Data Privacy Notice for Vendors

This Notice details policies and procedures regarding a collection, use, store and disclose ("Processor") of the personal data in accordance with the Personal Data Protection Act B.E. 2562 (2019). This Notice applies to Vendors ("Vendors"). Please read the privacy notice ("Notice") carefully to understand the University policies and procedures pertaining to the personal data.

1. Definition

"Personal Data" under this Notice refers to any information related to a person, which enables the identification of such person, whether directly or indirectly, including identifiable data such as number of national identification card, address, online information, any physical identity data, socio economical or cultural data.

"Vendors" refers to a person or persons who has legal obligations with the University, including but not limited to selling or buying of goods, services and business transactions.

2. Personal Data Collected by the University

2.1 Personal Data of the Vendors

The University shall collect, use, disclose the personal data as follows:

- Name-Last Name
- Address, House Registration
- National Identification Card or Passport
- Contact Telephone Number and/or Mobile Number
- Email Address
- Photo
- Name of Institute and Education Qualification
- Work experience
- Curriculum Vitae
- Work Permit (for non-Thais)
- Criminal Records
- Any information or records deemed important by the University to collect, use, disclose or process
- Any information the University has collected, processed, received, or disclosed when communicating with the Vendors before, during or after the selection process and the agreement, and/or the process of inquiring about goods or services provided by the Vendors

Furthermore, the University may request for the following additional information.

- Health data and disability
- Nationality
- Gender

- Religion or any other data which may be used to identify or certify your qualification or to offer as educational service of the University

2.2 Special Category Personal Data

The University shall collect special category personal data in accordance with Section 26 of the Personal Data Protection Act B.E. 2562 (2019), pertaining to racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, genetic data, biometric data or of any data. The University shall access, collect, use, disclose or control of the personal data with carefulness and in accordance with related laws/rules and regulations. In addition, the University shall notify the Vendors prior to or during the collection, use or disclosure of the special category personal data, for compliance with related laws.

2.3 Personal Data relating to criminal convictions and offences

The Vendors acknowledge that, in an event where criminal convictions and offences take place, before or during the period of studies, be it civic or criminal offences or any other offences, before or after the period of studies, the University reserves the right to collect or use information relating to criminal convictions and offences. The University shall carefully access, collect, use, disclose or control the Personal Data to the extent required by laws.

2.4 The University shall collect, process or use the personal data from external persons/the third party.

- Contact address, demographic information, reference or public information the University gathered/collated from the third party/affiliated persons on the prospective vendors who may enter into agreement with the University.
- Information on criminal offences, financial credit, work experience and education background which, as part of the background check process, the University shall collect or receive from related-government agencies or financial institutions, former employers or related-education institutions, within legal limit.

The University hereby wishes to inform the Vendors that, in order to protect and safeguard the security of the Vendors and to protect the interests of the University, the University has set up a closed-circuit television system ("CCTV") to ensure and safeguard the safety on the premises of the University. In this regard, the University or Service Providers outsourced by the University shall collect, use or process information from your still pictures or motion pictures or personal data when being present on the premises of the University, for safety of the University and other Vendors.

3. Personal Data Processed by the University

The University shall collect, use, disclose and process the personal data of the Vendors collected directly from the Vendors or from the external sources as described in Item 2.

In some cases, the University may request additional information from the Vendors, in order for the University to carry out contractual obligations or any other requests. The University

shall notify the Vendors when such needs arise. In this regard, failure to provide required information may result in a termination of contract or the University may be unable to carry out related requests by the Vendors.

4. Purpose and Legal Obligations to Process the Personal Data

The University shall process the personal data of the Vendors in order to select and evaluate the prospective vendors who are interested in providing services and working with the University to communicate/disseminate the information of the University and status of the agreement with the University. In case the University agrees to work with the Vendors, the University may process the personal data of the Vendors for service acquisition and registration as a new vendor in order to carry out any related-businesses/obligations with the University.

The University may use the personal data in relation to strategies and administration of the teaching and learning offered by the University, submission of reports to related-government agencies and financial planning. The University also uses the personal data as required by laws and for the implementation of related-rules and regulations.

