發布日期：107年9月

版本：1.0

金融科技創新園區

資訊安全管理規範

版本1.0

主辦單位：台灣金融服務業聯合總會

執行單位：財團法人資訊工業策進會

中 華 民 國 1 0 7 年 9 月

目錄

[壹、 資訊安全管理規範說明 1](#_Toc525732615)

[貳、 網路安全管理 2](#_Toc525732619)

[參、 實體及環境安全管理 5](#_Toc525732625)

[肆、 應用系統開發管理 6](#_Toc525732629)

[伍、 進駐團隊電信線路申裝管理 7](#_Toc525732633)

# 資訊安全管理規範說明

# 目的

為保障金融科技創新園區場域(以下簡稱本場域)資訊之安全、品質、機密性、完整性與可用性，特制定本管理規則。

# 定義

(一)本管理規範所稱本場域資訊，指本場域於業務範圍內做成或取得而存在於文書、圖畫、照片、磁碟、磁帶、光碟片、微縮片、積體電路晶片等媒介物及其他得以讀、看、聽或以技術、輔助方法理解之任何紀錄內之訊息。

(二) 本管理規範所稱人員，指在本場域提供資訊系統服務之廠商與其員工、以及進駐本場域進行相關資訊應用系統開發測試之團隊及其員工。

(三) 本管理規範所稱園區應用系統，指於線上提供服務之系統，但參數值設定後即可提供服務之套裝軟體除外。

# 規範制定依據

為確保資訊安全施行細則完整性，本辦法中施行細則以 CNS27002 資訊安全管理之作業規範為依據，進行場域適用性調整。

# 網路安全管理

## 第一條 網路安全管理

一、網路存取權限之管理

(一) 網路安全系統的最高使用權限，由權責主管決定。

(二) 網路管理人員應負責網路安全程序的擬訂，執行網路管理工具之設定與操作。

(三) 網路管理人員應負責發放並管理SSID，供授權的人員使用。

(四) 網路管理人員應依使用需求進行MAC、Switch Port、SSID等對應設定。

(五) 如使用者已非被授權者，網路管理人員應撤銷其使用者權限。

(六) 本場域所提供之網路存取為無償提供，使用者不得利用其作為其他收益行為。

二、防火牆之安全管理

(一) 場域與外界網路連接的閘道，應設置防火牆。

(二) 網路管理人員應配合資訊安全政策與相關規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統設定與存取權限。

(三) 網路管理人員應負責監督網路資料使用情形，檢查有無違反資訊安全政策與相關規定之事件發生。

三、使用者類型存取方式

 使用者類型區分7大類，並得依實際營運需求調整，說明如下:

|  |  |  |  |
| --- | --- | --- | --- |
| **網路使用類型** | **SSID** | **權限** | **網路管理** |
| 一般訪客 | FinTechSpace-Guest | 僅提供基本網際網路連線無法使用數位沙盒 | 每月變更一次密碼  |
| 校園-數位沙盒 | Academy | 校園課程專用(專案申請)限時限區使用數位沙盒 | 每次課程變更密碼 |
| 開放空間 | OPS | 開放空間座位 | MAC綁定存取 |
| 開放空間-數位沙盒 | OPS\_Digi\_Sandbox | 開放空間座位使用數位沙盒 | MAC綁定存取 |
| 獨立空間 | IDS | 獨立空間座位 | MAC綁定存取 |
| 獨立空間-數位沙盒 | IDS\_Digi\_Sandbox | 獨立空間座位使用數位沙盒 | MAC綁定存取 |
| 園區辦公室 | FTS-OA | 辦公區人員設備專用 | MAC綁定存取 |

四、數位沙盒存取管控限制

 數位沙盒共通管理平台具備連線IP限制及存取資料量限制等管控機制。連線以白名單的方式允許特定IP區段存取特定服務，存取資料量之限制則透過紀錄並分析各使用者之API使用歷程進行管控。

(一)連線 IP 限制:僅限定由園區IP特定區段連線使用。

(二)使用者存取限制: API使用存取限制將依各API供應者之要求設定，例如:證交即時資訊API限制單一團隊每日取用資料量上限為10GB，由凌晨12:00起算。

## 第二條 園區網路使用者行為規範

一、使用者不可對本園區網路資訊設備進行動態網路位址(DHCP)之發放，所有網路位址(IP)位址統一由本園區網路管控設備發放之。

二、為避免干擾本園區無線網路之運作，不得私架無線網路基地台。

三、配合園區資安要求，若有新增資訊網路設備安裝需求，須經園區管理單位申請同意後方能架設，且使用單位須確保不因架設後，影響園區資安。

四、如架設個別網路專線，發生影響園區網路服務品質或資安事件，園區得要求立即撤除該架設網路。

五、使用者不得有以下行為:

