มหาวิทยาลัยอัสสัมชัญ
ASSUMPTION UNIVERSITY

**Assumption University Order**

No.128/2023

Subject: Guidelines for the Operations of Personal Data Controller

---

In accordance with Assumption University Announcement No. 12/2566, regarding Personal Data Protection Policy B.E. 2566, no.3, assigning the vice-presidents, registrar, deans, and directors to act as Assumption University Personal Data Controller.

In order for the operations of the appointed persons to comply with Section 37 of the Personal Data Protection Act B.E. 2562, regarding the duties of the Personal Data Controller, the President - Rector Magnificus of Assumption University exercises authority in accordance with Section 43 of Private Higher Education Institutions Act B.E. 2546, as amended (No. 2) B.E. 2550, has therefore established the guidelines for the operations of the appointed Personal Data Controller, hereinafter referred to as "you" as follows:

No.1 Verify, consider, collect, compile, use, or disclose Personal Data of the divisions under your responsibility in accordance with the purposes specified in Assumption University Announcement No.12/2566.

No.2 Supervise/Control the security of Personal Data within your responsibility in accordance with Assumption University Announcement No.12/2566 by

**2.1 Administrative Safeguard**

(1) Specify access rights to Personal Data of personnel under your division. Define access levels based on the data processing duties, assigning codes or providing cabinet keys in cases where data is stored in document format. Maintain a registry of authorized personnel at each level, continuously review access rights and update them promptly if any changes occur. This is to ensure that the University Personal Data Protection Officers can verify the access rights of personal data.

(2) Establish terms and conditions for processing personal data, such as obtaining explicit consent from data owners before collecting, compiling, using, or disclosing any specific information. For instance, processing data for research purposes or making changes, transfers, or deletions of Personal Data should only be done upon receiving written authorization from you.

(3) Control/Verify compliance with the specified conditions by implementing a system that certifies adherence to these conditions. This includes examining historical data to confirm which individuals' Personal Data are accessed, modified, removed, or deleted.

**2.2 Technical Safeguard**

(1) Coordinate with the Information Technology Service Office (ITS) to provide the system security, data security, and online security by implementing software to prevent viruses and unauthorized data access.

(2) Regularly assess the security of devices used within your division. This involves controlling the usage of personal devices by personnel or service users connected with the organization devices, setting the policies regarding the use of personal devices for work purposes, and managing Bring-your-own-Device (BYOD) practices.

(3) Verify the accuracy of authentication using in accessing systems processing Personal Data within your division. The authentication factors may include passwords, security token, or biometrics.

(4) Verify that unrelated software is not installed and ensure that no illegal software is installed within your organization's information systems.

(5) Verify the disclosure of Personal Data, including data transportation, data transfer, data transmission, or storing data on storage devices both physical and electronic. Ensure that all sensitive and detailed information is securely transferred using encrypted communication channels, such as SSL Secured VPN, SFTP, accessing applications via HTTP, Pseudonymization, or encryption.

*Continued page 2 / (6) Establish...*

(6) Establish measures to ensure that data is readily available and can be verified at any time. For instance, store Personal Data on secure servers accessible only by authorized personnel, and provide daily backups of critical data.

**2.3 Physical Safeguard**

(1) Establish control access to offices or equipment used for storing Personal Data, such as server rooms, using electronic keys or key cards assigned to specific individuals to access document storage areas, consistently locked the rooms and the entry should only be permitted for authorized personnel.

(2) Maintain the security of workspaces related to Personal Data, as well as equipment used for storing Personal Data. This includes inspecting the quality of doors, windows, locks, bolts, or keys to ensure they are always in good condition. Implement adequate lighting, temperature and humidity control systems, backup power systems, fire extinguish equipment, waterproofing systems, access control with personal identification, alarm systems, and CCTV.

(3) Verify the dispose of documents or electronic equipment that are no longer in use to prevent leakage of Personal Data.

No.3 Handling other matters

3.1 Report any Personal Data breaches immediately upon discovery or receipt of a report to Personal Data Protection Officer via email: audpo@au.edu, using the form as attached to this order.

3.2 Maintain records of Personal Data Processing Activities (RoPA) for review by the Personal Data Protection Officer.

Ordered 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 order is to be interpreted, the Thai version shall prevail.**

*Office of Human Resources Management*

# Personal Data Breach Notification

Date: .....

To: Personal Data Protection Officer

The Faculty/Office of ..... has found the Personal Data Breach that poses a risk to the rights and freedom of person who is the owner of this Personal Data. The details are as follows:

| | |
|---|---|
| Details of Personal Data Breaches | **Specify details of the incident that poses a threat to Personal Data,** such as<br>1. Data being covertly copied by former personnel.<br>2. Unauthorized attack and access to the database.<br>3. Database being attacked by Ransomware, causing service unavailability for a period of time or delays in services.<br>4. Physical documents (papers) containing Personal Data being stolen. |
| Date and Time of Incident | **Please specify the date and time of incident.**<br>Date ..... Month ..... Year ..... Time ..... |
| Incident Reporters (if any) | **Specify the name and the position of reporter/witness.** |
| List of Affected Personal Data | **Specify a list of affected Personal Data from the incident,** such as<br>• Name - Surname<br>• Email<br>• Academic Performance and Health Record |
| The Impact Pattern(s) on Personal Data | **Specify the impact pattern(s) occurring on the Personal Data,** such as<br>• Being publicly disclosed and potentially causing harm to the Personal Data owner.<br>• Accidental deletion.<br>• Unauthorized access and misuse by individuals without permission. |
| The Number of Affected Personal Data Subjects | **Specify the number of affected Personal Data Subjects.** |
| Response Measures to Halt Data Breaches | **Specify measures/actions to stop threats**, such as immediate system suspension, instant email recall for mistakenly sending out, notifying the telecommunications service provider to immediately lock lost devices. |
| Report Incident to the Personal Data Subject (only if there is a high risk of impact on the rights and freedom a person) | **Specify the university's procedures for notifying the Personal Data Subject (if applicable) along with remedial measures,** such as sending a notification letter to the affected Personal Data Subject via email, including a link for the Personal Data Subject to immediately change his/her login password. |

.....

(.....)

Dean / Registrar / Director

Document attached to Order no.128/2023