

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>一、目標：</p> <ol style="list-style-type: none"> 1、針對軟硬體設備及與財務報告系統及其相關子系統制定資訊安全政策。 2、定期實施資訊安全檢查作業，落實資通安全政策，以確保資通安全無虞。 <p>二、權責單位：資訊部</p> <p>三、潛在風險：</p> <ol style="list-style-type: none"> 1、資訊安全控制是否依據整體財務報告系統及其相關子系統之資訊架構進行全盤考量。 2、員工資訊安全意識及技能是否有效落實資訊安全政策。 3、資通安全檢查機制及規範是否適當，確保資訊安全檢查作業之有效遵行。 4、未依資訊安全政策執行檢查，將無法確認資訊安全政策之有效落實 <p>四、控制重點：</p> <ol style="list-style-type: none"> 1、應安裝防火牆及防毒軟體並定期更新病毒碼。 2、應無法使用盜版軟體，無法任意從網際網路下載不明軟體進行安裝。 3、電腦軟體登入密碼應定期更換。 4、應確保資訊安全檢查或資訊安全宣導有效執行。 5、應成立資通安全推動組織、訂定資通安全政策及目標、訂定資通安全作業程序。 	<p>1、使用表單：</p> <p>(1)SSL-VPN 申請單</p>

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>6、 所有使用資訊系統之人員，應每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，應每年接受資訊安全專業課程訓練。</p> <p>7、 應鑑別並定期檢視公司之核心業務、鑑別應遵守之法令及契約要求。</p> <p>8、 應鑑別可能造成營運中斷事件之發生機率及影響程度。</p> <p>9、 應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。</p> <p>10、 應定期盤點資通系統，並定期辦理資安風險評估。</p> <p>11、 應將資安要求納入資通系統開發及維護需求規格。</p> <p>12、 應定期執行資通系統安全性要求測試。</p> <p>13、 應妥善儲存及管理資通系統開發及維護相關文件。</p> <p>14、 應對核心資通系統辦理資安檢測作業。</p> <p>15、 應依網路服務需要區隔獨立的邏輯網域，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。</p> <p>16、 資安防護控制措施應包含：防毒軟體、網路防火牆、具備電子郵件過濾機制、入侵偵測及防禦機制、進階持續性威脅攻擊防禦措施、資通安全威脅偵測管理機制(SOC)。</p> <p>17、 應針對機敏性資料之處理及儲存建立適當之防護措施。</p> <p>18、 應訂定到職、在職及離職管理程序，並簽署保密協議明確告知保密事項。</p> <p>19、 應建立使用者通行碼管理之作業規定。</p> <p>20、 應定期審查使用者帳號及權限。</p> <p>21、 應建立資通系統及相關設備適當之監控措施。</p> <p>22、 應建立遠端存取資通系統之管控機制。</p> <p>23、 應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。</p>	

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>24、應留意安全漏洞通告，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。</p> <p>25、應訂定資通設備回收再使用及汰除之安全控制作業程序。</p> <p>26、應訂定人員裝置使用管理規範。</p> <p>27、應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。</p> <p>28、資通系統或資通服務委外辦理，應訂定資訊作業委外安全管理程序、資通安全責任及保密規定，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。</p> <p>29、應訂定資安事件應變處置及通報作業程序，加入資安情資分享組織，若發生符合「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」規範之重大資安事件，應依相關規定辦理。</p> <p>30、資訊部應定期向董事會報告資通安全執行情形。</p> <p>31、定期辦理內部及委外廠商之資安稽核。</p> <p>32、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。</p>	

編號	作業項目	作業程序及控制重點	依據資料
CC-110	資通安全檢查作業	<p>五、作業程序：</p> <p>(一)、電腦系統安全作業：</p> <ol style="list-style-type: none"> 1. 公司資訊系統自動執行下列記錄 (log) 作業： <ol style="list-style-type: none"> (1) 公司外部登入之使用者 ID、登入時間。 (2) 網際網路瀏覽記錄。 (3) E-mail 收發記錄。 2. 防火牆事件記錄。 <p>(二)、SAP 及公司內部網域登入安全控制為 5 次，如累計 5 次登入錯誤時，資訊系統自動鎖定，須向資訊部申請解鎖。</p> <p>(三)、每月資訊部處查核資訊系統登錄、防火牆、主機事件檢視簿等紀錄 (log)，如有異常侵入狀況時，採取如封鎖 IP 等防範措施。</p> <p>(四)、每週資訊部確認主機作業系統之更新通知，確認後建立排程執行更新作業之派送及執行防毒系統病毒碼更新作業。</p> <p>(五)、資訊部每半年更新主機系統管理員帳號密碼；網域使用者密碼至少每 90 天須更換一次。</p> <p>(六)、網路使用採帳號管控，嚴禁洩露帳號密碼資訊予他人知悉。</p> <p>(七)、逾越預設閒置時間或可使用期限時，系統會對電腦進行鎖定。</p> <p>(八)、所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資</p>	<p>指引第二十一條</p> <p>指引第六條</p>

