PROCESS-SPECIFIC FLOW ANALYSIS

All processes listed in Part II should have its own Process-Specific Flow Analysis. This analysis is necessary to determine the full extent of the information flow in a process/project.

Origin and Use of the Information

For each of the documents/information mentioned above, please answer the following questions:

1. Why does the Department need the personal information used in the process/project? What does it do with it?

2. On a scale of 1 to 5, how important is this information to the Department's function and the process/project concerned? (1 being very important and 5 not very important)

3. Where does the information originate? How is this information collected? For example, the information may have come from the employee himself in answer to an interview or a survey.

4. Does the process utilize any form of technology for collection, processing, retention, etc.?

5. Is the information shared within the Department for other processes/projects?

6. Is the information given or shared to any other department or third party? If so, for what purpose?

Access to the Information

1. Who, within the Department, has access to the information in the project/process?

____

____

____

2. Are there individuals within the Department who are not allowed access to the information? What steps are taken, if any, to ensure that access is limited?

____

____

____

3. If a person from another Department wishes to access information under the project/process, is there a procedure that must be followed?

____

____

____

Retention and Disposal

1. At what point does the process/project terminate? After the Department's process/project is completed, where is the information stored?

____

____

____

2. Can a person access the information stored even after the process/project is completed? If so, how?

____

____

____

3. How does the Department dispose of or permanently store the information? How long is it kept until disposal?

____

____

____

PART IV – PRIVACY RISK SELF-ASSESSMENT

This self-assessment seeks to determine the Department's treatment of the information and if there are existing safeguards to address privacy risks. Similar to Part III, a separate self-assessment should be conducted for each process/project.

For each of the information/document mentioned above, please answer the following questions:

1. Does the Department have any policies, whether formal or informal, which you believe protect the information under the process/project?

____

____

____

2. Taking into consideration the importance of the process and the personal information being handled, do you believe that the Department's current procedures sufficiently protect the information of the individuals? What are the risks you foresee given the current procedure?

   ____
   ____
   ____

3. Considering the purpose of the information and the function of the Department, how would a stricter policy affect the Department's operation?

   ____
   ____
   ____

4. On a scale of 1 to 5 (1 being the most secure and 5 being no security), if the information being processed was yours, what level of security do you think the Department/organization should use to protect this data considering the consequences if the information is made available to everyone? Explain your choice briefly.

   ____
   ____
   ____

ANNEX E. PRIVACY NOTICE

Privacy Notice

Megawide Construction Corporation ("Megawide") respects your right to privacy. When you interact with us, you may share Personal Data with us. Personal Data refers to information that identifies you personally, alone or in combination with other information available to us (*e.g.*, your name, contact number, e-mail address, IP address, home address, among others). To ensure that your right to privacy is protected in the course of our dealings and when we process your Personal Data, we are committed to comply with the Philippines' Data Privacy Act, its Implementing Rules and Regulations, and other relevant government regulations and issuances. This Privacy Notice outlines our data privacy principles and practices. We recommend that you read this Privacy Notice to understand how we collect, use, and process your Personal Data.

Consent

By using our website or providing us your Personal Data, you will be treated as having given your permission for our collection, use, and processing of your Personal Data, and you have accepted the policies and practices described in this Privacy Notice.

If you do not allow the collection, use, and processing of your Personal Data, kindly refrain from using our website, and/or contact us for any privacy-related concerns.

We may modify this Privacy Notice at any time. To update yourself of any change in the processing of your Personal Data, please regularly review this Privacy Notice.

Why does Megawide collect and process your Personal Data?

Megawide collects only the Personal Data needed to effectively serve you and carry out its business operations. We may collect, use, and process your Personal Data for the following general purposes:

- to conduct due diligence prior to executing a contract, and to facilitate the fulfillment of the terms of the contract thereafter;
- to respond to your queries, complaints, and requests;
- to provide information about our services;
- to conduct research and analysis to improve customer experience;
- to maintain security; and
- to comply with legal, regulatory, and contractual requirements or obligations.

The use and processing of your Personal Data also depends on your transactions with us.

If you inquire about, or avail yourself of our services, we may collect, use, or process your Personal Data to:

- conduct appropriate credit investigation to assess the risk of transacting with you;
- prepare and execute the necessary contract to cover the transaction;

- update our records and keep your contact details and billing address up-to-date; and
- communicate any advisories, changes, and other information relevant to your contract with us.

