

4.4.2 訂定智慧化設施設備危機處理與緊急應變計畫及防範措施(包括資安、當機、駭客入侵)

【說明一】：智慧化設施設備異常事件處理計畫

1. 智慧化設施設備及相關人員定義如下：

- 甲、智慧化設施設備：包含本社區使用之中央監控系統、機弱電系統、物業管理系統軟硬體設備
- 乙、值班人員：指本社區輪值之值班人員。
- 丙、承辦人員：指本社區管理中心負責人員(如社區經理、總幹事)。
- 丁、負責人員：指本社區之管委會成員。
- 戊、維護廠商：指每年度依契約委外維護之廠商。

2. 緊急通報事項：

甲、災害防救事項

- i. 發生火災
- ii. 淹水
- iii. 因強烈地震、颱風造成災害

乙、安全維護事項

- i. 智慧化設施設備遭竊或疑似遭人入侵或發現形跡可疑人士。
- ii. 智慧化設施設備發現疑似爆裂物或可疑不明物品。
- iii. 智慧化設施設備內發生突發意外事件，有危及本社區設施及人員安全之虞。

丙、空調、機電系統無預警異常事件

- i. 因應智慧化設施設備因無預警空調或電力突發異常狀況，避免因沒有空調、高溫造成設備當機損毀。

3. 災害處理流程：

甲、災害防救事項

i. 發生火災：

- 1. 立即通知消防單位。
- 2. 值班人員發現火災應立即通報維護廠商、承辦人員。
- 3. 無法撲滅火勢或氮氣滅火系統動作前，值班人員應開啟門禁緊急強制開關，協助現場人員撤離。
- 4. 如火勢過大應立即離開現場。
- 5. 火災發生過後，應先行檢測主機系統及硬體受損程度，如系統無法正常使用或硬體嚴重受損時，應通知各維護廠商協助進行災難復原作業(或啟動備援作業)。

ii. 淹水、地震或颱風造成災害：

- 1. 值班人員應隨時注意新聞媒體，遇天然災害可能危急智慧化設施設備時，至現場查看災害情形，並做緊急處理：
- 2. 通報維護廠商及負責人員。
- 3. 通報受損設備之各維護廠商人員。
- 4. 若因淹水有漏電之虞時，應立即以電子郵件及電話聯繫各維護廠商同意由值班人員協助進行關機作業。如有立即危險又無法聯絡負責人員關閉設備，則逕行關閉分電盤總開關。

乙、安全維護事項：智慧化設施設備遭竊或疑似遭人入侵或發現行跡可疑人士、發現疑似爆裂物或可疑不明物品處理方式如下，

- i. 值班人員應立即通報承辦人員及負責人員告知需派員處理。
- ii. 值班人員查看現場情形圍起封鎖線並通報維護廠商。
- iii. 通報受損設備之各系統負責人員。

4. 空調、機電系統無預警異常事件

- 1. 機房電力、機房空調、機房門禁系統等故障情形嚴重時，機房值班人員查看現場情形做緊急處理並通報機房維護廠商及機房承辦人員。
- 2. 發電機供電中斷、空調或機電系統異常時，值班人員應立即通報維護廠商，詢問原因並請求最短時間內修復。
- 3. 電力或空調系統中斷時，值班人員應立即處理，必要時通知機房維護廠商進場搶修。
- 4. 門禁系統故障無法運作時改採人工管制，並立即通知機房維護廠商進行搶修。

5. 停電時緊急應變：

甲、因發電機可供之電源有限，值班人員應於停電前（若需停電超過 0.5 小時以上）或發現停電時（估算所需停電時間超過 0.5 小時以上），以下程序將主機關閉，待復電時再將主機開啟。

乙、若台電將於有停電計畫 0.5 小時以上，除有特殊任務而無法關機之伺服器或網路設備外，應於停電前關閉，電力恢復後再行開機。

丙、承上，若台電將計畫性停電超過 0.5 小時以上，由承辦人員公告停電消息於管理系統上，並以 e-mail 或電話通知各系統負責人員進行關機。

丁、如機房溫度高於 40 度以上，則須將機房門禁打開保持空氣流暢以降低溫度，待恢復供電後，恢復門禁並啟動空調主機。

5. 如有上開災變發生，造成短期間資訊設備當機或資料漏失無法回復正常，各系統負責人員應洽各業務單位相關作業人員，改採人工處理程序辦理，並將人工表單資料妥善保存，以供修復完畢後補正資料之需。

