環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
A.5 資訊安全政策 B.1 個人資料管理政策	I(1)資訊安全政策審查次數	≧1 次/學年度	查核資訊安全暨個人資料保護管理委員會議紀錄是否符合		
	I(2)資訊安全政策宣導次數	≧1 次/學年度	查核資訊安全暨個人資料保護管理委員會議紀錄是否符合		
	P(3)個人資料保護管理政策審查次數	≧1 次/學年度	查核資訊安全暨個人資料保護管理委員會議紀錄是否符合		
A.6 資訊安全組織 B.2 個人資料管理組織	(1)員工未確實簽署保密協議	≦2 件	查核內部/外部稽核結果是否符合		
	(2)資訊安全暨個人資料保護管理委員會議召開次數	≧1 次/學年度	查核資訊安全暨個人資料保護管理委員會議紀錄是否符合		
A.7 人力資源安全 B.3 人員認知與訓練	(1)檢查資通安全暨個人資料管理受訓時數	依教育部與所屬機關(構)及學校資通安全責任等級分級作業規定之受訓時數規定辦理 未參與教育訓練之	查核教育訓練紀錄是否符合		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
		正式同仁≦20%/學年度			
	I(2)離退人員帳號未確實刪除	≦2 件	檢查工作紀錄表		
A.8 資產管理	(1)資訊資產清單定期更新	≧1 次/年	查核資訊資產清單		
	(2)未依資訊資產清單符合分級與標示規定	≦2 件	檢查工作紀錄表		
	(3)定期執行風險評鑑	≧1 次/年	檢視資訊資產風險評估表		
A.9 存取控制 A.10 密碼學(加密控制)	(1)定期審查重要系統存取權限(帳號清查)	≧2 次/年	檢查工作紀錄表		
	(2)管理者、使用者密碼長度及複雜度未符合規範	≦2 件	查核內部/外部稽核結果是否符合		
	(3)帳號申請未依規定填寫表單	≦1 件	查核內部/外部稽核結果是否符合		
	(4)系統稽核日誌未開啟	≦1 件	內部抽查及實際狀況執行與查核		
	(5)未授權存取重要資料機密性資料之次數(BIA 上列計之服務主機)	＝0 件	內部抽查及實際狀況執行與查核		
	(6)電子資料未確實存放於相關資料夾內(螢幕淨空)	≦1 件	檢查工作紀錄表		
A.11 實體及環境	(1)經檢查未遵守機房門禁規定	≦2 件	查核內部/外部稽		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
安全			核結果是否符合		
	(2)檢查消防器材與 UPS 未定期保養	≦1 件	檢查工作紀錄表		
A.12 運作安全 A.13 通訊安全 B.10 資料安全議題	I(1)未定期監控重要伺服器執行作業之系統容量（例如 CPU、RAM、硬碟、資料庫）	≦2 件	檢查工作紀錄表		
	I(2)未定期監控網路資源使用率（例如：網路頻寬使用率滿載且持續超過一小時）	≦2 件	檢查工作紀錄表		
	I(3)病毒爆發次數（年）	≦3 次/年	事件紀錄		
	I(4)連外網路斷線次數（年）	≦3 次/年	事件紀錄		
	I(5)檢查病毒碼未即時更新	≦2 件	查核內部/外部稽核結果是否符合		
	I(6)檢查重要系統時間未加以同步	≦2 件	查核內部/外部稽核結果是否符合		
	I(7)檢查防火牆設定與防火牆進出規則申請表資料未相符	≦2 件	查核內部/外部稽核結果是否符合		
	I(8)技術安全稽核次數	≧2 次/年	掃瞄報告		
	P(9)含個人資料之重要系統之管理者、使用者密碼長度是否符合規範	稽核時每單位密碼長度未符合規範之同仁≦2 位/學年度	查核內部/外部稽核結果是否符合		
	P(10)個人電子資料未確實存放於相關資料	每單位發現個人電子資料未確實存放	查核內部/外部稽		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
	夾內(螢幕淨空)	於相關資料夾內≦2件/學年度	核結果是否符合		
A.14 系統獲取、開發及維護	(1)重要系統更新/上線前未經測試(BIA 上列計之服務)	＝0 件	依實際狀況執行		
	(2)重要系統開發或變更時未更新系統文件(BIA 上列計之服務)	≦2 件	依實際狀況執行		
	(3)重要系統上線未具有緊急復原機制(BIA 上列計之服務)	＝0 件	依實際狀況執行		
A.15 供應者關係 B.12 委外管理	I(1)第三方未確實簽署保密協議	≦2 件	查核內部/外部稽核結果是否符合		
