附件 4

範例：風險類型暨風險對策參考表

風險類型暨風險對策參考表			
作業情境	作業內容	具體風險類型	風險處理對策(參考範例)
處理利用	輸入/編輯	輸入錯誤資料或遺漏輸入資料	1. 明確輸入/編輯程序 2. 人員教育訓練 3. 輸入/編輯後再次檢查內容 4. 將輸入/編輯結果列印與電腦輸入/編輯資料對照 5. 按輸入個資的重要性採取重複輸入、交互檢查
		輸入時遭窺視	1. 個人電腦區域設置 OA 等阻隔設施 2. 個人電腦遠離外部人員 3. 離席時啟動登出功能 4. 一定時間無動作鎖定電腦、螢幕保護程式 5. 按個資重要性限制輸入專用處所、終端機及人員
		個資遭竄改	1. 限制輸入/編輯作業人員權限 2. 於必要時實施交互檢查輸入/編輯內容 3. 實施個資保護教育 4. 簽具切結書
	輸出/列印	不當存取	1. 權限設定(例如使用者工作所需最小權限原則) 2. 系統示警 3. 系統紀錄
		列印文件未及時取走致外洩	列印後迅速回收
		大量輸出/列印	系統示警
	影印	不當存取	1. 權限設定(例如使用者工作所需最小權限原則) 2. 多功能事務機等設備設定提示示警、紀錄
		影印文件未及時取走致外洩	影印後迅速回收
		影印錯誤、廢棄文件不當棄置致外洩	1. 使用碎紙機 2. 文件放置於專用廢紙箱，並採適當管控措施
	掃描	不當存取	1. 權限設定(例如使用者工作所需最小權限

			原則) 2. 多功能事務機等設備設定提示示警、紀錄
內部傳送	人員親送	收發記載不確實以致遺失	1. 確認收受紀錄媒體內容、件數 2. 雙方留存簽收收受紀錄
		紙本資料遭竊或遺失	1. 使用傳遞專用公文封、信封袋、公事包及隨身保管 2. 傳遞途中不作停留
		傳遞交付對象錯誤致遺失	1. 確認移交對象 2. 雙方留存收發紀錄
		USB 等外接記錄媒體遺失	1. 將 USB 等外接記錄媒體按儲存個資數量、種類等重要性加以密碼鎖碼或暗號化 2. 限制 USB 等外接紀錄媒體使用(例如儲存個資的種類、限用公務用 USB)
	Email	Email 網址或信件內容錯誤致外洩	1. 寄信之前再次確認寄送 Email 網址及寄信內容 2. 有必要時使用 Email 軟體所附的寄信網址再檢查功能 3. 規範 Email 使用(例如預設並套用傳遞群組、傳遞對象) 4. 將包含個資的文件以附加檔案方式加上設定密碼 5. 遮蔽他人機敏個資欄位傳送 6. 系統設定 Email 收回或刪除信件功能
		Email 傳送中被竊取	1. 將包含個資的文件以附加檔案方式加上設定密碼 2. 限制 Email 使用(例如限制使用公務用電子郵件) 3. 安裝防毒軟體、防火牆並定期更新防毒碼、使用弱點掃描
		Email 遺失	1. 規定 Email 的儲存場所 2. 保存收信的 Email 3. 系統設定 Email 收回或刪除信件功能
	系統/網路/FTP	透過網路伺服器傳送時被竊取	個資檔案加密傳送
	手機、通訊	透過手機、通訊軟體(LINE、	1. 限制通訊軟體使用(例如不得傳遞個資、個

