明志科技大學

Ming Chi University of Technology

個人資料檔案安全維護計畫

Personal Data File Security and Protection Plan

出 版 者：明志科技大學 圖書資訊處

Publisher: Office of Library and Information Services, Ming Chi University of Technology

文件編號：PS-02-005

Document No.: PS-02-005

機密等級：一般

Confidentiality Level: General

使用本文件前，如對版本有疑問，請與文件維護員確認最新版

Before using this document, please confirm the latest version with the document custodian if you have any doubt about the version.

本文件歷次變更記錄：

Revision History of this Document:

版次 Version	發行日 Issue Date	編撰者 Author	說明 Description	核准者 Approved by
1.0	2016/10/18	賴瑞忠	個人資料檔案安全維護計畫作業。 Personal Data File Security and Protection Plan operations.	沈明雄
2.0	2026/07/21	何嘉彤	新增資安措施與稽核相關規定。 Added information security measures and audit-related provisions.	劉祖華

目　　錄

Table of Contents

1 目的

Purpose

明志科技大學（以下簡稱本校）為落實個人資料檔案之安全維護及管理，防止個人資料被竊取、竄改、毀損、滅失或洩漏，以及業務終止後個人資料處理方法等相關個人資料管理事項，特訂定本校個人資料檔案安全維護計畫（以下簡稱本計畫）。

To implement the security maintenance and management of personal data files, to prevent personal data from being stolen, altered, damaged, destroyed or disclosed, and to regulate the handling of personal data after business termination and other related personal data management matters, Ming Chi University of Technology (hereinafter referred to as the "University") hereby formulates this Personal Data File Security and Protection Plan (hereinafter referred to as the "Plan").

2 適用範圍

Scope of Application

本計畫適用於本校全體教職員工生、臨時約聘/僱人員及接受本校委辦案派駐本校之人員。

This Plan applies to all faculty, staff and students of the University, temporary contract/hired personnel, and personnel stationed at the University under projects commissioned to the University.

3 依據

Basis

3.1 個人資料保護法。

Personal Data Protection Act.

3.2 個人資料保護法施行細則。

Enforcement Rules of the Personal Data Protection Act.

3.3 個人資料保護法之特定目的及個人資料之類別。

The Specific Purposes and Categories of Personal Data of the Personal Data Protection Act.

3.4 教育體系資通安全管理規範。

Regulations on Information and Communication Security Management for the Education System.

3.5 私立專科以上學校及私立學術研究機構個人資料檔案安全維護計畫實施辦法。

Regulations Governing the Implementation of Personal Data File Security and Protection Plans by Private Junior Colleges or Above and Private Academic Research Institutions.

3.6 教育體系個人資料安全保護基本措施及作法。

Basic Measures and Practices for Personal Data Security Protection in the Education System.

3.7 本校個人資料保護管理委員會設置辦法。

The University's Regulations Governing the Establishment of the Committee of Personal Data Protection and Management.

4 權責單位及管理人員

Responsible Units and Personnel

4.1 個人資料保護管理委員會

Committee of Personal Data Protection and Management

4.1.1 審議個人資料保護政策與制度。

Review and approve personal data protection policies.

4.1.2 審議個人資料教育訓練計畫、風險評鑑與風險改善計畫及稽核計畫。

Review and approve personal data education and training plans, risk assessment and risk treatment plans, and audit plans.

4.1.3 個人資料管理制度適法性與合宜性之檢視、審議及評估。

Inspection, review and evaluation of the legal compliance and appropriateness of the personal data management system.

4.1.4 本校個資保護安全維護措施之建立，及重大個人資料安全事件之應變、處理與協調。

Establish and maintain security measures for personal data protection, and respond to, handle and coordinate major personal data security incidents.

4.1.5 審議其他個人資料保護、管理之規劃及稽核執行事項。

Review of other plans and audit execution matters for the protection and management of personal data.

4.2 個資保護推動組

Personal Data Protection Promotion Team

4.2.1 由圖資長擔任負責人，統籌個資保護作業相關事宜。

The Dean of Library and Information Services shall serve as the Person in Charge coordinate matters related to personal data protection operations.

4.2.2 督導執行小組及稽核小組推動各項個資保護工作。

Supervise the Implementation Team and the Audit Team in promoting all personal data protection work.

4.2.3 負責規劃個人資訊管理制度之維運工作及文件之制（修）定作業。

The Promotion Team shall be responsible for planning the operation and maintenance of the personal data management system and the formulation (amendment) of documents.

4.3 執行小組

Implementation Team

4.3.1 協助各單位進行個資盤點與彙整。

Assist each unit in conducting personal data inventory and consolidation.

4.3.2 推動各單位個人資料管理、保護及維護等事項，並落實於相關業務及人員。

Promote personal data management, protection and maintenance in each unit, and implement them in relevant business operations and personnel.

4.3.3 辦理個資相關教育訓練及宣導作業。

Conduct personal data-related education, training and awareness activities.

4.4 個資稽核小組

Personal Data Audit Team

4.4.1 擬定稽核計畫。

Formulate audit plans.

4.4.2 辦理個資管理稽核作業。

Conduct personal data management audit operations.

4.4.3 複查稽核報告不符合事項之矯正措施。

Re-examine corrective measures for nonconformities identified in audit reports.