If you are a vendor/supplier, a potential vendor/supplier, or a contractor, we may collect, use, or process your Personal Data to:

- conduct the appropriate due diligence checks;
- evaluate your proposal, including your technical, financial, and operational capacity;
- assess the viability of your proposal and process your accreditation;
- communicate any decision on such proposal; and
- perform any other action as may be necessary to implement the terms and conditions of our contract.

If you want to join our workforce, we may collect, use, or process your Personal Data to:

- evaluate your suitability for employment and, with a written or expressed consent, retain your Personal Data for a maximum of five (5) years for future job opportunities that may be of interest to you;
- communicate with you about your employment application;
- when hired, process your Personal Data as may be necessary for purposes such as, but not limited to, payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand or require processing of your Personal Data (*e.g.*, to execute business transactions directly related and/or incidental to your job, business travels, socials, and so on);
- while employed, evaluate your performance and career development;
- upon separation, process your Personal Data for the exit interview and to prepare your final pay;
- provide assistance to, and account for, employees in case of emergency; and
- perform such other processing or disclosure that may be required in the course of Megawide's business or under law or regulations.

If you are a Megawide stockholder, we may use, collect, or process your Personal Data to:

- maintain and update your records with Megawide;
- administer your stock transactions; and
- comply with legal, regulatory, and contractual requirements or obligations.

If you are a visitor of Megawide or any of our project sites, we may use, collect, or process your Personal Data to:

- grant access to our premises; and
- maintain the security within our premises.

What Personal Data does Megawide collect?

Personal Data collected may include any of the following, among others:

- Your name;
- Your e-mail;
- Your other contact details;
- Your address;
- Your IP address; and/or
- Any information relevant to the feedback you have provided or the request or transaction you have made.

Further transactions with us may require the processing of your other Personal Data, such as but not limited to the following:

- financial details such as credit history, bank account, credit card, and debit card information;
- sensitive personal information, such as age, nationality, marital status, gender, health, education, and government-issued identification documents; and
- employment history.

How does Megawide collect my Personal Data?

When you access our website and/or communicate/interact with us, Megawide may collect your Personal Data and Non-Personal Data:

- *Personal Data sent to us by your web browser*

Your web browser may automatically send us Personal Data, which may include your IP address and location, or Non-Personal Data, which may include the pages you access, the operating system you use, and the name and version of your web browser. These are collected to improve your browsing experience. You may want to check your web browser to know more about the Personal Data sent to us by your web browser, and to modify your web browser settings as you see fit.

- *Personal Data collected by placing a cookie on your computer*

We may also obtain information about you by placing a cookie on your computer. This is typically done to ease navigation through our website. Cookies that may be used are of two kinds — session cookie and persistent cookie. A session cookie is used to place on your computer a computer-generated, unique identifier whenever you access our website. It does not identify you personally and expires as soon as you close your web browser. A persistent cookie does not expire when you close your browser, and stays on your computer, unless you delete it.

If you do not wish to receive cookies, you may modify your web browser settings to turn them off or delete them from your computer. If you reject our cookies, however, our website may not function properly.

- *Personal Data you knowingly and voluntarily provide*

We may also process the Personal Data you knowingly and voluntarily provide when you contact us. The Personal Data you provide will then be used to provide the service you requested. For instance, when you e-mail us a query, necessarily, we will collect your name and e-mail address to respond to you.

Why does Megawide collect and process your Personal Data?

Megawide collects only the Personal Data we need to effectively serve you. We may also use the Personal Data collected for various purposes such as customer service, investor relations, market research, and business development. We may use the Personal Data collected to respond to your queries, to process your requests and applications, to create services that will respond to your needs, and to otherwise carry out our business operations.

Where does Megawide store your Personal Data?

Your Personal Data is controlled by Megawide Construction Corporation, a company registered under Philippine laws, whose principal office is at 20 N. Domingo Street, Barangay Valencia, Quezon City, Philippines 1112.

For how long does Megawide retain your Personal Data?

Megawide will retain your Personal Data for as long as necessary to fulfill the purposes outlined in this Privacy Notice and communicated to you, unless a longer period is allowed or required by law.

To whom are your Personal Data disclosed?

