如興股份有限公司

玖、電子計算機處理循環CEL100

董事會通過修訂日期：2018.03.21

目錄

文件修訂一覽表

次數	董事會日期	修訂章節	修訂重點內容
1	2016/05/12	CEL107 CEL109	取消原有磁帶備份管理模式2.實際增加異地備份機制3.強化資訊安全上的管制(防火牆管控、機房門禁管控) 本次為全部重新修訂，其主要修訂重要說明如下：1.強化跨單位組織系統復原整合規畫2.廣度提升：含括機房主機、通信網路、資料庫、程式系統等3.明訂列出測試項目、期間4.含括後續更新之控制要點
2	2018/03/21	電子計算機處理循環 CEL110	1.修改網路系統安全評估方案 2.增加防火牆之安全管理機制(防火牆進出紀錄及其備份應至少保存兩年) 3.增加資訊安全政策(已另行發佈公告)
3			
4			

編 號	作業項目	作 業 程 序 及 控 制 重 點	依據資料

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL101	電子計算機處理部門之功能及職責 一、部門之功能	一、目標 推展各項應用系統，原物料控制系統和財務系統，發揮企業電腦化之最大效能，同時提供各部門最及時之資訊，服務公司所有電腦使用者。 二、工作範圍 (一)公司廠房電腦設置，安全管制，及資訊網路上之架設與維護。 (二)公司及工廠網路環境變更設定並保持數據線路之暢通。 (三)各部門所需之系統開發設計與維護。 (四)套裝軟體評核與選購、裝設、維護。 (五)硬體配備評核與採購。 (六)公司電腦硬體定期保養及送修維護管理。 (七)公司人員電腦化之教育訓練工作。 三、效益 (一)提供經營管理的資訊，提高時效性，協助決策，提昇管理。 (二)管理觀念的建立，提昇策略性之競爭力。 (三)客戶與廠商間服務之加強。 (四)促進各部門間之協調與溝通。 (五)提高企業形象及商譽。 (六)建立歷史資料，增加查詢分析功能。 (七)增加員工對企業的向心力。 (八)內部稽核控制之加強。 (九)提高決策品質，降低系統成本。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
	二、職能劃分	(十)早期發掘問題，擬訂解決方案。 (十一)減少重複繁雜工作，提高工作內容層次及系統效率。 一、資訊部門主管 (一)從事整體資訊控制，發展長短程計劃，及審核推行系統。 (二)根據公司的作業目標與方針策劃資訊部門的業務及控制預算。 (三)建議系統作業方案，電腦化投資方案。 (四)從事與其他單位之間的協調與配合工作。 (五)檢討與評核各項作業之進度與效果。 二、系統分析 (一)進行作業系統規劃與分析。 (二)撰寫系統規劃書。 (三)驗收作業系統。 (四)進行系統評估與改進。 (五)撰寫操作手冊。 三、程式設計 (一)程式設計工作。 (二)程式有關文件、流程圖之撰寫。 (三)準備測試資料或物件。 (四)協助系統分析師處理有關系統業務。 (五)程式測試、修改、維護。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		四、資料庫管理 (一)設計資料庫之內容與組織，並控制資料庫之查詢和使用。 (二)資料庫之維護、管理、備份及回存。 (三)網路工程變更及安全之設計。 (四)區域網路之技術支援與維護。 (五)通訊或系統程式撰寫，測試及維護。 五、文書管理 (一)操作手冊之製作印發與管理。 (二)資訊部門檔案管理。 ＜控制重點＞ 一、資訊部門與相關部門之職掌，是否明確劃分。 二、電子計算機處理部門職責之劃分，是否有效執行。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL102	系統開發及程式修改控制 一、系統開發 二、程式新增及修改	一、提出申請 (一)由使用單位依需求填寫「電腦作業新增/修改申請回覆單」，經部門主管核准後，轉資訊單位。 (二)資訊單位於了解使用單位之需求且評估效益可行後，進行系統開發。 二、系統開發作業 (一)設計階段 1.目標設定。 2.訂定需求。 3.使用單位作業規劃。 4.系統設計。 (二)執行階段 1.程式編寫與測試。 2.系統測試。 3.文件整理編纂／操作手冊。 4.系統維護。 一、各使用部門在提出各種程式新增或修改要求時，應填寫「電腦作業新增／修改申請回覆單」，說明需求及預期效益，經部門主管核准後，轉資訊單位。 二、經資訊人員評估需求可行後，依使用者需求設計或修改程式。	＜使用表單＞ 電腦作業新增/修改申請回覆單

