

Contract Agreement

Project : **VULNERABILITY ASSESSMENT AND PENETRATION TESTING**
Contract No. : **2021-CIMS(025)-NPSVP022a-C001**

SEP 29 2021

THIS AGREEMENT is made on the ___ day of _____ 20__ by and between:

CREDIT INFORMATION CORPORATION (CIC), a corporation duly organized and existing under the laws of the Republic of the Philippines, with principal office address at 6th Floor, Exchange Corner Building, 107 V.A. Rufino Street corner Esteban St., Legaspi Village, Makati City, Philippines, represented herein by its President and Chief Executive Officer, **ATTY. BEN JOSHUA A. BALTAZAR** (hereinafter referred to as "**Procuring Entity**");

- and -

NEXT GENERATION TECHNOLOGIES GLOBAL INC., represented by its Chief Information Officer, **PETER SANTIAGO**, authorized through Secretary Certificate dated August 2, 2021, with office address at 27th Floor, 88 Corporate Center, Sedeño Street, Salcedo Village, Makati City, (hereinafter referred to as "**Service Provider**");

-WITNESSETH That-

WHEREAS, upon invitation of the Procuring Entity, the **Service Provider** submitted a bid for the **Vulnerability Assessment and Penetration Testing** in the amount of **SEVEN HUNDRED FIFTY THOUSAND (PhP750,000.00)**, Philippine Pesos, inclusive of all applicable government taxes and charges, hereinafter called "**the Contract Price**";

WHEREAS, the Procuring Entity (or "PE") accepted the bid of the Service Provider (or "SP") through Resolution No. 2021-CIMS(025)-NPSVP-022a, which was approved by the Head of Procuring Entity on 2 September 2021.

NOW, THEREFORE, for and in consideration of the foregoing premises and of the mutual covenants and stipulations contained in this Agreement, the parties hereto have agreed, and do hereby agree and declare the following:

1. The following documents shall be deemed to form and be read and construed as part of this Agreement, viz.:

- (a) Terms of Reference (TOR);
- (b) Service Provider's Bid, including the eligibility requirements, technical and financial proposals, and all other documents or statements submitted in response to the Request for Proposal issued for the project;
- (c) Notice of Award;
- (d) Other contract documents that are subsequently required for execution or submission after the contract execution, such as the Notice to Proceed, Variation Orders, and Warranty Security; and
- (e) All provisions of RA No. 9184 and its 2016 revised IRR, including the Generic Procurement Manual, and associated issuances, which shall constitute as the primary sources for the terms and conditions of the Contract, and that which shall govern during contract implementation.

DURATION OF THE AGREEMENT

2. The Service Provider shall perform the services as enumerated in the Request for Proposal of the Procuring Entity (Annex B of the TOR) for an estimated period of sixty (60) calendar days, excluding remediation period of the Procuring Entity.

The examination of the systems shall be undertaken during off-office¹ hours and subject to reasonable guidelines of the Procuring Entity. Any amendment/modification of the work schedules shall be made only upon prior written approval of the Procuring Entity's Technical Working Group, in which case, the engagement shall be correspondingly extended for such period called for by the amendment/modification under the same terms, with no additional cost on the part of Procuring Entity.

Activities	W1	W2	W3	W4	W5	W6	W7-16	W17	W18
First pass									
Validation meeting									
Interim report									
Social engineering simulation & report									
Presentation to the IT & Cyber Security Committee 1									
Remediation by the PE									
Second pass									
Validation meeting									
Submission of final reports									
Presentation to the IT & Cyber Security Committee 2									

This Contract shall take effect on the date specified hereunder and shall continue to be enforce until full completion of the Project.

OBLIGATIONS OF THE SERVICE PROVIDER

3. The Service Provider shall perform the following duties and responsibilities:

The Service Provider shall perform the following activities in two (2) passes after the project kick off, followed by the social engineering simulation activity.

3.1 First Pass:

3.1.1. Reconnaissance:

- a. Discover and identify information from the Internet and other available resources (Dark Web, OSINT, etc.), all information that will represent Procuring Entity's Internet footprint.
- b. Report the information gathered as well as the methodology on how the information was discovered.

3.1.2. Identity Vulnerabilities:

- a. Probe resources (discovered/in-scope) to identify listening services. Identify and assess vulnerabilities that may be present in those exposed services. Produce a prioritized list of security vulnerabilities.