Megawide will not disclose your Personal Data to third parties without your consent. It may however share your Personal Data to its other business units. In such cases, your Personal Data will be used in a manner consistent with the purpose for which it was originally collected and to which you consented, and the Data Privacy Act, its Implementing Rules and Regulations, and all relevant regulations and issuances on privacy and data protection.

We may also share your Personal Data with third parties who perform services for us. Under such circumstances, we require our service providers to limit the use of the Personal Data we share with them in a manner consistent with the purpose for which it was originally collected and to which you consented, and the Data Privacy Act, its Implementing Rules and Regulations, and all relevant regulations and issuances on privacy and data protection. Our service providers will not process your Personal Data for any other purpose than what we have agreed with them.

We may also share your Personal Data to unrelated third parties, upon your request, when we are legally required to do so, or when we believe it is necessary to protect and/or defend our rights, property, or safety, and those of other individuals. Nevertheless, we will take all the necessary steps to protect your Personal Data.

ANNEX F. DATA PROTECTION OFFICER

The DPO of Megawide may be reached through the following:

Name:	Atty. Raymund Jay S. Gomez
Postal Address:	20 N. Domingo Street, Barangay Valencia Quezon City 1112
Telephone Number:	+632 6551111
E-mail Address:	rgomez@megawide.com.ph

ANNEX G. COMPLIANCE OFFICER FOR PRIVACY

The COP of Megawide may be reached through the following:

Name:	
Postal Address:	20 N. Domingo Street, Barangay Valencia Quezon City 1112
Telephone Number:	+632 6551111
E-mail Address:	atopacio@megawide.com.ph

ANNEX H. DATA PRIVACY RIGHT FORM

Data Privacy Right Form

Note: *A Data Subject who seeks to access and/or modify his/her Personal Data with the Company shall accomplish this Data Privacy Right Form. The Data Privacy Right Form may be filed with the Authorized Personnel previously dealt with by the Data Subject as processor of his/her Personal Data. The Authorized Personnel shall then endorse the same to the* ***Compliance Officer for Privacy (COP)*** *for the branch, sub-office, component unit, or department concerned, or in his absence, the* ***Head*** *of such branch, sub-office, component unit, or department, who must in turn determine the reasonableness of the exercise of the right. If found reasonable, the COP, if any, or the head of such branch, sub-office, component unit, or department shall approve and transmit the same to the branch, sub-office, component unit, or department concerned for implementation.*

Data Subject Information	
Name:	
Company Position, if any:	
E-mail:	
Contact Number:	
To prove my identity, I hereby enclose the following competent evidence of identity:	□ Company ID □ Driver's License □ Passport □ Others, please specify: ________________________
Description of Relevant Personal Data	
Description of the Relevant Personal Data:	
Date or period around which Personal Data was collected, if known:	
Name of the Department or Company Employee which/who processed the Personal Data, if known:	
Nature of Right to be Exercised	
I would like to exercise the following rights with respect to the above-described Personal Data: □ the right to be informed whether you hold my Personal Data □ the right to be furnished a copy of the Personal Data being processed by the Company □ the right to object to the processing of my Personal Data □ the right to reasonable access to my Personal Data □ the right to dispute the inaccuracy or error in my Personal Data □ the right to suspend, withdraw, or order the blocking, removal, or destruction of my Personal Data □ the right to obtain from the Company a copy of my Personal Data	

Further instructions/requests, if any:

____

____

____

____

____

____

____

Preferred Manner of Compliance

I would prefer that you:

- ☐ Send me a paper-based/physical copy of the Updated/Requested Personal Data through the following address: ____________________________________
- ☐ E-mail me an electronic copy of the Updated/Requested Personal Data through the following: __________________________________
- ☐ Others, please specify:
  ____

Signature

I hereby attest that all information stated in this form are all true and correct to the best of my knowledge. Any concealment, false statement, and/or non-declaration shall constitute fraud, which shall be ground to file a legal action against me; I therefore waive my rights to institute any case arising from this situation.

I have provided the information herein after having been informed of the purpose for its processing, and I expressly give my consent therefor. I understand that it is my choice as to what information I provide and that withholding or falsifying information may act against the best interests of my relationship with the Company. I am aware that I can access my personal information on request, and if necessary, correct information that I believe to be inaccurate. I understand that if, in exceptional circumstances, access is denied for legitimate purposes, I will be informed of the cause thereof and the remedies for the same.

