

營業場域電子看板資通安全管理指引

111.8.18 經濟部

壹、為協助百貨、超商、賣場及其他類似之營業場所設置各類電子看板之資通安全管理，特訂定本指引。

一、名詞定義

- (一)電子看板指各類設置於營業場所公共區域，供播放影像或音訊之電子顯示器。
- (二)電子看板資通系統或服務指可蒐集、控制、傳輸、儲存、流通、刪除或其他處理電子看板資訊之作業系統或服務。

二、電子看板資通系統管理

(一)系統及設備管理

- 1.將資安要求納入資通系統開發及維護、或服務提供之需求規格，包含機敏資料存取控制、用戶登入身分驗證及用戶輸入輸出之檢查過濾等。
- 2.系統所在環境，至少具備下列資安防護控制措施：
 - (1)防毒軟體。
 - (2)網路防火牆。
- 3.留意安全漏洞通告並定期評估設備、系統元件、軟體安全性漏洞修補。
- 4.為降低資安風險，不得使用中國大陸製軟體，並應避免使用中國大陸品牌產品。

(二)人員及場所管理

- 1.營業場所從業人員應定期監看電子看板，如有異常情形發生應即依本指引「貳、資安事件通報及應變處置」方式辦理。
- 2.針對電腦機房及重要區域應落實安全控制、人員進出管控並建立適當管理措施。

三、電子看板資通系統或服務委外辦理管理

- (一)訂定資通作業委外安全管理程序，包含委外選商、監督管理(如：對供應商與合作夥伴進行稽核)及委外關係終止等相關規定。
- (二)訂定委外廠商之資通安全責任及保密規定，於採購文件中載明服務水準協

議(SLA)、資安要求及對委外廠商資安稽核權。

(三)應要求委外廠商不得使用中國大陸製軟體，並應避免使用中國大陸品牌產品。

貳、資安事件通報及應變處置

- 一、訂定資安事件應變處置及通報作業程序，包含事件影響及損害評估，內外部通報流程、通報窗口及聯繫方式等。
- 二、電子看板系統發生異常或遭受攻擊時，應立即停止播放、封鎖系統並報警。
- 三、進行系統異常或攻擊來源追蹤及修復檢測作業，確認受影響資通設備並蒐集設備相關資訊(含實體主機 IP 位址、網際網路位址、設備廠牌與機型及作業系統名稱版本等)，於修復完成並確認安全無虞前應停用電子看板。

參、資安強化作為

- 一、確保電子看板系統網路環境之安全性並強化系統委外廠商資安管理。
- 二、定期辦理內部及委外廠商之資安稽核，並就發現事項擬訂改善措施，定期追蹤改善情形。
- 三、強化資通系統使用人員資安知識，相關人員應定期接受資通安全宣導課程，另負責資通安全之主管及人員，定期接受資通安全專業課程訓練。