

國立中山大學

個人資料保護管理政策

機密等級：一般

文件編號：IPS-NSYSU-A-001

版 次： 2.0

發行日期：107.11.01

個人資料保護管理政策					
文件編號	IPS-NSYSU-A-001	機密等級	一般	版次	2.0

目錄

1	個人資料之蒐集與處理	1
2	個人資料之利用及國際傳遞	1
3	個人資料之調閱與異動	2
4	個人資料之例外應用	2
5	個人資料之保護	3
6	利害關係人之參與及期許	4
7	個人資料保護政策之修正權	4

個人資料保護管理政策					
文件編號	IPS-NSYSU-A-001	機密等級	一般	版次	2.0

國立中山大學圖書與資訊處（以下簡稱本處）為落實個人資料之保護及管理並符合「個人資料保護法」之要求，特訂定個人資料保護管理政策（以下簡稱本政策）。個人資料保護管理之目標如下：

- 一、依「個人資料保護法」、「個人資料保護法施行細則」與「教育體系資通安全暨個人資料管理規範」要求，保護個人資料蒐集、處理、利用、儲存、傳輸、銷毀之過程。
- 二、為保護業務相關個人資料之安全，免於因外在威脅，或內部人員不當之管理與使用，致遭受竊取、竄改、毀損、滅失、或洩漏等風險。
- 三、提升對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境。
- 四、為提升同仁個人資料保護安全意識，每年定期辦理個人資料保護宣導教育訓練。
- 五、定期針對個人資料流程進行風險評鑑，鑑別可承受風險等級。

1 個人資料之蒐集與處理

- 1.1 因執行業務所需取得或蒐集之包括但不限於個人之姓名、出生年月日、國民身分證統一編號（護照號碼）、特徵、指紋、婚姻、家庭、教育、職業等個人資料，應遵循我國個人資料保護法（以下簡稱個資法）等法令，不過度且符合目的、相關且適當並公平與合法地從事個人資料之蒐集與處理。各權責單位主管負責所屬單位業務範圍之風險評鑑結果審核作業。

2 個人資料之利用及國際傳遞

- 2.1 於利用個人資料時，除需依個資法之特定目的必要範圍內之外，如需為

個人資料保護管理政策

文件編號	IPS-NSYSU-A-001	機密等級	一般	版次	2.0
------	-----------------	------	----	----	-----

特定目的以外之利用時，將依據個資法第十六條之規定辦理；倘有需取得用戶之書面同意之必要者，應依法取得當事人同意。

- 2.2 所蒐集、處理之個人資料，應遵循我國個資法及個資管理制度之規範，且個人資料之使用為營運或業務所需，方可為承辦同仁利用。
- 2.3 取得之個人資料，如有進行國際傳遞之必要者，定謹遵不違反國家重大利益、不以迂迴方法向第三國傳遞或利用個人資料規避個資法之規定等原則辦理，又，倘國際條約或協定有特別規定、或資料接受國對於個人資料之保護未有完善之法令致有損害當事人權益之虞者，將不進行國際傳遞，以維護個人資料之安全。

3 個人資料之調閱與異動

- 3.1 當接獲當事人依個資法第三條進行請求時，應依個資法及所訂之程序，於合法範圍內進行當事人之個人資料查詢或請求閱覽、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。

4 個人資料之例外應用

- 4.1 因業務上所擁有之個人資料負有保密義務，除當事人之要求查閱或有下列情形外，應符合個資法第十六條及相關法令規定，並以正式公文查詢外，不得對第三人揭露：
 - 4.1.1 司法機關、監察機關或警政機關因偵查犯罪或調查證據所需者。
 - 4.1.2 其他政府機關因執行公權力並有正當理由所需者。
 - 4.1.3 與公眾生命安全有關之機關（構）為緊急救助所需者。
- 4.2 對個人資料之利用，除個資法第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
 - 4.2.1 法律明文規定。

個人資料保護管理政策					
文件編號	IPS-NSYSU-A-001	機密等級	一般	版次	2.0

4.2.2為維護國家安全或增進公共利益所必要。

4.2.3為免除當事人之生命、身體、自由或財產上之危險。

4.2.4為防止他人權益之重大危害。

4.2.5公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。

4.2.6有利於當事人權益。

4.2.7經當事人書面同意。

5 個人資料之保護

5.1 成立個人資料保護組織「資訊安全暨個人資料保護推動委員會」，明確定義相關人員之責任與義務。

5.2 建立與實施個人資料管理制度(PIMS)，以確認本政策之實行；全體員工及委外廠商應遵循個人資料管理制度(PIMS)之規範與要求，並定期審查PIMS之運作。

5.3 為防止個人資料被竊取、竄改、毀損、滅失或洩漏，「圖書與資訊處」下設「個資保護管理暨維運小組」，統籌驗證範圍各項個資保護作業原則規劃事宜，由各組單位推派1人組成之，並依相關法令規定辦理個人資料檔案及個人資料檔案清冊安全維護及更新事項。

5.4 個人資料檔案應建立管理制度，分級分類管理，並針對接觸人員建立安全管理規範。

5.5 為確保所有個人資料安全，應強化個人資料檔案資訊系統之存取安全，防止非法授權存取，維護個人資料之隱私性，應建立安全保護機制，並定期查核。

5.6 個人資料檔案儲存於個人電腦者，應於該電腦設置可辨識身分之登入通行碼，並視業務及重要性，考量其他輔助安全措施。

個人資料保護管理政策

文件編號	IPS-NSYSU-A-001	機密等級	一般	版次	2.0
------	-----------------	------	----	----	-----

- 5.7 個人資料輸入、輸出、存取、更新、銷毀或分享等處理行為，應釐定使用範圍及調閱或存取權限。
- 5.8 各單位如遇有個人資料檔案發生遭人惡意破壞、毀損或作業不慎等安全事件，應進行緊急因應措施，並依個人資料保護通報程序辦理。
- 5.9 係以周全之措施、政策保護當事人之個人資料，包括之所有教職員工生，均受有完整之個資法及隱私權保護之教育訓練。倘有洩露個資之情事者，將依法追究其民事、刑事及行政責任。
- 5.10 受託單位(例委外廠商)與本處業務合作時，均應簽訂保密契約，使其充分瞭解個人資料保護之重要性及洩露個資之法律責任。倘有違反保密義務之情事者，將依法追究其民事及刑事責任。

6 利害關係人之參與及期許

- 6.1 個人資料保護及管理決議事項應納入「個資保護管理暨維運小組」報告，涉及重大決議之會議紀錄應提報「資訊安全暨個人資料保護推動委員會」、主管機關（教育部）或利害關係人(如企業雇主、畢業校友、學生家長、教職員工生及其他與相關人士等)，如有任何回饋事項，將列入下次「個資保護管理暨維運小組」管理審查會議之討論議題。
- 6.2 為確保矯正預防措施之有效運作，應落實管理審查機制，每年至少舉行一次管理委員會議，會議議題依據【個人資料保護組織程序書】內容辦理。

7 個人資料保護管理政策之修正

- 7.1 個人資料保護管理政策，每年定期或因時勢變遷或法令修正等事由，予以適當修訂，並陳「個資保護管理暨維運小組」後，公告實施，修正時亦同。