I. Introduction

This Privacy Manual is hereby adopted by Leisue, Inc. (herein referred to as Leisue) for its applications, including “Kyoo”, to comply with Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission. This company puts premium on the protection of your data privacy rights. We assure you that all personal data collected from you, our clients and customers, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform you of our data protection and security measures, and may serve as your guide in exercising your rights under the DPA.

II. Definition of Terms

For the purposes of this manual and in consonance with the DPA and its IRR, these terms are defined as follows:

A. "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.

B. "Commission" or the "NPC" shall refer to the National Privacy Commission of the Republic of the Philippines.

C. “Company” or “Corporation” shall refer to Leisue, Inc., its affiliates and subsidiaries (e.g. Kyoo), a corporation incorporated under the laws of the Republic of the Philippines

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

E. "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 personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so. It may be in a form of a Consent Form as specified in Annex “A”.

F. "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 DPA, its IRR,

and any other government-issued data privacy regulations and issuances, as well as in implementing this Manual.

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

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

I. "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.

J. "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 devices 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.

K. “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.

L. "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.

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

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

a) "Confidential Personal Data" pertains to all information to which Processing requires the written consent of the Data Subject concerned, such as but not limited to personal information, mobile phone number, e-mail, credit card numbers, and the like. It also includes Personal Information and Sensitive Personal Information; and

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

O. "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 unauthorized disclosures of, or access to Personal Data; and/or

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

P. "Privacy Impact Assessment" or "PIA" is a process undertaken and used to evaluate and manage the impact on privacy of a particular program, project, process, measure, system, or technology product of the Company or its PIP/s. It takes into account the nature of the Personal Data to be protected, the Personal Data flow, the risks to privacy and security posed by the Processing, current data privacy best practices, and the cost of security implementation. The Company shall conduct a PIA annually to be performed by key personnel of the Company.

Q. "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 Subject. This Manual outlines and embodies the Privacy Policy of the Company.

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

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

T. "Processing" refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. It may be done through automated means or by manual processing.

U. "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.

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

W. "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.

III. Scope and Limitations

All personnel of the Company, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy Manual.

IV. Processing of Personal Data

A. Collection

This company collects the basic contact information of clients and customers, including their full name, address, email address, contact number, or other seminar information. The Company's application/s shall collect such information through online registration forms. These information may be collected by the mobile or online application/s of the Company through a third party companies. The Users of the mobile or online application/s, including those utilizing the application/s through a third party company, understands that their information shall be collected by the Company.

B. Use

Personal data collected shall be used by the company for online queuing purposes, documentation purposes, for tracking of customers, and for other legitimate and related purposes.

C. Storage, Retention and Destruction

This company guarantees that personal data, including those obtained through third party companies, under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. The company will implement appropriate security measures in storing collected personal information, depending on the nature of the information. All information gathered shall not be retained for a period longer than five (5) years. After five (5) years, all hard and soft copies of personal information shall be disposed and destroyed, through secured means.

D. Access

Due to the sensitive and confidential nature of the personal data under the custody of the company, only the client and the authorized representative of the company shall be allowed to access such personal data, for any purpose, except for those contrary to law, public policy, public order or morals.

D. Disclosure and Sharing

All employees and personnel of the company shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the company shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

V. Security Measures

A. Organization Security Measures

1. Data Protection Officer (DPO), or Compliance Officer for Privacy (COP)

The designated Data Protection Officer is Rechelle C. Orense, who is concurrently serving as Project Manager of the organization.

2. Functions of the DPO, COP and/or any other responsible personnel with similar functions

The Data Protection Officer shall oversee the compliance of the organization with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security

measures, security incident and data breach protocol, and the inquiry and complaints procedure.

3. Duty of Confidentiality

All employees will be asked to sign a Non-Disclosure Agreement. All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

4. Review of Privacy Manual

This Manual shall be reviewed and evaluated annually. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

1. Format of data to be collected

Personal data in the custody of the organization may be in digital/electronic format and paper-based/physical format.

2. Storage type and location

All personal data being processed by the organization shall be stored in a data room, where paper-based documents are kept in locked filing cabinets while the digital/electronic files are stored in computers provided and installed by the Company. It shall be within the Company premises.

3. Access procedure of agency personnel

Only authorized personnel shall be allowed inside the data room. For this purpose, they shall each be given a duplicate of the key to the room. Other personnel may be granted access to the room upon filing of an access request form with the Data Protection Officer and the latter's approval thereof.