Furthermore, I warrant that I have: (i) obtained consent from the third parties mentioned above, if any, to disclose their information included in this form; and (ii) informed said third parties of the purpose for the disclosure and collection of information. I agree to indemnify and hold the Company free and harmless from any and all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, if any.

This consent for the Company to use or process the information herein shall be valid for the duration of my relationship and/or contract with the Company and for thirty (30) years thereafter, to comply with statutory and governmental rules and regulations.

____
Signature over Printed Name of Data Subject

ANNEX I. CONSENT FORM

Processing of Personal Data
Consent Form

I hereby attest that all information stated in this form are true and correct to the best of my knowledge. I understand that any concealment, false statement, and/or non-declaration shall constitute fraud, which shall be a ground to file legal action against me, and I waive my rights to institute any case arising from this situation.

I have provided the information herein after having been informed of the purpose for its processing, and I expressly give my consent therefor. I understand that it is my choice as to what information I provide and that the withholding or falsifying of information may act against the best interests of my relationship with the Company. I am aware that I can access my personal information on request, and if necessary, correct information that I believe to be inaccurate. I understand that if, in exceptional circumstances, access is denied for legitimate purposes, I will be informed of the cause thereof and the remedies for the same.

Furthermore, I warrant that I have: (i) obtained consent from third persons, if any, to disclose their information included in this form; and (ii) informed said third persons of the purpose for the disclosure and collection of information. I will indemnify and hold the Company free and harmless from any and all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, if any.

This consent for the Company to use or process the information herein shall be valid for the duration of my relationship and/or contract with the Company and for thirty (30) years thereafter, to comply with statutory and governmental rules and regulations.

____
Signature over Printed Name

ANNEX J. ACCESS REQUEST FORM

Access Request Form

Note: *Any person, including an employee who is not an Authorized Personnel but wishes to access Personal Data of Data Subjects pursuant to his/her function in the Company, shall accomplish this Access Request Form. Verbal request for access shall not be allowed. The Access Request Form may be filed with the Authorized Personnel who has custody of the Personal Data to be accessed. The Authorized Personnel may either approve or reject the same, depending on the merits of the reasons provided for the requested access. In no case shall access be approved if no meritorious reason is provided in the Access Request Form. If approved, the Authorized Personnel shall endorse for final approval the Access Request Form to the* ***Compliance Officer for Privacy (COP)*** *for the branch, sub-office, component unit, or department concerned, or in the absence of a COP, the* ***Head*** *of such branch, sub-office, component unit, or department. Once approved, the Access Request Form shall be transmitted to the branch, sub-office, component unit, or department concerned for implementation.*

Requestor Information	
Name:	
Company Position, if any:	
E-mail:	
Contact Number:	
Purpose of Request:	
As proof of my capacity to access the Personal Data, I hereby enclose:	□ Birth certificate, to prove filiation □ Court order □ Written authorization from Data Subject □ Others, please specify: ____________________________________
Requested Personal Data	
To whom Personal Data pertains to (i.e., name of Data Subject):	
Description of the Requested Personal Data:	
Date or period around which Personal Data was collected, if known:	
Name of the Department or Company Employee which/who processed the Personal Data, if known:	
Nature of Request	
I hereby request you to: □ Inform me whether you hold the Requested Personal Data □ Supply me a copy of the Requested Personal Data that you hold	

□ All of the above

Preferred Manner of Addressing the Request

I would prefer that you:

□ Send me a paper-based/physical copy of the Requested Personal Data through the following address:

____

____

□ E-mail me an electronic copy of the Requested Personal Data through the following:

____

□ Others, please specify:

____

Signature

I hereby attest that all information stated in this form are true and correct to the best of my knowledge. I understand that any concealment, false statement, and/or non-declaration shall constitute fraud, which shall be a ground to file legal action against me, and I waive my rights to institute any case arising from this situation.

I have provided the information herein after having been informed of the purpose for its processing, and I expressly give my consent therefor. I understand that it is my choice as to what information I provide and that withholding or falsifying information may act against the best interests of my relationship with the Company. I am aware that I can access my personal information on request, and if necessary, correct information that I believe to be inaccurate. I understand that if, in exceptional circumstances, access is denied for legitimate purposes, I will be informed of the cause thereof and the remedies for the same.

