管理系統文件

文件類別	第二階文件	
文件編號	ISMS-P-011	
文件名稱	實體與環境安全管理程序書	
發行單位	文件管制小組	
發行日期	111 年 02 月 17 日	
版　次	2.3	
訂修廢單位	審　查	核　准
資通安全處理小組		

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
2.0	104/04/30	2015 改版發行。
2.1	107/03/09	修改本文件 5.3.1.一般辦公區域管制單位及管制區域門禁卡使用登記表、管制區域進出管制登記表、管制區域檢查表、系統主機安全檢查表、辦公區域安全檢查表、個人電腦安全檢查表保存地點資訊科技中心單位名稱為圖書資訊處。
2.2	108/04/15	因應資通安全管理法修訂本文件。
2.3	111/02/17	修訂 5.5.2、5.5.4 程序為每年查檢；修改個人電腦安全查檢表編號為「PIMS-3-001-02 個人電腦安全檢查表」。 修訂 5.4.7.2 監視錄影紀錄應至少保留半個月以上。 修訂 5.4.7.3 程序，Log 查檢納入「ISMS-P-011-04 系統主機安全檢查表」。

1. 目的

   為促使本校實體與環境安全之防護，有一明確之規範，以避免資訊、資產遭未經授權存取、損害與干擾，而影響業務正常運作，特制定本程序書。

2. 適用範圍

   凡本校實體與環境安全之管理，均適用本程序書。

3. 參考文件

   3.1. ISMS-P-016 資通設備維護與管理程序書。

   3.2. ISMS-P-009 資通安全事件通報及應變管理程序書。

   3.3. ISMS-P-008 矯正及預防管理程序書。

4. 名詞定義

   4.1. 一般區域：本校實體範圍內，除管制區域之外的辦公場所。

   4.2. 管制區域：本校實體範圍內，用以存放關鍵或敏感性營運資訊、資產的場所，如資訊機房、倉儲庫房等等。

5. 作業內容

5.1. 實體與環境安全管理流程圖

作業流程	權責單位	相關表單
規劃管制區域	資通安全處理小組	
訂定區域管制規定	資通安全處理小組 管制區域管理人員	管制區域門禁卡使用登記表 管制區域進出管制登記表 管制區域檢查表
設備安全管理	資通安全處理小組	
查核	資通安全處理小組 管制區域管理人員 資通系統管理人員 相關業務承辦人員	管制區域檢查表 系統主機安全檢查表 辦公區域安全檢查表 個人電腦安全檢查表
異常		
異常處理	資通安全處理小組	
正常		
紀錄保存	相關業務承辦人員	

5.2. 規劃一般區域及管制區域

5.2.1. 本校將所管轄之區域區分為一般區域及管制區域。

5.2.2. 一般區域為本校除資訊機房外之辦公作業環境。

5.2.3. 一般區域及管制區域之安全作業規範，應透過適當方式傳達給具有進入一般區域及管制區域需求的人員知悉，並使其確實遵守。

5.3. 訂定區域管制規定

5.3.1. 一般辦公區域作業
非本校人員欲進入辦公區域，應有本處人員陪同。

5.3.1.1. 本校全體員工需保持警覺，留意辦公環境陌生人員出入狀況，若有非授權進入須馬上出面制止。

5.3.1.2. 未經許可，不得於本處管制區域內使用錄音、錄影或具有照相功能之資通設備。

5.3.1.3. 「密」等級（含）以上之資訊，應採取辦公桌面的淨空政策，以減少機密及敏感資訊遭未被授權的人員取用、遺失或是被破壞的機會。

5.3.1.4. 「密」等級（含）以上之資訊，不使用或下班時應存放在櫃子內並上鎖。

5.3.1.5. 列印或傳真「密」等級（含）以上之資訊時，作業完成後應立即從印表機或傳真機取走。

5.3.1.6. 個人電腦應設定螢幕保護程式，於電腦暫時無人使用時自行啟動，並設定密碼保護。自行啟動螢幕保護程式的時間設定不應超過 10 分鐘。

5.3.1.7. 辦公區域環境內嚴禁抽煙。

5.3.1.8. 辦公區域環境內應置放適當之消防設備，設備存放環境應保持淨空，並檢測以確保可用。

5.3.1.9. 應在一般辦公區域設置收發及裝卸區，以進行物料的收發及裝卸作業。

5.3.2. 管制區域的保護

5.3.2.1. 為確保管制區域內各項資通設備之安全，應採用門禁系統或鑰匙做為門禁管制，並將門禁或鑰匙使用權限登錄於「ISMS-P-011-01 管制區域門禁卡使用登記表」進行控管，以控管管制區域的通行權限。