6. 通報原則及方式：

甲、通報人員為值班人員，應與維護廠商及承辦人員聯絡，查明事情發生原委，於「社區異常事件維護紀錄單」詳細記載。

乙、通報內容：通告通報人姓名、身分、事件發生經過（包含事由、地點、時間、採取緊急處置情形並註記嚴重程度）。

丙、值班人員應查看現場情形作緊急處理，並通報承辦人員。

丁、事件處理情形及結果須及時回報相關人員，並層層通報至管委會。

戊、因故無法依前項通報及處理流程所訂人員通報時，則改以通報其代理人，並由代理人依流程完成通報。

己、事故發生在非辦公時間，則以行動電話及住家電話通報。

7. 災害發生過後，應先行檢測主機系統及硬體受損程度並依下列程序處理：

甲、由各系統負責人員研判故障類型，並先行設法排除，如無法解決時，應詳細記錄當時狀況及顯示之訊息後，立即就故障問題通知相關人員及維護廠商前來維修。

乙、如主機硬體嚴重受損時，應與維修人員連絡，並詳述損壞情形，以減少維修人員修復

之時間，並於最短時間內回復硬體設備，如短時間無法回復硬體設備時，應協調商借主機暫時使用。

丙、如遇系統受損或資料毀損無法回復時，應由備份系統回復資料，將損壞減低到最小之程度。

丁、如逾一小時無法修復時，應通知各單位，並督促相關廠商儘快修復。

8. 本計畫未盡事宜，將於後續管委會討論決議修改。

【說明二】：社區管理資訊安全維護計畫-網路安全控管

智慧化系統權限管理

1. 社區之智慧化系統應設置帳號密碼管理，密碼之要求需滿足：

1. 長度 8 碼以上。
2. 複雜度應包含英文大寫小寫、特殊符號或數字兩種以上。
3. 使用者每 90 天應更換一次。

2. 使用者使用智慧化系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用智慧化系統時，應立即停用或移除使用者 ID，系統管理者應定期清查使用者之權限。

特權帳號之存取管理

1. 系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 智慧化系統之特權帳號不得共用。

3. 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4. 智慧化系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5. 智慧化系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

防範惡意軟體之控制防範措施

(1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2) 電子郵件附件及下載檔案於使用前，宜於他處先掃描有無惡意軟體。

(3) 確實執行網頁惡意軟體掃描。

(4) 使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。

(5) 使用者不得私自使用已知或有嫌疑惡意之網站。

(6) 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

辦公室區域之實體與環境安全措施

(1) 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

(2) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

- (3) 機密性及敏感性資訊，不使用或下班時應該上鎖。
- (4) 機密資訊或處理機密資訊之智慧化系統應避免存放或設置於公眾可接觸之場域。
- (5) 顯示存放機密資訊或具處理機密資訊之智慧化系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
- (6) 資訊或智慧化系統相關設備，未經管理人授權，不得被帶離辦公室。

資料備份

1. 重要社區資料應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。
2. 社區應每季確認資料備份之有效性。且測試確認資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原智慧化系統。
3. 敏感或機密性資訊之備份應加密保護。

電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。
3. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
4. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。
5. 下班時應關閉電腦及螢幕電源。
6. 如發現資安問題，應主動循機關之通報程序通報。
7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

行動設備之安全管理

1. 涉及社區重要個資及相關用戶隱私之資料不得由未經許可之行動設備存取、處理或傳送。

社區異常事件紀錄表

紀錄編號：_____

填表日期： 年 月 日

異常原因	異常項目資產名稱：_____	
	異常發現時間： 年 月 日 時 分	
處理說明	 	
	異常排除時間： 年 月 日 時 分	
承辦人員		單位主管