Furthermore, I warrant that I have: (i) obtained consent from third persons, if any, to disclose their information included in this form; and (ii) informed said third persons of the purpose for the disclosure and collection of information. I will indemnify and hold the Company free and harmless from any and all claims arising from the breach of this warranty, for damages, and for actual legal fees to defend such claims, if any.

This consent for the Company to use or process the information herein shall be valid for the duration of my relationship and/or contract with the Company and for thirty (30) years thereafter, to comply with statutory and governmental rules and regulations.

____

____

Signature over Printed Name of Requestor

ANNEX K. DATA PRIVACY TRACKER

The *Data Privacy Tracker* is a log of all privacy-related incident/s, complaint/s and/or request/s from Data Subjects, access request/s, as well as a list of all Data Sharing and Outsourcing Agreements entered into by the Company.

PRIVACY-RELATED INCIDENTS LOG				
Date of Incident	**Type of Security Incident** (*e.g.*, denial of service, malware, theft of data or physical asset, alteration of data, etc.)	**Incident Count**	**Number of Data Subjects Affected**	**Description of the Security Incident and Chronology of Events**[1]

COMPLAINTS LOG			
Date of Complaint	**Data Subject**	**Nature and Description of Complaint**	**Action Taken by the Company**

EXERCISE OF DATA PRIVACY RIGHT LOG			
Date of Request	**Data Subject**	**Nature and Description of the Data Privacy Right Invoked**	**Action Taken by the Company**

[1] The **Description of the Security Incident** must include the (1) measures undertaken by the Company to address the incident; (2) assistance provided to Data Subjects Affected; (3) outcome; and (4) compliance with the notification requirement under the Data Privacy Manual, if applicable.

ACCESS REQUEST LOG

Date of Request	Name of Requestor	Data Subject	Nature and Description of the Access Request	Action Taken by the Company

DATA SHARING AGREEMENTS

Date of Execution	Effectivity/Term	Counterparty	Purpose of the Agreement and Personal Data Processed Under the Agreement

OUTSOURCING AGREEMENTS

Date of Execution	Effectivity/Term	Processor	Nature of Service	Purpose	Personal Data Processed

ANNEX L. ANNUAL SECURITY INCIDENT REPORT FORM

Annual Security Incidents and Breach Report

PERIOD: JANUARY ________ TO DECEMBER __________	Total
Total Number of Security Incidents and Personal Data Breach	
▪ SECURITY INCIDENTS (NOT AMOUNTING TO A PERSONAL DATA BREACH)	
▪ PERSONAL DATA BREACH	
• Personal Data Breach Mandatory Notification	
• Other Personal Data Breach (Notification Not Required)	

SECURITY INCIDENTS (HOW OCCURRED)		Total	
Types	**No. of Incidents**	**Types**	**No. of Incidents**
□ Theft		□ Communication Failure	
□ Fraud		□ Fire	
□ Sabotage/Physical Damage		□ Flood	
□ Malicious Code		□ Design Error	
□ Hacking/Logical Infiltration		□ User Error	
□ Misuse of Resources		□ Operations Error	
□ Hardware Failure		□ Software Maintenance Error	
□ Software Failure		□ Third Party Services	
□ Hardware Maintenance Error		□ Others	

PERSONAL DATA BREACH				
	Confidentiality Breach	**Integrity Breach**	**Availability Breach**	**Total**
Mandatory Reporting Required				
Mandatory Reporting Not Required				
Total				

PREPARED BY:
DESIGNATION:
DATE:

Summary Report of Security Incidents Amounting to a Personal Data Breach not covered by mandatory notification requirements

Personal Data Breach No. <#>
<NAME OF DATA PROCESSING SYSTEM>
<DATE>

Facts
<Who are the main people responsible>
<What are the events surrounding the breach?>
<Where was the data located, stored, or otherwise processed?>
<When did the data breach happen?>
<How was the breach detected?>
<Why did the data breach happen?>

Effects/Consequences
<What were the effects or consequences of the data breach?>
<How was the data affected?>
<Who were the data subjects affected?>
<How were the data subjects affected?>
<How long did it take to affect the data subjects?>

Remedies/Action Taken
<How long did it take to resolve the matter?>
<Who took charge in the remedial effort?>
<What actions were taken by such persons in charge?>
<When was the situation completely resolved?>
<What measures did the PIC take to ensure the data breach does not happen again.