4.5 各單位個資管理專人

Dedicated Personal Data Management Personnel of Each Unit

4.5.1 由各單位個資窗口擔任，推動單位內個資保護工作。

The personal data contact person of each unit shall serve as the dedicated personal data management personnel and promote personal data protection within the unit.

4.5.2 協助執行個資盤點及相關保護措施之落實。

Assist in conducting personal data inventory and implementing relevant protection measures.

4.5.3 協助稽核其他單位個資作業。

Assist in auditing the personal data operations of other units.

4.6 本校所有同仁

All Staff of the University

4.6.1 落實個人資料保護相關作業規範。

Implement the relevant operational regulations for personal data protection.

4.6.2 執行本校於各項個人資料保護之決策及交辦事項。

Execute the University’ s decisions and assigned tasks regarding personal data protection.

5 名詞定義

Definitions

5.1 特種個資：個資法第 6 條有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料。

Special categories of personal data: personal data specified in Article 6 of the Personal Data Protection Act concerning medical records, medical treatment, genetics, sex life, health examinations and criminal records.

5.2 國際傳輸：指將個人資料作跨國（境）之處理或利用。

International transmission: refers to the cross-border processing or use of personal data.

5.3 有關個人資料名詞定義，請查閱「個人資料文件名詞解釋彙整表」。

For definitions of terms related to personal data, please refer to the “Glossary of Personal Data Document Terms”.

6 作業內容

Operational Content

6.1 個人資料保護管理組織

Personal Data Protection Management Organization

6.1.1 本校為落實個人資料之保護及管理，設置「個人資料保護管理委員會」並由行政副校長一人擔任召集人，副召集人由圖資長擔任，執行秘書由圖資處專人擔任。委員會下設置個資保護推動組，推動組下設執行小組及稽核小組，各單位設置個資聯絡人擔任個資管理專人，負責推動單位內個資保護工作並協助稽核其他單位個資作業。有關委員會之組成、任務與權責，依本校「個人資料保護管理委員會設置辦法」之規定。

To implement the protection and management of personal data, the University establishes the "Committee of Personal Data Protection and Management," with the Vice President for Administrative Affairs serving as the Convener, the Dean of Library and Information Services as the Vice Convener, and a designated staff member of the Office of Library and Information Services as the Executive Secretary. A Personal Data Protection Promotion Team is established under the Committee; an Implementation Team and an Audit Team are established under the Promotion Team. Each unit shall designate a personal data contact person to serve as its dedicated personal data management personnel, responsible for promoting personal data protection within the unit and assisting in auditing the personal data operations of other units. The composition, duties, powers, and responsibilities of the Committee shall be governed by the University's "Regulations Governing the Establishment of the Committee of Personal Data Protection and Management."

6.1.2 個資外洩事件發生時，其聯繫與通報窗口由圖資處專人擔任，依相關規定辦理通報、聯繫及協調事宜，並協助相關單位進行緊急應變作業。

When a personal data breach incident occurs, the contact and notification point shall be assumed by dedicated personnel of the Office of Library and Information Services, who shall handle notification, liaison and coordination in accordance with relevant regulations, and assist relevant units in carrying out emergency response operations.

6.2 個人資料之範圍界定

Definition of the Scope of Personal Data

6.2.1 本校為教育單位，主管機關為教育部。本校所蒐集、處理或利用之個人資料主要為履行法定義務。

The University is an educational institution under the supervision of the Ministry of Education. The personal data collected, processed or used by the University is mainly for the fulfillment of statutory obligations.

6.2.2 本校個人資料管理範圍涵蓋全校，包括教育或訓練行政、學生資料管理、人事管理、產學合作、圖書館管理等業務所涉及之個人資料蒐集、處理、利用及國

際傳輸。

The scope of the University’ s personal data management covers the entire university, including the collection, processing, use and international transmission of personal data involved in education or training administration, student data management, personnel management, industry-academia cooperation, library management and other business operations.

6.2.3 本計畫之管理人員須定期檢視,發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置。

The management personnel under this Plan shall conduct regular reviews. Where personal data is found to be outside the necessary scope of the specific purpose, or where the specific purpose no longer exists or the retention period has expired and retention is no longer necessary, such data shall be deleted, destroyed, or otherwise appropriately handled by ceasing its collection, processing or use.

6.2.4 「特種個人資料」之蒐集、處理與利用：本校依照「學校衛生法」規定，學校應建立學生健康管理制度；健康檢查及疾病檢查結果，應載入學籍資料。依相關法規規定，可蒐集、處理與利用員工之健康檢查及醫療相關資訊。特種個人資料得經當事人書面同意蒐集、處理或利用。

Collection, processing and use of “special categories of personal data”: In accordance with the School Health Act, the University shall establish a student health management system; the results of health examinations and disease screenings shall be recorded in student records. In accordance with relevant laws and regulations, the University may collect, process and use health examination and medical-related information of employees. Special categories of personal data may be collected, processed or used with the written consent of the data subject.

6.2.5 依「個人資料保護法」立法精神，本校需進行全面性之個人資料盤點，範圍包括本校目前持有之個人資料、本校受委託蒐集、處理或利用之個人資料以及本校委託外部機關蒐集、處理或利用之個人資料皆屬之。

In line with the legislative spirit of the Personal Data Protection Act, the University shall conduct a comprehensive personal data inventory, covering personal data currently held by the University, personal data collected, processed or used by the University under commission, and personal data collected, processed or used by external agencies commissioned by the University.

