A BROWN COMPANY, INC.

DATA PRIVACY MANUAL

TABLE OF CONTENTS

PREFACE

A BROWN COMPANY, INC. (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 was 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 and private sector, which 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.

"**Compliance Officer for Privacy**" or "**COP**" refers to an individual duly authorized by the Company to perform some of the DPO's functions 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 implementing this Manual.

"**Data Processing Systems**" refers to 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, 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.

"**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 be in substantially the same 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 clients, employees (whether probationary, regular, casual, or project), members of the Board of Directors, consultants, employees, trainees, applicants, stockholders, partners, suppliers, subcontractors, service providers, office visitors, and other persons whose information 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 for the latter's Processing upon the instructions of the Company.

"**Outsourcing Agreement**" refers to any written contract entered into by the Company with a Personal Information Processor, 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 substantially the same form as that prescribed in Annex "C."

"**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**" pertain 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 passcode, 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**" pertain 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 pertaining to a Data Subject. The Company's service providers, if any, are PIP/s.

"**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 "D" 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 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.

"**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

The 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 PIPs, 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 and its employees and PIPs 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 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

Upon 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 "E."

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.

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 COPs of the Company, if any, shall be provided in Annex "F."

SECTION 3. GENERAL QUALIFICATIONS

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

SECTION 4. TERM

The DPO and the COP/s, if any, 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, 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 DPO or COP.

SECTION 6. FUNCTIONS OF THE DPO AND/OR COP

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

(a) monitor the Company's compliance with the Data Privacy Act, its IRR, issuances of the Commission, and other applicable laws and policies. For such purpose, the DPO and/or COP 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 a 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 him/her as the DPO 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, if any, of the Company may perform any of the functions of the DPO, except items (a), (b), and (c) above. Where appropriate, the COP/s, if any, shall assist the DPO in the performance of the latter's functions.

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

The Company may outsource the functions of the DPO and/or COP, if any, provided that the DPO and/or COP, 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 their Personal Data. The Company's employees and PIP/s, as the case may be, shall respect the Rights of the Data Subjects. To exercise said rights, the Data Subject may accomplish the Data Privacy Right Form prescribed in Annex "G," indicating therein the right he/she wishes to exercise with respect to his/her Personal Data and transmit the same to the Company through the latter's Authorized Personnel.

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 practical 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, 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., for the Company to assess the qualification of an applicant or the suitability of a current employee for promotion/transfer, it may require information as regards the applicant's educational attainment); or

(c) the Personal Data is being collected and processed pursuant to a legal obligation (e.g., for the Company 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 reasonable access to, upon demand, 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. Recipient/s 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; and

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

(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/s prescribed in Annex "D." In any case, the Company's Authorized Personnel, shall verbally 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 "H." Consent 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.

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 purposes, among others:

(a) for documentation and management of Company records;

(b) for business transactions and billings;

(c) for the Data Subject, particularly employees, to have access to the Information and Communications System/s and/or Filing System/s of the Company; and/or

(d) for the maintenance of safety and security.

The purpose/s of the Use and Processing of Personal Data per Data Processing System shall be laid down in Annex "A" on Data Processing Systems.

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 "G," from the Data Subject, provided that such request is not vexatious and/or unreasonable.

SECTION 3. RETENTION

3.1 **General.** Personal Data shall be stored only 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, and secure filing rooms. Where necessary to further its business and to keep its security software tools up to date, the Company reserves the right to change 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.** Only Authorized Personnel of the Company 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 **Data Privacy Right Form.** 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 "G." 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 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.

4.2.2 **Access Request Form.** 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 "I" 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 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.

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 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 the legal counsel of the Company, if any.

4.2.5 **Security of Access.** Whenever Authorized Personnel, Employees of the Company, whether Authorized Personnel or not, and PIPs 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 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 legal counsel of the Company, if any.

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 "H." 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 PICs 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, 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.** Personal Data in the custody of the Company may be in digital/electronic format and 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.** 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 access the Filing System/s 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 Incidents.

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. 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, through its IT Department or PIP, shall conduct periodic log review and analysis.