ANNEX M. CONFIDENTIALITY CLAUSE

“At all times during the term of my employment with the Company and thereafter, I shall hold in strictest confidence and will not disclose, use, or publish any of the Company’s Confidential Information, as well as any of the Personal Data collected and processed by the Company in the course of its key business operations and processes, except as such disclosure, use, or publication may be required in connection with my employment with the Company, or unless expressly authorized by specific Company resolution. In case of disclosure, use, or publication, I shall be responsible for any violation of this Agreement by the person or entity I have disclosed the Confidential Information and/or Personal Data to.

I shall use all reasonable efforts to preserve the secrecy and confidentiality of the Confidential Information and/or Personal Data, and to prevent such Confidential Information and/or Personal Data from falling into the public domain or possession of persons other than those authorized to have such information, including implementation of reasonable security measures and operating procedures. In addition, I undertake to immediately notify the Company in writing of any misuse or misappropriation of the Confidential Information and/or Personal Data which may come to my attention.”

ANNEX N. NON-DISCLOSURE AGREEMENT

Non-Disclosure Agreement
("Agreement")

In consideration of my employment or continued employment in **Megawide Construction Corporation** (hereinafter referred to as the "Company"), I hereby agree as follows:

(1) **Non-disclosure**

At all times during the term of my employment with the Company and thereafter, I shall hold in strictest confidence and will not disclose, use, or publish any of the Company's Confidential Information, as well as any of the Personal Data collected and processed by the Company in the course of its key business operations and processes, except as such disclosure, use, or publication may be required in connection with my employment with the Company, or unless expressly authorized by specific Company resolution. In case of disclosure, use, or publication, I shall be responsible for any violation of this Agreement by the person or entity I have disclosed the Confidential Information and/or Personal Data to.

I shall use all reasonable efforts to preserve the secrecy and confidentiality of the Confidential Information and to prevent such Confidential Information and/or Personal Data from falling into the public domain or possession of persons other than those authorized hereunder to have such information, including implementation of reasonable security measures and operating procedures. In addition, I undertake to immediately notify the Company in writing of any misuse or misappropriation of the Confidential Information and/or Personal Data which may come to my attention.

"**Confidential Information**" means information or material that is valuable to the Company and not generally known or readily ascertainable in the industry. It may be written, oral, expressed in electronic media, or otherwise disclosed, and may be tangible or intangible. This includes, but is not limited to:

(a) information concerning the Company's products and services;

(b) information concerning the Company's operation and marketing, including trade secrets, consolidated business services, cost information, accounting and unpublished financial information, and other information relating to the internal activities of Company, and generally all records, documents, and information pertaining to the Company's affairs and any other information received or prepared due to one's employment with Company;

(c) information concerning the Company's clients, suppliers, and employees; and

(d) any other information not generally known to the public which, if misused or disclosed, may reasonably be expected to adversely affect the Company.

All materials and information acquired in the course of, or with a view to, employment is presumed Confidential Information. Notwithstanding the unauthorized disclosure of Confidential Information, the intellectual property rights pertaining thereto remain to be the sole property of the Company.

"**Personal Data**" refers to all types of Personal Information, including Sensitive Personal Information, collected and processed by the Company. Personal Data may be classified as follows:

(a) "**Confidential Personal Data**" pertains to all other information to which access is restricted, and of which Processing requires the written consent of the individual concerned, such as but not limited to Employee 201 files and information contained therein, device passwords and/or passcodes, bank account numbers, ATM card numbers, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

(b) "**Public Personal Data**" pertains to Personal Information of individuals which may be disclosed to the public by the Company due to, or as required by, its business operations, and for government regulatory compliance and company disclosures.

"**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:

(a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political 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 government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension, or revocation, and tax returns; and

(d) specifically established by an executive order or an act of Congress to be kept classified.

(2) Return of Company Documents

Upon expiration of my employment contract with the Company, I will deliver to it any and all notes, memoranda, storage media, including software, documents, and computer printouts, together with all copies thereof, and any other material containing Confidential Information and/or Personal Data. I further agree that any property situated in the Company's premises and owned by the Company, including disks, flash drives, and other storage media, filing cabinets or other work areas, will be subject to the Company's inspection at any time, with or without notice.