6.2.6 完成個人資料盤點後，需產出下列文件，其維護權責單位為圖書資訊處：

Upon completion of the personal data inventory, the following documents shall be produced. The Office of Library and Information Services shall be responsible for maintaining these documents:

(1) 各單位個人資料檔案清冊。

(1) Personal data file inventory of each unit.

(2) 本校個人資料檔案風險評鑑表。

(2) The University’ s personal data file risk assessment form.

6.2.7 完成個資盤點後，如果所蒐集、處理或利用之個人資料類別不屬本校個人資料檔案清冊中所列之清單，即需對相關個資之當事人進行告知，並將所有告知行為與內容需有紀錄留存備查。

Upon completion of the personal data inventory, if the categories of personal data collected, processed or used are not listed in the University’ s personal data file inventory, the relevant data subjects shall be notified, and records of all notification actions and contents shall be retained for reference.

6.3 個資蒐集、處理與利用程序違反，可能導致行政處罰之行為

Violations of Personal Data Collection, Processing and Use Procedures That May Result in Administrative Penalties

個人資料保護推動組成員，需針對下列項目進行稽核，以確保本校對個人資料之管理符合「個人資料保護法」之規範，杜絕因違法而導致之各類罰責：

Members of the Personal Data Protection Promotion Team shall audit the following items to ensure that the University’ s management of personal data complies with the Personal Data Protection Act and to prevent administrative penalties arising from non-compliance:

6.3.1 未依規定蒐集個人資料（含告知個資當事人）。

Failure to collect personal data in accordance with regulations (including notifying the data subjects).

6.3.2 未依規定處理個人資料。

Failure to process personal data in accordance with regulations.

6.3.3 未依規定利用個人資料。

Failure to use personal data in accordance with regulations.

6.3.4 未妥善保管個人資料。

Failure to properly safeguard personal data.

6.3.5 未依規定提供當事人行使個資之權利。

Failure to provide data subjects with the exercise of their rights over personal data in accordance with regulations.

6.3.6 未依規定對個資委外作業進行必要之監督。

Failure to conduct necessary supervision of outsourced personal data operations in accordance with regulations.

6.4 個人資料檔案盤點、風險評鑑及風險管理

Personal Data File Inventory, Risk Assessment and Risk Management

6.4.1 本校各單位個資管理專人需依據實際作業，執行個人資料檔案鑑別作業，盤點出本校各單位關於各項業務或特定目的所涉及的作業，並於彙整後填於個人資料檔案清冊中。

The dedicated personal data management personnel of each unit shall, based on actual operations, carry out personal data file identification, take inventory of the operations involved in each business or specific purpose of each unit of the University, and record the consolidated results in the personal data file inventory.

6.4.2 個資管理部門除每年一次執行個資檔案鑑別作業，並應於營運組織變更、作業流程改變發生時，針對變動範圍內之作業程序與個資檔案進行個資檔案鑑別作業。

In addition to conducting personal data file identification once a year, the personal data management department shall, upon changes to the organizational structure or operational processes, conduct personal data file identification for the operational procedures and personal data files within the scope of the change.

6.4.3 用於進行清查之個人資料檔案清冊，應至少包括下列事項：保有單位、個人資料檔案名稱及檔案類型、個人資料之項目、類別、型態及數量、蒐集之特定目的、方式及來源、依個資法第 8 條或第 9 條向當事人告知之方式或得免為告知之情形、蒐集處理及利用相關業務或程序、依個資法第 6 條第 1 項、第 16 條或第 20 條第 1 項為目的外利用之情形、保存方式、期限及銷毀方式。

The personal data file inventory used for the inventory check shall include at least the following items: the holding unit; the name and type of the personal data file; the items, categories, forms and quantity of personal data; the specific purpose, method and source of collection; the method of notifying the data subject under Article 8 or Article 9 of the Personal Data Protection Act, or circumstances where notification may be exempted; the relevant business or procedures for collection, processing and use; circumstances of use beyond the specific purpose under Article 6, Paragraph 1, Article 16 or Article 20, Paragraph 1 of the Personal Data Protection Act; and the method of retention, retention period and method of destruction.

6.4.4 個資管理部門針對個人資料檔案清冊內容，依據風險評估分析構面（流程、人員、技術）進行風險分析，並將結果彙整於「風險評估表」。

The personal data management department shall conduct risk analysis on the contents of the personal data file inventory based on the risk assessment dimensions (process, personnel, technology), and consolidate the results in the “Risk Assessment Form”.

6.4.5 本校每年應至少執行一次風險評鑑。

The University shall conduct risk assessment at least once a year.

6.4.6 本校依個資檔案風險評鑑結果及可接受風險值之決議，各風險項目由個資管理部門業務承辦人針對需降低風險值之個資檔案綜整單位「個人資料風險處理計畫」，以期將風險降至可接受程度。

Based on the results of the personal data file risk assessment and the resolution on acceptable risk values, for each risk item, the business officers of the personal data

management department shall consolidate a "Personal Data Risk Treatment Plan" for the personal data files whose risk values need to be reduced, so as to reduce the risks to an acceptable level.

