環　球　科　技　大　學

個人資料風險評鑑與管理程序書

文件編號：ISMS-P2-004

機密等級：一般

版　　次：1.5

發行日期：2022/08/02

環球科技大學

文件名稱	個人資料風險評鑑與管理程序書	版本	1.5
文件編號	ISMS-P2-004	發行日期	2022/08/02
		頁次	-

修 訂 紀 錄

版次	發行日期	修訂頁次	修訂者	修訂內容摘要
1.0	2015/12/13			初版發行
1.1	2016/07/25	P.1~P.5	巫正淵	修改程序書文件頁首之文件名稱。
		P.2	巫正淵	20 筆為團體體訴訟的基礎線
		P.4	巫正淵	加上管理等級
1.2	2017/10/20	P.2~P.4	巫正淵	5.1.1 評估個人資料風險
		P.5	巫正淵	5.1.2 處理個人資料風險
1.3	2018/08/09	P.2	巫正淵	修正 ISMS 表單編號
1.4	2019/10/30	P.5~P.6	巫正淵	委員會合併後調整為資訊安全暨個人資料保護管理委員會。
1.5	2022/08/02	P.2	巫正淵	修正表 1：影響衝擊等級表中「敏感程度」各等級之定義

環球科技大學

文件名稱	個人資料風險評鑑與管理程序書	版本	1.5
文件編號	ISMS-P2-004	發行日期	2022/08/02
		頁次	-

目　錄

環球科技大學

文件名稱	個人資料風險評鑑與管理程序書	版本	1.5
文件編號	ISMS-P2-004	發行日期	2022/08/02
		頁次	1

1 目的

本校為制定共同遵行之風險評鑑標準，以協助有效執行風險控管，預防個資外洩事件之威脅，特訂定「環球科技大學個人資料風險評鑑與管理程序書」(以下簡稱本程序書)。

2 適用範圍

本校承辦業務相關作業流程之風險管理。

3 權責

3.1 個人資料管理代表(召集人)：負責業務範圍之個資風險評鑑結果審核作業(含可接受風險值、風險評鑑結果、風險改善計畫與控制措施之核定)。

3.2 個人資料管理執行小組：負責相關個資風險評鑑執行與結果之複核，並針對風險值超過可接受風險之個資，採取適當之控管措施。

4 名詞定義

4.1 可接受風險值

各項個資資產之最低風險容忍度。

4.2 殘餘風險(Residual Risk)

在採用相關控制措施之後剩餘的風險。

4.3 威脅(Threat)

可能對系統或組織造成傷害之意外事件。

4.4 弱點(Vulnerability)

因個資資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.5 風險(Risk)

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常用產生之影響及發生機率來衡量。

5 作業說明

5.1 為評估個人資料檔案之風險，本校應規劃個人資料風險評估與管理作業，風險評估作業應包括下列項目：

5.1.1 評估個人資料風險

5.1.1.1 建立風險評量的標準，包括：風險發生之機率與影響/衝擊之程度。個人資料檔案之風險評估應依據實際狀況，對照「影響衝擊等級表」(如表1)、「管理制度等級表」(如表2)及「風險發生可能性等級表」(如表3)之內容，並於「ISMS-04-064個資盤點清冊暨風險評鑑表」中進行之風險分析。

表1：影響衝擊等級表

評估項目	影響衝擊等級表		
	輕微(1)	嚴重(2)	非常嚴重(3)
個資數量(財務影響)	20筆(不含)以下微量個資(團體訴訟不成立)。	大量個資：一般個資20~5,000筆；特種個資20~1,000筆。	巨量個資:一般個資5,001筆以上;特種個資1,001筆以上)。
敏感程度	僅有一般識別資料，如:姓名、服務單位、職稱、電話、電子郵件帳號、地址等。	含有高風險個資，如：政府資料中之辨識者及財務資料等，如身分證統一編號、稅籍編號、保險憑證號碼、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼、學生證號等。	含有特種個人資料(病歷、醫療、基因、性生活、健康檢查及犯罪前科)、高關懷、轉銜、諮商輔導、低收入暨身心障礙者等之個人資料。
可識別性	個資查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	可以間接識別特定當事人者。	可以直接識別特定當事人者。
符法性(個資蒐集、處理、利用之範圍與目的)	已取得當事人同意蒐集、處理及利用個資，且未超過範圍與目的。	1.已取得當事人同意蒐集、處理及利用個資，雖資料蒐集範圍(過度)與目的不同(目的外之處理、利用)，已進行告知，但未取得書面同意。或已取得當事人同意蒐集、處理、利用個資，未踰越目	未取得同意而蒐集、處理或利用個資，也未進行告知。(例如:購買名單或於臉書上搜尋[處理或利用])。

