COMPLIANCE ANNEXES
SPECIAL UNDERTAKINGS

In the performance of the Services and its obligations under this Agreement, VENDOR specially undertakes to agree and abide by the following:

1. **Anti-bribery**. VENDOR, including its employees, agents, shareholders, affiliates and subsidiaries, shall not:

    1.1. offer or give or agree to give to any person any gift or consideration of any kind as an inducement or reward for performing or refraining to do any act in relation to the obtaining or execution of this Agreement, or for showing or refraining to show favor or disfavor to any person in relation to this Agreement;

    1.2. enter into an agreement in connection with which any commission or inducement has been paid or agreed to be paid by the VENDOR or on the VENDOR's behalf or to the VENDOR's knowledge unless particulars of any such commission or inducement and of the terms and conditions of any agreement for the payment thereof have been provided to CONVERGE in writing before the date of execution of the relevant agreement;

    1.3. pay or receive, nor promise or accept a promise to receive, a bribe or any other type of improper payment;

    1.4. make or promise any payment in violation of international or national or regional anti-bribery laws (including without limitations the United States Foreign Corrupt Practices Act and any applicable implementing legislation of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions);

    1.5. make or promise or offer to make any improper payment, loan, gift or transfer of anything of value, directly or indirectly:
        1.5.1. To or for the use or benefit of any government official or government employee (including employees or government-owned or controlled entities or corporations);
        1.5.2. To or for the use of any political party, official of a political party or candidate;
        1.5.3. To or for the use of any public international organization, or
        1.5.4. To an intermediary for payment to any of the foregoing, in order to obtain or retain business or to secure any advantage; or
        1.5.5. To any entity or corporations, or individuals, by itself or through an intermediary, that sis contrary or breaches any international and national laws applicable on corruption and bribery among individuals

    for the purpose of influencing or inducing any act or decision to secure an improper advantage in connection with, or in any way relating to any government authorization or approval involving CONVERGE, or to obtaining or retention of business by CONVERGE.

    1.6. from time to time during the term of this Agreement, at the reasonable request of CONVERGE, it will confirm in writing that it has complied with its undertakings under this section and will provide any information reasonably requested by CONVERGE to demonstrate such compliance;

    1.7. it will report to CONVERGE or to CONVERGE's Whistleblowing Platform (https://corporate.convergeict.com/whistleblowing-platform/) as soon as practicable any request or demand for any improper payments or other improper advantage of any kind received by the VENDOR from CONVERGE or any other person in connection with the performance of this Agreement; and

1.8. it will notify CONVERGE as soon as practicable of any breach of any of the undertakings contained in this Section of which it becomes aware.

2. **Human Rights.** VENDOR shall abide by all internationally recognized human rights (including without limitation the Universal Declaration of Human Rights and the International Labor Organization's Declaration on Fundamental Principles and Rights of Work), and the Human Rights Policy of CONVERGE. VENDOR ensures present and future non-complicity in any direct or indirect abuse of any and all human rights, regardless if they are carried out by a government or any other actor, whether the Party knew or should have known of its contribution to such abuse. Each Party will take the necessary action to assure direct and indirect compliance with the aforesaid.

3. **Labor.** VENDOR, including its employees, agents, shareholders, affiliates and subsidiaries, shall not and will not, directly or indirectly:

   3.1. make use of slave, forced or compulsory labor in any form, and/or
   3.2. engage children under the corresponding minimum ages for employment, as defined in all international labor standards and applicable national legislation on child labor, whether the Party knew or should have known of its contribution to such behaviors.

4. **Anti-OSAEC/CSAEM.** CONVERGE explicitly prohibits Online Sexual Abuse and Exploitation of Children (OSAEC) and Child Sexual Abuse or Exploitation Material or Child Sexual Abuse Material (CSAEM/CSAM). VENDOR shall not engage in any form or any conduct of streaming or live-streaming of OSAEC, CSAEM and CSAM in the use of their website, platform, server or facility or in the performance of its obligations under this Agreement. In particular, VENDOR shall not engage in any of the unlawful or prohibited acts under Section 4 of Republic Act No. 11930 or "Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act"."

5. **Environment.** VENDOR shall comply with all applicable laws relating to the environment, including the disposal of materials and discharge of substances, scraps or materials into the environment and having an actual or potential effect on any activities related to this Agreement.