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		三、當使用者提出緊急之程式修改要求 (註：此包括程式設計錯誤及特殊緊急需求時)，需經該部門主管及資訊部門相關人員之評估確認後，可不經相關作業流程，而予以逕行處理，以爭取時效，事後補填申請單簽核。 ＜控制重點＞ 一、資訊部門對系統之開發控制是否有做整體性規劃。 二、程式之新增及變更修改是否確實經核准辦理。 三、是否避免不必要之程序修改作業，以降低系統成本。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL103	編製電腦文書之控制 一、文書說明 二、文件管理	一、目的 (一)訓練新人員。 (二)維持及修訂現有系統及程式。 二、範圍 (一)系統及程式之敘述和流程圖。 (二)電腦操作員之操作指令。 (三)操作人員及使用者所遵循的控制程序。 (四)必要的輸入、輸出之敘述及管制。 資訊部門有新文件或檔案時，由專人存檔保管。 ＜控制重點＞ 一、操作或管理手冊等文書說明是否確實建立。 二、納入正式作業之文件或檔案，是否切實保管記錄。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依　據　資　料
CEL104	程式及資料之存取控制 一、操作控制 二、密碼控制 三、權限控制 四、其他控制	一、非資料處理人員，機房未經核准不得擅入。 二、使用者用完電腦時必須離線，個人電腦不使用時需關機。 三、禁止擅自利用資訊中心系統設備，處理與本身業務無關的作業。 一、每一位使用者都有獨自的使用帳號和使用密碼，需求人員必須填寫電腦系統及程式使用申請表，並經部門主管核准，由資訊部門建立。 二、授權使用密碼者應建檔列管，密碼安全系統應定期更換，個人之密碼不得借他人使用。 三、職員離職或更換工作，其所用帳號應立即註銷或更新。 四、檔案、資料庫應設密碼及限制，原始程式及可執行程式，除密碼管理外，應注意資源之管理。 一、使用者依權限擁有適當作業功能。 二、資料使用權限應有分層授權系統，稽核及管理人員無權限更新資料庫。 一、資訊人員離職時先填寫申請書，經單位主管核准，辦理離職移交程序後，方可離職，移交程序表需各交接人簽名，作業才算正式完成，資訊部門人員離職時需移交程序如下： (一)列出所有曾經開發系統之清單。 (二)備份所有開發之系統程式及資料磁片。 (三)移交所有系統程式相關發展文件及操作手冊。 (四)說明系統存放軟體之所在目錄。 ＜控制重點＞ 一、程式檔案的存取使用是否加以管制。 二、程式檔案的存取使用是否均留下可追蹤的記錄。 三、權責主管是否定期覆核相關記錄。	＜依據資料＞ 1.電腦系統及程式使用申請表