2.1.2 The Company shall cause the monitoring of its Information and Communications System/s through the employment of File Integrity Monitoring (FIM).

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 to all devices, including tablets and smartphones that regularly access the Internet. The COPs, 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 (WAF) to protect its servers and databases from malicious online attacks.

2.2.3 To ensure compatibility and data security, the COPs, if any, and/or the heads of branches, sub-offices, component units, and departments shall first review and evaluate software applications 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, shall notify the end user of such risk and the software application shall immediately be uninstalled. A Security Incident Report, in the form prescribed in Annex "J," shall be prepared when necessary.

2.4 **Encryption, Authentication, and Other Technical Security Measures**

2.4.1 **Encryption.** 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 shall 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 COPs, 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.

3.4 **Confidentiality Clauses and/or Non-Disclosure Agreements.** A confidentiality clause substantially in the form prescribed in Annex "K" 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 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 "L" hereof, may be executed by the Company to protect confidential information given to an employee or any other party.

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 all COPs of the Company as members, or a team of five (5) members from the PIP/s contracted by the Company for said purpose, shall be constituted, which shall be responsible for ensuring immediate action in the event of a Security Incident or Personal Data Breach. The DPO shall lead the Data Privacy Response Team.

SECTION 2. DUTIES OF THE DATA PRIVACY RESPONSE TEAM

The Data Privacy Response Team shall, among others:

(a) ensure the implementation of the privacy and data protection policy of the Company;

(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 prepare a detailed documentation of every Security Incident encountered, to be submitted to the Company's Management. The Report 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. The Report shall substantially be in the form prescribed in Annex "J" hereof, unless the Commission prescribes its official template for the same, in which case, the latter shall be used.

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.

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 involves:

(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. 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 "G." 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 "I."

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 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 cases 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 5 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 shall take effect on 5 April 2018, until revoked or amended by the Company.

Approved by:

ROBERTINO E. PIZARRO
Chairman of the Board

ELPIDIO M. PARAS
Chairman of the Risk Committee

ANNEXES

ANNEX A. DATA PROCESSING SYSTEMS

DPS Name:	**SALES AND MARKETING 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 Sales and Marketing Department manages the Sales and Marketing Processing System (the "System"). The System helps the Company in promoting its products and services and in closing deals and agreements with clients, lot owners, and homeowners. The Sales and Marketing Department uses the System to maintain records of clients and their Personal Data, document transactions, provide assistance to clients, and answer their queries. The Personal Data of clients are collected by asking them to fill out the Personal Information Sheets requesting the following Personal Data: (1) Full Name; (2) Home Address; (3) E-mail Address; (4) Business Address; (5) Telephone Numbers; (6) Age; (7) Birthday; (8) Marital Status; (9) Photograph; (10) TIN; (11) SSS; (14) Passport Numbers; and (15) Other Government IDs. Personal Data collected are encoded into the System. The Personal Data collected and processed by the Sales and Marketing Department are used by the Collection Department to know where to mail written communications and by the Compliance Department for bank financing, Pag-IBIG financing, and processing of transfer of titles, among others. The Personal Data collected are also used for the remittance of withheld taxes to the Bureau of Internal Revenue. The Personal Data collected and processed may be accessed by Authorized Personnel only, and upon request, by clients. The physical documents are stored in a secured filing room, while the electronic documents are stored in secured computer devices.	
Whether the Processing of Personal Data is subcontracted or outsourced:	No.	
Details of PIP, if any:	**Is there a subcontracting or outsourcing agreement?**	N/A
	PIP Name:	N/A
	PIP E-mail:	N/A
	PIP Address:	N/A
	PIP Contact Number/Extension Number:	N/A
	PIP Description/Purpose:	N/A
Whether the Personal Data is shared outside of the Philippines:	No.	
Categories of Data Subjects:	Clients (lot buyers/owners, home buyers/owners)	

To whom Personal Data will be disclosed (provide the type of organization – whether public or private, and name of organization):	Bureau of Internal Revenue (public) Pag-IBIG (public) Registry of Deeds (public) Bank/s (private) Other regulatory government agencies

