



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	1 / 10

管理系統文件

文件類別	第二階文件	
文件編號	IMS-P-011	
文件名稱	實體與環境安全管理程序書	
發行單位	國立虎尾科技大學	
發行日期	111年07月02日	
版次	3.3	
適用單位/範圍	全校	
訂修廢單位	審查	核准

(原版簽名頁保存於IMS推動小組)



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	2 / 10

訂 修 廢 記 錄		
版次	發行日期	訂修廢內容摘要
1.0	106/01/11	初版發行
2.0	106/10/03	修正條文 5.3.2.5
3.0	108/09/09	因應資通安全管理法施行及配合法規用詞，將「資訊」一詞修改為「資通」。
3.1	109/06/12	修改保存地點為「各單位」
3.2	110/03/29	<p>(1)刪除 3.參考文件「附錄 A 資通安全管理規範」，增訂「國際標準資訊安全管理系統 (ISO27001：2013)」。</p> <p>(2)修訂 5.3.1.7 為：個人電腦應設定螢幕保護程式請參照「IMS-W-001 一般資通設備安全管理作業標準書」。</p> <p>(3)修訂「5.5.3 IMS-P-011-04 辦公區域安全檢查表」改使用「IMS-W-003-01 辦公區域安全檢查表」。</p> <p>(4)修訂「5.5.4 IMS-P-011-05 個人電腦安全檢查表」改使用「IMS-W-003-02 個人電腦安全檢查表」。</p> <p>(5)修訂 6.4 「IMS-P-011-04 辦公區域安全檢查表」為：「IMS-W-003-01 辦公區域安全檢查表」。</p> <p>(6)修訂 6.5 「IMS-P-011-05 個人電腦安全檢查表」為：「IMS-W-003-02 個人電腦安全檢查表」。</p>
3.3	111/07/02	修訂條文 5.5.2 及 5.5.3



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	3 / 10

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，以避免資通資產及各項資通系統，遭未授權的存取、損害與干擾，進而影響業務正常運作。

2. 適用範圍

本校實體與環境安全之管理。

3. 參考文件

3.1 資通安全管理法。

3.2 資通安全管理法施行細則。

3.3 國際標準資訊安全管理系統(ISO27001：2013)。

3.4 教育體系資通安全暨個人資料管理規範。

3.5 IMS-P-016 資通設備維護與管理程序書。

3.6 IMS-P-009 資通安全事件管理程序書。

3.7 IMS-P-008 矯正預防及持續改善管理程序書。

4. 名詞定義

4.1 一般區域

本校實體環境範圍內，除管制區域以外的辦公作業環境。

4.2 管制區域

本校實體環境範圍內，用以存放關鍵(核心)或高機敏性的營運資訊及資通資產設施的場所（如本校電子計算機中心資訊機房、倉儲庫房等等），提供實體安全防護，以確保資通資產機密性、完整性及可用性，降低資通安全事件之發生。



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	4 / 10

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
<pre> graph TD A([規劃管制區域]) --> B[訂定區域管制規定] B --> C[設備安全管理] C --> D{查核} D -- 異常 --> E[異常處理] E --> F([紀錄保存]) D -- 正常 --> F </pre>	<p>IMS 推動小組</p> <p>IMS 推動小組 管制區域管理人員</p> <p>IMS 推動小組</p> <p>管制區域管理人員 資通系統管理人員 相關業務承辦人員</p> <p>IMS 推動小組</p> <p>IMS 推動小組</p>	<p>人員機房進出紀錄表 資通設備維護及系統變更紀錄單 管制區域檢查表</p> <p>資通設備維護及系統變更紀錄單</p> <p>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</p>



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	5 / 10

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

5.3.1.1 非本校人員欲進入其辦公區域，須經業務承辦人員同意後始可進入。

5.3.1.2 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。

5.3.1.3 未經許可，不得於本校辦公區域內使用錄音、錄影或具有照相功能之資通設備。

5.3.1.4 機密等級屬「機敏」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。

5.3.1.5 機密等級屬「機敏」之資訊，不使用或下班時應存放在櫃子內並上鎖。

5.3.1.6 列印或傳真機密等級屬「機敏」之資訊時，作業完成後應立即從印表機或傳真機取走。

5.3.1.7 個人電腦應設定螢幕保護程式請參照「IMS-W-001 一般資通設備安全管理作業標準書」。

5.3.1.8 辦公區域環境內嚴禁抽煙。

5.3.1.9 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。

5.3.2 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，應採用門禁系統做為門禁管制，若需管制區域門禁進出權限，應填寫