6. **Health and Safety.** VENDOR, including its employees, agents, shareholders, affiliates and subsidiaries, shall comply with all applicable laws, CONVERGE requirements, approved codes of practice and industry guidance relating to health and safety. A Health and Safety program is in place which sets out arrangements for: the identification, management and control of hazards and risks associated with the activities/services to be provided, training and certification of personnel, formal induction and permit processes before work commences, reporting of all incidents and near misses, periodic auditing for compliance to health and safety rules and the effectiveness of health and safety arrangements.

DATA PRIVACY AND
INFORMATION SECURITY REQUIREMENTS

1. **Definition of Terms**. As used in this Annex, the following terms have the meanings specified below:

1.1. "Agreement" means the agreement to which this Annex is affixed.

1.2. "Authorized Persons" means authorized employees of VENDOR who have a need to know or otherwise access CONVERGE Personal Data to enable the Parties to perform its obligations with the Agreement and are bound in writing by confidentiality obligations sufficient to protect Personal Data in accordance with the terms and conditions of this Annex.

1.3. "CONVERGE" means the Converge ICT Solutions, Inc., which is a Party to the Agreement.

1.4. "CONVERGE Personal Data" means any Personal Data provided by the CONVERGE to the VENDOR in connection with the Agreement, necessary to fulfill the services provided by the VENDOR.

1.5. "Controller" means an entity that controls, administers and manages the processing of Personal Data, or instructs another to Process Personal Data on its behalf.

1.6. "COUNTERPARTY" means CONVERGE's counter-party to the Agreement.

1.7. "Data Processing Systems" means any application or system used to process CONVERGE Personal Data.

1.8. "Data Protection Law" means the law that protects the fundamental rights and freedom of a Data Subject and secure processing of their Personal Data.

1.9. "Data Subject" means an individual whose personal, sensitive personal, or privileged information is processed.

1.10. "Annex" means this Annex.

1.11. "Information Security Incident" means an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of Personal Data. It shall include incidents that would result to a Personal Data Breach, if not for safeguards that have been put in place.

1.12. "Personal Data" means any information that could identify a Data Subject.

1.13. "Personal Data Breach" means 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.

1.14. "Processing of Personal Data" (and variants of it, such as "Processing" or "Process") mean 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 of data.

1.15. "Processor" means a person or entity that Processes Personal Data for and on behalf of, and under the instructions of, a Controller.

1.16. "Sensitive Personal Information" means an individual's Personal Data consisting in government-issued identification number (including social security number, driver's license number or state-issued identified number); financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; biometric or health data.

1.17. "Sub-processor" means a third party or an external entity engaged by the VENDOR to Process Personal Data of CONVERGE.

1.18. "Party" or together as "Parties" refers to the CONVERGE and the VENDOR.

2. **CONVERGE Personal Data.**

2.1. To achieve the purposes laid down in this Annex, CONVERGE may share or transfer to the VENDOR, or instruct the VENDOR to collect and further process on its behalf, Personal Data, Sensitive Personal Information, Privileged Information and such other Personal Data of the Data Subjects.

2.2. In the Processing of CONVERGE Personal Data upon the prior written instruction of the CONVERGE, the VENDOR may further engage the services of a Sub-Processor, provided that such engagement must be covered by a duly executed Outsourcing Agreement.

3. **Obligations of the Processor in Processing CONVERGE Personal Data.**

3.1. In the Processing of CONVERGE Personal Data pursuant to this Annex, the VENDOR undertakes to:

3.1.1. process CONVERGE Personal Data only upon the documented instructions of CONVERGE, including transfers of Personal Data to another country or an international organization, unless such transfer is authorized by law;
3.1.2. ensure that an obligation of confidentiality is imposed on Authorized Persons and other persons authorized to process the CONVERGE Personal Data;
3.1.3. Implement appropriate security measures and comply with the data privacy laws, regulations, and relevant government issuances;
3.1.4. not engage the service of a Sub-Processor without prior written approval from CONVERGE; provided, that any such arrangement shall ensure that the same obligations for data protection under the Agreement are implemented, considering the nature of the Processing;
3.1.5. assist CONVERGE, by appropriate technical, physical 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;
3.1.6. assist CONVERGE in ensuring compliance with the data privacy laws, regulations, and relevant government issuances, considering the nature of Processing and the information available to the VENDOR;
3.1.7. at the choice of CONVERGE, delete or return all CONVERGE Personal Data to CONVERGE 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;

3.1.8. make available to CONVERGE 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 CONVERGE or an auditor mandated by the latter, and

3.1.9. immediately inform CONVERGE if, in its opinion, an instruction infringes data privacy laws, regulations, and relevant government issuances.