DPS Name:	**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 Human Resources (HR) Department manages the Human Resources Data Processing System (the "System"). The Human Resources Department is in charge of staffing, managing and developing talent, managing the Company's compensation system and pay programs, responding to workplace concerns, and managing employee and labor relations. To perform its functions, the HR Department uses the System to collect and process Personal Data from employees, which include the following: (1) Name; (2) Home Address; (3) E-mail Address; (4) Business Address; (5) Telephone Numbers; (6) Age; (7) Birthday; (8) Marital Status; (9) Photograph; (10) Biometrics; (11) Religious Beliefs/Affiliations; (12) Education; (13) Health; (14) History of misdemeanors/violations; (15) TIN, SSS, Passport No., Government IDs; (16) Name and Birthdates of Spouse and Children, if any. The Personal Data are collected from employees and applicants through interviews and forms filled out during the pre-employment process. Employees are also asked to update the Personal Data kept by the HR Department. The Personal Data are processed for any of the following purposes: (1) To assess the qualifications of the applicants and suitability for the job applied for; (2) To create, update, and/or maintain the 201 files of employees; (3) To have readily accessible information on employees when requested or needed by different departments within the Company;

	(4) To comply with government requirements, such as SSS, PhilHealth, and Pag-IBIG contributions, remittance of taxes, updating of records; and (5) To assist the employees in availing themselves of HMO services. The Personal Data processed by the HR Department may be accessed by Authorized Personnel only. While the Payroll Unit of the Company has exclusive access to biometrics, all other employees who wish to access the Personal Data collected must seek the approval of the HR Department Head. Electronic documents bearing the Personal Data processed are kept in computers and applications that are password-protected, while physical documents bearing the Personal Data are kept in a secured filing room, which may be accessed by Authorized Personnel only.	
Whether the Processing of Personal Data is subcontracted or outsourced:	No.	
Details of PIP, if any:	**Is there a subcontracting or outsourcing agreement?**	N/A
	PIP Name:	N/A
	PIP E-mail:	N/A
	PIP Address:	N/A
	PIP Contact Number/Extension Number:	N/A
	PIP Description/Purpose:	N/A
Whether the Personal Data is shared outside of the Philippines:	No.	
Categories of Data Subjects:	Applicants, employees (previous and current)	
To whom Personal Data will be disclosed (provide the type of organization – whether public or private, and name of organization):	Asalus Corporation (Intellicare) (private); Bureau of Internal Revenue (public); SSS (public); Pag-IBIG (public); PhilHealth (public).	

DPS Name:	**INVESTOR RELATIONS 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 Investor Relations Data Processing System (the "System") is used to provide the Company's stockholders and prospective investors of an accurate account of the Company's business, particularly its operations, finances, major business decisions, and other developments. It is also used to prepare and file

	the necessary reports and disclosures to the Philippine Stock Exchange (PSE) and Securities and Exchange Commission (SEC), in compliance with the Securities Regulation Code, and SEC and PSE rules and regulations. The System is managed by the Compliance Officer, Accountant, and Administrative Assistant of the Company ("Authorized Personnel"). The Personal Data collected and processed under this System are the following: (1) Name; (2) Home Address; (3) TIN; and (4) Stockholder Number. Said Personal Data are obtained by the Authorized Personnel from the Stock and Transfer Agent of the Company, Professional Stock Transfer, Inc. The electronic documents bearing the Personal Data collected are stored in password-protected computer devices in the Company premises, while the physical documents bearing the Personal Data are kept in locked filing cabinets. The Personal Data are used by the Company to send out notices for stockholders' meetings, and in cases of dividend distribution, or when necessary for compliance with laws and the rules and regulations of PSE and/or SEC. Only Authorized Personnel may access the Personal Data, and if any other individual would like to access the Personal Data, approval of the Compliance Officer is required.	
Whether the Processing of Personal Data is subcontracted or outsourced:	Yes	
Details of PIP, if any:	**Is there a subcontracting or outsourcing agreement?**	Yes
	PIP Name:	Professional Stock Transfer, Inc.
	PIP E-mail:	profstocktransferinc@gmail.com
	PIP Address:	10F Telecom Plaza Building 316 Senator Gil Puyat Avenue, Makati City
	PIP Contact Number/Extension Number:	(632) 6874053 or 8016123
	PIP Description/Purpose:	The PIP uses the GENESIS Stock Transfer System to electronically process transfers, dividends, and generate reports required by the SEC, PSE, Philippine Depository and Trust Corporation (PDTC), and other regulatory bodies.
Whether the Personal Data is shared outside of the Philippines:	No.	
Categories of Data Subjects:	Stockholders, investors	
To whom Personal Data will be disclosed (provide the type of organization – whether public or private, and name of organization):	Securities and Exchange Commission (public) Philippine Stock Exchange (private) PDTC (private)	