6.4.7 風險處理計畫執行完畢後，個資管理部門應進行改善成效評估，確認相關風險已降低至可接受程度，並留存評估紀錄。如改善後風險仍高於可接受值，應重新啟動風險處理程序。

After the risk treatment plan has been implemented, the personal data management department shall evaluate the effectiveness of the improvement, confirm that the relevant risks have been reduced to an acceptable level, and retain the evaluation records. If the risk after improvement remains higher than the acceptable value, the risk treatment procedure shall be re-initiated.

6.4.8 有關個人資料檔案清冊之清查、彙整與風險評鑑、風險管理之實施方式，另訂「個人資料檔案清查暨風險管理程序書」規範之。

The implementation of the inventory check and consolidation of the personal data file inventory, risk assessment and risk management shall be separately governed by the "Personal Data File Inventory and Risk Management Procedure".

6.5 個人資料事故之預防、通報及應變機制

Prevention, Notification and Response Mechanism for Personal Data Incidents

6.5.1 當本校保有之個人資料檔案遭受不可抗力之天然災害或人為破壞(損毀、竊取、洩漏、竄改、違法利用、設備破壞)，或違法蒐集個資，遭媒體揭露、當事人提起訴訟，或造成本校聲譽受損時，應依本程序立即辦理通報作業。

When personal data files held by the University suffer from natural disasters of force majeure or man-made damage (destruction, theft, disclosure, alteration, unlawful use, or equipment damage), or when unlawful collection of personal data is exposed by the media, litigation is filed by data subjects, or the University's reputation is damaged, notification shall be carried out immediately in accordance with this procedure.

6.5.2 當發生個資事件時，由事件發現人員向圖書資訊處通報，並填寫「個資安全事件通報處理紀錄表」，通知個資管理單位評估事件影響範圍、可能造成之損失，及預定採取之應變處理措施，並判斷個資安全事件等級。整體應變機制流程如下：

When a personal data incident occurs, the person who discovers the incident shall notify the Office of Library and Information Services and fill out the "Personal Data Security Incident Notification and Handling Record Form", and notify the personal data management unit to assess the scope of impact of the incident, possible losses and the response measures to be taken, and determine the level of the personal data security incident. The overall response mechanism process is as follows:

(1) 啟動組織內部通報機制。

Activate the organization’ s internal notification mechanism.

(2) 危害初步控管（終止或減緩個資事件持續擴大）。

Preliminary hazard control (terminate or mitigate the continued expansion of the personal data incident).

(3) 評估事件影響與衝擊程度。

Assess the impact and severity of the incident.

(4) 識別個資事件發生原因。

Identify the cause of the personal data incident.

(5) 資料公開：擬定對外說明文件（如果影響範圍擴及組織外部人員），並通報個資當事人及必要之主管機關，內容需包括：防止再發所採行之措施、發生之原因、補償機制（確定學校疏失時）及學校對外聯繫窗口與聯絡方式。

Public Notification: prepare external explanatory documents (if the scope of impact extends to persons outside the organization), and notify the data subjects and, where necessary, the competent authorities. The contents shall include: measures taken to prevent recurrence, the cause of the incident, compensation mechanisms (where the University’ s negligence is confirmed), and the University’ s external contact point and contact information.

(6) 事件檢討：建立事件處理分析報告，經決策主管核覆後結案。

Incident review: prepare an incident handling analysis report, to be closed after approval by the decision-making supervisor.

(7) 文件歸檔：將事件所有處理經過及文件完整歸檔，包括事故發生相關紀錄、事件處理經過、事故分析報告及通報紀錄。

Document filing: completely file all handling processes and documents of the incident, including records related to the occurrence of the incident, the handling process, the incident analysis report and the notification records.

6.5.3 個資事件發生時，依通報順序逐級陳報，應於 36 小時內完成校內通報程序；經確認為個資事件後，應於事故發現時起 72 小時內通報主管機關。

When a personal data incident occurs, it shall be reported level by level in accordance with the notification sequence, and the internal notification procedure shall be completed within 36 hours; upon confirmation as a personal data incident, the competent authority shall be notified within 72 hours from the discovery of the incident.

6.5.4 本校應就風險評鑑中所可能面臨之各種個資事故情境，每年至少進行一次應變演練，並詳細記錄演練之過程與檢討結果，以確保應變機制運作之有效性；演練紀錄應留存備查。

The University shall conduct response drills at least once a year for the various personal data incident scenarios that may be encountered as identified in the risk assessment, and record in detail the process and review results of the drills to ensure

the effectiveness of the response mechanism; drill records shall be retained for reference.

6.5.5 有關個人資料安全事故之通報與處理方式，另訂「個人資料事件之預防、通報及應變程序書」規範之。

The notification and handling of personal data security incidents shall be separately governed by the "Personal Data Incident Prevention, Notification and Response Procedure".

6.6 當事人權利行使

Exercise of Data Subject Rights

6.6.1 本校個人資料檔案清冊中所列之各項個人資料檔案，依法接受個人資料當事人行使當事人權利包括：請求查詢或請求閱覽、請求製給複製本、請求補充或更正、請求停止蒐集、處理、利用、請求刪除。

For each personal data file listed in the University's personal data file inventory, the University shall, in accordance with the law, accept the exercise of data subject rights, including: requesting an inquiry or review, requesting copies, requesting supplementation or correction, requesting cessation of collection, processing or use, and requesting deletion.