(一) 非法使用他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，入侵他人之電腦或其相關設備。

(二) 非法取得、刪除或變更他人電腦或其相關設備之電磁紀錄。

(三) 以電腦程式或其他電磁方式干擾他人電腦或其相關設備。

(四) 以任何方式濫用網路資源，大量傳送電子垃圾郵件或類似資訊，及其他影響本園區網路系統正常運作之行為。

(五) 以電子郵件、線上談話、電子佈告欄或其他類似功能之方法，從事散布謠言、詐欺、誹謗、侮辱、猥褻、騷擾、威脅或其他違反社會善良風俗之資訊。

(六) 其他不符本園區網路設置目的之行為。

前項各款行為涉及不法情事者，使用者應依相關法令規定自負法律責任。

## 第三條 園區網路使用者智慧財產權規範

本園區進駐單位應要求其使用者尊重智慧財產權，並不得為下列可能涉及侵害網路智慧財產權之行為：

* + 1. 使用未經授權之電腦程式。
		2. 下載或重製受著作權法保護之著作。
		3. 未經著作權人之同意，將受保護之著作公開於網路上。
		4. 任意轉載電子佈告欄或其他線上討論區之文章。
		5. 其他可能涉及侵害智慧財產權爭議之行為。

## 第四條 園區網路連線限制與中斷使用

本園區進駐單位有下列各款情形之一者，管理單位得限制或暫時中斷本園區網路之連線：

* 1. 違反相關法令或本管理規範之情事。

 (二) 涉及國家安全。

 (三) 為配合司法機關之調查。

 (四) 為阻斷不當或不法行為存續或擴散。

 (五) 更新、遷移網路設備，測試、維護或檢查網路及相關系統。

* + 1. 不明原因非中斷不足以排除網路障礙。

##  第五條 園區網路服務聲明

 本園區網路為服務性質無償提供，請進駐單位自行建立資訊安全與營運持續等風險管理控制措施，若因網路中斷或惡意攻擊等行為，致系統服務中斷或營業利益損失等情形，本園區不負相關賠償責任。

# 實體及環境安全管理

## 第一條 實體管理

一、資通訊設備之設置，應防止斷電或其他電力供應不正常。

二、電力及通信用的電纜線宜予適當的保護，並謹慎使用電源延長線。

## 第二條 自攜式資訊設備使用安全

一、本場域人員使用自攜式資通訊設備，應確認使用軟硬體之合法授權。

二、於本場域使用之資通訊設備，應具備基本安全防護機制，如防毒軟體，並確認病毒碼為最新版本。

## 第三條 環境安全

一、實體環境應依重要性或機密性設置必要的安全管制（例如電子門禁等）。

二、本場域進出人員皆得申請門禁卡，申請時應由申請書上簽名領取。

三、申請人應填具「門禁卡申請異動資料表」後，向本場域管理人員提出申請。本場域管理人員依本要點審核、簽認通過後，應即進行資料記錄建檔備查及發放作業。

四、人員變動及遺失補發：

(一) 申請人所申請之門禁卡之持有人異動時，應於填具「門禁卡申請異動資料表」後，向本場域管理人員提出申請。本場域管理人員依本要點審核，簽認通過後，應即進行資料記錄建檔備查及發放作業。

(二) 申請人所申請之門禁卡之持有人遺失門禁卡時，應即告知本場域管理人員取消該門禁卡之設定，並填具「門禁卡申請異動資料表」向本場域管理人員申請補發，且應繳交工本費，每張新台幣叁百元整。

五、門禁管制：

開放時間：

固定座位區: 24小時門禁管理進出使用。

非固定座位區: 週一至週五 09：00 至 18：00（不含國定例假日）。

六、配合事項：

（一） 本場域管理人員每半年進行人員名冊之清查作業。

（二） 人員完成辦理退出本場域手續，且不再進出場域時，必須將門禁卡繳回，如遺失應賠償，每張新台幣叁百元整。

# 應用系統開發管理

## 第一條 園區應用系統環境之安全

一、系統管理人員應訂定應用系統之備份與回復程序。

二、系統管理人員變更作業系統時，應評估對園區應用系統的影響。

## 第二條 園區應用系統驗證之安全

一、開發人員應於應用系統開發階段，執行程式碼安全檢查，包括防範園區應用系統開發人員植入木馬程式。

二、園區應用系統上線前，應完成下列安全性檢測需求：

(一) 源碼掃描：提供掃描報告，並完成修補中級以上的風險問題。

(二) 弱點掃描：提供掃描報告，並完成修補中級以上的風險問題。

(三) 壓測報告：提供壓測報告，說明應用程序資源耗用等。

## 第三條 園區應用系統變更之安全

開發人員應依下列原則制定園區應用系統變更程序：

(一) 園區應用系統之變更，非經申請不得為之。

(二) 園區應用系統之變更，應依據本規範第三條重新提出驗證報告。

# 進駐團隊電信線路申裝管理

## 第一條 電信線路申裝規定

* 1. 獨立空間進駐團隊始有權利提出自設電信線路需求。
	2. 每一獨立空間僅能申請一路，連接方式須遵照園區設置要求。
	3. 申裝及使用費用由團隊自行繳付(目前僅中華電信拉光纖至園區)。
	4. 申裝之團隊，除自行負擔電信公司申請費用及頻寬費用外，須另行負擔園區網路專線施工及設定費用。

## 第二條 電信線路使用規定

1. 電信線路使用，以不影響園區網路服務品質、園區資訊安全為主。如發生上述事項，進駐團隊於管理人員要求後，應立即撤除該電信線路。
2. 進駐團隊不得於園區內架設伺服器。如因此造成公共安全意外，需負擔賠償、修繕等相關費用及責任。