Data Privacy Notice for Employees of the University

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 all Employees of the University, including all affiliated offices and units of the University —executives, full-time instructors, adjunct instructors, personnel and staff (referred to as "Employees" or "You"). Please read the privacy notice ("Notice") carefully to understand the University policies and procedures pertaining to your 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

2. Your Personal Data Collected by the University

2.1 Personal Data of the Job Applicants

In order to consider the job applicants for employment, the University shall collect, use, process and disclose the personal data, as follows:

- Name-Last Name
- Address, House Registration, Place of Origin
- National Identification Card or Passport
- Contact Telephone Number
- Mobile Number
- Email Address
- Title of Educational Institution and Education Qualification
- Details of Work Experience
- All information related to job applicants
- Curriculum Vitae
- Work Permit (for non-Thais)
- Criminal Records
- Current work history/job experience, including information about former employers, place of former employment and address, period of former employment, salary details, work-related behavior or work-related history, etc.

The University may contact the reference persons as mentioned during your job application process, as required and as necessary within legal limits, in order to protect the interest of the University.

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 Employees' Personal Data

Apart from the personal data which the University has collected during the job application process, the University shall collect, use, process or disclose the Employees' personal data in relation to a performance evaluation/appraisal. In addition, the University, as the employer, shall collect, use, process or disclose your personal data, in order to carry out any obligations as stated in an employment contract or a labor contract or any legally binding contracts between you and the University, as follows:

- Information related to ailments and causes of absence
- Bank Account details
- National Identification Card and House Registration
- Visa and Work Permit (for Non-Thai Employees, if any)
- Sick Leave Records
- Information related to Absence/Leave (including Holidays, maternity leave or other types of leave/absence)
- Retirement Information
- Salary, Benefit and Welfare
- Emergency Contact Persons
- Health Data
- Job-related Performance, Behaviors and Performance Evaluation/Appraisal
- Disciplinary Records
- Criminal Records and Offences
- Any information related to your records as the employee of the University or contracted person
- Any information deemed important by the University in relation to the performance evaluation/appraisal or contract fulfillment, in order to protect the interest of the University

2.3 Special Category Personal Data

The University shall collect the Employees' 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 Employees prior to or during the collection, use or disclosure of the special category personal data, for compliance with related laws.

2.4 Personal Data relating to criminal convictions and offences

The Employees 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.

2.5 The University shall collect, process or use the personal data from external persons/the third party, as follows:

- Any information about the educational background and work experience, which the University shall collect, use, process or disclose during the job application process or during employment as required, for example, for a promotion. The University may confirm with your former employers and education institutions your records of personal data
- For information related to professional certificates or education qualification, the University, when necessary, may need to verify the information of such certificates or qualifications with the third party.
- Health data, within legal limit, the University shall collect, use, process or disclose information about your health received from hospitals or health centers or from any persons to verify your health conditions, in order to fulfil employment obligations or to approve any welfare you are entitled to receive.
- Information from other employees or students, which the University may receive in a form of report, notification, complaints under the University's rules and regulations or as required by laws, in order for the University to acknowledge related personal data such as name, behavior, activities or any other information.
- Immigration-related information, the University may receive your personal data from related-government agencies such as the Immigration Bureau, the Embassy and Consul such as information of the National Identification Card Number, Passport or Visa-related information or entries into Thailand, in order for the University to assist you with traveling, for the benefit of the personal data holders, in compliance with required laws, rules and regulations. The information may be different depending on the rules and regulations of each country.

The University hereby wishes to inform the Employees that, in order to protect and safeguard the security of the Employees 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 Employees.

3. Personal Data Processed by the University

The University shall collect, use, disclose and process the personal data of the Employees collected directly from the Employees or from the external sources as described in Item 2, in order to carry out obligations as stated in the employment contract or any legal

binding agreement or for arrangement of benefit and welfare, provision of equipment, amenities, supplies and services offering by the University, including work history at the University, job performance records, salary, benefit and welfare information and emergency contact person details.

In some cases, the University may request additional information from the Employees such as health insurance and insurance. However, please note that in order for the University to carry out contractual obligations or any other requests. The University shall notify the Employees 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 Employees.

4. Purpose and Legal Obligations to Process the Personal Data

The University shall process the personal data for the purposes as follows:

- To submit reports to related-agencies.
- To administer programs and related-services appropriately and efficiently
- To explore opportunities for fundraising activities.
- To verify identity of Employees
- To prepare the University for emergency situations
- To implement the University's rules and regulations and comply with related-laws.
- To issue an invoice, collect outstanding debts, return a refund and receive a payment.
- To provide service and support for internal research study carried out by the University
- To coordinate and facilitate functions such as seminars, trainings or workshops.
- To provide assistance and support for the Employees Association related-activities and any other promotional activities.

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

- The University has legal rights to raise funds to support the teaching and learning of the University or to support the Employees Association or any affiliated persons, in order to comply with related-laws, rules and regulations of the University and to administer the programs for teaching and learning efficiently, appropriately and ethically. The Employees may request from the Data Protection Officer (DPO) additional information on lawful profit the University recorded/described in the data processing records of the Employees/Employees.
- The University may have to process the personal data of the Employees in order to carry out any obligations on any agreements entered between the University and the Employees or when the Employees require any services from the University, or when

the University receives any donation made by the Employees. The Employees may request for the information directly 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 Employees 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 Employees may request for further information from the Data Protection Officer ("DPO") when the University processes sensitive data with the Employees' given consent. The Employees 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 Employees 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 Employees 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 Employees' contact details as listed to other university personnel and the general public. However, the Employees 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 Employees 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 Employees 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 Employees may contact the DPO of the University to check the data retention period.

8. The Rights to Personal Data

At any time, the Employees 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. OR 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 pertaining to students, related-schools or status of the Employees, any journals or printed matters published by the University in relation to education, recruitment, fundraising or any other related-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

In order to exercise the rights to the personal data as prescribed above, the Employees 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 Employees 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 Employees 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.