6.6.2 當事人應填具「個人資料權利行使申請表」或依本校相關業務申請辦法辦理申請，如為代理人申請則另需檢附委託書及出示相關身分證明文件。

Data subjects shall fill out the "Personal Data Rights Exercise Application Form" or apply in accordance with the application procedures for the relevant business of the University. Applications made by an agent shall additionally be accompanied by a power of attorney and relevant identity documents.

6.6.3 本校各單位於受理個人資料當事人行使當事人權利案件處理期限如下：查詢或請求閱覽、請求製給複製本應於十五日內為准駁之決定，必要時，得予延長十五日內並以書面通知請求人。請求補充或更正、請求停止蒐集、處理或利用、請求刪除應於三十日內為准駁之決定，必要時，得予延長三十日內並以書面通知請求人。

The time limits for the University's units to handle cases of data subjects exercising their rights are as follows: for requests for inquiry or review or for copies, a decision on approval or rejection shall be made within fifteen days, which may be extended by up to fifteen days where necessary, with written notice to the applicant; for requests for supplementation or correction, cessation of collection, processing or use, or deletion, a decision on approval or rejection shall be made within thirty days, which may be extended by up to thirty days where necessary, with written notice to the applicant.

6.6.4 本校網站設置個資申訴案件投訴信箱或網頁，由本校個資保護聯絡窗口為對外單一窗口，接受當事人申訴案件。

The University shall set up a complaint mailbox or webpage for personal data complaints on its website, with the University’ s personal data protection contact point serving as the single external window to accept complaints from data subjects.

6.6.5 有關個資保護聯絡窗口受理各項案件之處理方式，請查閱「當事人權利行使作業說明書」。

For the handling of cases accepted by the personal data protection contact point, please refer to the “Data Subject Rights Exercise Operation Manual”.

6.7 個人資料蒐集、處理及利用

Collection, Processing and Use of Personal Data

6.7.1 本校各單位應於業務執行、服務提供或透過資訊系統蒐集個資前，應依個資法第 8 條規定告知當事人蒐集之目的與範圍，並且遵循適當、相關且符合資料最小化原則，避免取得無關或超過蒐集目的之個人資料，並請當事人填寫「個人資料蒐集聲明暨同意書」取得同意。若當事人未滿 18 歲，依民法規定應取得法定代理人之同意。

Before collecting personal data in the course of business execution or service provision or through information systems, each unit of the University shall notify the data subject of the purpose and scope of collection in accordance with Article 8 of the Personal Data Protection Act, follow the principles of appropriateness, relevance and data minimization, avoid obtaining personal data irrelevant to or exceeding the purpose of collection, and ask the data subject to fill out the “Personal Data Collection Statement and Consent Form” to obtain consent. If the data subject is under 18 years of age, the consent of his/her legal representative shall be obtained in accordance with the Civil Code.

6.7.2 本校保有個人資料之處理，應依據個資法第 15 條規定應有特定目的並符合特定情形，並依個人資料檔案分類之結果進行保護，若委託其他機關代為處理保有之個人資料，應依個資法施行細則第 8 條之要求進行適當之監督。

The processing of personal data held by the University shall have a specific purpose and comply with specific circumstances in accordance with Article 15 of the Personal Data Protection Act, and such data shall be protected in accordance with the classification results of personal data files. Where the processing of held personal data is commissioned to other agencies, appropriate supervision shall be conducted in accordance with the requirements of Article 8 of the Enforcement Rules of the Personal Data Protection Act.

6.7.3 本校同仁因履行法定義務而進行個人資料之利用，應依相關法令法規辦理，且於利用前應先確認利用的目的是否和原先蒐集的特定目的相同。

Staff of the University who use personal data for the fulfillment of statutory obligations shall do so in accordance with relevant laws and regulations, and shall, before such use, first confirm whether the purpose of use is consistent with the

original specific purpose of collection.

6.7.4 本校個資涉及國際傳輸時，須遵循輸入、輸出國家之相關個資法令法規之規定；或藉由契約與行政協議形式確保個人資料保護之責任。

Where the University’ s personal data involves international transmission, the relevant personal data laws and regulations of the importing and exporting countries shall be complied with; or the responsibility for personal data protection shall be ensured through contracts or administrative agreements.

6.7.5 有關個人資料蒐集、處理及利用之作業管制詳細規定，另訂「個人資料蒐集、處理及利用程序書」規範之。

Detailed regulations on the operational control of the collection, processing and use of personal data shall be separately governed by the “Personal Data Collection, Processing and Use Procedure”.

6.8 資料與設備安全管理

Data and Equipment Security Management

6.8.1 本校對所有保管個人資料、管理個人資料儲存媒體，以及可以存取個人資料之人員依本校資訊安全相關規定進行必要之權限管理，各類權限之授予以最小且滿足業務所需為限。

The University shall carry out necessary access control, in accordance with the University’ s information security regulations, over all personnel who safeguard personal data, manage personal data storage media, or have access to personal data. All access rights granted shall be limited to the minimum necessary to meet business needs.