5.3.2.2. 無門禁鑰匙者（如：廠商、訪客等），因業務需要進入管制區域，須由專人陪同進入。進入管制區域時須於「ISMS-P-011-02 管制區域進出管制登記表」登錄；若須將資通設備攜入或攜出，亦須於「ISMS-P-011-02 管制區域進出管制登記表」註明攜帶物品及用途。

5.3.2.3. 管制區域內應設置適切之環境監控及防護設施（包括：電力供應系統、溫濕度空調系統、消防系統、監視系統、門禁管制系統），並留下監控及維護紀錄，以提供安全的作業環境，確保資通安全事件發生時能夠及時處理，避免事態擴大。

5.3.2.4. 管制區域內門禁管制系統與監視系統之電子紀錄須適當保護，並定期查核以確定沒有異常情況。

5.3.2.5. 管制區域內執行例行性查核、設備維護及任何異動（變更）作業均須留下紀錄並定期查核，確保各項作業均被授權執行。

5.3.2.6. 管制區域內資通設備存放之機櫃，須保持上鎖狀態，其因維護或查核需要開鎖時，應維持最短時間之開鎖狀態，鑰匙須妥善保管。

5.3.2.7. 管制區域內物件的擺置應單純化，進入管制區域人員應保持地板的清潔，並禁止下列之行為：

5.3.2.7.1. 禁止飲食、放置飲料食物及存放私人物品。

5.3.2.7.2. 禁止喧嘩、嬉戲、吸煙、奔跑等不安全動作。

5.3.2.7.3. 不得隨意觸碰、破壞、任意移動或佔用機房內相關之資通設備與公用設施。

5.3.2.7.4. 應保持環境整齊及清潔，不得任意堆置物品或佔用公共

空間。

5.3.2.7.5. 除維護或施工目的外，凡危險物質（如有毒或腐蝕性物品）及易燃物一律禁止攜入或堆置於管制區域內。

5.3.2.8. 管制區域管理人員，應每日檢查管制區域內相關設施是否有異常狀況，並將檢查結果記載於「ISMS-P-011-03 管制區域檢查表」，如發現異常狀況，應即時通知設備管理者、相關權責主管或廠商，並進行異常處理。

5.4. 設備安全管理

5.4.1. 設備安置與保護

5.4.1.1. 重要資通設備應裝置於管制區域內，並依管制區域的進出管制措施管制人員進出，以避免未經授權存取系統的機會。

5.4.1.2. 管制區域內資訊資產之進出均須進行管控，並經申請程序及適當權責人員之同意，其進出均須留存紀錄以供後續查驗。

5.4.1.3. 資通設備安置時應遵循以下原則：

5.4.1.3.1. 處理「密」等級（含）以上資料的資通設備，應放置在員工可以注意及照顧的地點。

5.4.1.3.2. 需要特別保護的重要設備，應放置在管制區域中，與一般的設備進行區隔。

5.4.1.3.3. 應檢查及評估火災、煙、水、震動、電力供應等可能的風險。

5.4.1.4. 資通設備遷入管制區域前，應先行確認該設備之作業系統運作正常並經防毒軟體掃毒，確保系統安全無虞後始得遷入。

5.4.2. 電源供應

5.4.2.1. 電腦設備之設置應予以保護，防止斷電或其他電力不正常所導致的傷害。電源供應系統應依據原廠製造廠商所提供之規格安裝設置。

5.4.2.2. 重要資通設備應考量安置預備電源，並使用不斷電系統。

5.4.2.3. 不斷電系統應定期進行維護測試，並依據測試結果或廠商評估之建議，定期進行電池之更換。

5.4.2.4. 應謹慎使用電源延長線，以免電力無法負荷導致火災等危害安全之情事發生。

5.4.3. 電纜線安全

5.4.3.1. 電力及通訊用的電纜線，應予適當的保護，以防止被破壞或是資料被截取。

5.4.3.2. 電力及通訊纜線的保護原則如下：

5.4.3.2.1. 連接資通設施的電源及通訊線路，應有外殼包覆保護並盡量置於高架地板下，避免暴露損毀。

5.4.3.2.2. 網路通訊線路不可暴露在實體建築之外，以防止遭截取或是受到破壞。

5.4.4. 設備維護

5.4.4.1. 應妥善維護及管理設備，以確保設備的完整性及可用性。

5.4.4.2. 設備維護的原則如下：

5.4.4.2.1. 管制區域內重要之維運設備（如：門禁系統、空調系統及消防系統等）及資通設備（如：系統主機、網路及資安設備等），應與專業廠商簽訂維護契約，定期實施保養與妥善維護，並留下紀錄備查，以確保設備的完整與安全。

