上市上櫃公司資通安全管控指引
修正條文對照表

日期：115 年 11 月 9 日

修正條文	現行條文	說明
第九條 鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)，設置適當之備份機制及備援計畫，包含供災難復原之異地備份，以及防範勒索軟體加密之離線備份或不可變更備份機制。	第九條 鑑別可能造成營運中斷事件之發生機率及影響程度，並明確訂定核心業務之復原時間目標(RTO)及資料復原時間點目標(RPO)，設置適當之備份機制及備援計畫。	1.增列異地備份，以及防範勒索軟體加密之離線備份或不可變更備份機制。 2.參考「資通安全責任等級分級辦法」應辦事項有關營運持續、備份及復原之要求，強化核心業務之備援與資料復原韌性，爰修正本條。
第十條 制定核心業務營運持續計畫，定期辦理核心業務營運持續計畫演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善。	第十條 制定核心業務持續運作計畫，定期辦理核心業務持續運作演練，演練內容包含核心業務備援措施、人員職責、應變作業程序、資源調配及演練結果檢討改善。	依據「資通安全責任等級分級辦法」資通系統防護基準之規定，調整「持續運作」計畫修正為「營運持續」計畫。
第十五條 妥善儲存及管理資通系統開發及維護相關文件及系統源碼。	第十五條 妥善儲存及管理資通系統開發及維護相關文件。	參考「資通安全責任等級分級辦法」資通系統防護基準之系統源碼備份要求，增列程式碼之儲存及管理規範。
第十六條 鑑別資通系統使用之第三方軟體、服務、函式庫或其他元件，並宜於契約規範供應商主動通報安全性漏洞，於時限內提供修補程式或安全更新。	無(本條新增)	1.本條新增，增訂第三方元件識別、漏洞通報及修補更新相關規範。 2.參考「資通安全責任等級分級辦法」資通系統防護基準有關系統與服務獲得、供應鏈及弱點管理之要求，爰增訂本條。
第十七條 針對核心資通系統應辦理下列資安檢測作業，並完成弱點修	第十六條 對核心資通系統辦理下列資安檢測作業，並完成系統弱點修	1.條次變更，原第十六條修正為第十七條。 2.參考「資通安全責任

修正條文	現行條文	說明
補；另針對對外服務資通系統，建議依風險評估結果，自下列作業中擇定適當項目辦理： 一、定期辦理弱點掃描。 二、定期辦理滲透測試。 三、定期辦理資料庫安全檢視作業。 四、系統上線前及定期執行源碼掃描安全檢測。 五、依公司風險程度，評估辦理紅隊演練。	補。 一、定期辦理弱點掃描。 二、定期辦理滲透測試。 三、系統上線前執行源碼掃描安全檢測。	等級分級辦法」應辦事項及資通系統防護基準之強化資通系統安全檢測機制，除核心資通系統外，增列對外服務資通系統依風險評估結果辦理適當之資安檢測，並增列定期資料庫安全檢視、定期源碼掃描及依風險程度評估辦理紅隊演練等相關要求。
第十八條 依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施；針對核心系統或機敏性資料區域，宜進一步運用微分段(Micro-segmentation)技術細化隔離邊界。	第十七條 依網路服務需要區隔獨立的邏輯網域(如：DMZ、內部或外部網路等)，並將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施。	1.條次變更，原第十七條修正為第十八條。 2.參考「資通安全責任等級分級辦法」資通系統防護基準有關網路區隔及邊界防護之要求，增列核心系統或機敏性資料區域宜運用微分段技術細化隔離邊界，爰修正本條。
第十九條 具備下列資安防護控制措施： 一、防毒軟體。 二、網路防火牆。 三、如有郵件服務者，具備電子郵件過濾機制。 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者，具備應用程式防火牆。 六、進階持續性威脅攻擊防禦措施。 七、端點偵測與應變機制(EDR)。	第十八條 具備下列資安防護控制措施： 一、防毒軟體。 二、網路防火牆。 三、如有郵件伺服器者，具備電子郵件過濾機制。 四、入侵偵測及防禦機制。 五、如有對外服務之核心資通系統者，具備應用程式防火牆。 六、進階持續性威脅攻擊防禦措施。 七、資通安全威脅偵測管理機制(SOC)。	1.條次變更，原第十八條修正為第十九條。 2.增列端點偵測與應變機制(EDR)，並因應郵件服務型態之變化，酌修郵件伺服器相關文字。 3.參酌「資通安全責任等級分級辦法」應辦事項有關端點防護、威脅偵測及資安防護之要求，爰修正本條。

