發布日期：111年12月

版本：2.0

金融科技創新園區

場域資訊安全管理規範

版本2.0

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110年12月

|  |  |  |  |
| --- | --- | --- | --- |
| 修訂歷史紀錄欄 | | | |
| 版次 | 承辦者 | 摘 要 | 發行/修訂生效日期 |
| V1.0 | 金融科技創新園區 | 場域資訊安全管理規範 | 107.09 |
| V2.0 | 金融科技創新園區 | 更新版面及門禁卡管理規範、新增場域定義、共用事務機使用規範 | 111.12 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**目錄**

[第壹章、 資訊安全管理規範說明 - 4 -](#_Toc119681478)

[第貳章、 網路安全管理 - 5 -](#_Toc119681479)

[第參章、 實體及環境安全管理 - 8 -](#_Toc119681480)

[第肆章、 應用系統開發管理 - 9 -](#_Toc119681482)

[第伍章、 進駐團隊電信線路申裝管理 - 10 -](#_Toc119681483)

# 資訊安全管理規範說明

1. **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。

1. **定義**
2. 本管理規範所稱之「本場域」包含台北市中正區南海路1號13樓之場域空間，並包含獨立辦公室、固定座位、非固定座位等。
3. 本管理規範所稱之「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。
4. 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。
5. 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。
6. **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

1. **網路安全管理**
2. 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。
3. 網路存取權限之管理
4. 網路安全系統的最高使用權限由權責主管決定。
5. 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。
6. 網路管理人員應負責發放並管理SSID，供授權的人員使用。
7. 網路管理人員應依使用需求進行MAC、Switch Port、SSID等對應設定。
8. 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。
9. 防火牆之安全管理
10. 場域與外界網路連接的閘道，應設置防火牆。
11. 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。
12. 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。
13. 無線網路使用者類型存取方式
14. 無線網路使用者類型區分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 |

1. 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。

1. 連線 IP 限制:

僅限定於園區IP特定區段及經園區審議會議核可之遠距存取IP(VPN)之連線使用。

1. 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。

1. **園區網路使用者行為規範**
2. 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。
3. 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。
4. 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。
5. 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。
6. 使用者不得有以下行為:
7. 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。
8. 非法取得、刪除或變更他人電腦或其相關設備之電磁紀錄。
9. 以電腦程式或其他電磁方式干擾他人電腦或其相關設備。
10. 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。
11. 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。
12. 其他不符本園區網路設置目的之行為。
13. 其它涉及不法情事之行為，使用者應依相關法令規定自負法律責任。
14. **園區網路使用者智慧財產權規範**
15. 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：
16. 使用未經授權之電腦程式。
17. 下載或重製受著作權法保護之著作。
18. 未經著作權人之同意，將受保護之著作公開於網路上。
19. 任意轉載電子佈告欄或其他線上討論區之文章。
20. 其他可能涉及侵害智慧財產權爭議之行為。
21. **園區網路連線限制與中斷使用**
22. 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：
23. 違反相關法令或本管理規範之情事。
24. 涉及國家安全。
25. 為配合司法機關之調查。
26. 為阻斷不當或不法行為存續或擴散。
27. 更新、遷移網路設備，測試、維護或檢查網路及相關系統。
28. 不明原因非中斷不足以排除網路障礙。
29. **園區網路服務聲明**
30. 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

1. **實體管理**
2. 資通訊設備之設置，應防止斷電或其他電力供應不正常。
3. 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。
4. **自攜式資訊設備使用安全**
5. 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。
6. 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。
7. **環境安全**
8. 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）。
9. 本場域進出人員(包含場域管理人員及進駐團隊人員)應申請門禁卡進出。其他訪客則應於每次進入時向櫃台登記。
10. 門禁卡應以下述方式申請：
11. 本場域管理人員在接獲門禁卡申請需求時，應先審核其申請需求之合適性，並於申請通過進行資料記錄建檔備查及發放作業。
12. 人員變動及遺失補發：
13. 本場域管理人員在接獲門禁卡人員異動或遺失之申請需求時，應先審核其申請需求之合適性，並於申請通過進行資料記錄建檔備查及發放作業。
14. 門禁管制：
15. 本園區開放時間為：
16. 獨立辦公室與固定座位區: 24小時門禁管理進出使用。
17. 非固定座位區: 週一至週五 09：00 至 18：00（不含國定例假日）。
18. 配合事項：
19. 本場域管理人員每半年進行人員名冊之清查作業。(應再補充依據清查結果進行的後續處理程序，如:有需移除者會在特定時間內移除)

# 應用系統開發管理

1. **範圍**
2. 園區自行開發或委由第三方開發、建置、維護、處理與管理之活動，皆為適用範圍。
3. **園區應用系統環境之安全**
4. 系統管理人員應訂定應用系統之備份與回復程序。
5. 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。
6. **園區應用系統驗證之安全**
7. 開發人員應於應用系統開發階段，即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。
8. 園區官方網站上線前，應完成下列安全性檢測需求：
   1. 源碼掃描：提供掃描報告，並完成修補中級以上的風險問題。
   2. 弱點掃描：提供掃描報告，並完成修補中級以上的風險問題。
   3. 壓測報告：提供壓測報告，說明應用程序資源耗用等。
9. **園區應用系統變更之安全**
10. 開發人員應依下列原則制定園區應用系統變更程序：
11. 園區應用系統之變更，非經申請不得為之。
12. 園區應用系統之變更，應依據本規範第十三條重新提出驗證報告，並完成修補。

# 進駐團隊電信線路申裝管理

1. **電信線路申裝規定**
2. 獨立空間進駐團隊始有權利提出自設電信線路需求。
3. 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。
4. 申裝及使用費用由團隊自行繳付(目前僅限拉中華電信光纖至園區)。
5. 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。
6. **電信線路使用規定**
7. 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。
8. 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。
9. **共用多功能事務機使用管理**
10. 使用共用之多功能事務機處理個資後，須立即將資料取走。