	I(2)委外廠商專案執行狀況未依規定執行評鑑	≦2 件	評鑑紀錄		
	P(3)抽查組織個人資料若有轉包情形是否簽訂正式書面協議(例契約)	稽核時每單位內接觸單位內個資之廠商,未簽署保密協議或具相關切結文件≦1 位/學年度	查核內部/外部稽核結果是否符合		
A.16 資訊安全事故管理	(1)發生資安事件未依規定處理	≦1 件	查核內部/外部稽核結果是否符合		
	(2)發生個資安全事件	≦2 次	依實際狀況執行		
	(3)發生資安事件影響工時	≦18 小時	依實際狀況執行		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
A.17 營運持續管理之資訊安全層面	(1)檢討業務永續運作計畫演練執行情形	≧1 次/年	演練紀錄		
	(2)執行風險評鑑與營運衝擊分析(BIA)	≧1 次/年	風險評鑑紀錄		
	(3)未定期備份重要系統資料	≦2 件	查核內部/外部稽核結果是否符合		
A.18 遵循性	(1)經檢查安裝非合法軟體	＝0 件	查核內部/外部稽核結果是否符合		
	(2)定期執行資安稽核次數	≧1 次/年	查核內部/外部稽核結果是否符合		
	(3)矯正措施未於規定時間內改善完成	≦2 件	查核內部/外部稽核結果是否符合		
B.4 個人資料之識別與風險管理	(1)個人資料檔案是否進行風險評鑑	未執行風險評鑑≦1 單位/學年度	查核內部/外部稽核結果是否符合		
	(2)高於可接受風險值之個人資料檔案，是否進行風險處理	每單位高於可接受風險值之個人資料檔案未進行風險處理≦2 件/學年度	查核內部/外部稽核結果是否符合		
B.5 公正與合法的處理	(1)蒐集前是否確認蒐集目的與範圍	每單位違反事件≦2 次/學年度	查核內部/外部稽核結果是否符合		
	(2)蒐集個資時是否告知個資法要求事項	每單位違反事件≦2 次/學年度	查核內部/外部稽核結果是否符合		
	(3)抽查個人資料蒐集是否逾越特定目的之	每單位違反事件≦2 次/學年度	查核內部/外部稽		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
	必要範圍		核結果是否符合		
B.6個人資料特定目的處理	(1)抽查個人資料處理是否逾越蒐集特定目的	每單位違反事件≦2次/學年度	查核內部/外部稽核結果是否符合		
	(2)抽查個人資料利用是否逾越蒐集特定目的之處理	每單位違反事件≦2次/學年度	查核內部/外部稽核結果是否符合		
B.7適當相關與正確性	(1)是否均識別各單位個人資料檔案	每單位發現個人資料檔案未識別≦5筆/學年度	查核內部/外部稽核結果是否符合		
	(2)個資盤點清冊暨風險評鑑表是否定期更新	每單位未檢視或更新「個人資料檔案清冊」≧1次/學年度	查核內部/外部稽核結果是否符合		
B.8保存與處置	(1)含個人資料之紙本文件是否置於上鎖櫃子保存	稽核時每單位休假或公出時未上鎖存放含有個人資料之紙本文件之同仁≦2位/學年度	查核內部/外部稽核結果是否符合		
B.9當事人權利	(1)未依規定填寫事件通報單與事件事故處理單	稽核時每單位發現個資事故,但未填寫事件通報單與事件事故處理單≦1 次/學年度	依實際狀況執行		
B.10資料安全議題	(1)含個人資料之重要系統之管理者、使用者密碼長度是否符合規範	稽核時每單位密碼長度未符合規範之同仁≦2位/學年度	查核內部/外部稽核結果是否符合		
	(2)個人電子資料未確實存放於相關資料夾內(螢幕淨空)	每單位發現個人電子資料未確實存放於相關資料夾內≦2件/學年度	查核內部/外部稽核結果是否符合		
B.12委外管理	(1)抽查組織個人資料若有轉包情形是否簽	稽核時每單位內接觸單位內個資之廠	查核內部/外部稽		

環 球 科 技 大 學

製表日期：　　年　　月　　日

有效性量測表					
表單編號	ISMS-04-049	機密等級	敏感	版本	4.2

文件管制紀錄編號：

量測項目		目標水準	量測方式	量測結果	執行/差異說明
	訂正式書面協議(例契約)	商,未簽署保密協議或具相關切結文件≦1位/學年度	核結果是否符合		

在相同一列 ISMS 及 PIMS 量測項目下，有 I：僅適用 ISMS，有 P：僅適用 PIMS

目標水準及量測方式：於 109 學年度第一次資訊安全暨個人資料保護管理委員會(109.10.13)審議

製表人：　　執行秘書(審查)：＿＿＿＿＿＿(日期)　　**個資長/資安長**(頒布)：＿＿＿＿＿＿(日期)