6.8.2 本校人員應妥善保管個人帳號及密碼，不得供予他人使用（密碼長度 12 碼以上，同時需為英文字母、數字或特殊字元的組合），並定期更換密碼，同一密碼使用期限最長應不超過 3 個月，儘量避免重複或循環使用舊的密碼。

University personnel shall properly safeguard their personal accounts and passwords and shall not provide them to others (passwords shall be at least 12 characters in length and consist of a combination of letters, numbers or special characters), and shall change passwords regularly. The maximum period of use of the same password shall not exceed 3 months, and repeated or cyclical use of old passwords shall be avoided as far as possible.

6.8.3 本校個人電腦應設定螢幕保護程式（不應超過 10 分鐘），並安裝防毒軟體及定期更新病毒碼。

Personal computers of the University shall be configured to automatically lock (e.g., via screen saver) after no more than 10 minutes of inactivity, and shall have antivirus software installed with virus definitions updated regularly.

6.8.4 本校機敏性等級之個人資料檔案於個人電腦宜加密儲存，以保護其機密性。

Personal data files of the University classified as sensitive should be stored in

encrypted form on personal computers to protect their confidentiality.

6.8.5 存放個人資料之伺服器、應用系統及資料庫，於系統效能許可下應啟用稽核日誌，記錄使用者存取、修改、刪除等操作，日誌至少留存 6 個月，以保存相關稽核軌跡資訊，供事故追查及稽核之用。

For servers, application systems and databases storing personal data, audit logs shall be enabled where system performance permits, to record user operations such as access, modification and deletion. Logs shall be retained for at least 6 months to preserve audit trail information for incident investigation and audit purposes.

6.8.6 保有個人資料之系統應定期備份，備份資料視需要採取加密機制，並妥善保管備份媒體；應定期進行備份資料之還原測試，以確保備份之有效性及資料可用性。

Systems holding personal data shall be backed up regularly; backup data shall be encrypted as needed and the backup media shall be properly kept. Restoration tests of backup data shall be conducted regularly to ensure the validity of backups and the availability of data.

6.8.7 本校蒐集、處理或利用個人資料達一定筆數（如百筆）以上之系統，應設置使用者身分確認及保護機制、個人資料顯示之隱碼機制（如身分證字號末 4 碼以****標示）、網際網路傳輸之安全加密機制、資料庫存取控制及保護監控措施，並針對系統上線前辦理弱點掃描及滲透測試，上線後持續辦理防止外部網路入侵及異常使用行為之監控與因應機制。

For systems of the University that collect, process or use personal data reaching a certain number of records (e.g., one hundred records) or more, the following shall be implemented: user identity verification and protection mechanisms; masking mechanisms for the display of personal data (e.g., marking the last 4 digits of the national ID number with ****); secure encryption mechanisms for Internet transmission; database access control and protective monitoring measures; vulnerability scanning and penetration testing before the system goes online; and, after going online, continuous monitoring and response mechanisms against external network intrusion and abnormal usage behavior.

6.8.8 未使用或下班時，個人資料書面文件及可攜式資訊設備或儲存媒體，應遵守桌面淨空政策，放置於抽屜或櫃子上鎖，以避免個資外洩。

When not in use or after working hours, paper documents containing personal data and portable information equipment or storage media shall comply with the clear desk policy and be placed in locked drawers or cabinets to prevent personal data leakage.

6.8.9 各類個人資料儲存媒體淨化方式如下：

The sanitization methods for various personal data storage media are as follows:

(1) 紙本：焚燒或使用碎紙機粉碎。

Paper: incineration or shredding with a paper shredder.

(2) 硬碟：消磁、直接摔毀；USB 隨身碟可破壞塑膠殼內部之記憶體顆粒。

Hard disks: degaussing or direct physical destruction; for USB flash drives, the memory chips inside the plastic casing may be destroyed.

(3) 光碟片：將光碟折斷、使用支援之碎紙機將碟片粉碎。

Optical discs: breaking the disc, or shredding the disc with a shredder that supports discs.

(4) 所有儲存機敏性資料之媒體，在報廢或要重複利用前，必須經過前項所述淨化措施，且整個淨化過程必須全程予以紀錄（例如拍照或攝影），以備後續之稽核。

All media storing sensitive data must undergo the sanitization measures described in the preceding items before disposal or reuse, and the entire sanitization process must be fully recorded (e.g., by photography or video recording) for subsequent audit.

6.8.10 有關資料、設備與實體環境安全之詳細規定，請查閱「個人資料安全作業說明書」。

For detailed regulations on data, equipment and physical environment security, please refer to the “Personal Data Security Operation Manual”.

6.9 人員管理及教育訓練

Personnel Management and Education and Training

6.9.1 本校教職員生、約聘僱人員、外包廠商皆應遵守本校個人資料保護政策及個資管理制度相關文件之規範。

All faculty, staff and students, contract personnel and outsourced vendors of the University shall comply with the University’s personal data protection policy and the relevant documents of the personal data management system.

6.9.2 本校人員於到職時，應簽署「個人保密切結書」，並克盡保密之責。

University personnel shall sign the “Personal Confidentiality Agreement” upon taking office and shall fulfill their duty of confidentiality.

6.9.3 本校每年應訂定或辦理一般人員教育訓練計畫及課程，並依要求人員每年需達 3 小時以上時數。

The University shall formulate or conduct education and training plans and courses for general personnel every year, and, as required, personnel shall complete at least 3 hours of training per year.

