版本修訂摘要

| 版數 | 條文 | 變更內容摘要 | 修訂者 | 修訂日期 |
|---|---|---|---|---|
| 1 | | 新訂 | 李文桐 | 114/9/25 |
| | | | | |

第 1 條 目的

為確保公司內各據點間重要資訊之機密性、完整性及可用性，本政策依照「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，及參照上市上櫃公司資通安全管控指引。

第 2 條 名詞定義

一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。

三、核心業務：公司維持營運與發展必要之業務。

四、核心資通系統：支持核心業務持續運作必要之資通系統。

五、機敏性資料：依公司業務考量，評估需保密或具敏感性之重要資料，如涉及營業秘密資料或個人資料等。

第 3 條 資通安全政策

為維護本公司資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。藉由本公司全體同仁共同努力以達成下列目標：

一、保護本公司研發、業務、生產、服務之資訊安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

二、保護本公司研發、業務、生產、服務之資訊安全，避免未經授權的修改，以確保其正確性與完整性。

三、確保本公司各項業務、服務等之執行，須符合相關法規之要求。

第 4 條 資通安全管理架構與權責分工

本公司之資通安全政策及目標，由董事會下的永續發展及提名委員會督導的資訊安全推動小組來啟動公司的資訊安全管理系統；由該委員會指派適當人員擔任資安專責人員，以負責推動、協調監督及審查資通安全管理事項，並由資訊總務科實際執行資安計畫之網管成員共同組成。主要任務有：

一、整合公司內資通安全資源，由管理中心為最高階資安單位，負責協調督導資通安全相關政策、措施、機制之運作。

二、資訊安全相關措施、技術規範之研擬及安全技術之研究、建置等事項，會由

資訊總務科協助辦理。

三、公司內各據點間資料及報表之安全需求研議、使用管理、保護及資訊機密維護等事項，由各相關業務單位負責辦理。

四、公司內資訊機密維護之稽核管理事項，由公司稽核單位會同相關業務單位負責辦理

第 5 條 資訊安全管理指導原則

訂定資通安全作業程序，包含核心業務及其重要性、資通系統盤點及風險評估、資通系統發展及維護安全、資通安全防護及控制措施、資通系統或資通服務委外辦理之管理措施、資通安全事件通報應變及情資評估因應、資通安全之持續精進及績效管理機制等所有使用資訊系統之人員，每年進行資訊安全宣導，另負責資訊安全之主管及人員，需接受資訊安全課程訓練。

第 6 條 核心業務的鑑別

鑑別並定期檢視公司之核心業務及應保護之機敏性資料。

第 7 條 鑑別應遵守之法令及契約要求

第 8 條 鑑別核心業務的復原時間

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。

第 9 條 核心業務的持續運作制定

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。

第 10 條 資通系統的盤點

定期盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值。

第 11 條 核心業務資安風險評估

於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。

第 12 條 資通安全系統的規格

將資安要求納入資通系統開發及維護的需求規格，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。

第 13 條 資通安全系統的測試

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。

第 14 條 資通安全系統的維護

妥善儲存及管理資通系統開發及維護相關文件。

對核心資通系統辦理定期辦理弱點掃描作業，並進行系統弱點的修補。

第 15 條 資通安全防護控制措施

依網路服務需要，區隔出獨立的邏輯網域(DMZ、內部及外部網路)，並將開發測試與正式作業環境區隔，且針對不同作業環境建立適當之資安防護控制措施，訂定「人員裝置使用管理規範」作為公司內部員工使用各資訊設備與軟體的依據。

資安防護控制措施如下：

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。

第 16 條 機敏性資料的防護措施

針對機敏性資料之處理及儲存之防護措施，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，請參考「機敏性資料處理與儲存防護措施規範」:

一、作業環境與設備管理

二、存取權限與帳號管理

三、資料加密與安全傳輸

四、資料遮蔽與非正式環境應用

五、員工保密責任與資料處理規範

六、委外合作與資料外部接觸

資通設備回收再使用及汰除之安全控制作業，參考「報廢電腦處理程序」，以確保機敏性資料確實刪除

第 17 條 使用者資通安全系統管制措施

本公司針對相關使用者資安防護控制措施。資安防護控制措施如下：

一、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。

二、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。

三、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。

四、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。

五、針對電腦機房及重要區域之安全控制、人員進出管控等項目建立適當之管理措施

第 18 條 資通系統委外辦理的管理措施

本公司將資通系統委外辦理時，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下：

一、於委外辦理時，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。

二、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 19 條 資通安全事件管理措施

本公司若發生符合「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」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。

本公司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的管理措施。

第 20 條 資通安全事件管理措施

本公司資通安全管理作業程序經董事會決議通過後施行，修正時亦同

第 21 條 本作業程序訂定於民國 114 年 9 月 25 日。