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL105	資料輸出入控制 一、輸入作業之控制	一、使用單位應依照系統所需之輸入資料，設計合適之輸入異動單位。 二、各項輸入異動單證必須要有配合系統規格的單證號碼。 三、各項輸入單證，必須完成相關單位的簽核作業後，始得由使用單位指派專人輸入並由輸入人簽章。 四、系統須具備有輸入主鍵值之控制功能，藉由主鍵資料完成相對資料的自動輸入。 五、系統之各項輸入模組，必須設計符合使用單位所製定之限制條件。 六、系統運作參數的設定必須經過資訊部門的審核。 七、使用單位之主管應就其具有影響性之系統操作功能提出使用者之權限規範並確保具有關鍵性之操作能由訓練合格的成員完成之，並負責系統運作之結果。 ＜控制重點＞ 一、資料的輸入處理是否留下可供確認的記錄。 二、應用程式內對資料的正確性是否有核對功能，能以報表方式列出。	
	二、輸出作業之控制	一、所有之輸出報表皆必須列檔，記錄報表名稱、報表用途、報表編號。 二、報表之輸出符合報表之標準表頭格式。 三、屬於決策性之報表，其列印分數應限定乙份，並由用單位專人負責列印，以防止報表之重覆而引起混淆。 ＜控制重點＞ 一、機密性或敏感性資料的輸出是否有適當的管制。 二、輸出產生時，是否留下記錄以供追蹤查核。 三、輸出資料使用後，若無保存需要，是否經過適當的毀棄處理。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL106	資料處理之控制 一、資料之處理	一、資料之處理依據系統程序，由電腦程式控制，應符合內部控制規章處理。 二、資料之修改應填「電腦資料修改申請單／資料修改回應單」，經主管核可後方可進行修改。 三、資訊部門複查歸檔留存。 四、磁帶內之資料至少保留一週。	
	二、資料輸入方式之檢核	一、批次輸入時利用檔案轉換，涉及到整批異動資料庫，由資訊部門負責且事先須作資料備份及輸入資料之檢核，並列印清單核對。 二、個人輸入係利用工作站輸入，須由程式作資料檢核，並須顯示錯誤訊息及處理方法。	
	三、線上查詢	查詢程式應與異動程式分開處理以避免資料遭異動，且線上查詢應考慮安全控制，非相關部門人員不得任意查詢其他部門資料。	
	四、資料異動	如遇有因系統問題或操作不當，導致資料錯誤，須直接異動資料庫時，須以簽呈註明異動原因經部門主管及資訊部門主管核可後方可異動 ＜控制重點＞ 一、資料之存取讀用是否加以管制。 二、資料修改是否確實經核准後辦理。 三、資料是否依規定備份保存。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL107	檔案及設備之安全管理 一、檔案安全管理 二、設備安全管理	一、作業程序： (一).資料檔案之安全控制 1. 應用程式及資料檔，應妥善備份；資料應依其重要性，進行日、週、月等不同週期之備份作業，並設定適當之存放期限，針對應永久保存之資料則應另行使用適當媒體儲存。 2. 備份之資料媒體需適當記錄於備份記錄表中，並應於備份儲存媒體建立有意義檔案名稱以利辨識備份內容。 3. 備份資料應定期執行測試作業，適當記錄於備份資料測試紀錄表，以確保備份資料之可用性。 4. 備份資料應異地存放，媒體存放處所環境應合於電腦機房安全標準，並適當記錄於備份異地存放紀錄表(如系統自動記錄畫面)。 5. 資料及文件應就其重要性妥適區分安全等級，並透過系統設定或文件管理達到安全控管之目的。 6. 系統使用單位對於檔案之使用應依照程式及資料存取控制作業辦理。 7. 為避免檔案資料或硬體設備遭病毒毀損，應建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。 (二).電腦設備之安全控制 1. 資訊設備於購入時，資訊單位應會同使用單位驗收，並登記於資訊設備清單列冊管理；移轉資訊設備則應填具設備移轉記錄單，經移出與移入單位經	＜依據資料＞ 1.備份記錄表 2.備份異地存放紀錄表 3.資產盤點清冊 4.資產異動單 5.資產 外修/出售/外借/報廢 申請單 6.筆電設備記錄表 7.資產管理辦法