I shall not reverse engineer or reverse compile, whether to determine content or manner of production, refine, or customize, in any way whatsoever, all or any part of the Confidential Information and/or Personal Data without the Company's prior written consent, nor shall I copy, reproduce in any form, or store in any retrieval system or database any Confidential Information and/or Personal Data without the prior written consent of the Company, except for such copies and storage as are strictly required by the Company.

(3) Remedies

Any unauthorized disclosure of the Confidential Information and/or Personal Data will result in the immediate termination of my employment with the Company. The Company shall have the right to enforce this Agreement and any of its provisions by injunction, specific performance, or other equitable relief, without bond, without prejudice to any other rights and remedies that the Company may have in case of breach of this Agreement.

In the event the Company is compelled to seek judicial relief in order to enforce its rights under this Agreement, I, in addition to damages that may be awarded by the Court and without prejudice to any criminal and civil proceeding which may arise due to violation of the terms of the Agreement, hereby agree to pay ₱500,000.00 as liquidated damages, and ₱50,000.00 as and by way of attorney's fees, aside from the costs of litigation and other expenses which the Company may be entitled to.

All actions arising from any breach of this Agreement shall be filed in the appropriate courts of Quezon City, to the exclusion of all other courts of equal jurisdiction.

(4) Entire Agreement

This Agreement contains the entire agreement between the parties with respect to the subject matter hereof and supersedes and merges all prior discussions between us. No amendment, interpretation, or waiver of any of the provisions of this Agreement shall be effective, unless made in writing. Any subsequent modifications in my duties and responsibilities will not affect the validity or scope of this Agreement.

(5) Separability Clause

Should any provision of this Agreement be declared void or unenforceable by any competent authority or court, then the remaining provisions will continue in full force and effect.

(6) Non-waiver

No waiver by the Company of any breach of this Agreement shall be a waiver of any preceding or succeeding breach. No waiver by the Company of any right under this Agreement shall be construed as a waiver of any other right. The Company shall not be required to give notice to enforce strict adherence to all terms of this Agreement.

I agree and understand that nothing in this Agreement shall confer on me any right with respect to continuation of my employment with the Company, nor shall it interfere in any way with the Company's right to terminate my employment.

(7) Effectivity

This Agreement will be binding upon my heirs, executors, administrators, agents, and other legal representatives, and will be for the benefit of the Company, its successors, and its assigns. I cannot assign my obligations under this Agreement without the prior written consent of the Company.

This Agreement shall be effective as of the first day of my employment with the Company and shall survive the termination of my employment.

(8) Governing Law

The laws of the Philippines shall govern the validity of this Agreement, the construction of its terms, and the interpretation and enforcement of the rights and duties of the parties.

IN WITNESS WHEREOF, this Agreement has been executed this __ day of ____________ 201_ at _________________.

____
Signature over Printed Name
Date:
____

Noted by:

____

President
Megawide Construction Corporation

SUBSCRIBED AND SWORN to this _____ day of __________ 201_ at __________, affiant exhibiting to me his/her Community Tax Certificate No. __________ issued on __________ at __________ and Government ID ________________ as his/her competent evidence of identity.

Doc. No. ____;
Page No. ____;
Book No. ____;
Series of 201_.

ANNEX O. DATA PRIVACY PROTECTION CLAUSE

Data Privacy Protection Clause

"**DATA PRIVACY PROTECTION.** The [INDIVIDUAL VENDOR/SUPPLIER/SUBCONTRACTOR/STOCKHOLDER] agrees and consents to the collection, recording, organization, storage, updating or modification, retrieval, use, consolidation, retention, and other means of processing of his personal data, such as but not limited to, his name, home address, e-mail address, business address, telephone numbers, age, birthday, marital status, photograph, TIN, SSS, HDMF, Passport, and such other government-issued identification, by MEGAWIDE for the purpose of executing this Agreement, [particular purpose/s], and such other purposes as will give effect to this Agreement. The [INDIVIDUAL VENDOR/SUPPLIER/SUBCONTRACTOR/STOCKHOLDER] agrees that he has the choice as to what information he provides, and that the withholding or falsifying of information may act against the best interest of this Agreement and his relationship with MEGAWIDE. The [INDIVIDUAL VENDOR/SUPPLIER/SUBCONTRACTOR/STOCKHOLDER]'s consent for MEGAWIDE to collect, record, organize, store, update or modify, retrieve, use, consolidate, retain, and otherwise process the personal data of the [INDIVIDUAL VENDOR/SUPPLIER/SUBCONTRACTOR/STOCKHOLDER] shall be valid for the duration of this Agreement and for thirty (30) years thereafter or until the purpose for which this Agreement was executed has been achieved, whichever is later."