3.1.3. Exploit:

- a. Attempt to exploit identified vulnerabilities using a combination of automated and manual tests to uncover all potential issues and may not

¹ Based on OO Number 346 series of 2020, Skeleton workforce-work hours shall be from 9:00 AM to 3:00 PM with no noon break on days approved by the management. Work-from-Home shall observe the 8:00 AM to 5:00 PM with noon break. Should there be changes on this OO regarding working hours, this shall be observed by BOTH PARTIES

be limited to the following Open Web Application Security Project (OWASP) top 10 application security risks:

1. All forms of Injection flaws;
2. Cross-Site Scripting (XSS) which may allow attackers to execute scripts in the victim's browser to hijack user sessions;
3. Security misconfiguration of the systems involved;
4. Missing Function Level Access Control which may let attackers to forge application requests in order to access functionality in PE's web applications without proper authorization;
5. Using Components with Known Vulnerabilities which may undermine PE's application defenses, and enable a range of possible attacks.
6. Broken Authentication and Session Management which may allow attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws.
7. Insecure Direct Object References which may allow attackers to manipulate insecurely exposed references to an internal implementation object to access sensitive data.
8. Sensitive Data Exposure which may allow attackers to steal or modify weakly protected sensitive data to conduct fraud, identity theft, or other crimes.
9. Cross-Site Request Forgery (CSRF) which may allow attackers to force the victim's browser to requests.
10. Invalidated Redirects and Forwards which may allow attackers to redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

3.1.4. Review of Application Architecture:

Attempt to find, download, and review server-side scripts, configuration files, include files and HTML source codes. Check for issues such as database connection strings, configuration settings, unauthorized directory listings and commented code.

3.1.5. Analyze Risk:

Evaluate the identified areas of weakness, and rate the findings based on the risk that each poses to the PE. The SP shall use PE's risk rating criteria.

3.2. Second Pass/Validation

3.2.1. The SP will perform a second pass to validate the implementation of the recommendations during the first pass

3.2.2. The activity will be performed after the PE has implemented the recommended measure to mitigate identified risks. Please refer to the project timeline below.

3.2.3. The SP shall perform similar procedures as described above to validate if findings in the First Pass have been resolved.

3.3. Social Engineering Simulation

3.3.1. Phishing and other social engineering simulation activities

3.3.1.1 Secure clearance from the PE prior to start of the engagement for the conduct of pre-assessment, noting the relevant policies and the existing training of the PE's employees.

3.3.1.2. Perform information gathering and develop the simulation plan of activities with PE.

- 3.3.1.3. Based on the agreed terms of procedures and conditions, coordinate with the relevant parties for the conduct of the Phishing and other social engineering attack simulation activities;
- 3.3.1.4. Based on the result of the Phishing and other social engineering attack simulation activities, assess the awareness of PE's employees, and communicate the same with the PE's management.

3.4. Attack simulation and e-learning platform

3.4.1. Provide a phishing and e-learning platform that is listed as leader in Gartner Magic Quadrant for Security Awareness Computer-Based Training for seventy-five users (75);

3.4.2. The platform will be used to perform basic attack simulations and provide follow-up e-learning content, to enable the PE to continue its campaign after the end of the engagement.

3.4.3. The platform must support the following:

3.4.3.1. Phishing simulator

- Built-in phishing templates
- Easy to use template builder
- Phished learner training

3.4.3.2. Security awareness training

- Provide training modules, videos
- Pre-built training plans
- Personalized & role-based training
- Industry & compliance training
- Posters, newsletters & supporting resources

3.4.3.3. Learning experience

- Personalized learner dashboard
- Gamified & experiential learning
- Training recommendations
- Course Completion certificates

3.4.3.3. Reporting & assessments

- Dashboard reports
- Learner activity & risk scores
- Automated campaign reports
- Assessments
- Industry benchmarks

DELIVERABLES

4. The Service Provider shall submit and present to PE, based on the scope of work as proposed by the latter and accepted by the former², and in accordance with the timeline, a comprehensive report consisting of the following:

4.1. Project Plan

Submission of a project plan detailing all the dates for the work phase, deliverables, review meetings, report delivery and report allocations.

4.2. Interim Report

Submission of an interim report in the form of threat and vulnerability matrix that details the description of the vulnerabilities, impact and criticality of the vulnerabilities, impact and criticality and recommendation.

4.3. Executive Report

Submission of an executive summary report detailing the engagement's scope, approach and summary recommendations aimed at senior management. Must

² Please refer to attached Request for Proposal

contain non-technical description of all findings along with discussions of the inherent business risks and recommended risk management strategies.

