上市上櫃公司資通安全管控指引
修正條文對照表

日期：113 年 9 月 10 日

修正條文	現行條文	說明
第一條 為協助上市、上櫃公司(以下簡稱公司)強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業，特訂定本資通安全管控指引。	第一條 為協助上市、上櫃公司(以下簡稱公司)強化資通安全防護及管理機制，並符合「公開發行公司建立內部控制制度處理準則」第九條使用電腦化資訊系統處理者相關控制作業，特擬定本資通安全管控指引。	因「上市上櫃公司資通安全管控指引」已於 110 年 12 月 23 日正式公告後實施，爰酌修本條文字敘述。
第二十三條 建立資通系統及相關設備適當之監控措施，包含身分驗證存取紀錄（如：失敗登入、非作業時間登入、多位使用者使用同一來源 IP 登入成功等）、存取資源紀錄、重要行為、重要資料異動、偵測攻擊與未授權之連線、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。	第二十三條 建立資通系統及相關設備適當之監控措施，如：身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等，並針對日誌建立適當之保護機制。	1. 本條增列監控措施項目。 2. 修正身分驗證存取紀錄之態樣例示，以確保監控機制之有效性，爰修正本條。 3. 依據「資通安全實地稽核項目檢核表(適用特定非公務機關)」稽核項目 9.11 項，針對攻擊與未授權連線應有適當之監控機制，爰增列偵測攻擊與未授權之連線。
第二十四條 建立遠端存取資通系統之管控機制，如：建立安全的遠距連線機制（如：VPN、VDI）、採多重身分驗證、採加密連線、採最小授權原則、留存完整使用者操作稽核軌跡、監控與警示異常操作行為、執行安全性漏洞更新等安控措施，並教育居家辦公者應對網路風險保持警覺等。		1. 本條新增，增訂遠端存取資通系統之管控機制。 2. 本條新增係參考臺灣電腦網路危機處理暨協調中心(TWCERT/CC)之「遠距辦公資安專區」及「證券商因應嚴重特殊傳染病申請居家辦公指引」，針對遠端存取資通系統應有適當之管控機制，爰增訂本條。
第二十五條 針對提供公眾活動或使用之場		1. 本條新增，增訂強化告示牌、電子看板等設備之

修正條文	現行條文	說明
地，宜強化告示牌、電子看板等傳播影像或聲音功能設備之管理。		管理。 2.依據「營業場域電子看板資通安全管理指引」，建議強化公眾場所之告示牌及電子看板等設備之管理，爰增訂本條。
第二十六條 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。	第二十四條 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護(如溫溼度控制)等項目建立適當之管理措施。	條次變更，內容未修正。
第二十七條 留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。	第二十五條 留意安全漏洞通告，即時修補高風險漏洞，定期評估辦理設備、系統元件、資料庫系統及軟體安全性漏洞修補。	條次變更，內容未修正。
第二十八條 訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。	第二十六條 訂定資通設備回收再使用及汰除之安全控制作業程序，以確保機敏性資料確實刪除。	條次變更，內容未修正。
第二十九條 訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。	第二十七條 訂定人員裝置使用管理規範，如：軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等管控使用規則。	條次變更，內容未修正。
第三十條 每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。	第二十八條 每年定期辦理電子郵件社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。	條次變更，內容未修正。
第三十一條 訂定資訊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)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措	第二十九條 訂定資訊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)及委外關係終止之相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措	條次變更，內容未修正。

修正條文	現行條文	說明
施。	施。	
第三十二條 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。	第三十條 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。	條次變更，內容未修正。
第三十三條 公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。	第三十一條 公司於委外關係終止或解除時，確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。	條次變更，內容未修正。
第三十四條 訂定資安事件應變處置及通報作業程序，包含判定事件影響及損害評估、內外部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式，得參考臺灣電腦網路危機處理暨協調中心(TWCERT/CC)「企業資安事件應變處理指南」。	第三十二條 訂定資安事件應變處置及通報作業程序，包含判定事件影響及損害評估、內外部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式。	1.條次變更。 原第三十二條修正為第三十四條。 2.增訂本條後段文字，因近年來上市上櫃公司遭駭客攻擊事件頻傳，故加強宣導各公司，得參考臺灣電腦網路危機處理暨協調中心(TWCERT/CC)「企業資安事件應變處理指南」，針對資安事件之事前準備、事中應處、事後改善進行相對應之處理方式。
第三十五條 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，如：所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。	第三十三條 加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，如：所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。	條次變更，內容未修正。
第三十六條 發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券	第三十四條 發生符合「臺灣證券交易所股份有限公司對有價證券上市公司重大訊息之查證暨公開處理程序」或「財團法人中華民國證券	條次變更，內容未修正。

修正條文	現行條文	說明
櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。	櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。	
第三十七條 資通安全推動組織定期向董事會或管理階層報告資通安全執行情形，確保運作之適切性及有效性。	第三十五條 資通安全推動組織定期向董事會或管理階層報告資通安全執行情形，確保運作之適切性及有效性。	條次變更，內容未修正。
第三十八條 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，且定期追蹤改善情形。	第三十六條 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，且定期追蹤改善情形。	條次變更，內容未修正。
第三十九條 應於年報敘明資安政策、具體管理方案、投入資安管理之資源、重大資安事件之損失與可能影響及因應措施等資訊。		1. 本條新增，增訂年報應敘明事項。 2. 為強化上市上櫃公司資訊安全管理機制，依據「公開發行公司年報應行記載事項準則」第 18 條，爰增訂本條，應於年報敘明資安政策、具體管理方案、投入資安管理之資源、重大資安事件之損失與可能影響及因應措施等資訊。
第四十條 評估導入 ISO27001、CNS27001 等資訊安全管理系統標準，或其他具有同等或以上效果之系統或標準，取得第三方驗證，並持續維持其驗證有效性，亦或評估通過美國註冊會計師協會（AICPA）發展之 SOC 2 服務組織之 Type 2 合規標準認證，以維持公司穩健之資訊安全。		1. 本條新增，增訂建議通過 SOC 2 服務組織之 Type 2 合規標準認證。 2. 依據「113 年度公司治理評鑑指標」編號 2.24 項，建議上市上櫃公司透過導入 ISO27001、CNS27001 等資訊安全管理系統標準或其他具有同等或以上效果之系統或標準，或通過 SOC 2 服務組織之 Type 2 合規標

修正條文	現行條文	說明
		準認證，以降低企業資安風險並確保公司之資訊安全，爰增訂本條。
第四十一條 除法令、臺灣證券交易所股份有限公司及財團法人中華民國證券櫃檯買賣中心相關章則另有規定外，本指引條文，上市、上櫃公司可衡諸產業特性、規模大小及資安風險適度採行之。	第三十七條 除法令、臺灣證券交易所股份有限公司及財團法人中華民國證券櫃檯買賣中心相關章則另有規定外，本指引條文，上市、上櫃公司可衡諸產業特性、規模大小及資安風險適度採行之。	條次變更，內容未修正。