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		辦人員與主管簽核後送交資訊部存查。 2.電腦設備及其存放之資料於報廢時應填具資訊設備報廢申請單，申請進行報廢程序，以避免機密資料流失。 3.為避免報廢電腦硬碟機密及敏感資料外洩，應訂定電腦設備報廢作業程序；電腦設備報廢前應將硬碟內機密性、敏感性資 料及授權軟體予以移除，實施安全性覆寫或實體破壞，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。 4.筆記型電腦設備之攜出攜入則應填寫筆記型電腦記錄表。 (三).通訊設備管理 1. 通信網路應加強安全防禦，以防止資料遭截取，必要時應採取加密措施。 2. 重要網站及伺服器系統，應以防火牆或同等級之防禦措施做區隔，以降低整體風險。 3. 防火牆應有專人管理，其設定應經權責主管之核准，並應以適當方式保存防火牆進出紀錄。 4. 使用外部設施管理服務前，應執行適當之風險評估，商議適當之控制措施，與廠商協議後併入合約中。 5. 若設備線路發生故障時，資訊單位應派員立即檢查，以瞭解線路故障原因，	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依　據　資　料
		必要時通知廠商或電信單位進行維修。 (四)電腦機房之管制 1. 電腦機房應設有適當之門禁管制（例如：門鎖、刷卡或指紋機）；資訊部人員對非作業人員進出電腦機房，應請其登記於電腦機房進出管制登記表，並於資訊部人員陪同下方可進入，嚴禁未經許可人員擅入機房。 資訊單位主管應定期覆核授權進出機房人員，並檢視門禁管制記錄。 2. 各項資訊設備依預定使用目的存放於電腦機房內，不應放置其他易燃或危險物品。 3. 機房內應設置獨立之空調設備以維持穩定正常之溫濕度狀態。 4. 應安裝自動電壓穩定裝置，以維護設備安全及系統穩定性。重要設備應裝設不斷電系統（UPS）及電源供應器以避免作業因停電而中斷。 5. 不斷電系統等機房防護設備，應定期檢查與維護，並測試其堪用性。 6. 電腦機房使用之空調、電源等相關設備，應有適當之備援對策。 二、控制重點： (一).資料檔案之安全控制 1. 應用程式及資料檔，依其重要性執行日、週、月等不同週期之備份作業。 2. 備份之資料媒體需適當記錄於備份紀錄表中，並應於備份儲存媒體貼上內外標籤以利辨識備份內容。	〈依據資料〉 1. 停電及資料回復作業辦法