	軟體	Juiker)傳送時被竊取	資檔案加密傳送) 2. 安裝防毒軟體、防火牆並定期更新防毒碼、使用弱點掃描 3. 使用公務用電腦、手機
		手機、通訊軟體(LINE、Juiker)閒置時遭外部人員窺視	1. 設定手機鎖定、螢幕保護程式 2. 通訊軟體設定密碼及自動登出
保管	個人電腦	不當存取	1. 處理權限設定(例如使用者工作所需最小權限原則) 2. 防範登錄帳號密碼被他人知悉 3. 不使用密碼記憶功能 4. 定期變更密碼 5. 定期檢查有無不當存取 6. 將包含個資的檔案設定密碼並存放於專用資料夾
		個人電腦故障致無法讀取該資料	蒐集資料後立刻將資料存於伺服器專用資料夾
		個人電腦遭外部攻擊	1. 安裝防毒軟體、防火牆並定期更新防毒碼、使用弱點掃描 2. 實體隔離(例如禁止遠距連線作業)
		個人電腦安裝非法軟體導致外洩	1. 禁止安裝非法軟體 2. 系統示警 3. 定期資安稽核
	資料庫/主機伺服器	不當存取資料	1. 設定伺服器專用資料夾 2. 依職務區隔設定存取權限 3. 使用者帳號定期審查 4. 設置資料庫/主機伺服器專用存放機房，限制人員進入、使用權限 5. 系統有設定記錄使用者活動日誌 6. 主管或授權者定期審查使用者活動日誌
		伺服器專用資料夾故障致無法讀取該筆資料	1. 定期將伺服器專用資料夾資料以其他方式備份 2. 按個資重要性將備份分散保管
		伺服器遭外部攻擊	1. 安裝防毒軟體並定期更新防毒碼、使用弱點掃描 2. 實體隔離(例如禁止遠距連線作業)

	抽屜/個人檔案櫃/儲存裝置	不當存取(資料沒有依規定放入個人櫃或抽屜,直接放置於桌上遭窺視)	1. 個資資料依規定放入個人櫃或抽屜，並上鎖存管 2. 紙本文件作業場所遠離外部人員
		保管資料的文件櫃忘記上鎖遭竊取致外洩。	1. 文件櫃外部不標示保管文件種類內容 2. 文件/個人檔案櫃確實上鎖 3. 個資資料歸檔於檔案室，業務完竣後不留存
		USB 等儲存裝置保管不當致資料外洩	1. 限制 USB 等儲存裝置使用(申請許可使得使用) 2. USB 等儲存裝置專人、專櫃上鎖保管
	檔案室	不當存取(任何人都可以進入檔案室取得資料)	1. 限制人員進入檔案室、使用調閱權限 2. 重要資訊上鎖保管
外部傳送	人員親送	收發記載不確實以致遺失	1. 確認收受紀錄媒體內容、件數 2. 雙方留存簽收收受紀錄
		紙本資料遭竊或遺失	1. 使用傳遞專用公文封、信封袋、公事包及隨身保管 2. 途中不作停留
		傳遞交付對象錯誤致遺失	1. 確認移交對象 2. 雙方留存收發紀錄
		USB 等外接紀錄媒體遺失	1. 將 USB 等外接紀錄媒體按儲存個資數量、種類等重要性加以密碼鎖碼或暗號化 2. 限制 USB 等外接紀錄媒體使用(例如儲存個資的種類、限用公務用 USB)
	郵寄	郵寄過程中遺失	1. 採取掛號、雙掛號可留紀錄的郵寄方法 2. 限制郵寄使用(例如限制重要個資不得郵寄方式傳遞)
	傳真	傳真收發記載不確實以致遺失	1. 將收到的紀錄媒體轉交業管人員時留存確認紀錄 2. 使用加密傳真機
		傳真處所或傳真內容搞錯致外洩	1. 傳真前確認傳真處所電話及傳真內容 2. 傳真前先與傳針對象電話聯絡 3. 確認傳真傳送紀錄 4. 使用加密傳真機 5. 限制傳真使用(例如限制重要個資不得傳真方式傳遞)