3.2. **Engagement of Sub-Processors**.

3.2.1. VENDOR shall not, directly or indirectly, disclose CONVERGE Personal Data to any person other than its Authorized Persons, without express written consent from CONVERGE, unless and to the extent required by government authorities or as otherwise, to the extent expressly required by Data Protection Laws, in which case, VENDOR shall use best efforts to notify CONVERGE before such disclosure or as soon thereafter as reasonably possible.

3.2.2. CONVERGE may authorize the VENDOR to engage a Sub-Processor provided, that any such arrangement shall ensure the same obligations and/or requirements for securing Personal Data under this Annex. At any point, the VENDOR requires the services of a Sub-Processor to Process Personal Data, VENDOR shall engage the Sub-Processor in writing.

4. **Security Measures**. VENDOR undertakes to observe and implement the following reasonable and appropriate physical, technical, and organizational security measures to ensure privacy and data protection. These security measures aim to protect CONVERGE 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.

4.1. **Risk Assessment and Mitigation**. VENDOR shall conduct periodic Risk Assessments and when there are significant changes to operations, organization, and information technology. Results of Risk Assessments must be documented and shall implement corresponding risk mitigation strategies.

4.2. **Information Security Management.**

4.2.1. **Information Security Policy**. VENDOR shall document and implement applicable information security policy that address the risks and information security controls identified during the risk assessment process. The information security policy should be comprehensive that covers all areas of information security, complies with the requirements of applicable laws including data protection laws, reviewed and approved by appropriate management and executives, communicated and socialized to all employees and relevant third-party contractors, and reviewed and/or updated on an annual basis.

4.2.2. **Information Security Management Organization**. VENDOR shall have identified resource who are capable and qualified in the field of information security to carry out the information security management program.

4.2.3. **Confidentiality**. VENDOR shall treat CONVERGE Personal Data processed pursuant to this Annex with utmost confidentiality. Further, VENDOR shall ensure that their Authorized Persons as well as Sub-Processors, if any, engaged in the Processing of CONVERGE Personal Data under this Annex, understand and are fully informed of the confidential nature of CONVERGE 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 VENDOR.

4.3. **Human Resource Security**.

4.3.1. **Background Screening**. VENDOR shall conduct adequate background checks on its employees and third-party contractors who will gain access to CONVERGE Personal Data in accordance with relevant data protection laws or regulations. The level of background checks should be appropriate to the function or role of an employee or third-party contractor as well as the sensitivity of the information being accessed or processed, including any risks associated with the processing of personal data or information. Unless prohibited by law, the background checks such as (a) identity verification, (b) criminal records, (c) employment history and (4) educational attainment shall be performed prior to employee or third-party on-boarding.

4.3.2. **Information Security and Data Privacy Awareness Training**. VENDOR shall conduct awareness trainings relevant to information security and data privacy to its Authorized Persons and third-party contractors on an annual basis who have access to or process CONVERGE Personal Data. VENDOR shall ensure that proper data privacy and information security awareness trainings are conducted to its Authorized Persons within thirty (30) days of hire and prior to accessing or processing CONVERGE Personal Data. Certification or proof of training completion of Authorized Persons shall be recorded, maintained, and stored in adherence with its records retention program.

4.4. **Access Control**.

4.4.1. VENDOR shall implement and document a formal access control policy that would support the provisioning, updating, reviewing and de-provisioning of user accounts for Data Processing Systems holding or allowing access to CONVERGE Personal Data. User accounts should be provisioned on a need-to-know basis or created aligned with the principle of 'least privilege', and corresponding approvals must be properly documented. VENDOR shall forbid the use of generic accounts, shared accounts, and shared passwords in order to properly identify the actual user and track their activities.