修正條文	現行條文	說明
八、資通安全威脅偵測管理機制(SOC)。		
第二十條 針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。	第十九條 針對機敏性資料之處理及儲存建立適當之防護措施，如：實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽、人員管理及處理規範等。	條次變更，內容未修正。
第二十一條 訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。	第二十條 訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。	條次變更，內容未修正。
第二十二條 建立使用者密碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制、首次登入變更密碼機制；並評估於核心資通系統採取多因子鑑別等零信任架構(Zero Trust Architecture)。	第二十一條 建立使用者通行碼管理之作業規定，如：預設密碼、密碼長度、密碼複雜度、密碼歷程記錄、密碼最短及最長之效期限制、登入失敗鎖定機制，並評估於核心資通系統採取多重認證技術。	1.條次變更，原第二十一條修正為第二十二條。 2.將「通行碼」修正為「密碼」，增列首次登入變更密碼機制，並將「多重認證技術」修正為「多因子鑑別等零信任架構」。 3.參考「資通安全責任等級分級辦法」資通系統防護基準有關識別與鑑別、密碼管理及多因子鑑別之要求，並參酌政府及金融業推動零信任架構之相關政策，爰修正本條。
第二十三條 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。	第二十二條 定期審查特權帳號、使用者帳號及權限，停用久未使用之帳號。	條次變更，內容未修正。
第二十四條 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	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	條次變更，內容未修正。

修正條文	現行條文	說明
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。	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。	
第二十五條 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)、採多因子鑑別、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。	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.條次變更，原第二十四條修正為第二十五條。 2.參考「資通安全責任等級分級辦法」資通系統防護基準將「多重身分驗證」更名為「多因子鑑別」。
第二十六條 針對提供公眾活動或使用之場地，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。	第二十五條 針對提供公眾活動或使用之場地，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。	條次變更，內容未修正。
第二十七條 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。	條次變更，內容未修正。
第二十八條 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。	條次變更，內容未修正。
第二十九條 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	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	條次變更，內容未修正。

修正條文	現行條文	說明
保機敏性資料確實刪除。	保機敏性資料確實刪除。	
第三十條 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。	條次變更，內容未修正。
第三十一條 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。	條次變更，內容未修正。
第三十二條 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施。	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施。	條次變更，內容未修正。
第三十三條 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。	條次變更，內容未修正。
第三十四條 終止或解除委外關係時，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。	1.條次變更，原第三十三條修正為第三十四條。 2.為使條文文字簡潔明確，爰酌修本條文字，內容未作實質修正。
第三十五條 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	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	1.條次變更，原第三十四條修正為第三十五條。 2.增列定期辦理資安事件應變處置演練，以驗證應變程序有效性。 3.參考「資通安全責任

修正條文	現行條文	說明
協調中心(TWCERT/CC)「企業資安事件應變處理指南」；並定期辦理應變處置演練以驗證其有效性。	協調中心(TWCERT/CC)「企業資安事件應變處理指南」。	等級分級辦法」應辦事項有關資通安全事件通報、應變及演練之要求，爰修正本條。
第三十六條 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)。	條次變更，內容未修正。
第三十七條 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。	條次變更，內容未修正。
第三十八條 使用人工智慧(AI)系統或服務，若涉及核心業務、機敏性資料，或具介接、操作、異動或觸發資通系統功能者，應依業務性質及風險程度採取下列風險管理措施： 一、衡諸採行數位發展部「人工智慧風險分類框架」或所屬產業中央目的事業主管機關發布之人工智慧(AI)指引。 二、宜訂定員工使用人工智慧(AI)系統或服務之安全規範，對未經授權之使用行為採取適當之管理措施。 三、導入、開發或重大變更人工智慧(AI)系統或服務，應依	無(本條新增)	本條新增，考量人工智慧(AI)技術快速發展及其衍生之資通安全、供應鏈、資料保護與治理風險，參考國內外相關規範及指引，增訂本條規定，以強化 AI 應用之風險管理及資通安全。 參考規範如下： 1.數位發展部「人工智慧風險分類框架」 2.金融監督管理委員會「金融業運用人工智慧（AI）指引」、「金融業運用代理 AI 安全諮詢文件」 3.經濟部產業發展署

修正條文	現行條文	說明
風險程度辦理適當之安全評估或測試，定期檢視模型運作狀況，並落實人工智慧(AI)模型與第三方元件之供應鏈風險管理。 四、運用具備規劃步驟、呼叫工具、跨系統存取資料以推進任務能力之代理 AI（Agentic AI），應限制其用途、資料、工具、目的地及執行權限；涉及對核心業務、機敏性資料或資通系統具有重大影響或不可逆之自動化操作，應建立人工核准、安全護欄或其他適當之控制機制。 五、應依風險程度建立適當之監控及紀錄機制，以追溯重要操作、行為偏離及異常事件。		「製造業 AI 導入指引」 4. ISO/IEC 42001:2023 5. NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0) and Generative AI Profile (NIST AI 600-1) 6. COSO, Achieving Effective Internal Control Over Generative AI
第三十九條 使用人工智慧(AI)系統或服務，若僅供查詢、摘要、翻譯、教育訓練、內部草稿或其他低風險輔助用途，且未涉前條所列應用者，得依既有之資通安全管理措施辦理。	無(本條新增)	本條新增，說明同前條。
第四十條 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。	條次變更，內容未修正。
第四十一條 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。	條次變更，內容未修正。
第四十二條 應於年報敘明資安政策、具體	第三十九條 應於年報敘明資安政策、具體	條次變更，內容未修正。

修正條文	現行條文	說明
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。	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。	
第四十三條 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。	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。	條次變更，內容未修正。
第四十四條 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。	條次變更，內容未修正。