



## Assumption University Announcement

No.13/2023

Subject: Personal Data Security Measures B.E. 2566 (2023)

As deemed appropriate in order to carry out the University's operations to effectively maintain the security of Personal Data, the President - Rector Magnificus, by the virtue of Section 43 of the Private Institution of Higher Education Act B.E. 2546 (2003), as amended (No.2) B.E. 2550 (2007), hereby establishes the Personal Data security measures for Assumption University as follows:

No.1 This Announcement is entitled, "Assumption University Announcement of Personal Data Security Measures B.E. 2566 (2023)".

No.2 The objectives of this Announcement are aimed:

2.1 To establish the University's Personal Data security measures encompassing aspects related to the management, as well as the technical measures and physical measures, regarding Person Data access control;

2.2 To enable stakeholders to lawfully use as a principle of Personal Data protection;

2.3 To ensure that the University carries out the protection of Data Subject's Personal Data and Data Privacy in a standardized and comprehensive manner.

No.3 In this Announcement,

"University"	means	Assumption University;
"President - Rector Magnificus"	means	President - Rector Magnificus of Assumption University;
"Division"	means	faculty, institute, major/department, center, office;
"Policy"	means	Personal Data Protection Policy indicated in the University's Announcement;
"Personal Data"	means	information about a person who can be identified either directly or indirectly, but not including information of a deceased person;
"Personal Data Processing"	means	the collection, storage, use, or disclosure of Personal Data, or any sequence of activities carried out on Personal Data, whether automated or not. These activities encompass the recording, arrangement, structuring, retention, changes or adjustment, as well as reception, use, or disclosure by transferring or disseminating any actions to cause the availability, arrangement or merging, as well as the removal, erasure, or damage of Personal Data;
"Personal Data Controller"	means	the vice-presidents, deans, registrar, and directors who have power to make decisions on the collection, storage, use, or disclosure of the Personal Data;

Continued page 2 / "Personal..."



“Personal Data Processor”	means	the University’s personnel who carry out the Personal Data Processing in accordance with the order of the Personal Data Controller;
“Data Subject”	means	students, personnel, alumni, and individuals including persons with parental power to act on behalf of minors, or custodians with power to act on behalf of the incompetent, or curators with power to act on behalf of the quasi-incompetent;
“Personal Data Protection Officer”	means	a staff, appointed by the University, for protecting Personal Data.

#### No.4 Personal Data Security

4.1 The University has the Personal Data security measures in accordance with provisions of the law and other necessary standards in order to maintain Confidentiality, Integrity, and Availability by the following security operations.

##### 4.1.1 Administrative Safeguard

(1) Prevention is acted against unauthorized persons for processing Personal Data from accessing the Personal Data Processing system, such as specifying a person authorized to access the Personal Data Processing system by Active Directory, setting policies regarding code use and code change to access Personal Data and authorization for specific personnel of the University or only for authorized external specialists only to access, administer and maintain the data center or the Information Technology network system.

(2) Personal Data access is restricted only to the Personal Data Processor who has a necessary job-related requirement so as to use the data at each hierarchical level and to ensure that records and backups of data access, or the restriction to the use in an appropriate or legally mandated period.

(3) Authorized persons are prevented from accessing and processing Personal Data beyond their permitted rights and duties.

(4) Audit trails are taken in action if Personal Data of any person is found to have been accessed, altered, removed from the system, or erased.

(5) A compliance with orders is under control and can be certified to ensure that Personal Data Processing conforms to the terms and contracts between the Personal Data Controller and the Personal Data Processor, such as requiring that the Personal Data Processor can alter, move, or delete Personal Data only upon receiving specific and precise instructions from the Personal Data Controller, or stipulating that when the Personal Data Process receives a written instructions for the Personal Data Controller, the Personal Data Processor must establish procedures or methods to ensure that processing complies with audit trails, and so forth.

(6) The control of data separation ensures that Personal Data collected for different purposes must be processed separately.