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>(九)、每年不定期進行一次資通安全自我檢查，並填具資通安全自我檢查表，由權責人員及主管進行覆核。</p> <p>(十)、遠端存取 VPN 管理機制：</p> <ol style="list-style-type: none"> 1. 如因疫情或業務需要遠距離辦公，依權限申請書申請權限，資訊管理單位並不定時清查刪除無使用 VPN 之權限。 2. 帳號及密碼限本人使用，如發現異常使用將鎖定帳號等防禦措施。 3. VPN 連線通道採 IPsec 加密，多因子身份驗證、授權存取限定、Idle 自動斷線等機制，確保連線資訊安全。 4. VPN 帳號連入軌跡應有相應 Log 可供查詢。 5. 遠端存取使用安全性，每年不定期透過資安教育訓練教育及宣導資安網路相關風險等注意事項。 <p>(十一)、資通安全事件通報與應變機制：</p> <ol style="list-style-type: none"> 1. 通報流程： <ol style="list-style-type: none"> (1) 疑似資訊安全事件發生時，發現人員應依事件歸屬通報資訊部，並通知直屬主管。 (2) 權責單位於收到通知後，研判是否為資訊安全事件。 (3) 發現人員應於確認資訊安全事件後，填寫資訊安全事件報告單，由權責人員及主管進行覆核及處理。 2. 資訊安全危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟： <ol style="list-style-type: none"> (1) 事前建置安全防護機制：建置資訊安全管理系統及整體防護架構。 	<p>指引第十六條</p> <p>指引第二十四條</p> <p>指引第二十七條</p>

編號	作業項目	作業程序及控制重點	依據資料
CC-110	資通安全檢查作業	<p>(2) 事中主動預警與緊急應變：</p> <p>A. 事件辨識：辨識事件之歸屬及採取之對策，如：內部資安事件、外力入侵事件、天然災害或重大突發事件等，並決定處理的方法與程序。</p> <p>B. 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。</p> <p>C. 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全工作組提出建議方案。</p> <p>D. 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。</p> <p>(3) 事後復原追蹤鑑識偵查：</p> <p>A. 後續事件追蹤以避免及降低類似資訊安全事件重複發生機率，並檢視現有環境安全漏洞，經由研析相關資料，以釐清事件發生之原因與責任。</p> <p>B. 受損單位依復原程序實施災後復原重建。</p> <p>C. 重大資訊安全事件應保留事件發生之線索，如有需要得向國家資通安全會報技術服務中心或警調單位申請數位鑑識（電腦、網路鑑識）。</p> <p>(4) 檢討及改善：資訊安全事件確認處理完成後，應檢討現行管控措施之完整性，並適當修訂相關作業規範或建置及調整控制措施，必要時應召開檢討會議。</p>	

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>(十二)、資通安全政策及推動組織</p> <ol style="list-style-type: none"> 成立資通安全推動組織以負責推動、協調監督及審查資通安全管理事項。 (請參照：RGP06-33 資通安全管理辦法-資訊安全組織) 訂定資通安全政策及目標並定期檢視政策及目標且有效傳達員工其重要性。 (請參照：RGP06-33 資通安全管理辦法-資安政策及目標) 訂定資通安全作業程序。 (請參照：RGP06-33 資通安全管理辦法-資訊安全相關具體執行措施) <p>(十三)、核心業務及其重要性</p> <ol style="list-style-type: none"> 鑑別並定期檢視公司之核心業務。 (請參照：RGP06-33 資通安全管理辦法-核心業務及重要性) 鑑別應遵守之法令及契約要求。 (請參照：RGP06-33 資通安全管理辦法-總則) 鑑別可能造成營運中斷事件之發生機率及影響程度。 (請參照：CC-109 系統復原作業、RGP06-33 資通安全管理辦法-核心業務及重要性) 制定核心業務持續運作計畫。 (請參照：CC-109 系統復原作業、RGP06-33 資通安全管理辦法-核心業務及重要性) <p>(十四)、資通系統盤點及風險評估</p> <ol style="list-style-type: none"> 定期盤點資通系統。 (請參照：RGP06-32 風險評鑑與管理程序) 	<p>指引第三條</p> <p>指引第四條</p> <p>指引第五條</p> <p>指引第七條</p> <p>指引第八條</p> <p>指引第九條</p> <p>指引第十條</p> <p>指引第十一條</p>