		的，且有進行告知但未取得書面同意。 2. 已取得當事人同意蒐集、處理及利用個資，但資料蒐集、處理、利用範圍(過度)與目的不同(目的外之處理、利用)，且未進行告知或已告知但不同意。	

表2：管理制度等級表

評估項目	評估等級標準		
	已建立，並落實(1)	已建立、未落實(2)	未建立(3)
保存、銷毀	已建立保存、銷毀、監督程序，且已落實該等作業。	已建立保存、銷毀、監督程序，但未落實。 (或尚未建立保存、銷毀、監督程序，但有部分實理作業。)	尚未建立保存、銷毀、監督程序，亦無實施任何措施。
安全管理制度	已建立安全控管程序及相關文件，且已落實。	已建立安全控管程序及相關文件，但部分未落實。 (或未建立，但已有實施部份安全控管)	未建立安全控管程序及相關文件，亦無任何安全控管。

表3：風險發生可能性等級表

等級	評估標準
可能性低(1)	➢ 很少發生或無發生可能性。 ➢ 3年期間沒有發生過。 ➢ 已有控制措施與完整紀錄。
可能性中(2)	➢ 可能發生或偶爾發生。 ➢ 1到3年期間發生次數小於3次(含)。 ➢ 已有控制措施，但無完整紀錄。
可能性高(3)	➢ 經常發生。 ➢ 1年內發生2次以上(含)。 ➢ 沒有控制措施與紀錄。

5.1.1.2 個人資料管理執行小組須針對各項個人資料之使用及控管狀況，依據「影響衝擊等級表」之各個評估項目，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「ISMS-04-064個資盤點清冊暨風險評鑑表」。

5.1.1.3 識別風險發生之可能性及影響/衝擊程度，將此3項評分進行相乘，即求出該個人資料檔案之風險值。風險值=影響衝擊等級x管理制度等級x風險發生可能性等級。

5.1.1.4 將經由風險值計算公式所得之風險值，對應至「風險值分布矩陣圖」(如下圖1)以判斷風險值之分布情況。

風險值分布矩陣				
影響衝擊等級(A)	風險發生可能性等級(R)			管理制度等級(M)
	可能性低(1) R1	可能性中(2) R2	可能性高(3) R3	
輕微(1) A1	A1* M1*R1=1	A1* M1*R2=2	A1* M1*R3=3	已建立，並落實(1)M1
	A1* M2*R1=2	A1* M2*R2=4	A1* M2*R3=6	已建立、未落實(2)M2
	A1* M3*R1=3	A1* M3*R2=6	A1* M3*R3=9	未建立(3)M3
嚴重(2) A2	A2* M1*R1=2	A2* M1*R2=4	A2* M1*R3=6	已建立，並落實(1)M1
	A2* M2*R1=4	A2* M2*R2=8	A2* M2*R3=12	已建立、未落實(2)M2
	A2* M3*R1=6	A2* M3*R2=12	A2* M3*R3=18	未建立(3)M3
非常嚴重(3)A3	A3* M1*R1=3	A3* M1*R2=6	A3* M1*R3=9	已建立，並落實(1)M1
	A3* M2*R1=6	A3* M2*R2=12	A3* M2*R3=18	已建立、未落實(2)M2
	A3* M3*R1=9	A3* M3*R2=18	A3* M3*R3=27	未建立(3)M3

圖1：風險值分布矩陣圖

5.1.2 處理個人資料風險

依風險評估結果，經資訊安全暨個人資料保護管理委員會決定可接受風險值後，對於高於可接受風險值之個人資料檔案進行風險處理，擬定改善措施，並填入「ISMS-04-064個資盤點清冊暨風險評鑑表」。

5.2 覆核

5.2.1 持續改善

為保持本風險評鑑方法之有效性與適用性，個人資料管理執行小組應定期檢討「ISMS-04-064個資盤點清冊暨風險評鑑表」之項目，以期確保本校個資資產均處於最佳保護之下。

5.2.2 風險重新評估

5.2.2.1 每年應至少執行1次風險評鑑。

5.2.2.2 當範圍內有以下的狀況發生之時，則實施不定期的複核，以更新及確保個資資產風險評估的正確性及完整性：

5.2.2.2.1有新增、變更或移除個資資產。

5.2.2.2.2組織業務調整。

5.2.2.2.3個資外洩事件發生。

5.3 附則

本程序書經資訊安全暨個人資料保護管理委員會議通過，陳請校長核定後實施；修正時亦同。

6 附表

6.1 ISMS-04-064 個資盤點清冊暨風險評鑑表