DPS Name:	**NKAC MARKETING DATA PROCESSING SYSTEM**	
Whether particular DPS is managed as PIC, PIP, or both:	PIP	
Type of DPS:	Manual or paper-based and electronic	
Purpose/Description of DPS:	The Sales and Marketing Department manages the North Kitanglad Agricultural Company, Inc. (NKAC) Marketing Processing System (the "System"). The System is used by the Company to fulfil its obligation under its Marketing Agreement with NKAC (the PIC) to market and sell the individual lots in Mountain Pine Farms, Kalugmanan, Manolo Fortich, Bukidnon, and to close deals and agreements with clients, lot owners, and homeowners. The Sales and Marketing Department uses the System to maintain records of clients and their Personal Data, accurately document transactions, provide assistance to clients, and answer their queries. The Personal Data of clients are collected by asking them to fill out Personal Information Sheets that require them to provide the following Personal Data: (1) Full Name; (2) Home Address; (3) E-mail Address; (4) Business Address; (5) Telephone Numbers; (6) Age; (7) Birthday; (8) Marital Status; (9) Photograph; (10) TIN; (11) SSS; (14) Passport Numbers; and (15) Other Government IDs. Personal Data collected are encoded into the System. The Personal Data collected and processed by the Sales and Marketing Department are used by the Collection Department, to know where to mail written communications, and by the Compliance Department, to draft necessary documentations (e.g., Deed of Absolute Sale, Contract to Sell). The Personal Data collected are also used for the remittance of withheld taxes to the Bureau of Internal Revenue. The Personal Data collected and processed may be accessed by Authorized Personnel only, and upon request, by clients. The physical documents are stored in a secured filing room, while the electronic documents are stored in password-protected computer devices. The PIC, NKAC, takes care of processing the transfer of titles to clients.	
Whether the Processing of Personal Data is subcontracted or outsourced:	No.	
Details of PIP, if any:	**Is there a subcontracting or outsourcing agreement?**	N/A
	PIP Name:	N/A
	PIP E-mail:	N/A
	PIP Address:	N/A
	PIP Contact Number/Extension Number:	N/A
	PIP Description/Purpose:	N/A
Whether the Personal Data is shared outside of the Philippines:	No.	
Categories of Data Subjects:	Clients (lot buyers/owners, home buyers/owners)	

To whom Personal Data will be disclosed (provide the type of organization – whether public or private, and name of organization):	Bureau of Internal Revenue (public) Pag-IBIG (public) Bank/s (private) NKAC (private)

ANNEX B. DATA SHARING AGREEMENT TEMPLATE

DATA SHARING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

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

A Brown Company, Inc., a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at Xavier Estates Uptown, Airport Road, Balulang, Cagayan de Oro City 9000, represented herein by its _____, _____ (hereinafter referred to as "**ABCI**");

- 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, ABCI desires to _____;

WHEREAS, COMPANY B desires to _____;

WHEREAS, the foregoing purposes will require ABCI 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. "**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.

3. "**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.

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

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

6. "**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.

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

8. "**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**" pertain 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**" pertain to Personal Information of Data Subjects which may be disclosed to the public by the Parties due to, or as required by, its business operations, and for government regulatory compliance and company disclosures.