5.4.4.2.2. 設備的維護只能由授權的維護人員執行，且需有人員陪同。

5.4.4.2.3. 設備的維護作業應予以紀錄並留存，以為日後稽核之參考。

5.4.4.2.4. 設備之維護規範，請依據「ISMS-P-016 資通設備維護與管理程序書」之規定辦理。

5.4.5. 場外設備及設備攜出之安全

5.4.5.1. 應建立資通設備攜出管制程序，避免資通設備未經同意即攜出本校。

5.4.5.2. 因業務需要將資通設備攜出，請依據「ISMS-P-016 資通設備維護與管理程序書」之相關規定辦理。

5.4.6. 資訊資產報廢及再使用之安全

5.4.6.1. 含有儲存媒體的資通設備（例如電腦、硬碟、磁帶、光碟等），應在報廢、移轉及再使用之前進行檢查，以確保任何機密性、敏感性的資料及版權軟體已確實移除。

5.4.7. 日誌存管

5.4.7.1. 事件日誌(Log)應包括資料庫、作業系統、應用系統或程式及網路管理系統等有關使用者身份、系統的活動、登入及登出、存取內容、系統配置的變更、使用權限及所執行的交易記錄等。

5.4.7.2. 事件日誌需加以保護並至少留存 3 個月以上，監視錄影紀錄應至少保留半個月以上，並視需要納入「ISMS-P-015 資訊備份管理程序書」管控以作為未來事件鑑識取證之佐證參考。

5.4.7.3. 相關日誌檔案至少由管理者定期審查乙次，並納入「ISMS-P-011-04 系統主機安全檢查表」檢查項目。

5.5. 查核

5.5.1. 每月由管制區域管理人員將「ISMS-P-011-03 管制區域檢查表」查核結果，向權責主管回報，並於「ISMS-P-011-03 管制區域檢查表」簽章，以確保各項管制區域管理控制措施確實執行。

5.5.2. 每年由資訊系統管理人員依據「ISMS-P-011-04 系統主機安全檢查表」中之各項檢查項目逐一進行查檢，並將查檢之結果記錄於檢查表中，送交權責主管審核。若發現不符合項目時，須由資訊系統管理人員進行調整至符合檢查項目之需求為止。

5.5.3. 每半年由業務承辦人員，依「ISMS-P-011-05 辦公區域安全檢查表」之檢查項目逐一進行查核作業，並於檢查表上簽名，送交主管審核。

5.5.4. 每年由業務承辦人員，將「PIMS-3-001-02 個人電腦安全檢查表」發給所有人員，並依檢查表中之各項檢查項目進行自評，檢查表填完並經單位主管審核後，送交業務承辦人員進行抽驗。

5.5.5. 業務承辦人員如發現不符合項目時，應報請主管指定相關人員協助進行異常狀況處理。

5.6. 異常處理

5.6.1. 查核結果若產生異常，則由權責主管指派專人進行異常狀況之處理，並依據「ISMS-P-009 資通安全事件通報及應變管理程序書」規定留下處理紀錄，以供後續評估及改善。

5.6.2. 異常狀況若無法即期處理及改善，則依據「ISMS-P-008 矯正及預防管理程序書」之相關規定執行矯正與預防措施，進行問題矯正及風險預防的作業。

5.7. 紀錄保存

相關業務承辦人員應參照如下規範，妥善保存各項紀錄。

編號	表單名稱	保存地點	保存期限
1	管制區域門禁卡使用登記表	圖書資訊處	至少 1 年
2	管制區域進出管制登記表	圖書資訊處	至少 1 年
3	管制區域檢查表	圖書資訊處	至少 1 年
4	系統主機安全檢查表	圖書資訊處	至少 1 年
5	辦公區域安全檢查表	圖書資訊處	至少 1 年
6	個人電腦安全檢查表	圖書資訊處	至少 1 年