4.4.2. Only Authorized Persons of VENDOR may access CONVERGE Personal Data processed by VENDOR. VENDOR shall ensure that any person acting under its authority, and who has access to CONVERGE Personal Data collected under this Annex, processes CONVERGE Personal Data exclusively for the purpose/s identified in this Agreement.

4.4.3. User Access Monitoring. Access to CONVERGE Personal Data by all Authorized Persons shall be monitored by VENDOR in accordance with its own data privacy and information security policies.

4.5. **Physical Security**. Facilities where CONVERGE Personal Data are being processed should be limited to Authorized Persons and adequate physical security controls must be implemented to safeguard CONVERGE Personal Data from unauthorized access and unauthorized disclosure.

4.6. **Equipment Protection**. Equipment that either process or store CONVERGE Personal Data should be located within an isolated, dedicated, and secured facility such as server rooms or a data center.

4.6.1. Authorized Persons shall ensure that unattended equipment and sessions are protected. VENDOR shall enforce a clean desk policy and store CONVERGE Personal Data when it is not being processed. Session timeouts shall be implemented on Data Processing Systems to automatically terminate idle sessions and require Authorized Persons to re-authenticate and resume their data processing activities on Data Processing Systems.

4.6.2. To reduce the risk of unauthorized access or unauthorized disclosure of CONVERGE Personal Data, authentication controls must be enforced on network printers. VENDOR shall document and implement adequate security controls relevant to teleworking, remote access, mobile device and use of removable storage media.

4.6.3. VENDOR shall enforce encryption techniques or at a minimum, multi-factor authentication on Data Processing Systems when accessed via remote access communication or through Virtual Private Network (VPN). Only allow and properly configure the necessary ports and protocols necessary for a specific Data Processing System.

4.6.4. VENDOR shall permit Authorized Persons to store or process CONVERGE Personal Data on personal devices. A BYOD program should be implemented by the VENDOR that includes set of controls equivalent to VENDOR issued corporate devices. Read-Only access is only allowed to removable storage devices in the form of either memory sticks, USB drives or Bluetooth storage devices that stores CONVERGE Personal Data and should be encrypted. There should be a documented procedure wherein Authorized Persons are allowed write permissions to removable storage media devices temporarily, subject to a formal approval and risk assessment process.

4.6.5. At any time during the term of the Agreement at the CONVERGEs written request or upon termination or expiration of the Agreement for any reason, VENDOR shall instruct all Authorized Persons to promptly return to the CONVERGE all copies, whether in written, electronic or other form of media of CONVERGE Personal Data in its possession of such Authorized Persons, or securely destroy and dispose of all such copies, and certify in writing to CONVERGE that such CONVERGE Personal Data has been returned to the CONVERGE or disposed of securely. VENDOR shall comply with all reasonable directions provided by CONVERGE with respect to the return or disposal of CONVERGE Personal Data.

4.7. **Environmental Security**. In protecting Authorized Persons and equipment that stores and process CONVERGE Personal Data, VENDOR shall implement environmental security controls. These environmental safety measures shall include the following unless permitted by law, (a) installation of humidity and temperature controls in its server room or data center, (b) fire suppression systems and alarms that must be properly tested, maintained and properly installed, (c) maintain appropriate contact list of authorities active response to civil unrest or natural disasters, (d) backup power support in the form of UPS, generators or separate grid connection.

4.8. **Asset Management**

4.8.1. **Asset Inventory**. VENDOR's information assets must be inventoried and identified and must be recorded within an asset register. At a minimum, VENDOR's asset inventory shall include information such as the asset's version, license, operating system, hardware specification, and the identified asset owner. Information assets must be properly labelled and classified according to its asset value, sensitivity, criticality and risks resulting from unauthorize disclosure.

4.8.2. **Acceptable Use**. Authorized Persons shall adhere to VENDOR's documented and implemented policies for securing and handling assets. All assets shall be returned to the VENDOR immediately upon termination which be must properly monitored and tracked upon return.

4.8.3. **System Hardening**. VENDOR shall document and implement a formal system hardening procedure and baseline configuration. Any unsupported on non-VENDOR accredited software must not be available for use and installed.

5. **Representation and Warranties.**

5.1. Data Sharing. VENDOR shall neither share nor disclose CONVERGE Personal Data received by virtue of this Annex to any other party, nor Process the same for any purpose other than those laid down in the Agreement, or incidental thereto, without the prior written consent of the concerned Data Subjects.