9. "**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.

10. "**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.

11. "**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. ABCI and COMPANY B are PICs.

12. "**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.

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

14. "**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.

15. "**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.

16. "**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.

17. "**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, ABCI may share or transfer Personal Information, Sensitive Personal Information, and such other Personal Data to COMPANY B.

2. **Operational Details of Data Sharing.** In sharing or transferring Personal Data to each other under this Agreement, the Parties must 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 ABCI*. For the purpose of _____, ABCI 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. 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 for 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) 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 ABCI*.** The DPO of ABCI may be reached through the following:

Postal Address:	Xavier Estates Uptown Airport Road, Balulang Cagayan de Oro City 9000
Telephone Number:	+6388 8588784 to 85
E-mail Address:	aveguilos@abrown.ph

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

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 _____ 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 _____.

A BROWN COMPANY, INC.	**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*
A Brown Company, Inc. 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 nine (9) 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 (the "Agreement") is made and executed this _____ in _____ by and between:

A Brown Company, Inc., a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at Xavier Estates Uptown, Airport Road, Balulang, Cagayan de Oro City 9000, represented herein by its _____, _____ (hereinafter referred to as "**ABCI**");

- 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, ABCI desires to _____, and for such purpose, has to collect and process Personal Data;

WHEREAS, the Processor is engaged in the business of _____;

WHEREAS, ABCI 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;

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. "**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.

3. "**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.

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

5. "**Outsourcing**" refers to the disclosure or transfer of Personal Data by ABCI to the Processor for the Processing of Personal Data under this Agreement.

6. "**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**" pertain 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**" pertain to Personal Information of Data Subjects which may be disclosed to the public by the Parties due to, or as required by, its business operations, and for government regulatory compliance and company disclosures.

7. "**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.

8. "**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.

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

10. "**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.

11. "**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.

12. "**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.

13. "**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, ABCI 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 ABCI, 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 ABCI

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

(a) Identity of ABCI and the Processor who will be given access to the Personal Data;

(b) Purpose/s of Outsourcing;

(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 Outsourcing and the manner of Processing.

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

3. **Control over Processing.** ABCI 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 ABCI, 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 instruction from ABCI: 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 ABCI, 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 ABCI 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 ABCI, delete or return all Personal Data to ABCI 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 ABCI 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 ABCI or another auditor mandated by the latter;

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

ARTICLE VI. SECURITY MEASURES

1. 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 ABCI 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 for 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 ABCI.

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 ABCI.

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 ABCI of the Personal Data Breach;

(ii) investigate the Personal Data Breach and inform ABCI 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) 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 ABCI.*** The DPO of ABCI may be reached through the following:

Postal Address:	Xavier Estates Uptown Airport Road, Balulang Cagayan de Oro City 9000
Telephone Number:	+6388 8588784 to 85
E-mail Address:	aveguilos@abrown.ph

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

Postal Address:	
Telephone Number:	
E-mail Address:	

ARTICLE IX. TERMINATION

ABCI 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 _____ 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 _____.

A BROWN COMPANY, INC.	**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***
A Brown Company, Inc. 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 nine (9) 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 NOTICE

Privacy Notice

A Brown Company, Inc. ("ABCI") 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, and IP address). 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 the collection, use, and processing of your Personal Data, and 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 do not use our website or contact us.

ABCI may modify this Privacy Notice at any time. To update yourself of any changes in the processing of your Personal Data, you may need to regularly review this Privacy Notice.

Why does ABCI collect and process my Personal Data?

ABCI 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:

(1) To conduct due diligence prior to the execution of a contract, and to facilitate the fulfillment of the terms of the contract thereafter;

(2) To respond to your queries, complaints, and requests;

(3) To provide information about our products and services which may be of interest to you;

(4) To conduct research and analysis to improve customer experience;

(5) To maintain security; and

(6) 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 acquire a property, or when you apply to become a tenant in any of our properties, we may collect, use, or process your Personal Data to:

(1) Conduct appropriate credit investigation to assess the risk of transacting with you;

(2) Administer the sale and turnover of a particular property, which may include the preparation of all documentation leading to the transfer of title, and the performance of all financial processes (reservation fees, amortization, handover fees, etc.) as a result of our transaction;

(3) Prepare and execute the necessary contract to cover the transaction;

(4) Update our records and keep your contact details and billing address up to date; and

(5) Communicate any advisories, changes, and other information relevant to your contract with us.