4.4. Technical Report

Submission of a technical report covering identified security risks, exposures and proposed recommendation aimed at technical staff and should provide them with complete solutions.

4.5. Executive presentation

A presentation of the identified risks during the first and second pass to the IT & Cyber Security Committee of the board of directors.

4.6. Phishing simulation report

Submission of a phishing simulation activity report covering identified risks pertaining to employee security awareness.

PAYMENT

5. Payments shall be subject to the "Warranty" provisions in the form of either retention money in an amount equivalent to at least one percent (1%) of every progress payment, or a special Bank Guarantee in the amount equal to at least one percent (1%) of the total Contract Price required in Section 62 of R.A. 9184 and its IRR.

6. The **Service Provider** shall be liable for the damages for the delay in its performance of the Contract and shall pay the **Procuring Entity** liquidated damages, in an amount of at least equal to one-tenth (1/10) of one percent (1%) of the cost of the unperformed portion for every day of delay. Once the cumulative of liquidated damages reaches ten percent (10%) of the amount of the contract, the Procuring Entity may rescind or terminate the contract, without prejudice to other courses of action and remedies available to the Procuring Entity.

7. In consideration of the payments to be made by the Procuring Entity to the Service Provider, the Service Provider hereby covenants to perform and deliver aforementioned services to the Procuring Entity. The total contract cost shall be paid in full after completion of the project subject to the acceptance of the deliverables by the Inspection and Acceptance Committee. Payment shall be made based on the schedule below and subject to submission of billing statement, and other supporting documents by the Service Provider:

1.	<i>Upon completion of the interim report & social engineering report</i>	90%
2.	<i>Upon submission of the Final Report</i>	10%
	<i>Total</i>	100%

RESPONSIBILITIES OF PROCURING ENTITY

8. Procuring Entity's responsibilities with respect to this project are as follows:

8.1. Grant the Service Provider's authorized representative access to its premises, equipment and facilities located therein to perform its obligations, provided that such representative shall be accompanied by the duly assigned personnel of the PE's Technical Support Department.

8.2. Secure the necessary access pass and building permit required by the facility administrator and assume responsibility for the safe custody and use of the equipment installed by the Service Provider.

8.3. Monitor the provided services and verify if the parameters under the Service Level Agreement are met and performed by the Service Provider.



8.4. Issuance of a Certificate of Inspection and Acceptance to the Service Provider upon successful completion of the testing certifying that the Service Provider conforms to all requirements stipulated in this document.

8.5. Pursuant to General Procurement Policy Board (GPPB) Resolution No. 019-2006 dated 06 December 2006, at the end of each year, the PE will conduct an assessment of the quality of service provided particularly the cost charged by the Service Provider and the range of services it offers against other service providers in the area.

NON-DISCLOSURE AND CONFIDENTIALITY


9. In consideration of the premises or covenants contained herein, and as a condition to protect from disclosure the Procuring Entity's non-public, confidential or proprietary information, the Service Provider shall adhere to the non-disclosure policy of the former by executing a Non-Disclosure and Confidentiality Agreement with the same (Appendix CIC-1).

AMENDMENT

10. Any amendment to this Agreement shall be made in writing and signed by the Procuring Entity and the Service Provider.

IN WITNESS whereof the parties hereto have caused this Agreement to be executed in accordance with the laws of the Republic of the Philippines on the day and year first above written.


SIGNED, SEALED AND DELIVERED BY:



ATTY. BEN JOSHUA A. BALTAZAR
PRESIDENT and CEO



PETER SANTIAGO
NEXT GENERATION TECHNOLOGIES GLOBAL INC.



MARBIN M. FADRIQUELA
PROCURING ENTITY'S WITNESS

SIGNED IN THE PRESENCE OF:

Digitally signed by
Fadriquela Marbin
Moraleda



LEAH ROSE PALOGAN
NEXT GENERATION TECHNOLOGIES GLOBAL INC.
WITNESS

Certified Funds Available:




Cabasis Maria
Siena Masaoy
2021.007.20091
MA. SIENA M. CABASIS
ACTING CHIEF ACCOUNTANT

REPUBLIC OF THE PHILIPPINES) S.S.
MAKATI CITY, METRO MANILA)

ACKNOWLEDGEMENT

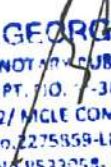
BEFORE ME, a Notary Public for and in Makati City, Metro Manila, Philippines, this
_____ day of SEP 29 2021, personally appeared the following:

Name	Competent Evidence of Identification	Date of Issue/ Expiry Date	Place of Issue
ATTY. BEN JOSHUA A. BALTAZAR	UMID CEN 021-1322-9960-7	2017	Manila
PETER SANTIAGO 	DL N0107012151	2023/8/24	San Juan

They are both known to be the same persons who signed the foregoing document and acknowledged to me that their signature/s proven their free acts and the identity/ies they represent.

