

電子看板資通安全管理須知

- 一、為推動資通安全管理法第六條第一項所定資通安全整體防護事宜，協助公務機關完備電子看板之管理，降低設備遭入侵、內容遭竄改、錯假訊息擴散、維運管理失當及供應鏈所生之資通安全風險，特訂定本須知。
- 二、本須知用詞，定義如下：
 - (一)電子看板：指用於播放公告、宣導或資訊之顯示設備，其包含看板播放端、管理端及內容更新機制。
 - (二)看板播放端：指實際播放電子看板內容之終端設備。
 - (三)管理端：指中控平台、內容管理系統、管理伺服器或其他用以派送、排程、管理或維運電子看板內容之系統。
 - (四)離線單機型電子看板：指未接取任何對外網路，僅透過實體介面由人工手動更新內容之電子看板。
 - (五)網路連線型電子看板：指可連網更新內容，並得透過程式或管理系統進行內容派送、排程及維運之電子看板。
- 三、公務機關應明確釐訂管理權責分工，並辦理下列事項：
 - (一)權責分工原則由業務單位統籌辦理，並請資訊單位協助資通安全防護相關事項；如為委外維運，則由業務單位請委外廠商配合完備資通安全相關措施，並由資訊單位複核。
 - (二)建立並定期更新電子看板清冊及業務聯繫窗口資訊，並得結合資產盤點作業辦理。
 - (三)定期檢查設備外觀，確認無遭破壞或加裝側錄裝置等異常狀態。
 - (四)通用作業系統應部署端點防護軟體，並關閉非必要服務、連接埠及封鎖閒置之實體介面。
 - (五)定期執行作業系統及應用軟體之安全性更新。
- 四、公務機關對電子看板之帳號管理及內容發布，應符合下列事項：
 - (一)依最小權限原則配置帳號，禁止共用帳號及密碼或使用預設密碼；因應運作需要得設置受控之專用服務帳號支援自動登入。
 - (二)建立內容發布流程，包括上架審核、版本更新、緊急下架或回復等程序，並留存內容發布及設定變更紀錄。

五、公務機關委外辦理電子看板建置或維運管理，應落實委外及供應鏈安全管理，並符合下列事項：

(一)公務機關應依資通安全管理法第十條規定，落實受託者之選任及監督；其委外契約應載明服務範圍、資安責任分工、故障與異常通報、復原時限、弱點修補及日誌留存等要求。

(二)電子看板之產品、軟體或雲端服務如有危害國家資通安全之疑慮時，應依資通安全管理法第十一條及危害國家資通安全產品審查辦法等相關規定辦理。

六、離線單機型電子看板除依第三點至前點規定辦理外，並應符合下列事項：

(一)外接儲存媒體限用公務儲存媒體，且接取前應完成惡意程式掃描。

(二)留存人工更新紀錄，記載更新時間、內容來源及作業人員。

七、網路連線型電子看板除依第三點至第五點規定辦理外，並應符合下列事項：

(一)看板播放端及管理端應採獨立網段區隔；看板播放端不得與一般辦公內網混用。

(二)連線跨越公開網路者，應採 Site-to-Site VPN 或加密連線機制；管理介面禁止直接暴露於網際網路，並應採白名單存取控制及多因子認證機制。

(三)設備應建立唯一身分識別及專屬連線授權機制（如憑證或權杖），並由管理端定期輪替且不得共用。

(四)完整留存設備登入、內容更新、網路連線等日誌，保存期限依資通安全責任等級分級辦法附表十資通系統防護基準有關事件日誌與可歸責性構面之控制措施辦理，並得介接至集中日誌平台。

(五)遠端維護應採申請核准制，限縮連線對象、時段及權限，過程應集中控管並留存紀錄，作業完成後立即關閉。

八、電子看板發生異常畫面、疑似入侵或其他資通安全事件時，應辦理下列事項：

- (一)拍照或錄影存證，並記錄時間、畫面及處置動作。
- (二)優先防止錯假訊息持續散布；必要時得關閉看板播放端電源，或採斷網措施抑制擴散並保留跡證。
- (三)依資通安全管理法及相關規定，通報資安窗口並於時限內辦理資通安全事件通報。
- (四)復原前應完成惡意程式清除、弱點修補、帳密重設及權限盤點等措施，確認後始得重新使用。
- (五)其餘未盡事項，依各機關資通安全事件通報及應變處理作業程序規定辦理。