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		3.備份資料應定期執行測試作業，以確保備份資料之可用性。 4.備份資料應異地存放，媒體存放處所環境應合於電腦機房安全標準。 (一).電腦設備之安全控制 1. 應建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。 2. 購入資訊設備資訊應會同使用單位驗收，並登記於資訊設備清單列冊管理。 3.移轉資訊設備應填具設備移轉紀錄單，經移出與移入單位經辦人員與主管簽核後送交資訊存查。 4.電腦設備及其存放之資料於報廢時應填具資訊設備報廢申請單，申請進行報廢程序，以避免機密資料流失。 5. 依資產管理辦法之報廢規定辦理報廢程序：電腦設備報廢前應將硬碟內機密性、敏感性資料及授權軟體予以移除，實施安全性覆寫或實體破壞，確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，應簽訂保密合約。 6. 筆記型電腦設備之攜出攜入則應填寫筆記型電腦紀錄表。 (二).通訊設備管理 1. 通信網路應加強安全防禦，以防止資料遭截取，必要時應採取加密措施。 2. 若設備線路發生故障時，資訊應派員立即檢查，以瞭解線路故障原因，必要時通知廠商或電信單位進行維修。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		(四)電腦機房之管制 1. 電腦機房應設有適當之門禁管制；資訊單位人員對非作業人員進出電腦機房，應請其登記於「電腦主機房進出管制登記表」，並於資訊組人員陪同下方可進入，嚴禁未經許可人員擅入機房。 2. 資訊單位主管應定期覆核授權進出機房人員，並檢視門禁管制紀錄。 3. 機房內應設置獨立之空調設備、自動電壓穩定裝置、不斷電系統（UPS）、電源供應器等機房防護設備。 4. 不斷電系統等機房防護設備，應定期檢查與維護，並測試其堪用性。 5.機房內不應放置其他易燃或危險物品。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依　據　資　料
CEL108	硬體及系統軟體之購置、使用及維護 一、軟、硬之請購、訂購及驗收 二、軟、硬體之使用 三、軟、硬體之維護	一、由使用單位提出需求，經資訊人員評估公司現有硬體設備及軟體後，認為有必要增添，才填立「請購、詢價、驗收單」或「簽呈」經核決主管簽核後辦理。 二、請購之規格由資訊人員考慮公司設備整體配合情形，加以訂定。 三、簽核後之「請購、詢價、驗收單」轉資訊單位辦理採購作業。 四、訂購及驗收依本公司「採購作業管理辦法」之相關規定辦理。 一、由資訊人員判定軟、硬體之操作手冊，各使用人應依手冊規定使用各項設備或軟體。 二、資訊人員對新操作人員進行使用說明及訓練，以使其順利上線。 一、本公司均使用合法之套裝軟體，故於使用時發生問題，應由資訊人員聯絡原出廠公司負責維修。 二、本公司使用之硬體及系統軟體每年與廠商簽定維護合約，進行定期保養及故障維修。 三、資訊系統硬體設備之外修作業，依本公司「固定資產管理辦法」之相關規定辦理。 ＜控制重點＞ 一、各項資訊設備之請購審核是否會同資訊單位辦理。 二、軟、硬體請購之規格是否考慮公司整合需求。 三、是否編制各項軟、硬體使用或操作手冊。 四、對新操作人員是否施以足夠之訓練及說明。 五、合法使用軟體之授權證明是否妥善保管。 六、是否簽定硬體及系統軟體之維護合約。	＜依據資料＞ 1. 採購作業管理辦法 ＜使用表單＞ 1.請購、詢價、驗收單 2.簽呈 3.訂購單 4.合約書

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL109	系統復原計畫及測試程序 一、災害系統復原計劃	一、含括天然災害或其他環境因素、人為因素所造成，並導致單一系統或其他影響公司營運作業之事件發生來定義之；如發生上述狀況均應即時通知資訊人員處理。 上述狀況含括： 1. 通信網路設備損壞處置/備援 2. 病毒、垃圾郵件等網路型態攻擊處置 3. 資訊服務終止處置/備援 4. 內部資料庫、程式及檔案中止處置/備援 5. 資訊機房損壞處置/備援 二、資訊人員應依照發生等級，啟動相對應處置方式。 三、確認災害問題，應盡速排除狀況，保證作業安全、穩定及資料完整性。 四、若因災害發生導致資料無法完全置回應有系統時，應請使用者補回相關資料。 五、 核定之備援及回復計畫，由下列人員執行： (1)非人工備援作業由資訊單位人員為之。 (2)人工備援作業由使用該應用系統之業務單位人員為之。 六、緊急應變計劃應詳細記錄回復步驟，包括： 1.啟動備援機相關設定 2.取出最近之資料備份，完成復原測試 3.檢視回復測試結果是否正常，並加以記錄存檔 4.檢視測試結果，並將測試報告結果呈送資訊中心主管	