		傳真放置於傳真機上逾時致外洩	1. 確認傳真對象在後再傳真，並於傳真後與對象核對確認 2. 傳真傳出後迅速回收 3. 傳真機設置於遠離外部人員處所
		報廢或退還傳真機時外洩	系統設定程序定期刪除多功能傳真機的硬碟資料庫並實施刪除動作
	Email	Email 網址或信件內容錯誤致外洩	1. 寄信之前再次確認寄送 Email 網址及寄信內容 2. 有必要時使用 Email 軟體所附的寄信網址再檢查功能 3. 規範 Email 使用(例如預設並套用傳遞群組、傳遞對象) 4. 將包含個資的文件以附加檔案方式加上設定密碼 5. 遮蔽他人機敏個資欄位傳送 6. 系統設定 Email 收回或刪除信件功能
		Email 傳送中被竊取	1. 將包含個資的文件以附加檔案方式加上設定密碼 2. 限制 Email 使用(例如限制使用公務用電子郵件) 3. 安裝防毒軟體、防火牆並定期更新防毒碼、使用弱點掃描
		Email 遺失	1. 規定 Email 的儲存場所 2. 保存收信的 Email 3. 系統設定 Email 收回或刪除信件功能
	系統/網路/FTP	透過網路伺服器傳送時被竊取	1. 個資檔案加密傳送 2. 實體隔離
	外機關系統界接	系統遭駭客或外部攻擊	依本署 ISMS 資訊安全風險評鑑與管理作業程序等處理
	手機、通訊軟體	透過手機、通訊軟體(LINE、Juiker)傳送時被竊取	1. 限制通訊軟體使用(例如不得傳遞個資、個資檔案加密傳送) 2. 安裝防毒軟體、防火牆並定期更新防毒碼、使用弱點掃描 3. 使用公務用電腦、手機
		手機、通訊軟體(LINE、Juiker)閒置時遭外部人員窺視	1. 設定手機鎖定、螢幕保護程式

			2. 通訊軟體設定密碼及自動登出
刪除銷毀	刪除	未到刪除日期前過失刪除	1. 訂定具體刪除日期 2. 設定程序須確認後才刪除 3. 刪除並留存紀錄由部門主管檢查
		刪除不夠落實致外洩	1. 規定刪除程序並確實刪除 2. 重要個資刪除設定應由主管檢查確認 3. 電子個資資料以格式化方式刪除 4. 儲存個資可攜媒體不再使用或損毀時，將硬體設備進行實體破壞
	銷毀	未到銷毀日期前過失銷毀	1. 規定各個個資的保存期間， 2. 設定程序須確認後才銷毀。 3. 銷毀並留存紀錄由部門主管檢查
		銷毀處理不夠確實致外洩	1. 規定銷毀程序並確實銷毀 2. 重要個資銷毀設定應由主管檢查確認 3. 紙本個資資料使用碎紙機、水銷方式銷毀至無法辨識 4. 紙本個資資料禁止回收使用
委外作業	選商	廠商曾發生個資外洩事件、重大資安事件之紀錄	評估及選擇可提供符合組織對個人資料保護需求之受委託廠商(例如通過 ISO 27001、BS10012、TPIPAS、ISO29100 等驗證)
	簽約	廠商未採取適當安控措施導致外洩	委託外部單位處理個人資料簽訂契約，並包含適當安控措施、契約明確規範，當資料逾保存期限或契約終止時，有關個人資料之銷毀、交還原組織或其他處理方式
		廠商之轉包/分包商外洩	1. 與受委託廠商所簽訂之契約中包含不得將個人資料處理作業進行轉包/分包之規定 2. 若允許轉包/分包，受委託廠商與其複委託廠商(下包商)所簽訂之契約應要求複委託廠商實行與受委託廠商相同等級之安控措施
	履約	廠商於契約期間外洩	1. 契約期間內，定期監督或實地審查受委託廠商之安控措施是否落實執行、 2. 定期依據與受委託廠商所簽訂之契約進行監督 3. 當資料逾保存期限或契約終止時確認有關

			個人資料之銷毀、交還原組織或其他處理之方式
	銷毀	廠商未確實銷毀	1. 紙本個資資料委託廠商銷毀前契約約定權利義務(包括賠償條款、保密協議) 2. 紙本個資資料委託廠商銷毀時進行監銷並留存紀錄。
其他	人員考核、獎懲	人員因個人債務、不當交往等因素洩漏、販售個資	1. 風險人員考核 2. 法紀宣導
		人員受不當指示查詢、傳遞個資	1. 風險人員考核 2. 申訴提報機制