The University has legal basis to process the collected personal data in order to offer services, as follows:

- The University has legal rights to select and hire the prospective vendors who are qualified and agree to comply with the rules and regulations relating to the management and administration of the University, including the administration of teaching and learning in an appropriate and ethical manner. The University shall process the personal data of the Vendors in relation to the afore-mentioned purposes. The Vendors may request further information from the Data Protection Officer (DPO).
- The University shall process the personal data of the Vendors in order to meet the obligations stated in the agreement between the Vendors and the University, including the payment for services to the Vendors, a verification process to inspect if the Vendors carry out their agreement as obliged. The Vendors may request for further information from the Data Protection Officer (DPO).
- The University may have to process the personal data in order to comply with the laws. In case of the special category personal data pertaining to (1) racial, ethnic origin, political opinions, cult, religious or philosophical beliefs, trade union data (2) biometric data and genetic data and (3) health data and sexual behavior, the University is obliged to analyze the personal data whether or not (i) the University receives the consent of related Vendors to proceed; (ii) the University is required by law to process the personal data; or (iii) the University is to protect the interests of the University.
- The Vendors may request for further information from the Data Protection Officer ("DPO") when the University processes sensitive data with the Vendors'

given consent. The Vendors may withdraw their consent at any time under the terms and conditions as specified by the University by contacting the DPO. In the event where the consent is withdrawn, the University may process the personal data as required by law or as to protect the interests of the University. However, when there is a withdrawal of consent, the University shall inform the Vendors accordingly which information is to be processed as required by laws or as to protect the interests of the University.

- In addition, the University shall process the personal data for other purposes, including for historical research, statistics or science for archives, and for public interest. When possible, for these purposes, the University shall avoid using any identifiable data or the University shall limit the use of the personal data for research purposes or for collecting secondary data, including the use of pseudonymization, in order to avoid a violation of personal data.

5. Receiver of the Personal Data

The University realizes a significance of an assurance of confidentiality of the personal data and assures a limit of access of the personal data to only those with related-duties, personnel and staff of the University and third-party service providers who are affiliated with the University. The University shall disclose and share only necessary information in order to process information related to service offering and to protect the interests of the University, and the University hereby agrees to protect the personal data from any unauthorized access. The Vendors may contact the DPO for further information pertaining to the 3rd party service providers to whom the personal data is disclosed. The University may disclose the Vendors' contact details as listed to other university personnel and the general public. However, the Vendors are entitled to request for a deletion of their personal data under the terms and conditions and within a period as specified by the University.

The University shall disclose the personal data to other universities or affiliated offices for related-university business and activity, travel arrangement, or activity coordination, professional affiliations and research. The University may also disclose the personal data to government agencies related to immigration, tax and revenue, national security and crime, or any other activities required by laws.

In addition, the Vendors agree with the University to disclose or transfer the personal information to affiliates or alliances and business partners of the University in order for business operation, compliance of policies, and legitimate interest of the University, including any other cases announced by the University from time to time.

6. Transfer of the Personal Data to the Third Country

The University may transfer the personal data to the Third Country for research purposes, as deemed necessary. The Vendors agree to a transfer of the personal data to countries outside of Thailand or to affiliated persons or offices or under the jurisdiction of other countries whether or not the personal data protection laws of those countries meet the legal standards of Thailand.

The University shall proceed with any appropriate procedures which have the same standards applicable in Thailand for personal data protection.

7. Data Retention Period

The University shall collect the personal data as required and as necessary during the period required by law. The Vendors may contact the DPO of the University to check the data retention period.

8. The Rights to Personal Data

At any time, the Vendors have the rights to the personal data, as follows:

- Rights to know and inquire about the purposes for the collection, use, process or disclosure of the personal data
- Rights to know about the types of related-personal data
- Rights to know/inquire about the receiver of the personal data
- When possible and applicable, the rights to know about the data retention period. In the event when it is not possible, the rights to information about the requirements for data retention period
- Rights to have access to the personal data, and to request for a correction of any inaccurate/incomplete personal data
- Rights to request for a copy of the personal data in electronic forms in an intelligent format, which you may forward to the 3rd party directly or you may request the University to forward such information
- Rights to object to the process/analysis of the personal data for marketing-related purposes or other purposes
- Rights to request for a deletion of the personal data per case-by-case basis, for example, when it is deemed unnecessary to store and retain the information to meet the requirement of data retention or in the event when there is a withdrawal of consent for the collected personal data, or an objection to the process of the collected personal data
- Rights to appeal to related-governing agencies for a breach of personal data

In order to exercise the rights to the personal data as prescribed above, the Vendors are required to submit a request in writing to the DPO of the University, as detailed in Item 9, as follows:

9. Data Protection Officer

If the Vendors wish to make a request to any of the items listed in Item 8 or to request further information related to the collection, use or disclosure of the personal data collection, they may contact the DPO as detailed below.

The Data Protection Officer
The Committee for Personal Data Protection of Bangkok University
Address: 9/1 Phahonyothin Road, Klong Nueng Sub-district, Klong Luang District, Pathum Thani Province 12120
Tel: 02 407 3888

Email: pdpc@bu.ac.th

10. A Withdrawal of Consent

If the Vendors no longer allow the University to collect, use, process or disclose the personal data, they may withdraw their consent by submitting a request for a withdrawal of consent to the DPO of the University.

A withdrawal of consent must be carried out under the terms and conditions of related rules and regulations, announcements pertaining to the personal data protection policies and procedures as determined/specified by the University.