九、公務機關得請公有場域委外營運之民間業者，就其場域之電子看板，參考本須知進行自主管理；公務機關應與民間業者建立通報機制，請民間業者於接獲異常情事時，能即時應處，並於處置後向公務機關回報結果。

十、本須知實施前，未能符合規範之電子看板，應於既有契約履約期限屆滿或設備汰換時配合調整；調整前公務機關應採取適當之補償性防禦措施（Compensating Controls）。

十一、資通安全管理法所定之特定非公務機關，得參考本須知之規定辦理。

電子看板資通安全管理須知

規定	說明
一、為推動資通安全管理法第六條第一項所定資通安全整體防護事宜，協助公務機關完備電子看板之管理，降低設備遭入侵、內容遭竄改、錯假訊息擴散、維運管理失當及供應鏈所生之資通安全風險，特訂定本須知。	一、本須知之訂定目的。 二、電子看板涉及內容派送、離線單機型、網路連線型與委外管理等情形，為降低設備遭入侵、內容遭竄改、錯假訊息擴散、維運管理失當及供應鏈所生之資通安全風險，爰訂定本須知，作為公務機關辦理電子看板資通安全管理之依據。
二、本須知用詞，定義如下： （一）電子看板：指用於播放公告、宣導或資訊之顯示設備，其包含看板播放端、管理端及內容更新機制。 （二）看板播放端：指實際播放電子看板內容之終端設備。 （三）管理端：指中控平台、內容管理系統、管理伺服器或其他用以派送、排程、管理或維運電子看板內容之系統。 （四）離線單機型電子看板：指未接取任何對外網路，僅透過實體介面由人工手動更新內容之電子看板。 （五）網路連線型電子看板：指可連網更新內容，並得透過程式或管理系統進行內容派送、排程及維運之電子看板。	一、就電子看板、看板播放端、管理端、離線單機型電子看板及網路連線型電子看板等重要用詞予以定義。 二、電子看板以是否接取對外網路區分類型，作為後續適用不同管理措施之基礎。
三、公務機關應明確釐訂管理權責分工，並辦理下列事項： （一）權責分工原則由業務單位統籌辦理，並請資訊單位協助資通安全防護相關事項；如為委外維運，則由業務單位請委外廠商配合完備資通安全相關措施，並由資訊單位複核。 （二）建立並定期更新電子看板清冊及業務聯繫窗口資訊，並得結合資產盤點作業辦理。	一、公務機關權責分工原則、資產盤點、外觀檢測、作業系統防護及定期更新等作業。 二、為強化內部分工，避免因分工問題衍生風險，提供公務機關內部及委外之分工原則予公務機關參考。 三、為降低行政作業成本，建議公務機關得結合現行資產盤點作業，盤點電子看板設備，檢視設備外觀及建立業務聯繫窗口資訊。 四、就作業系統與應用軟體之端點防護及定期更新等工作納入規範，使公

(三)定期檢查設備外觀，確認無遭破壞或加裝側錄裝置等異常狀態。 (四)通用作業系統應部署端點防護軟體，並關閉非必要服務、連接埠及封鎖閒置之實體介面。 (五)定期執行作業系統及應用軟體之安全性更新。	務機關留意作業系統本身之安全性。
四、公務機關對電子看板之帳號管理及內容發布，應符合下列事項： (一)依最小權限原則配置帳號，禁止共用帳號及密碼或使用預設密碼；因應運作需要得設置受控之專用服務帳號支援自動登入。 (二)建立內容發布流程，包括上架審核、版本更新、緊急下架或回復等程序，並留存內容發布及設定變更紀錄。	一、說明帳號管理及內容發布之要求。 二、就帳號管理之重要事項（包含最小權限、禁止共用帳密、禁止使用預設密碼等）加以規範；另考量看板播放端具二十四小時不間斷運作需求，爰於維持資通安全管理原則下，允許設置受控管之專用服務帳號，並透過權限限制、登入限制及監控機制降低風險。 三、就內容發布流程建立規範，以協助公務機關建立內容發布機制，強化電子看板之資通安全管理作為。
五、公務機關委外辦理電子看板建置或維運管理，應落實委外及供應鏈安全管理，並符合下列事項： (一)公務機關應依資通安全管理法第十條規定，落實受託者之選任及監督；其委外契約應載明服務範圍、資安責任分工、故障與異常通報、復原時限、弱點修補及日誌留存等要求。 (二)電子看板之產品、軟體或雲端服務如有危害國家資通安全之疑慮時，應依資通安全管理法第十一條及危害國家資通安全產品審查辦法等相關規定辦理。	一、委外及供應鏈資通安全管理要求。 二、電子看板建置及維運常涉及外部廠商，爰依資通安全管理法第十條規定，定明公務機關應落實受託者之選任及監督，並於委外契約載明資安責任分工與通報復原等事項，以強化委外管理。 三、電子看板如為大陸廠牌產品或有危害國家資通安全之疑慮時，明定公務機關應依循資通安全管理法第十一條及危害國家資通安全產品審查辦法採取相應措施，以降低供應鏈風險。
六、離線單機型電子看板除依第三點至前點規定辦理外，並應符合下列事項： (一)外接儲存媒體限用公務儲存媒體，且接取前應完成惡意程式掃描。	一、離線單機型電子看板之特定管理要求。 二、離線單機型電子看板雖未接取網路，仍可能因外接儲存媒體或人工更新流程而產生風險，爰就儲存媒體使用及人工更新紀錄加以規範。