編 號	作業項目	作 業 程 序 及 控 制 重 點	依據資料
	二、測試程序	5 確認測試結果可行後，開放使用者重新登入使用 6.同時應記載，相關維護廠商資料及相關聯絡方式，以為緊急狀況發生時，查核之需。 七、災難復原均須要詳實填寫「資訊災害處理紀錄」，以利未來相關改善作業。 一、目的： (一)演練災難不同等級狀況發生時，資訊人員處置能力 (二)驗證是否災難處置作業符合實際解決方案 (三)找出相關作業缺失並列表改善 二、緊急應變計劃之測試程序，擬定各項情境，並擬定相關復原措施： 1.依照 L1~L5 層級設定相關測試演練 2.演練如牽扯到電信公司；該部分則不列入實際演練過程；資訊人員僅需持有聯繫方式、窗口即可 3.每次演練都需提前設定演練計畫、預估效益、時間記錄並將相關演練資料，依照等級提供給相關主管 三、緊急應變計劃測試週期： 1.ERP 部份：以測試主機執行，每年乙次。 2.MAIL 部份：以備援主機(或另覓較低階之測試主機)執行，每年兩次(6/12 月份)。 3.AD 部分：每年二次(6/12 月)切換(停用其中一台) 4.網路設備、異地備援資料復原測試(透過備用主機測試模擬)每年二次(6/12 月)	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依　據　資　料
		四、資訊人員測試完成後，均須詳實填寫「回復測試報告表」以利相關作業改善參考。 ＜控制重點＞ 一、使用者發現異常訊息時，是否立即通知資訊人員處理。 二、資訊人員是否有依照「災害系統復原計劃及測試作業程序」進行狀況處理。 三、資訊人員是否將異常情形及處理方式詳細記錄並呈核，以為日後參考依據。 四、系統測試如有錯誤，是否由使用者填單請資訊人員處理。 五、測試錯誤之排除是否留有記錄，以備查考。	＜使用表單＞ 1. 資訊災害處理紀錄／回復測試報告表

編　號	作業項目	作　業　程　序　及　控　制　重　點	依　據　資　料
CEL110	資通安全檢查之控制 一、資通安全檢查之控制程序	一、資訊部門應以公司業務需求及資訊政策目標等，訂定資訊安全政策以為資訊作業之安全水準。 二、權責單位應定期（每年至少乙次）依據本作業循環各章節及「資訊安全政策」辦理資訊安全檢查作業（內部辦理或委託外部專業機構），以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。 三、針對前開之檢查作業結果，辦理政策或資訊控制作業之修訂，並留存檢查紀錄、追蹤改善情形等。 四、資訊部門每年執行資通安全檢查至少應包含如下作業： (一)網路系統安全評估： 1.網路系統安全設定是否依規定設定(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。 2.是否定期或適時修補網路運作環境之安全漏洞（含伺服器、筆記型、個人端及營業處所內供共用之電腦等）。 3.是否有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應對內部隨時公告。 4.各電腦主機、重要軟硬體設備是否有專人負責。 (二)防火牆之安全管理： 1.防火牆是否建立並依政策予以設定。 2.防火牆應有專人管理。 3.防火牆進出紀錄及其備份應至少保存兩年。 4.重要網站及伺服器系統應以防火牆與外部網際網路隔離。 5.防火牆系統之設定應經權責主管之核准。 (三)電腦病毒及惡意軟體之防範：	<依據資料> 1.公開發行公司建立內部控制制度處理準則 2.資訊安全政策