6. 附件

6.1. ISMS-P-011-01 管制區域門禁卡使用登記表。

6.2. ISMS-P-011-02 管制區域進出管制登記表。

6.3. ISMS-P-011-03 管制區域檢查表。

6.4. ISMS-P-011-04 系統主機安全檢查表。

6.5. ISMS-P-011-05 辦公區域安全檢查表。

6.6. PIMS-3-001-02 個人電腦安全檢查表。

開南大學
KAINAN University

管制區域門禁卡使用登記表

※ 門禁卡需經圖書資訊處處長核可後發給申請人使用。

門禁卡卡號	類別	申請事由	申請人員	核發人員	核發日期	註銷日期	註銷人員	審核主管
	☐申請							
	☐註銷							
	☐申請							
	☐註銷							
	☐申請							
	☐註銷							
	☐申請							
	☐註銷							
	☐申請							
	☐註銷							
	☐申請							
	☐註銷							

開 南 大 學
KAINAN University

管 制 區 域 進 出 管 制 登 記 表

NO	日期			單位	姓名	陪同人員	進/出	時間		攜出、入設備/用途說明	進出原因/作業內容
	年	月	日					時	分		
1							進			□無	
							出			□有	
2							進			□無	
							出			□有	
3							進			□無	
							出			□有	
4							進			□無	
							出			□有	
5							進			□無	
							出			□有	
6							進			□無	
							出			□有	
7							進			□無	
							出			□有	
8							進			□無	
							出			□有	
9							進			□無	
							出			□有	
10							進			□無	
							出			□有	
11							進			□無	
							出			□有	
12							進			□無	
							出			□有	

開 南 大 學
K A I N A N U n i v e r s i t y

年 月 管 制 區 域 檢 查 表

檢查項目		檢 查 內 容	檢查頻率	第一週					第二週					第三週					第四週					第五週				
				一	二	三	四	五	一	二	三	四	五	一	二	三	四	五	一	二	三	四	五	一	二	三	四	五
機房環境檢查	機房溫度	機房溫度介於 20℃~27℃之間	每天																									
	機房濕度	濕度介於 25%~85%之間	每天																									
	UPS 不斷電系統	運作負載量低於 70%	每週																									
	硬體設備	各類主機與網路設備之外觀燈號及運作正常	每天																									
	資安設備	防火牆與防護設備之外觀燈號及運作正常	每天																									
網路及系統服務檢查	訊鐘同步	各資訊系統伺服主機時鐘已同步	每月																									
	磁碟容量 (Volume/使用空間/總容量)	磁碟陣列儲存空間使用量低於 90%	每週																									
		伺服主機儲存空間使用量低於 80%	每週																									
	網路流量	網路各線路頻寬使用量低於 85%	每週																									
	Web Server	校務資訊系統(http://portal.knu.edu.tw/)運作正常	每天																									
		學校入口網站(http://www.knu.edu.tw/)運作正常	每天																									
		電子公文系統(http://edoc.knu.edu.tw/kw)運作正常	每天																									
	網管系統	網頁功能與 DB 服務運作正常	每天																									
	E-mail	電子郵件系統網頁與收發(POP3 及 SMTP)運作正常	每天																									

備註說明	1. **打「V」代表「正常 」/ 打「X」代表「異常」**。如有異常狀況無法及時處理時請填寫「ISMS-P-008 矯正及預防管理程序書」研擬改善措施進行異常處理。機房檢查人員請於月底將檢查表送交權責主管簽核。			
檢查人員	網路媒體組		系統開發組	權責主管審核

開　南　大　學
K A I N A N　U n i v e r s i t y

系　統　主　機　安　全　檢　查　表

單位別		查核人員		檢查日期	
系統名稱		IP 位址		管理者	

	檢查項目	檢查狀況	查核紀錄
1	系統管理者除特殊情況外並無共用"Administrator"（Windows 平台）或是"root"（Unix 平台）作為登入之帳號。	□是 □否	
2	電腦系統登入有設定帳號及密碼，密碼長度至少 8 碼，密碼內容已使用「數字」、「英文字母大寫/小寫」或「特殊符號」等混合使用（至少 3 種以上）。	□是 □否	
3	有啟動螢幕保護程式（時間小於 10 分鐘）且設定密碼保護功能。	□是 □否	
4	已安裝防毒軟體，病毒碼已更新至最新版本。	□是 □否	
5	已啟動 NTP（時鐘同步/ GMT＋8）功能。	□是 □否	
6	未使用非法或未經授權之軟體，無違反智慧財產權（IPR）相關法令法規之情事。	□是 □否	
7	「系統管理者帳號」皆已被授權核准使用（查核者需核對實際存在帳號與被授權之帳號是否相吻合）。	□是 □否	
8	有啟動 Log 服務且正常運作。	□是 □否	
9	已完成變更系統管理者密碼（每六個月變更一次）。	□是 □否	
權責主管審核			