5.2. Data Privacy Compliance. VENDOR hereby represents and warrants that in the Processing of CONVERGE Personal Data under this Annex, it shall comply, and/or is compliant, with Data Protection Laws, regulations, and other relevant government issuances. VENDOR further represents and warrants that they have in place appropriate Security Measures that endeavor to protect CONVERGE Personal Data they process under this Annex from any Information Security Incident, including Personal Data Breach.

6. **Data Subject Rights.**

6.1. **Rights of the Data Subject**. In the Processing of CONVERGE Personal Data, VENDOR commits to respect and uphold the following rights of the Data Subjects:

6.1.1. the right to be informed when the Data Subject's Personal Data are being, or have been processed;

6.1.2. the right to object to the Processing of the Data Subject's Personal Data;

6.1.3. the right to reasonable access, upon demand, to the Data Subject's Personal Data;

6.1.4. the right to dispute the inaccuracy or error of the Data Subject's Personal Data, and have the Parties accordingly correct or cause the correction thereof, unless such is vexatious or unreasonable;

6.1.5. the right to suspend, withdraw, or order the blocking, removal, or destruction of the Data Subject's Personal Data from VENDOR's Data Processing Systems;

6.1.6. the right to obtain a copy of the Data Subject's Personal Data, where the Data Subject's Personal Data is processed by electronic means; and

6.1.7. the right to complain before government authorities of any data privacy violation committed by either Party in the Processing of the Data Subject's Personal Data under this Annex.

6.2. **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 VENDOR under this Annex. A Data Subject who seeks to access and/or modify his/her Personal Data and/or exercise any of the rights under Section 6.1 hereof may address the Data Subject's request in writing to the Parties.

7. **Personal Data Breach Notification**.

7.1. If the VENDOR becomes aware of any Personal Data Breach or suspects a Personal Data Breach is going to occur, involving any of its personnel, premises, facilities, systems, and/or privacy policies, it shall:

7.1.1. inform CONVERGE of the Personal Data Breach within twenty-four (24) hours;
7.1.2. investigate the Personal Data Breach and inform CONVERGE of the result thereof;
7.1.3. 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
7.1.4. inform the relevant government authorities of such event, if legally required to do so.

7.2. In case of any Information Security Incidents other than Personal Data Breach, and any unsuccessful or attempted Personal Data Breach, VENDOR shall notify the CONVERGE within twenty-four (24) hours. 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.

7.3. VENDOR shall use best efforts to immediately remedy any Personal Data Breach and prevent any further breaches at VENDOR's expense in accordance with applicable Data Protection Laws, regulations, and standards. In case the Personal Data Breach is due to the fault or negligence of VENDOR, it shall reimburse CONVERGE for actual costs incurred by CONVERGE in responding to, and mitigating damages caused by, any Personal Data Breach, including all costs of notice and/or remediation.

7.4. In the event of any Personal Data Breach, VENDOR shall promptly use its reasonable efforts to prevent a recurrence of any such Personal Data Breach.

7.5. The obligation of the VENDOR to report or respond to a Personal Data Breach under Section 7.1 hereof is not and will not be construed as an acknowledgement by the Parties of any fault or liability for the Personal Data Breach.

8. **Managing Security Compliance**.

8.1. Upon CONVERGE's request, to confirm VENDOR's compliance with this Annex, as well as any applicable Data Protection Laws, regulations and industry standards, VENDOR grants CONVERGE permission to perform an assessment, audit, examination or review of all controls in VENDOR's organizational, physical and technical Security Measures in relation to all CONVERGE Personal Data being handled and/or services being provided to CONVERGE pursuant to the Agreement.

8.2. VENDOR shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores or transports CONVERGE Personal Data pursuant to the Agreement. In addition, upon CONVERGE's request, VENDOR shall provide CONVERGE with the results of any audit by or on behalf of VENDOR performed that assesses the effectiveness of VENDOR's information security program as relevant to the security and confidentiality of CONVERGE Personal Data shared during the course of the Agreement.

8.3. VENDOR shall conduct Privacy Impact Assessments, to identify potential risks arising from Processing of CONVERGE Personal Data.