4. Monitoring and limitation of access to room or facility

All personnel authorized to enter and access the data room or facility must fill out and register with the online registration platform of the organization, and a logbook placed at the entrance of the room. They shall indicate the date, time, duration and purpose of each access.

5. Design of office space/work station

The computers are positioned with considerable spaces between them to maintain privacy and protect the processing of personal data.

6. Persons involved in processing, and their duties and responsibilities

Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to bring their own gadgets or storage device of any form when entering the data storage room.

7. Modes of transfer of personal data within the organization, or to third parties

Transfers 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.

8. Retention and disposal procedure

The organization shall retain the personal data of a client for five (5) years from the date of obtaining such data. Upon expiration of such period, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure technology.

C. Technical Security Measures

1. Monitoring for security breaches

The organization shall use an intrusion detection system to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system.

2. Security features of the software/s and application/s used

The organization shall first review and evaluate software applications before the installation thereof in computers and devices of the organization to ensure the compatibility of security features with overall operations.

3. Process for regularly testing, assessment and evaluation of effectiveness of security measures

The organization shall review security policies, conduct vulnerability assessments and perform penetration testing within the company on regular schedule to be prescribed by the appropriate department or unit.

4. Encryption, authentication process, and other technical security measures

Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

VI. Breach and Security Incidents

A. Creation of a Data Breach Response Team

A Data Breach Response Team comprising of three (3) officers or personnel of the Company shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

B. Measures to prevent and minimize occurrence of breach

The organization shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

C. Procedure for recovery and restoration of personal data

The organization shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

D. Notification protocol

The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

E. Documentation and reporting procedure of security incidents

The Data Breach Response Team shall prepare a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

VII. Inquiries and Complaints

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their personal data. The Data Subject has the following

rights: right to reasonable access to personal data, right to dispute inaccuracy/error, right to request suspend, withdraw or block, remove personal data, right to complain and indemnity due to inaccurate/incomplete, outdate.

They may write to the organization at privacy@leisue.com and briefly discuss the inquiry, together with their contact details for reference.

Complaints may be filed in three (3) printed copies, or sent to privacy@leisue.com. The concerned department or unit shall confirm with the complainant its receipt of the complaint.

VIII. Amendment and/or Revisions

Any provisions of this Manual could be amended, revised or revoked by this company through a Board Resolution.

IX. Effectivity

This Manual was approved by the Board of Directors of the Company through a Board Resolution this __ day of _____, 2019 and shall take effect immediately.

APPROVED:

Chairman	**Chief Legal Officer, Compliance Officer**
For the Board	**and Data Protection Officer**

X. Annexes

A. Online Consent Form

I, understand and agree that by providing my personal data and by clicking the applicable icon or button in the "Kyoo" application, I am agreeing to the Privacy Notice and giving my full consent to Leisue Inc., its personnels and its affiliates as well as its partners and service providers, if any, to collect, store, access and/or process any personal data I may provide herein, such as but not limited to my name, contact number/s, and email address, whether manually or electronically, for the

period allowed under the applicable law and regulations, and for the processing of my request or message.

I acknowledge that the collection and processing of my personal data is necessary for such purposes. I am aware of my right to be informed, to access, to object, to erasure or blocking, to damages, to file a complaint, to rectify and to data portability, and I understand that there are procedures, conditions and exceptions to be complied with in order to exercise or invoke such rights.

B. Privacy Notice

Leisue Inc., including Kyoo, and its affiliates respects your right to privacy especially when it comes to your personal and data information. The moment you interact with us, you may share the said personal data with us. Personal Data refers to information that identifies you personally, alone or other information you provided with us. To ensure that your right to data 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. We recommend you read this Privacy Notice and Leisue Inc.'s Privacy Manual to understand how we collect, use and process your Personal Data.

C. Inquiry, Complaints, Erasures and Corrections

For inquiries regarding the processing of personal information stated in this Privacy Notice, as well as any concerns or complaints regarding data privacy, or the exercise of your rights as a Data Subject under the DPA, you may contact the DPO as follows, provided that any complaint should be in writing, clearly state the material facts, specify your contact information, include supporting evidence and be submitted to the following office address or email address:

Rechelle C. Orense

Data Protection Officer

Unit 1102, One World Place,

32nd St, Bonifacio Global City,

Taguig, Philippines

Tel: (02) 8824-9106

Email: privacy@leisue.com