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<p>2. 定期辦理資安風險評估，就核心業務及核心資通系統鑑別其可能遭遇之資安風險，分析其喪失機密性、完整性及可用性之衝擊，並執行對應之資通安全管理面或技術面控制措施等。</p> <p>(十五)、資通系統發展及維護安全</p> <p>1. 將資安要求納入資通系統開發及維護需求規格，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。</p> <p>2. 定期執行資通系統安全性要求測試，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測試等。</p> <p>3. 妥善儲存及管理資通系統開發及維護相關文件。</p> <p>4. 對核心資通系統辦理資安檢測作業。 (請參照：RGP06-33 資通安全管理辦法-資通系統掃描)</p> <p>(十六)、資通安全防護及控制措施</p> <p>1. 依網路服務需要區隔獨立的邏輯網域，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。</p> <p>2. 具備下列資安防護控制措施：</p> <p>(1) 防毒軟體。</p> <p>(2) 網路防火牆。</p> <p>(3) 郵件伺服器具備電子郵件過濾機制。</p> <p>(4) 入侵偵測及防禦機制。</p> <p>(5) 對外服務之核心資通系統具備應用程式防火牆。</p> <p>(6) 進階持續性威脅攻擊防禦措施。</p> <p>(7) 資通安全威脅偵測管理機制(SOC)。</p> <p>3. 針對機敏性資料之處理及儲存建立適當之防護措施。</p>	<p>指引第十二條</p> <p>指引第十三條</p> <p>指引第十四條</p> <p>指引第十五條</p> <p>指引第十六條</p> <p>指引第十七條</p> <p>指引第十八條</p> <p>指引第十九條</p>

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	<ol style="list-style-type: none"> 4. 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。 5. 建立使用者通行碼管理之作業規定。 (請參照：CC-104 程式及資料的存取作業) 6. 定期審查使用者帳號及權限，停用久未使用之帳號。 (請參照：CC-104 程式及資料的存取作業) 7. 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、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。 8. 電腦機房及重要區域之安全控制。 (請參照：CC-107 檔案及設備安全作業) 9. 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。 10. 機房設備與儲存媒體在汰除或重複使用前，使用單位應進行拍照及簽呈或報廢單簽核作業，並經資訊部最高主管核可，且由資訊部於報廢單簽名確實已消磁、低階格式化或進行實體破壞，帳務單位方可除帳。 11. 訂定人員裝置使用管理規範。 (請參照：CC-104 程式及資料的存取作業) 12. 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。 	<p>指引第二十條</p> <p>指引第二十一條</p> <p>指引第二十二條</p> <p>指引第二十三條</p> <p>指引第二十六條</p> <p>指引第二十七條</p> <p>指引第二十八條</p> <p>指引第二十九條</p> <p>指引第三十條</p>

編 號	作 業 項 目	作 業 程 序 及 控 制 重 點	依 據 資 料
CC-110	資通安全檢查作業	(十七)、 資通系統或資通服務委外辦理之管理措施 1. 訂定資通系統或資通服務委外辦理之管理措施。 (請參照：RGP06-33 資通安全管理辦法-資通系統或服務委外辦理之管理)	指引第三十一~三十三條
		(十八)、 資通安全事件通報應變及情資評估因應 1. 訂定資安事件應變處置及通報作業程序。 (請參照：RGP06-33 資通安全管理辦法-資安事件通報程序)	指引第三十四條
		2. 加入資安情資分享組織。 (請參照：RGP06-33 資通安全管理辦法-參加情資分享組織)	指引第三十五條
		3. 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」規範之重大資安事件，應依相關規定辦理。	指引第三十六條
		(十九)、 資通安全之持續精進及績效管理機制 1. 資通安全推動組織定期向董事會報告資通安全執行情形，確保運作之適切性及有效性。	指引第三十七條
		2. 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。	指引第三十八條
		3. 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。	指引第三十九條