6.9.4 禁止使用即時通訊軟體、外部信箱（如 Gmail 等）傳輸及存取個人資料檔案；禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

Personnel shall not use instant messaging applications or external email services (such as Gmail) to transmit or access personal data files. Personnel shall also not disclose personal data obtained through their duties on social networking sites, blogs,

public forums, or other Internet-based platforms.

6.9.5 本校人員離職應於規定時間內關閉該人員所使用之各類權限以及通行證件，並依規定列冊移交相關儲存媒體及資料，由主管實施監交作業。

Upon resignation of University personnel, all access rights and passes used by such personnel shall be deactivated within the prescribed time, and relevant storage media and data shall be listed and handed over in accordance with regulations, with the supervisor overseeing the handover.

6.9.6 針對違規人員之懲處建議，並依情節輕重移送相關單位辦理懲處。

Disciplinary recommendations shall be made for violators and referred to the relevant units for disciplinary action according to the severity of the circumstances.

6.9.7 有關人員管理及教育訓練之實施方式，另訂「人員管理及教育訓練程序書」規範之。

The implementation of personnel management and education and training shall be separately governed by the "Personnel Management and Education and Training Procedure".

6.10 委外管理

Outsourcing Management

6.10.1 供應商與作業人員應遵守本校個資安全管理制度及資訊安全管理制度之規定。

Suppliers and their operating personnel shall comply with the University's personal data security management system and information security management system.

6.10.2 供應商作業人員到點服務除需依規定簽署供應商保密切結書外，請購單位應告知作業項目及場所相關安全管理規定。

In addition to signing the supplier confidentiality agreement as required, when supplier personnel provide on-site services, the requisitioning unit shall inform them of the operation items and the relevant security management regulations of the premises.

6.10.3 除非相關法律有特別之規定，受委託廠商應於履約完成後進行個人資料載體之返還，以儲存方式而持有之個人資料需安全的刪除，並提供確切之證據，請購單位得對於有疑慮之項目進行實地之查核。

Unless otherwise specifically provided by relevant laws, the commissioned vendor shall return the personal data carriers upon completion of the contract, securely delete personal data held in storage, and provide concrete evidence thereof. The requisitioning unit may conduct on-site inspections of items in question.

6.10.4 對於受託蒐集、處理或利用個人資料之廠商，本校應每年至少辦理一次稽核，查核其執行情形並記錄稽核結果備查；如有委外查核疑慮，得另行辦理不定期實地查核。

For vendors commissioned to collect, process or use personal data, the University shall conduct an audit at least once a year to examine their implementation and record

the audit results for reference; where there are concerns regarding outsourced operations, additional unscheduled on-site inspections may be conducted.

6.10.5 有關對於受委託之監督管理實施方式，請查閱「個人資料業務委外監督管理作業說明書」。

For the implementation of supervision and management of commissioned parties, please refer to the "Personal Data Outsourcing Supervision and Management Operation Manual".

6.11 個人資料內部稽核管理

Personal Data Internal Audit Management

6.11.1 本校內部稽核，由個資稽核小組針對本校之個資管理制度、個資清查、風險評估與風險管理、個資事故應變措施、演練等作業及適法性，每年應至少辦理一次定期查核，以確保其成效。稽核結果應以書面報告呈交個人資料保護管理委員會，並作為年度管理審查之重要輸入資料。

The University's internal audit shall be conducted by the Personal Data Audit Team, which shall carry out a regular audit at least once a year on the University's personal data management system, personal data inventory check, risk assessment and risk management, personal data incident response measures, drills and other operations, as well as their legal compliance, to ensure their effectiveness. The audit results shall be submitted to the Committee of Personal Data Protection and Management in a written report and shall serve as an important input for the annual management review.

6.11.2 為確保稽核之客觀性，各單位個資聯絡人執行跨單位互審稽核時，不得稽核其本身所屬單位之個人資料業務；個資保護推動組（圖書資訊處）負責統籌規劃個資保護制度之管理專責人員，不得同時擔任稽核工作小組之查核人員。

To ensure the objectivity of audits, when the personal data contact persons of each unit conduct cross-unit mutual audits, they shall not audit the personal data business of their own units; the dedicated management personnel of the Personal Data Protection Promotion Team (Office of Library and Information Services) responsible for the overall planning of the personal data protection system shall not concurrently serve as auditors of the audit working team.

6.11.3 本校外部稽核，由本校以外單位所進行的個資業務稽核，如主管機關個資業務檢查等。

The University's external audit refers to personal data business audits conducted by units outside the University, such as personal data business inspections by the competent authorities.

6.11.4 有關個人資料檔案安全稽核機制之實施方式，另訂「個人資料保護內部稽核程序書」規範之。

The implementation of the personal data file security audit mechanism shall be

separately governed by the "Personal Data Protection Internal Audit Procedure".

6.12 個人資料使用紀錄、軌跡資料及證據保存

Preservation of Personal Data Usage Records, Trail Data and Evidence

6.12.1 本校個人資料相關文件或紀錄，依單位需求訂定保存期限，屆滿保存期限之紀錄由各單位個資管理專人編造銷毀清冊，辦理銷毀後，銷毀清冊副本交付圖書資訊處留存。

For personal data-related documents or records of the University, retention periods shall be set according to the needs of each unit. For records whose retention periods have expired, the dedicated personal data management personnel of each unit shall compile a destruction inventory; after destruction, a copy of the destruction inventory shall be submitted to the Office of Library and Information Services for retention.