WITNESS MY HAND AND SEAL on the date and place first above written.

Doc. No. 377
Page No. 76
Book No. 140
Series of 2021


ATTY. GEORGE DAVID D. SISON
NOTARY PUBLIC FOR MAKATI CITY
APPT. NO. 7-382- UNTIL DEC. 31, 2021
ROLL NO. 68402/ NICLE COMPLIANCE NO. VI-0021936/3-29-2019
IBP O.R. No. 2275859-LIFETIME MEMBER MAY. 8, 2017
PTR NO. 9533058- JAN 04, 2021- MAKATI CITY
EXECUTIVE BLDG. CENTER MAKATI AVE., COR., JUPITER ST. MAKATI CITY

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

This NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT is made and entered into this day of _____, 2021 (the "Effective Date") by and between

CREDIT INFORMATION CORPORATION ("CIC") a government-owned and controlled corporation existing by virtue of Republic Act No. 9510 or the Credit Information System Act with principal address at 6th Floor Exchange Corner Building cor. Esteban and Bolanos Streets, Legaspi Village, Makati City, represented by its President, **Atty. BEN JOSHUA A. BALTAZAR**, herein referred to as the **DISCLOSING PARTY**;

-and-

NEXT GENERATION TECHNOLOGIES GLOBAL INC., a corporation duly organized and existing under and by virtue of the laws of the Republic of the Philippines, with principal office address at 27th Floor, 88 Corporate Center, Sedeño Street, Salcedo Village, Makati City, and represented herein by its Chief Information Officer, **PETER SANTIAGO**, herein referred to as the **RECEIVING PARTY**.

Furthermore, the DISCLOSING PARTY and RECEIVING PARTY may hereinafter be collectively referred to as PARTIES.

WHEREAS, in connection with the ensuing business relationship, the CIC anticipates the need to discuss with and disclose to the RECEIVING PARTY, certain information and materials of a non-public, confidential, or proprietary nature; and

WHEREAS, the PARTIES wish to set forth their mutual understanding of the restrictions on the use, dissemination, and disclosure of CIC's non-public, confidential, or proprietary information disclosed to the RECEIVING PARTY.

NOW, THEREFORE, in consideration of the premises or covenants contained herein, and as a condition to protect CIC from disclosure of its non-public, confidential or proprietary information, the PARTIES hereby agree as follows:

1. As used herein:

- a. Information" is defined as communication or data, in any form, including, but not limited to, oral, written, graphic, electronic, or electromagnetic form, that is disclosed, conveyed, or provided in connection with or relative to the project.



- b. Confidential Information" is defined as any of the following, which is communicated by CIC to the RECEIVING PARTY, directly or indirectly, to wit:

Any and all kinds of information, know-how, data, process, technique, program, design, drawing, formula, test, work in process, engineering, manufacturing, marketing, financial or personnel matter, whether in oral, written, graphic, magnetic, electronic, or other form of communication, that is learned by or disclosed to the RECEIVING PARTY in the course of discussions, studies, or other work undertaken between the PARTIES provided that the same is either conspicuously marked "confidential" or "proprietary", is known or reasonably should be known by the RECEIVING PARTY to be confidential or proprietary, or is of a confidential or proprietary nature, and that it is made in the course of discussions, studies, or other work undertaken between the PARTIES.

Notwithstanding the foregoing enumeration, in case of doubt as to whether particular information is confidential, the same shall be treated as confidential.