(7) Effective communication systems and mechanism are arranged to keep up-to-date circumstances among the Personal Data Protection Officer, Personal Data Processor and other authorized personnel.

(8) Business Continuity Plan is arranged, in which methods of prevention, protection and recovery of Personal Data are also indicated.

(9) Review of user access rights is arranged in a consistent manner or at least once a year, and when the necessity for a person responsible for Personal Data and the operator of Personal Data operators find no longer necessity to access Personal Data, such as through staff relocation or the termination of employee contract, his/her access rights to the data must be immediately revoked.

(10) Periodically checking of the Personal Data Security Measures is arranged to ensure that the implemented measures being used are appropriate and effective.



(11) Personal data security measures and personal data protection guidelines are created and disseminated for the University personnel and related persons to be acknowledged. As well, awareness of the importance of Personal Data Protection is promoted for the mentioned groups of persons to strictly comply with the measures and guidelines.

#### 4.1.2 Technical Safeguard

(1) System security is arranged, such as security in network and Information Technology systems related to Personal Data Processing.

(2) Data security is arranged, such as checking the security system in which the data is stored to ensure appropriate access control is in place and that information is stored securely.

(3) Online security is arranged, such security of the website and the application, or online services related to Personal Data.

(4) Device security, including safety of tools or related devices, is arranged, such as controlling the external device usage by the personnel or services users who connect their devices to the University's, by setting policies regarding bringing their own devices to work or Bring-Your-Own-Device (BYOD), and so forth.

(5) Authentication is required for accessing the system used for processing Personal Data. Factors used for authentication may include passwords, security tokens, or biometrics, and so forth.

(6) The installation of software unrelated to the University's operations is prohibited, and it is strictly forbidden to install illegal software in the University's information systems.

(7) Disclosure of Personal Data is controlled and monitored, whether it involves data transportation, data transfer, data forwarding, or data storage in data storage devices, both materially and electronically, such as requirements for all important and sensitive data to be transferred using secure encrypted communication channels, e.g., SSL Secured VPN, SFTP, access to an application using https, pseudonymization, or encryption, and so forth.

(8) Availability of Personal Data is under control in order for data to be protected from accidental destruction or loss, such as a provision of centralized, anti-virus and security software, requirement for important and sensitive data stored on the server to be housed in a secure, certified data center, requirement for measures to ensure of data availability at all times, especially network capacities supporting operations during peak working hours, and requirement for the daily backups of important data, and so forth.

#### 4.1.3 Physical Safeguard

(1) Access control is established to the restricted area or devices to collect Personal Data and the workplace for workers working on Personal Data. For example, using electronic keys or personalized key cards to enter or exit the buildings or the workplace, determining the restricted areas such as the server room, or the Personal Data storage room have to be locked and the access shall be given to only the authorized persons.

(2) Clear identification of persons is required, by using appropriate approaches, such as showing the identification card of personnels or visitors, clearly determining accessible areas to the personnels and visitors, and so forth.

(3) The security for the buildings, devices for the Personal Data storage and working areas of operators involving Personal Data is provided, such as maintaining the good conditions of doors, windows, bolts, knobs, or padlock, security guards, lighting, temperature and humidity control system, backup power system, fire extinguishing devices and system, water leakage protection system, the authentication system for the access control, notification alarm system or CCTV system and so forth.

(4) Provide inspection before disposal of unused documents or electronic devices to prevent the leakage of Personal Data.



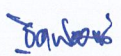
No.5 The Personal Data Controller shall maintain the provisions of Personal Data in accordance with this announcement.

Announced on August 7, 2023

*Rev. Bro. Bancha Saenghiran, f.s.g., Ph.D.*

Rev. Bro. Bancha Saenghiran, f.s.g., Ph.D.  
President - Rector Magnificus

**Note: If this announcement is to be interpreted, the Thai version shall prevail.**

  
Office of Human Resources Management 