6.12.2 有關個人資料使用紀錄管理之細部規定，另訂「個人資料文件及紀錄管理程序書」規範之。

Detailed regulations on the management of personal data usage records shall be separately governed by the "Personal Data Document and Record Management Procedure".

6.13 個人資料安全維護之整體持續改善

Overall Continuous Improvement of Personal Data Security Maintenance

6.13.1 本校各單位於個人資料安全維護推行過程，應接受稽核，並針對稽核發現之缺失檢討其根本原因，提出消除已知缺失事項之改正措施與消除其根本原因防止再發之矯正措施。

Each unit of the University shall be subject to audits during the implementation of personal data security maintenance, review the root causes of deficiencies identified in audits, and propose corrective actions to eliminate the identified deficiencies as well as corrective measures to eliminate their root causes and prevent recurrence.

6.13.2 有關改正措施與矯正措施之實施與追蹤方式，另訂「個人資料保護持續改善程序書」規範之。

The implementation and tracking of corrective actions and corrective measures shall be separately governed by the "Personal Data Protection Continuous Improvement Procedure".

6.14 業務終止後個資處理與紀錄機制

Personal Data Handling and Record Mechanism After Business Termination

6.14.1 定期檢視：學校各單位須於每學期期末，檢核所屬個資檔案，發現有非屬特定目的必要範圍內之個人資料或特定目的消失、期限屆滿而無保存必要者，應予刪除、銷毀或其他停止蒐集、處理或利用等適當之處置，並填具「個人資料銷毀申請表」。

Regular review: each unit of the University shall, at the end of each semester, review

its personal data files. Where personal data is found to be outside the necessary scope of the specific purpose, or where the specific purpose no longer exists or the retention period has expired and retention is no longer necessary, such data shall be deleted, destroyed, or otherwise appropriately handled by ceasing its collection, processing or use, and the "Personal Data Destruction Application Form" shall be filled out.

6.14.2 處理方式及留存紀錄如下：

The handling methods and records to be retained are as follows:

(1) 銷毀：銷毀之方法、時間、地點及證明銷毀之方式，並填具「個人資料銷毀申請表」。

(1) Destruction: the method, time and place of destruction and evidence of destruction, with the "Personal Data Destruction Application Form" filled out.

(2) 移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

(2) Transfer: the reason, recipient, method, time and place of the transfer, and the legal basis on which the recipient may hold the personal data.

(3) 刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。

(3) Deletion, cessation of processing or use of personal data: the method, time or place of the deletion, cessation of processing or use.

6.14.3 各單位須留存之必要紀錄及種類：

Necessary records and their types to be retained by each unit:

(1) 個資交付、傳輸的紀錄。

Records of personal data delivery and transmission.

(2) 個人資料新增及修改之相關紀錄。

Records related to additions and modifications of personal data.

(3) 提供當事人行使權利之紀錄。

Records of data subjects exercising their rights.

(4) 所屬人員權限新增、變動及刪除之紀錄。

Records of additions, changes and deletions of personnel access rights.

(5) 個人資料刪除、銷毀之紀錄。

Records of deletion and destruction of personal data.

(6) 辦理個資教育訓練之紀錄（由圖書資訊處統整）。

Records of personal data education and training (consolidated by the Office of Library and Information Services).

以上紀錄建議至少保存五年，並於每學期末將執行情形回報個人資料保護推動組備查。

The above records are recommended to be retained for at least five years, and the implementation status shall be reported to the Personal Data Protection Promotion Team for

reference at the end of each semester.

7 相關資料

Related Documents

7.1 個人資料保護政策

Personal Data Protection Policy

7.2 個人資料保護管理委員會設置辦法

Regulations Governing the Establishment of the Committee of Personal Data Protection and Management

7.3 個人資料保護推行組織與責任分工程序書

Personal Data Protection Organization and Division of Responsibilities Procedure

7.4 個人資料文件及紀錄管理程序書

Personal Data Document and Record Management Procedure

7.5 個人資料檔案清查暨風險管理程序書

Personal Data File Inventory and Risk Management Procedure

7.6 個人資料蒐集、處理及利用程序書

Personal Data Collection, Processing and Use Procedure

7.7 個人資料事件之預防、通報及應變程序書

Personal Data Incident Prevention, Notification and Response Procedure

7.8 人員管理及教育訓練程序書

Personnel Management and Education and Training Procedure

7.9 個人資料保護內部稽核程序書

Personal Data Protection Internal Audit Procedure

7.10 個人資料保護持續改善程序書

Personal Data Protection Continuous Improvement Procedure

7.11 當事人權利行使作業說明書

Data Subject Rights Exercise Operation Manual

7.12 個人資料業務委外監督管理作業說明書

Personal Data Outsourcing Supervision and Management Operation Manual

7.13 個人資料安全作業說明書

Personal Data Security Operation Manual

8 施行

Implementation

本計畫經個人資料保護管理委員會會議通過，陳請校長核定後發布實施，修訂時亦同。

This Plan shall be adopted by the meeting of the Committee of Personal Data Protection and Management and submitted to the President for approval before implementation; the same shall apply to any amendments.

▲ 回審議三