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		1.應安裝防毒軟體，並及時更新程式及病毒碼。 2.應定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。 3.防毒應涵蓋個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。 4.勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。 5.為防範電腦病毒擴散,影響電腦安全,，公司應訂定電子郵件使用安全政策。 <控制重點> 一、是否訂定「資訊安全政策」以為資訊安全作業之依據 二、應定期評估自身網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。 三、應定期或適時修補網路運作環境之安全漏洞（含伺服器、攜帶型、個人端及營業處所內供共用之電腦等）。 四、有關電腦網路安全(如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等)之事項應對內部隨時公告。 五、應建立防火牆，並設專人管理，且防火牆進出紀錄及其備份應至少保存兩年。 六、防火牆系統之設定應經權責主管之核准。 七、應定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。 八、防毒應涵蓋個人端（含攜帶型及共用之電腦等）及網路伺服器端電腦。 九、公司應訂定電子郵件使用安全政策，以防範電腦病毒擴散，影響電腦安全。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
CEL111	公開資訊申報作業 一、公開資訊申報作業程序	一、網路申報系統的最高使用權限，應經權責主管人員審慎評估後，交付可信賴的人員管理，防止非相關人員存取系統資訊。 二、最高使用權限人員，應依各業務範圍、權責分別設定使用者之帳號及權限，並且不得私自更換使用，使用者一旦離開原職務，應立即撤銷該使用者之帳號及權限。 三、使用者之帳號及密碼，應避免使用容易被識破及猜測的密碼，並且應定期更改密碼。 四、公司應申報之公開資訊、重大訊息等項目，應依相關法令辦理，並於規定時限內申報完成。 五、資料製作及申報方式：公開資訊之申報檔案分為格式化檔案及非格式化檔案兩大類。 (一)格式化檔案：申報內容為標準化格式，申報方式又分二種，可任選其一： 1.申報人員可於申報時，直接至申報網頁上依欄位填報； 2.或在申報前先至申報網站下載所需之檔案格式（利用記事本開啟），依所下載檔案內之說明直接在下載檔案內填寫相關欄位資料，填寫完畢後存檔再予以上傳及檢核，上傳後如顯示“檢核無誤！”再到「申報內容查詢及確認」選項中查看所上傳之資料正確與否，申報作業才算完成。 屬於格式化檔案之申報作業包含有：公司內部人股權異動申報作業、現金增資及發行公債申報作業、大陸投資申報作業、重大訊息申報作業、月營業額背書保證與資金貸放資訊及各項產品業務營收統計資料、取得或處分資產申報作業、衍生性商品交易資訊申報作業、庫藏股申報作業...等項目，因大小項目繁多，不便逐一敘述，詳細申報項目及操作方式，申報人員應依「公開資訊觀測站」申報操作手冊辦理。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		2.非格式化檔案：係指申報人員應將財務報告、財務預測、公開說明書、年報、議事手冊及議事錄等書面資料製作成單一化檔案，於上傳前應檢視檔案是否可以正常開啟且與書面資料一致沒有缺漏後，始可透過網路上傳電子檔案（非格式化檔案）至申報網站，上傳電子檔案後，如未出現收件序號時，應至網站上確定檔案是否上傳成功，畫面若出現該筆記錄，則表示該檔案已上傳成功；若無時，則應重新上傳該檔案。檔案上傳成功後，應於隔日至申報網站及本身電子郵件信箱查詢上傳檔案是否已被申報網站接受，若未被接受，則應重新製作電子檔案並再次上傳。 上傳之檔案應以下列檔案格式擇一製作： 1.MS-WORD 之 DOC 檔。 2.MS-EXCEL 之 XLS 檔。 3.Adobe Acrobat 之 PDF 檔。 4.華印科技 DynaDoc 之 WDL 檔。 5.一般純文字之 TXT 檔。 6.Winzip 壓縮過之 zip 檔。 六、申報資料、方式與申報時限： (一)申報人員應依「公開發行公司應公告或向本會申報事項一覽表」及「公開資訊觀測站」申報操作手冊之規定辦理。 (二)應申報項目之檔案格式、資料內容、申報時限及申報方式，日後如有增減變動或名稱變更時，應依主管機關最新頒布之函令辦理。	

編　號	作業項目	作　業　程　序　及　控　制　重　點	依據資料
		<控制重點> 一、各項資料申報應於期限內辦理。 二、傳輸檔案應符合規定。 三、檔案上傳前應確實核對上傳資料正確與否。 四、檔案上傳後應確認已上傳成功並為證期會指定之資訊申報網站所接受。 五、隨時注意主管機關相關函令之修正，申報項目應配合最新函令做適時的修正。	