DATA PRIVACY AND NON-DISCLOSURE AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This Data Privacy and Non-Disclosure Agreement (the "Agreement") is made and executed this___in_____by and between:

PHILIPPINE INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal address at 700 Shaw Boulevard Mandaluyong City, Philippines, represented herein by its Deputy Executive Director, JOSUE I. SENGCO, (hereinafter referred to as "**PICPA**");

- and -

_____, (Position)_____, with principal address at_____ _____(hereinafter referred to as "**PICPA Officer/Employee**");

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

WITNESSETH:

WHEREAS, PICPA processes personal and sensitive information ("Personal Data") of its members ("Data Subjects") required for membership monitoring, election, professional development and related services pursuant to PICPA's purpose as the Accredited Integrated Professional Organization (AIPO) of Philippine Certified Public Accountants;

WHEREAS, PICPA Officer/Employee is required to perform tasks mandated by PICPA, its by-laws and related issuances and resolutions;

WHEREAS, the foregoing purposes will require PICPA and PICPA Officer/Employee to access Personal Data of Data Subjects;

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

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 PICPA Officer/Employee's employment, election or appointment and shall continue for a period of three (3) years (the "Term") after PICPA Officer/Employee's employment, election or appointment. 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 Access**" refers to the disclosure or transfer of Personal Data under the control or custody of PICPA to PICPA Officer/Employee, 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. PICPA 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 Access.** To achieve the purposes laid down in this Agreement, PICPA may share or transfer Personal Information, Sensitive Personal Information, and such other Personal Data to PICPA Officer/Employee.

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

(a) ***Information on Data Access.*** Prior to collecting Personal Data from a Data Subject and Data Access, 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 Access 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 Access and Processing.

(c) ***Data Access.*** 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.

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 during PICPA Officer/Employee's term of employment, election or appointment, or as long as may be necessary to accomplish the purpose of Data Access 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 PICPA 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 PICPA.

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 through PICPA's DPO, as follows:

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

DPO of PICPA:	Arnold A. Apdua
Postal Address:	700 Shaw Boulevard Mandaluyong City, Philippines
Telephone Number:	+639175655199
E-mail Address:	arnoldapdua@gmail.com

ARTICLE VII. 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 Mandaluyong 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_____.

PHILIPPINE INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS	**PICPA OFFICER / EMPLOYEE**
By:	Name: JOSUE I. SENGCO
	Deputy Executive Diretor
[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***
Philippine Institute Of Certified Public Accountants Represented by:Josue I. Sengco	SSS ID #03-1477922-1	
PICPA Officer / Employee		

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 2020.