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	6 / 10

「IMS-P-013-01 資通系統使用權限申請單」，經單位主管核准後向承辦人員提出申請，以控管管制區域的通行權限。

5.3.2.2 無門禁卡者（如：委外廠商、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「IMS-P-011-01 人員機房進出紀錄表」中登錄；若須將資通設備攜入或攜出，亦須於「IMS-P-011-01 人員機房進出紀錄表」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 管制區域內的門禁管制系統之電子紀錄至少需留存 3 個月，監視系統之電子紀錄至少需留存 15 日曆天，且有適切的保護措施，並定期查核以確定沒有異常情況。

5.3.2.5 管制區域內執行設備維護及任何異動（變更）作業時，須填寫「IMS-P-016-02 資通設備維護及系統變更紀錄單」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：

5.3.2.6.1 禁止飲食、放置飲料食物及存放私人物品。

5.3.2.6.2 禁止喧嘩、嬉戲、吸煙、奔跑等不安全動作。

5.3.2.6.3 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。

5.3.2.6.4 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。

5.3.2.6.5 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。

5.3.2.6.6 磁帶、磁碟等消耗品應放置於規定場所，不得隨意放置，且不得私自取用磁帶、磁碟等公用物品。



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	7 / 10

5.3.2.7 管制區域管理人員，應定期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「IMS-P-011-02 管制區域檢查表」，如發現異常狀況，應即時通知設備管理者、相關權責主管或委外廠商，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 重要資通設備應安置於管制區域內，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 管制區域內資通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 處理機密等級屬「機敏」之資訊的資通設備，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 需要特別保護的設備，應考量與一般的設備區隔，安置在獨立的區域。

5.4.1.3.4 應檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等可能的風險。

5.4.1.3.5 電子計算機中心人員需熟悉機房滅火器擺設位置及操作方法。

5.4.1.3.6 除考量同一樓層地板可能導致的危險外，應考量鄰近建築樓層地可能導致的危險。

5.4.1.3.7 備援資料應存放於安全距離以外的地點或儲存設備，避免伺服器內資料受到毀損時，造成無法復原之災害損失。

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。



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	8 / 10

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，並依據測試結果或委外廠商評估之建議，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 連接資訊設施的電源及通訊線路，應有外殼包覆保護並盡可能置於高架地板下，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、網路及資通安全設備等），應與專業委外廠商簽訂維護契約，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 應依據原廠使用說明或操作手冊之規定，進行資通設備的維護作業。



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	9 / 10

5.4.4.2.3 資通設備的維護只能由授權的維護人員執行，且需有人員陪同。

5.4.4.2.4 維護委外廠商於現場進行資通設備的修（維）護作業時，須於「IMS-P-016-02 資通設備維護及系統變更紀錄單」中登錄修（維）護狀況，並檢附維護委外廠商維修紀錄備查，以為日後稽核之參考。

5.4.4.2.5 資通設備之維護規範，請依據「IMS-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「IMS-P-016 資通設備維護與管理程序書」之相關規定辦理。

5.4.6 資通資產報廢及再使用之安全

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。

5.5 查核

5.5.1 每月由管制區域管理人員將「IMS-P-011-02 管制區域檢查表」查核結果，向權責主管回報，並於「IMS-P-011-02 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 配合主機作業系統帳號審查作業，每年至少一次進行一次主機安全性查核。由資通系統管理人員依據「IMS-P-011-03 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，須由資通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 每年由各單位資安及個資保護專責人員，依「IMS-W-003-01 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。



文件編號	IMS-P-011	文件名稱	實體與環境安全管理程序書		
機密等級	內部使用	版次	3.3	頁次	10 / 10

5.5.4 每年由業務承辦人員，將「IMS-W-003-02 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「IMS-P-009 資通安全事件管理程序書」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「IMS-P-008 矯正預防及持續改善管理程序」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	人員機房進出紀錄表	各單位	至少 3 年
2	管制區域檢查表	各單位	至少 3 年
3	系統主機安全檢查表	各單位	至少 3 年
4	辦公區域安全檢查表	各單位	至少 3 年
5	個人電腦安全檢查表	各單位	至少 3 年

6. 附件

6.1 IMS-P-011-01 人員機房進出紀錄表。

6.2 IMS-P-011-02 管制區域檢查表。

6.3 IMS-P-011-03 系統主機安全檢查表。

6.4 IMS-W-003-01 辦公區域安全檢查表。

6.5 IMS-W-003-02 個人電腦安全檢查表。