能率創新股份有限公司

資通安全管控政策

113.11.13 董事會通過

1.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，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，擬定本辦法。

2.適用範圍

本公司員工、接觸本公司業務資料之外聘人員、委外服務提供廠商人員及訪客。

3.名詞定義

1. 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。
2. 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。
3. 核心業務：公司維持營運與發展必要之業務。
4. 核心資通系統：支持核心業務持續運作必要之資通系統。
5. 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。

4.資通安全政策及推動組織

為強化本公司之資訊安全管理、確保資料、系統及網路安全，設立資訊課為資訊安全權責單位，由本公司高階主管兼任資安專責主管,綜理資訊安全政策推動及資源調度事物，一名資訊安全專責人員，負責進行資訊安全制度之規劃、監控、執行資訊安全管理作業及危機處理。

1.資訊安全之目標：

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。

2.資訊安全之範圍：

(1)人員管理及資訊安全教育訓練。
(2)電腦系統安全管理。
(3)網路安全管理。
(4)系統存取管制。
(5)系統發展及維護安全管理。
(6)資訊資產安全管理。
(7)實體及環境安全管理。
(8)資訊系統永續運作計畫管理。
(9)資訊安全稽核。

3.資訊安全的原則及標準：

(1)定期辦理資訊安全教育訓練及宣導，包括資訊安全政策、資訊安全法令規定、資訊安全作業程序、以及如何正確使用資訊科技設施等，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，並遵守資訊安全規定。
(2)為預防資訊系統及檔案受電腦病毒感染，對於電腦病毒應採取偵測及防範措施，對入侵及惡意攻擊應建立主動式入侵偵測系統，以確保電腦資料安全之要求。

(3)為預防本公司遭遇天災或人為之重大事件，將造成重要資訊資產及關鍵性業務或通訊系統等中斷，應建立資訊系統永續運作規劃之政策。

4.員工應遵守之相關規定：

(1)資訊單位接收帳號申請單後，建立「使用者代號」。

(2)電腦資料及設備，不得任意破壞、攜出、外借、不正當修改，維護資料完整性。

(3)禁止使用無版權軟體。

(4)進入主機後，若作業結束或長時間不使用機器時，應退出機器，以免資料機密外洩，為別人所破壞或造成當機之困擾。

(5)電腦設備之擺放位置除以方便為原則外，應遠離茶水、咖啡、日曬或潮溼地點，以延長其壽命。

(6)離職或新舊職務交接時，由資訊單位衡量資料相關性作適當處置。

(7)電腦設備無法正常作業時，使用者應立即通知資訊單位，以便檢查或維修。

5. 資通安全防護及控制措施

1. 依網路服務需要，區隔出獨立的邏輯網域(內部及外部網路)，且針對不同作業環境建立適當之資安防護控制措施。
2. 具備下列資安防護控制措施：(防毒軟體、網路防火牆、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、重要資料定期備份排程) 。
3. 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。
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，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。
6. 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。

7. 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。
8. 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。
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. 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。
11. 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。
12. 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。

6. 資通系統盤點及風險評估

1. 定期盤點資通系統，並建立核心資訊資產清冊，鑑別其資訊資產價值。
2. 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。

7.資通系統發展及維護安全

1. 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。
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。
3. 妥善儲存及管理資通系統開發及維護相關文件。
4. 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。

8. 資通系統或資通服務委外辦理之管理措施

1. 於委外辦理時，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。
2. 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。
3. 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。

9. 資通安全事件通報應變

1. 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。
2. 發生符合「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。

10. 資通安全之持續精進及績效管理機制

1. 資通安全推動人員定期向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。
2. 定期辦理內部或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。

11. 附則

本辦法如有未盡事宜，由資訊安全主管另行定之。

本辦法經董事會通過後施行，修正時亦同。