ANNEX P. DATA PRIVACY RESPONSE TEAM

Data Privacy Response Team

The Data Privacy Response Team of Megawide may be reached through the following:

Postal Address:	20 N. Domingo Street, Barangay Valencia Quezon City 1112
Telephone Number:	+632 6551111
E-mail Addresses:	

ANNEX Q. MANDATORY PERSONAL DATA BREACH NOTIFICATION TO DATA SUBJECTS

Megawide Construction Corporation
20 N. Domingo, Brgy. Valencia, Quezon City

<DATE>

<DATA SUBJECT>
<ADDRESS>

Subject: <DATA BREACH> dated <DATE>
<NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of MEGAWIDE CONSTRUCTION CORPORATION, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>.

Nature of the Breach

- *Provide a summary of the events that led up to the loss of control over the data.*
- *Describe the likely consequences of the personal data breach.*

Measures taken to Address the Breach.

- *Provide information on measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.*
- *Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.*
- *Describe steps the organization has taken prevent a recurrence of the incident.*

Measures taken to reduce the harm or negative consequences of the breach.

- *Describe actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.*

Assistance to be provided to the affected data subjects.

- *Include information on any assistance to be given to affected individuals.*

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer Raymund Jay S. Gomez
20 N. Domingo, Barangay Valencia, Quezon City
rgomez@megawide.com.ph
+632 6551111

We commit to provide more information to you as soon as possible, as they become available, with our best efforts.

Sincerely,
MEGAWIDE CONSTRUCTION CORPORATION

RAYMUND JAY GOMEZ
DATA PROTECTION OFFICER

ANNEX R. MANDATORY NOTIFICATION OF PERSONAL DATA BREACH FOR THE NATIONAL PRIVACY COMMISSION

Megawide Construction Corporation
20 N. Domingo, Brgy. Valencia, Quezon City

<DATE>

Chairman Raymund Liboro
National Privacy Commission
Pasay City, Metro Manila Philippines

Subject: <DATA BREACH> dated <DATE> of <DATABASE>
<NPC REGISTRATION NO.>

Gentlemen:

I write in behalf of MEGAWIDE CONSTRUCTION CORPORATION, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of MEGAWIDE CONSTRUCTION CORPORATION and the responsible persons thereof, are as follows:

Head of the Organization

EDGAR B. SAAVEDRA
President
20 N. Domingo, Brgy. Valencia, Quezon City
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFO>

Data Protection Officer

RAYMUND JAY S. GOMEZ
20 N. Domingo, Brgy. Valencia, Quezon City
rgomez@megawide.com.ph
+632 6551111

Process Owner

<NAME>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>
<TELEPHONE>
<OTHER CONTACT INFO>

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- *Describe the nature of the personal data breach.*

Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.

- *Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.*

- *Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.*
- *Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.*
- *Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.*
- *Describe the likely consequences of the personal data breach. Consider effect on company or agency, data subjects and public.*

Personal Data Possibly Involved.

- *List all sensitive personal information involved, and the form in which they are stored or contained.*
- *Also list all other information involved that may be used to enable identity fraud.*

Measures taken to Address the Breach.

- *Describe in full the measures that were taken or proposed to be taken to address the breach.*
- *Describe how effective these measures are.*
- *Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.*
- *Indicate actions of the organization to minimize/mitigate the effect on the affected individual. Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.*
- *Indicate of the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.*
- *Describe the steps the organization has taken to prevent a recurrence of the incident.*

Should you require further information on this matter, contact us using the information above. Any information that is indicated as unavailable at this time will be determined and reported within five (5) days, or as soon as possible, as they become available.

Sincerely,
MEGAWIDE CONSTRUCTION CORPORATION

RAYMUND JAY GOMEZ
DATA PROTECTION OFFICER