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

(1) Conduct the appropriate due diligence checks;

(2) Evaluate your proposal, including your technical, financial, and operational capacity;

(3) Assess the viability of your proposal and process your accreditation;

(4) Communicate any decision on such proposal and issue a Letter of Award together with the contract; and

(5) 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:

(1) Evaluate your suitability for employment and, with a written or expressed consent, retain your Personal Data for a maximum of ten (10) years for future job opportunities that may be of interest to you;

(2) Communicate with you about your employment application;

(3) When hired, to process your Personal Data, as may be necessary for your employment such as, but not limited to, payroll, benefits application, allowances and refunds processing, tax processing, retirement benefits, and other purposes that demand processing of your Personal Data (e.g., to execute business transactions directly related and/or incidental to your job, business travels, anniversaries, social activities, emergencies, and so on);

(4) While employed, to evaluate your performance and career development;

(5) Upon separation, to process your Personal Data for the exit interview and to prepare your final pay;

(6) Provide assistance and account for employees in case of emergency; and

(7) Perform such other processing or disclosure that may be required in the course of ABCI's business or under law or regulations.

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

(1) Maintain and update your records with ABCI;

(2) Administer your stock transactions; and

(3) Comply with legal, regulatory, and contractual requirements or obligations.

If you are a visitor of ABCI, we may use, collect, or process your Personal Data to:

(1) Grant access to the premises of ABCI; and

(2) Maintain the security within the premises of ABCI.

What Personal Data does ABCI collect?

ABCI may collect and process any of the following Personal Data, among others:

(1) Your name;

(2) Your e-mail;

(3) Your other contact details;

(4) Your address;

(5) Your IP address; and/or

(6) Any information relevant to the feedback you have provided.

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

(1) Basic personal information, such as full name, nickname, home addresses/billing address/shipping address, e-mail address, contact numbers;

(2) Financial details such as credit history, bank account, credit card, and debit card information;

(3) Sensitive personal information, such as age, nationality, marital status, gender, health, education, and government-issued identification documents; and

(4) Employment history.

How does ABCI collect my Personal Data?

When you access our website and/or when you communicate/interact with us, ABCI 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. On the one hand, 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. On the other, a persistent cookie does not expire when you close your browser, and stays on your computer, unless you delete them.

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. We may also process the Personal Data you provide through the submission of job application form, business proposals, or property inquiry.

Where does ABCI store my Personal Data?

Your Personal Data is controlled by A Brown Company, Inc., a company registered under Philippine laws, whose principal office is at A Brown Company, Inc., Xavier Estates, Masterson Avenue, Upper Balulang, Cagayan de Oro City 9000 Philippines.

For how long does ABCI retain my Personal Data?

We 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 my Personal Data disclosed?

ABCI 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 purposes 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.

How does ABCI protect my Personal Data?

The security of your Personal Data is important to us. We employ appropriate organizational, technical, and physical security measures to protect the Personal Data you provide against accidental, unlawful, or unauthorized destruction, loss, alteration, access, disclosure, or use and other unlawful forms of processing.

What are my rights with respect to my Personal Data?

As owner of Personal Data, you have the right to be informed of the Personal Data being or that have been processed by ABCI, the right to gain reasonable access to your Personal Data, the right to object to the processing of your Personal Data, the right to suspend, withdraw, or order the removal or destruction of your Personal Data, the right to dispute any error in your Personal Data and have us correct it immediately, the right to obtain a copy of the Personal Data in electronic format, the right to file a complaint before the National Privacy Commission if you think your right to privacy and data protection was violated, and the right to claim damages.

How do I contact ABCI?