2. The RECEIVING PARTY agrees that (1) all Confidential Information shall be used solely for the purpose of considering and implementing the **VULNERABILITY ASSESSMENT AND PENETRATION TESTING PROJECT** as requested by the DISCLOSING PARTY; (2) All Confidential Information shall remain at all times the property of the DISCLOSING PARTY; and (3) except as may be required by applicable law or legal process, the RECEIVING PARTY shall not distribute, disclose or disseminate such Confidential Information to anyone, except those employees of the RECEIVING PARTY who need to know such Confidential Information for the purpose for which it is disclosed, unless and until such time as:

- a. Such information is generally available to the public other than as a result of a breach of this Agreement; or
- b. Such information is already in the possession of the RECEIVING PARTY without restriction and prior to any disclosure hereunder; or
- c. Such information is or has been lawfully disclosed to the RECEIVING PARTY by a third party, not employed by or otherwise affiliated with the DISCLOSING PARTY, who is not known by the RECEIVING PARTY to be prohibited by contractual, legal, or judgment obligation from disclosing the same; or
- d. Such information is obliged by law or proper government authority to be disclosed, in which case, the RECEIVING PARTY shall notify the DISCLOSING PARTY in writing of the circumstances under which such disclosure will be made, including the nature of the disclosure and the entity to which it is to be made.

Notwithstanding the above, if the RECEIVING PARTY is obliged or required by any court or governmental, regulatory, or other body or person, to disclose Confidential information, it shall, if so required in writing and for valid and lawful reasons by the DISCLOSING PARTY, and if practicable or feasible, cooperate with the



DISCLOSING PARTY in opposing such requirement or request, subject to the duty of the DISCLOSING PARTY to shoulder the necessary litigation and related expenses for the purpose.

3. Neither party shall, without the prior written consent of the DISCLOSING PARTY:
 - a. disclose to any person that it possesses such Confidential Information;
 - b. disclose any or all parts of the Confidential Information to any person, including any third party or other employee of the DISCLOSING PARTY, unless such persons are required to have knowledge of the Confidential Information for the PARTIES to achieve their mutual purposes, as may be determined by the original DISCLOSING PARTY, and they have been advised of the confidential and proprietary nature of the Confidential Information and have agreed to protect the same; or
 - c. reproduce , copy or permit to be reproduced or copied Confidential Information in any medium or form; Provided, that the RECEIVING PARTY shall AT ALL TIMES protect the Confidential Information by using the same degree of care to prevent its unauthorized use, dissemination or publication as the RECEIVING PARTY uses to protect its own confidential information of a like nature, but no less than a reasonable degree of care, and that the RECEIVING PARTY shall enforce this Agreement against those persons to whom it is authorized to disclose the Disclosing Party's Confidential Information for and on behalf of the Disclosing Party.
4. Violation of any material provision of this Agreement shall render the RECEIVING PARTY liable for damages suffered by the DISCLOSING PARTY on account of such violation, without prejudice to other remedies available to the DISCLOSING PARTY under law or equity.
5. It is understood that this Agreement is not to, and does not, obligate any PARTY to enter into any further agreements or proceed with any possible relationship or other transaction with the other PARTY as long as it does not contravene the provisions of this Agreement.
6. All Confidential Information supplied by the DISCLOSING PARTY is without any express or implied warranty of any kind. Unless agreed in writing, the DISCLOSING PARTY does not warrant or make any representations regarding the use or the results of the use of the Confidential Information in terms of their correctness, accuracy, reliability, or otherwise. The RECEIVING PARTY agrees to hold the DISCLOSING PARTY free from any liability and/or any claims arising out of the use of or in reliance to the Confidential Information.
7. This Agreement shall survive, and the duty of the RECEIVING PARTY to hold Confidential Information in confidence shall remain in effect for a period of two (2) years or until the DISCLOSING PARTY sends RECEIVING PARTY written notice releasing the RECEIVING PARTY from this Agreement.



