志豐電子有股份限公司
KINGSTATE ELECTRONICS CORPORATION

文件名	資通安全管理政策與程序	制訂日期	11/05/2024	頁　碼	1/5
編　號	KS-M-A-P-007-1.1	版　本	1.0	部　門	資訊單位
制　定	高嘉志	審　閱	林依萍	批　准	葉方瑜
日　期	11/05/2024	日　期	11/05/2024	日　期	11/05/2024

第 1 條 訂定目的

為強化資通安全防護及管理機制，確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，參考「上市上櫃公司資通安全管控指引」，並符合「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之規範，特訂定本資通安全管理規範。

第 2 條 資通安全政策及推動組織

1. 成立資通安全推動組織，組織配置適當之人力、物力與財力資源，並指派適當人員擔任資安專責主管及資安專責人員，以負責推動、協調監督下列資訊安全管理事項：
   (1). 資訊安全政策之核定及督導。
   (2). 資訊安全責任之分配及協調。
   (3). 資訊資產保護事項之監督。
   (4). 資訊安全事件之檢討及監督。
   (5). 其他資訊安全事項之核定。
   (6). 定期召開資訊安全會議。
2. 本資通安全政策與程序由副總經理以上主管核定，並定期檢視政策及目標且有效傳達員工其重要性。
3. 本資通安全政策與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。
4. 所有使用資訊系統之人員，每年接受資訊安全宣導課程，另負責資訊安全之主管及人員，每年接受資訊安全專業課程訓練。

第 3 條 核心業務及其重要性

1. 鑑別並定期檢視公司之核心業務及應保護之機敏性資料。
2. 鑑別應遵守之法令及契約要求。
3. 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。
4. 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、應變作業規定、資源調配及演練結果檢討改善。

第 4 條 資通系統盤點及風險評估

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

第 5 條 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下列資安檢測作業，並完成系統弱點修補。
   (1). 定期辦理弱點掃描。
   (2). 定期辦理滲透測試。
   (3). 系統上線前執行源碼掃描安全檢測。

第 6 條 資通安全防護及控制措施

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。
2. 公司網路應評估建置下列資安防護控制措施：
   (1). 防毒軟體。
   (2). 網路防火牆。
   (3). 電子郵件過濾機制。
   (4). 入侵偵測及防禦機制。
   (5). 對外服務之核心資通系統者，應具備應用程式防火牆。
   (6). 進階持續性威脅攻擊防禦措施。
   (7). 資通安全威脅偵測管理機制（SOC）。
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、在職及離職相關管理規定，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。
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. 依資通系統及相關設備重要性等級建立適當之監控措施，宜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，由資訊部指定專人辦理，並針對日誌建立適當之保護機制。
8. 建立遠端存取資通系統之管控機制，並教育居家辦公者應對網路風險保持警覺等。
9. 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。
10. 針對電腦機房及重要區域之安全控制、人員進出管控、環境維護等項目建立適當之管理措施。
11. 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。
12. 訂定資通設備回收再使用及汰除之安全控制作業相關規定，以確保機敏性資料確實刪除。
13. 訂定人員裝置使用管理規範。
14. 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。
15. 資訊安全防護設定如需異動，需經由資訊部門核定後，由專責人員修改，並紀錄異動歷程。
16. 定期檢討防火牆安全權限及電腦網路安全事項。
17. 定期評估資通安全防護系統之軟體/韌體版本更新，以因應各種網路攻擊。

18. 憑證安全管理：
    (1). 資訊平台與外部連結時，須建置憑證金鑰。
    (2). 憑證金鑰之產生、儲存、使用、備份、銷毀、更新及復原作業等，應建立嚴格的安全管理機制。