If you wish to exercise any of the abovementioned rights with respect to privacy and data protection, access your Personal Data, or stop us from using or processing your Personal Data, you may e-mail us through any of the addresses provided in this website, or write to us at A Brown Company, Inc., Xavier Estates, Masterson Avenue, Upper Balulang, Cagayan de Oro City 9000 Philippines.

The **Data Protection Officer** of ABCI may be reached through the following:

Postal Address:	Xavier Estates Uptown Airport Road, Balulang Cagayan de Oro City 9000
Telephone Number:	+6388 8588784 to 85
E-mail Address:	aveguilos@abrown.ph

You may also use any of the above means if you have queries and/or feedback about our Privacy Notice or privacy and data protection practices.

ANNEX E. DATA PROTECTION OFFICER

The DPO of ABCI may be reached through the following:

Postal Address:	Xavier Estates Uptown Airport Road, Balulang Cagayan de Oro City 9000
Telephone Number:	+6388 8588784 to 85
E-mail Address:	aveguilos@abrown.ph

ANNEX F. COMPLIANCE OFFICER FOR PRIVACY

The COP of ABCI for _____ may be reached through the following:

Postal Address:	
Telephone Number:	
E-mail Address:	

ANNEX G. 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.

The consent for the Company to use or process the information herein shall be valid for the duration of 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 H. CONSENT FORM

Processing of Personal Data
Consent Form

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 persons mentioned above, 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 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.

The consent for the Company to use or process the information herein shall be valid for the duration of 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 I. 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 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 Data Subject mentioned above, if any, to disclose their information included in this form; and (ii) informed said Data Subject 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.

The consent for the Company to use or process the information herein shall be valid for the duration of 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 J. SECURITY INCIDENT REPORT FORM

Annual Security Incidents and Breach Report

PERIOD: JANUARY 20__ TO DECEMBER 20__	Total
Total Number of Security Incidents and Personal Data Breach	
▪ SECURITY INCIDENTS	
▪ PERSONAL DATA BREACH	
• Personal Data Breach Mandatory Notification	
• Other Personal Data Breach (Notification Not Required)	

SECURITY INCIDENTS		Total	
Types	**No. of Incidents**	**Types**	**No. of Incidents**
☐ Denial of service		☐ External hacking	
☐ Compromised information, not involving Personal Data		☐ Malware	
☐ Compromised asset		☐ E-mail	
☐ Unlawful activity		☐ Policy violations	
☐ Internal hacking		☐ Others	

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

RISK IDENTIFICATION			
Risks	**Data Protection Principles Involved**	**Threats**	**Vulnerabilities**
Unauthorized or Unlawful Processing	• Transparency, Openness, and Purpose Specification		
	• Data Quality (Relevant and Accurate Data)		
	• Legitimate Purpose *Lawfulness, Purpose, and Use Limitation*		
	• Proportionality *Collection Limitation and Data Retention*		
	• Security of Personal Data *Confidentiality, Integrity, Availability*		
Violation of Rights of Data Subject	• Data Subject Rights and Individual Participation		

RISK IDENTIFICATION			
Risks	**Data Protection Principles Involved**	**Threats**	**Vulnerabilities**
Non-Compliance	• Accountability and Compliance		

RISK EVALUATION			
Impact	**Consequence**	**Recovery**	
☐ Negligible	☐ No effect, Few Inconvenience	Overcome with no problem	1
☐ Low	☐ Significant	Overcome with few difficulties	2
☐ Medium	☐ Significant	Overcome with serious difficulties	3
☐ High	☐ Significant or Irreversible	May not overcome	4

Probability	**Likelihood**	**Description**
☐ Negligible	☐ Highly Unlikely	☐ It may occur in exceptional circumstances
☐ Low	☐ Difficult	☐ Not expected, but there is a light possibility that it may occur
☐ Medium		
☐ High		

ANNEX K. 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 L. NON-DISCLOSURE AGREEMENT

Non-Disclosure Agreement

In consideration of my employment or continued employment in **A Brown Company, Inc.** (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**" pertain 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**" pertain 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 _____ 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
A Brown Company, Inc.

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_.