8. Each PARTY reserves all rights it may have by law or contract to its Confidential Information and no rights or obligation other than those expressly stated herein are granted or implied from this Agreement, unless otherwise agreed in writing_ by the PARTIES. No license is hereby granted by one PARTY to the other, directly or indirectly, under any existing patent, invention, discovery, copyright, trade secret, trademark, service mark, or other intellectual property held or obtained in the future by either PARTY.
9. Each PARTY warrants that it has full right and authority to enter into this Agreement, and that it is, unless expressly identified otherwise, the owner of its respective Confidential Information; and that it has the right to disclose its Confidential Information to the other party and to authorize the other party to use the same for the mutual purpose or purposes of the PARTIES.
10. The PARTIES agree to immediately notify each other in writing or otherwise if any one of them becomes aware of any disclosure of Confidential Information that it knows or believes to be unauthorized by the other PARTY.
11. The DISCLOSING PARTY may, at any time, request the RECEIVING PARTY to return any material containing, pertaining to or relating to the Confidential Information and all related documentation and all copies and installations thereof and may, in addition, request the RECEIVING PARTY to furnish a written statement to the effect that, upon such return, the RECEIVING PARTY has not retained in its possession, or under its control, either directly or indirectly, any such material. As an alternative to the return of the material contemplated herein, the RECEIVING PARTY shall, at the instance of the DISCLOSING PARTY, destroy such material and furnish the DISCLOSING PARTY with a written statement to the effect that such material has been destroyed. The RECEIVING PARTY shall comply with the foregoing request within seven (7) days of receipt of such a request. Notwithstanding anything to the contrary in this Agreement, the RECEIVING PARTY shall not be obligated to erase Confidential Information that is contained in an archived computer system backup made in accordance with the RECEIVING PARTY's security and/or disaster recovery procedures provided that such archived copy will (i) eventually be erased or destroyed in the ordinary course of the RECEIVING PARTY's data processing procedures; and (ii) such copy shall remain fully subject to the obligations of confidentiality stated herein, until the earlier of the erasure or destruction of such copy, or the expiration of such confidentiality obligations.
12. The PARTIES agree and acknowledge that any breach of the obligations contained in this Agreement will cause irreparable loss and would not be compensable by monetary damages alone. Accordingly, CIC shall, in addition to the other remedies a PARTY may have at law or in equity, be entitled to obtain a specific performance or injunctive relief against the RECEIVING PARTY in respect of the threatened or actual breach of this Agreement.



13. If any provision of the foregoing terms shall be unlawful, void, or for any reason is unenforceable, then that provision shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.
14. This Agreement shall be governed by and construed in accordance with the laws of the Republic of the Philippines.
15. This Agreement sets forth the entire covenant and understanding between the PARTIES concerning the confidentiality of the information disclosed pursuant to this Agreement, and supersedes all previous agreements, negotiations, commitments, writings and discussions between them as to the subject prior to the date hereof. There are no prior representations or warranties between the parties relating to the Confidentiality of the Information of this Agreement. This Agreement shall not be modified except in writing, signed by the PARTIES.
16. If any term or provision of this Agreement should be declared illegal or invalid by a court of competent jurisdiction, the remaining terms and provisions of this Agreement shall remain unimpaired and in full force.
17. It is recognized by the PARTIES that this Agreement is subject to review by the Office of the Government Corporate Counsel (OGCC), whose comments and suggestions shall be herein incorporated.

IN WITNESS WHEREOF, the Parties have executed this Agreement effective as of the date first written above.

RECEIVING PARTY

DISCLOSING PARTY

NEXT GENERATION TECHNOLOGIES
GLOBAL INC

Credit Information Corporation

By:

By:


PETER SANTIAGO


ATTY. BENJOSHUA A. BALTAZAR

SIGNED IN THE PRESENCE OF:

ACKNOWLEDGMENT

REPUBLIC OF THE PHILIPPINES)
CITY, METRO MANILA) SS.

Makati City

BEFORE ME, a Notary Public for and in the City of _____, on this **SEP 29 2021** day of _____ 2021, personally appeared the following person/s:

NAME	GOVERNMENT ID	DATE/PLACE OF ISSUE
ATTY. BEN JOSHUA A. BALTAZAR	UNID CRN 021-1322-9900-7	2017 / Manila
PETER SANTIAGO	DL N0107012157	2023/8/24 San Juan

who have been identified by me through the foregoing competent evidence of identities, personally appeared before me and attested to me that the signatures appearing on the foregoing instrument was voluntarily affixed by them and that the instrument is their free and voluntary act and deed, as well as of the corporations they respectively represent.

This instrument refers to a NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT which consists of six (6) pages, including the page whereon this acknowledgment is written, and which is signed by the Parties and their instrumental witnesses on each and every page hereof.

Doc. No. 272
Page No. 76
Book No. 170
Series of 2021.

ATTY. GEORGE DAVID D. SITON
 NOTARY PUBLIC FOR MAKATI CITY
 APPT. NO. 11-382- UNTIL DEC. 31, 2021
 BILL NO. 68402 / MCLE COMPLIANCE NO. VI-0021936/3-29-2019
 IBP O.R. NO. 2275350-LIFETIME MEMBER MAY. 3, 2017
 PTD No. 8533058- JAN 04, 2021- MAKATI CITY
 EXECUTIVE BLDG. CENTER MAKATI AVE., COR., JUPITER ST. MAKATI CITY