※查核人員若發現不符合事項時，應於「查核紀錄」欄，詳細填寫查核之具體事證。
※經查核若有違反上述之各項檢查項目並經確認無誤後，由系統管理者進行調整至符合上述需求為止，再請單位主管進行複查，直至完全符合檢查項目為止。

開　南　大　學
KAINAN University

辦公區域安全檢查表

查核區域：

檢查項目			上半年 檢查日期 年 月 日	下半年 檢查日期 年 月 日
辦公區域安全管制	1	各項機敏（機密）文件，已收妥且存放於上鎖之抽屜或儲櫃（確保實體安全）。	□ 是 □ 否	□ 是 □ 否
	2	影印機、傳真機、印表機及其他事務性機器未遺留機敏（機密）文件。	□ 是 □ 否	□ 是 □ 否
	3	重要之可攜式設備及可攜式儲存媒體（如外接式硬碟、隨身碟或其他電磁紀錄物）均已收入上鎖之抽屜或儲櫃。	□ 是 □ 否	□ 是 □ 否
辦公區域環境管制	1	重要辦公區域已設置消防設施，設施已有定期進行檢測且有檢測紀錄(確保其持續有效且可用)。	□ 是 □ 否	□ 是 □ 否
	2	辦公區域內未存放高揮發性之易燃物品（如：酒精），以避免火災發生。	□ 是 □ 否	□ 是 □ 否
	3	進入設有門禁系統之管制區域內應取得授權並隨手關門，確保辦公環境之安全。	□ 是 □ 否	□ 是 □ 否
	4		□ 是 □ 否	□ 是 □ 否
檢查人員簽名				
權責主管審核				

※無法立即處理解決時，需填寫「ISMS-P-008-01 矯正及預防處理單」登錄列管，並研擬改善措施進行異常處理。

開南大學
KAINAN University

個人電腦安全檢查表

員工姓名		組別		分機	
資產編號		檢查日期			

		檢查項目	檢查狀況	查核紀錄
個人電腦安全查核	1	個人電腦系統（含應用系統）登入已設定帳號及密碼（長度至少 8 碼），密碼未置放於顯而易見之處。	□是 □否	
	2	電腦已啟動螢幕保護程式且設定密碼保護（閒置超過 10 分鐘即啟動螢幕保護程式）。	□是 □否	
	3	電腦未安裝來路不明或未經授權核准之軟體（含 P2P），請依本公司「ISMS-P-017-01 合法軟體授權使用清冊」或軟體授權資訊進行查核。	□是 □否	
	4	電腦已安裝防毒軟體，且病毒碼已更新至最新版本。	□是 □否	
	5	電腦作業系統已定期自動或手動執行 Windows Update（安裝作業系統之高優先順序更新檔案）	□是 □否	
	6	電腦未使用未經授權且核准使用之無線網路設備（無線基地台、3.5G 行動通訊網卡）	□是 □否	
	7	未使用未經授權核准使用之燒錄設備、可攜式設備及可攜式儲存媒體（如：外接式硬碟、隨身碟或其他電磁紀錄物）。	□是 □否	
	8	承辦業務之機敏文件，不使用、下班或長時間離座時，應收妥且存放於上鎖儲櫃（確保實體安全）。	□是 □否	
	9	瀏覽器安全性設定：是否已設定「網際網路」之安全層級為「中高」以上？	□是 □否	
	10	電腦已安裝及啟用防火牆安全防護功能？	□是 □否	

稽查人員		單位主管	

※稽查人員若發現不符合事項時，應於「查核紀錄」欄，詳細填寫查核之具體事證。

※經查核若有違反上述之各項檢查項目並經確認無誤後，由資訊人員協助將電腦進行調整至符合上述需求為止，再請稽查人員進行複查，直至完全符合檢查項目之要求為止。