第 7 條　資料存取

1. 系統資料由系統管理者依使用者群組及其業務範圍訂定不同使用權限，無權限者不得存取資料內容。
2. 資訊系統均需有帳號及密碼登入管理功能，依使用者業務範圍區分帳號群組、組織、功能等類別，每位同仁需使用個人專屬帳號及密碼登入後方可使用系統。
3. 使用者須妥善保管個人帳號及密碼，且密碼需符合公司規定之長度及複雜度並定期更換之。
4. 個人密碼應絕對保密，若發現外洩應即更改，以確保資訊安全。
5. 員工人事異動經權責主管核定後，應依其異動狀況停用或刪除其帳號及許可權。
6. 資料依重要性區分，設定不同的保存或銷毀期限，除另有規定外，保存期限至少五年。
7. 使用單位經由系統所取得之機密性資料均應嚴加管制，限制傳閱、影印、複製、攝影、轉出或以其他方式記錄。
8. 公司同仁於公司外部使用公司系統時，需使用公司指定之 VPN 軟體連線並通過身分驗證後方可使用。
9. 使用者經由公用網路傳輸機密資料時，應採取資料加密機制。

第 8 條　系統原始碼管理

1. 資訊系統之相關原始碼，應依機密等級給予適當安全屬性，不同安全屬性之文件應分開，並以相對應的安全措施加以保存。
2. 調閱相關原始碼須經資訊部門主管核定並記錄。
3. 委外 / 委託開發時應適度進行安全評估與規劃，並明確定義需求內容與權責、保密與保護法規及風險控管且須監督受託方依約執行與驗收。

第 9 條　資通系統或資通服務委外辦理之管理措施

1. 宜訂定資訊作業委外安全管理規定，包含委外選商、監督管理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. 宜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。

第 10 條 備份作業管理

1. 為確保集團資訊系統之資料完整性與正確性，應依照資訊系統重要性適當設有多重資料備份保護機制，以確保災害發生時，能根據不同等級的損害進行資訊資料的重建工作。
   (1). 本機資料備份：存放於運行中的主機上。
   (2). 異機資料備份：存放於同機房的其他主機上。

(3). 異地資料備份：存放於異地地點。

2. 資訊部門應依媒體裝置運營業務及重要性設評估設備的營運資產價值，劃分人員與備份維護計畫，並監控備份維護主機運作，並保持日誌（LOG）的完整性以利追查。
3. 備份以硬碟儲存裝置為主，其他媒體為輔，並須存放於隔熱防火、防潮整潔之場所，且至少有一份備份資料應與主機異機安全保存。
4. 重要資料的新舊備份，均應依公司規定之時效妥善保存。
5. 定期進行災難復原演練作業，並於過程中記錄主機名稱、日期、起迄時間、內容、過程、結果及操作人員等內容，以確保備份資料之有效性與完整性。

第 11 條 病毒防治

1. 公司所有伺服器主機、個人電腦、筆記型電腦均應安裝公司指定之防毒軟體，掃毒紀錄應由專人定期檢視，並將紀錄留存備查，若檢查過程發現異常應立即採取必要之措施以防制電腦病毒與惡意軟體等的侵入。
2. 個人電腦使用軟體，應依下列原則辦理：
   (1). 防毒軟體應定期更新版本及病毒碼。
   (2). 防毒軟體應定期或即時掃描電腦系統及資料儲存媒體。
   (3). 電腦使用之軟體須由資訊部門審核後，方可安裝使用。
   (4). 對來路不明及內容不確定的資訊媒體，應於使用前詳加檢查是否感染電腦病毒。
   (5). 定期將必要的資料及軟體予以備份。
3. 電腦設備如遭病毒感染，應立即中斷網路連結（有線/無線），並通知資訊人員處理，直到確認病毒已消除後，方可恢復連線。

第 12 條　　個人資料保護

資訊系統之運作功能及資料存取應符合個人資料保護規範，依據「個人資料保護作業要點」相關規定辦理。

第 13 條　　資安遵守

1. 資訊部門應制定系統使用規範，並防止內、外非相關人員取得機密資訊或影響系統正常運作。
2. 同仁不得利用系統進行非正常或未經許可之作業，以獲取不當之資訊或利益。
3. 同仁應遵守本程序之相關規定，違者按情節輕重依相關規定予以處分。

第 14 條　　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相關規定，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協調中心（TWCERT/CC）之「企業資安事件應變處理指南」。
2. 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。
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」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 15 條　　資通安全之持續精進及績效管理機制

1. 資通安全推動組織應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。
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。
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。
4. 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 16 條　　本程序經董事會通過後實施，修正時亦同。

第 17 條　　本程序新訂於 2024 年 11 月 05 日。