(二)留存人工更新紀錄，記載更新時間、內容來源及作業人員。	
七、網路連線型電子看板除依第三點至第五點規定辦理外，並應符合下列事項： (一)看板播放端及管理端應採獨立網段區隔；看板播放端不得與一般辦公內網混用。 (二)連線跨越公開網路者，應採 Site-to-Site VPN 或加密連線機制；管理介面禁止直接暴露於網際網路，並應採白名單存取控制及多因子認證機制。 (三)設備應建立唯一身分識別及專屬連線授權機制（如憑證或權杖），並由管理端定期輪替且不得共用。 (四)完整留存設備登入、內容更新、網路連線等日誌，保存期限依資通安全責任等級分級辦法附表十資通系統防護基準有關事件日誌與可歸責性構面之控制措施辦理，並得介接至集中日誌平台。 (五)遠端維護應採申請核准制，限縮連線對象、時段及權限，過程應集中控管並留存紀錄，作業完成後立即關閉。	一、網路連線型電子看板之特定管理要求。 二、此類型設備涉及網段區隔、跨網連線、設備身分識別、授權管理、日誌留存及遠端維護等事項，爰就其安全控管需求加以規範，以降低橫向移動、未授權連線及資料外洩風險。
八、電子看板發生異常畫面、疑似入侵或其他資通安全事件時，應辦理下列事項： (一)拍照或錄影存證，並記錄時間、畫面及處置動作。 (二)優先防止錯假訊息持續散布；必要時得關閉看板播放端電源，或採斷網措施抑制擴散並保留跡證。 (三)依資通安全管理法及相關規定，通報資安窗口並於時限內辦理資通安全事件通報。 (四)復原前應完成惡意程式清除、弱點修補、帳密重設及權限盤	一、電子看板資通安全事件應變及通報要求。 二、電子看板異常畫面可能涉及內容遭竄改、系統遭入侵或錯假訊息散布，爰就存證、抑制擴散、事件通報及復原前處置事項加以規範。

點等措施，確認後始得重新使用。 (五)其餘未盡事項，依各機關資通安全事件通報及應變處理作業程序規定辦理。	
九、公務機關得請公有場域委外營運之民間業者，就其場域之電子看板，參考本須知進行自主管理；公務機關應與民間業者建立通報機制，請民間業者於接獲異常情事時，能即時應處，並於處置後向公務機關回報結果。	一、公有場域委外營運民間業者之管理要求。 二、公有場域委外營運之民間業者（如火車站內超商或社會住宅內物業管理公司等），雖非本規範之納管對象，考量公務機關負有該等場域所有權及管理權責，爰規定得請前開民間業者參考本須知自主管理，以利維護該等場域之電子看板資通安全。 三、明定公務機關與民間業者須建立通報機制，以利掌握民間業者之應處情形。
十、本須知實施前，未能符合規範之電子看板，應於既有契約履約期限屆滿或設備汰換時配合調整；調整前公務機關應採取適當之補償性防禦措施（Compensating Controls）。	一、現有設備未能符合本須知要求之處理方式。 二、參考實務單位建議，針對現行未能符合規範之電子看板設備訂定過渡措施，同時要求公務機關須針對是類設備採取相應之防護措施。
十一、資通安全管理法所定之特定非公務機關，得參考本須知之規定辦理。	關鍵基礎設施提供者、公營事業、特定財團法人或受政府控制之事業、團體或機構等資通安全管理法管轄之特定非公務機關，考量其業務影響範圍及重要性，爰規定得參考本須知辦理資通安全管理。