

環球科技大學

內部稽核查檢表

表單編號	ISMS-04-065	機密等級	敏感	版本	2.3
------	-------------	------	----	----	-----

稽核查檢日期：

文件管制紀錄編號：

項次	領域	稽核項目	符合	部分符合	不符合	不適用	說明
1	組織	是否已組成個人資料保護單位，同時可清楚說明維護內部個人資料之管理作業權責？					
2	組織	承上題，上述要求是否已有文件化，載明成立個人資料保護管理單位及角色？並配置相當資源？					
3	組織	是否指派專人進行個人資料檔之管理及維護？					
4	組織	是否已清楚瞭解單位內有關個人資料之蒐集、處理、利用之範圍？					
5	組織	是否已辨識單位個資保護措施與個人資料保護法之適法性是否一致？					
6	組織	是否訂定經管理階層核准之宣告利害關係人、員工個人資料如何與何時被蒐集、利用及保護之個人資料管理政策？					
7	組織	是否已設置「個資保護聯絡窗口」並將聯繫方式置於單位網站？					
8	告知	直接蒐集個人資料是否已取得當事人書面、電話、傳真或電子方式同意？（法令授權免通知者除外）					
9	告知	依法向當事人直接蒐集個資時，是否明確說明蒐集個人資料的單位名稱、目的、個資類別、期間、地區、對象、處理方式、當事人行使					

環球科技大學

內部稽核查檢表

表單編號	ISMS-04-065	機密等級	敏感	版本	2.3
------	-------------	------	----	----	-----

項次	領域	稽核項目	符合	部分符合	不符合	不適用	說明
		權利及方式及不提供之影響？					
10	告知	是否提供清楚與明顯的說明予利害關係人或單位人員，有關個人資料的安全維護方式？					
11	告知	是否提供清楚與明顯的說明予利害關係人或單位人員，有關當事人如何更正或刪除其個人資料？					
12	告知	間接蒐集之個人資料是否已規劃告知當事人？					
13	告知	是否訂定提供當事人申訴、抱怨程序與管道？					
14	蒐集處理利用	進行個人資料蒐集時是否遵循所屬主管單位的法規或公約？（例如金融、保險、社會安全、健康照護等）					
15	蒐集處理利用	是否識別間接蒐集之個人資料之適法性及特定目的之合理性？					
16	蒐集處理利用	針對特種個資（病歷、醫療、基因、性生活、健康檢查及犯罪前科）及敏感性個資（當事人之種族、黨派、宗教信仰、社團組織及身心狀況）進行蒐集、利用及處理，是否取得法令依據？					
17	蒐集處理利用	是否有針對個人資料不同等級處理進行安控措施？（含備份檔案及軌跡檔案）					
18	蒐集處理利用	是否訂定及執行人員安全管理措施，並就個別作業設定所屬人員不同之權限並控管之？					

環球科技大學

內部稽核查檢表

表單編號	ISMS-04-065	機密等級	敏感	版本	2.3
------	-------------	------	----	----	-----

項次	領域	稽核項目	符合	部分符合	不符合	不適用	說明
19	蒐集處理利用	與其他單位個人資料交換是否已識別個人資料之適法性及特定目的利用之合目的性？					
20	蒐集處理利用	與其他單位個人資料交換是否已採取適當保護措施？					
21	蒐集處理利用	將資料傳送於境外，該境外地區是否有個資保護法令，且已取得中央目的主管單位同意？					
22	訓練	是否已進行有效的個人資料保護全面性(含新人)人員宣導及教育訓練？					
23	訓練	是否針對負責管理及維護個人資料檔案之專人進行有效的專業教育訓練或取得專業證照(如具BS 10012 LA或相關個資證照等)？					
24	程序	是否已建立個人資料內部管理程序或規則，以確保單位內個人資料蒐集、處理、利用、刪除及傳輸符合特定目的要求？					
25	程序	是否有訂定當事人查詢、變更、刪除資料之程序？					
26	程序	是否有訂定當發生個人資料被竊取、洩漏、竄改或其他侵害者事件之主動通知程序？					
27	程序	是否有訂定風險評估及管理程序？					
28	程序	是否有訂定個資事故通報程序？					
29	程序	是否有訂定個資事故應變					

環球科技大學

內部稽核查檢表

表單編號	ISMS-04-065	機密等級	敏感	版本	2.3
------	-------------	------	----	----	-----

項次	領域	稽核項目	符合	部分符合	不符合	不適用	說明
		處理程序？					
30	程序	是否有訂定文件管理程序？					
31	程序	是否有訂定當個人資料蒐集目的消失或屆滿之資料刪除程序？					
32	程序	是否訂有個人資料檔案維護計畫及業務終止後個人資料處理方法等相關事項之辦法？					
33	程序	是否訂有維護資料正確性程序？					
34	程序	是否妥善保管個人資料與其儲存媒體？					
35	持續營運	是否已定期執行稽核作業，以確保相關個人資料保護管理措施之有效性？					
36	持續營運	是否定期檢視個資政策及個資保護執行結果？					
37	單位	是否指派專人進行個人資料檔之管理及維護？					
38	蒐集處理利用	是否每年盤點單位內所有的個人資料，並建立清冊以利管理？					
39	蒐集處理利用	是否每年針對流程盤點後之單位內所有的個人資料，進行風險評鑑並呈核？					
40	蒐集處理利用	個人資料檔案之查閱與使用，是否填寫「ISMS-04-067 個資查詢或調閱申請單」建立必要之使用紀錄、軌跡資料及證據保存措施？					
41	蒐集處理	個人資料檔案之刪除與銷毀，是否填寫「ISMS-04-069					

環球科技大學

內部稽核查檢表

表單編號	ISMS-04-065	機密等級	敏感	版本	2.3
------	-------------	------	----	----	-----

項次	領域	稽核項目	符合	部分符合	不符合	不適用	說明
	利用	<u>資訊設備報廢暨個人資料刪除/銷毀/返還清冊</u> 建立必要之使用紀錄、軌跡資料及證據保存措施？					
42	實務	是否已將個資業務委外監督管理機制納入合約條款，並進行適當之稽核？					
43	實務	個人資料檔案嚴禁存放於電腦桌面。					
44	實務	紙本個人資料檔案應存放於可上鎖之抽屜或櫃內。					
45	實務	防毒軟體設自動更新並檢查為最新防毒碼。					
46	實務	個人電腦密碼應為8碼以上，且以大小寫字母、數字及符號組成較強之密碼。					
47	實務	個人電腦螢幕保護機制設定15分鐘（含）以下，自動啟動防護機制，並須勾選登入身份識別。					
48	實務	個人資料檔案須壓縮加密碼後再行mail寄送。					
49	實務	電子郵件軟體應關閉信件預覽功能。					

稽核員：

稽核組長：