可寧衛股份有限公司

資通安全風險管理作業程序

一、目的

為強化資通安全防護及管理機制，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，確保公司網路和資訊使用環境安全、穩定，並強化資通安全風險管理架構，依「上市上櫃公司資通安全管控指引」訂定本作業程序。

二、名詞定義、內容範圍及權責單位

名詞定義如下

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。

本作業程序所指資通安全內容範圍內容包括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。公司資安保護目標的實際作業遵循基本要求再進階強化，並據以評估實效，按需要進行修正改善。

本公司資通安全推動的權責單位為資訊部，派任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。資訊部定期對員工發布資訊安全宣導，另負責資訊安全之主管及人員，宜持有資訊安全相關之專業證照或參加相關課程訓練。

三、核心業務及其重要性

權限申請表單經直屬單位主管依業務需求審查其使用權限之適當性，並由系統管理者設定程序化控制措施，以確保維持資訊安全的必要等級以符合法律、法規、契約及營運要求。

加強資安宣導，督導全體同仁落實資通安全管理，持續進行適當的資通安全教育訓練，建立「資通安全，人人有責」的觀念，促使同仁瞭解資通安全相關法令要求之重要性，進而遵守法令及規定，藉此提高資通安全認知及能力，降低資通安全風險，達成資通安管理法及個人資料保護法等相關法令要求事項。

為確保各資訊系統之電腦資料完整與正確，與預防因天然災害或人為疏失造成資料遺失，因此資訊系統定期執行備份並估算回存所需時間，以供緊急應變計畫參考。各項備份作業完成後由備份管理

者進行備份結果之查核，若發現備份失敗或異常狀況，則由備份管理者進行異常處理，以確保備份作業之完整性及有效性。

四、資通系統盤點及風險評估

每年最少一次盤點資通系統，並建立核心系統資訊資產清冊，以鑑別其資訊資產價值；每年最少一次資訊資產衝擊影響評估，藉以客觀的評估各資產的風險，了解未來可能遭受之危害，以達先期改善之效。

資訊資產衝擊影響評估標準如下：

等級	內 容 說 明
嚴重	▪ 事件處理不當可能對本公司形象造成嚴重損害 ▪ 已嚴重影響單位整體業務之運作，超出組織可承受範圍內。 ▪ 造成的損害可能影響單位整體業務或所有系統（可能影響本公司所有人員及合作夥伴） ▪ 復原的措施僅能由特定專業人員才能進行或修復人員 ▪ 復原可能要超過 8 小時才能完成
輕微	▪ 對於本公司整體業務執行影響不大; ▪ 造成的損失可能僅影響單一業務或系統（可能影響僅個人或少數幾人） ▪ 可以由個人進行復原 ▪ 修復或進行復原的措施可以在 4 小時內完成
微弱	▪ 對於業務執行沒有影響 ▪ 可以立即完成復原 ▪ 若持續發生且次數頻繁，對業務執行可能帶來潛在風險。

五、資通系統發展及維護安全

應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。另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妥善儲存及管理資通系統開發及維護相關文件。

每年最少一次進行資訊資產弱點及威脅分析，藉以客觀的評估各資產的風險，了解未來可能遭受之危害，以達先期改善之效。

弱點及威脅評估標準如下：

等級	內 容 說 明
高	▪ 弱點未受到適當控制，尚無初步計畫但有認知。 ▪ 未實施保護或保護機制無效，威脅來源於短期內即可攻擊成功。
中	▪ 弱點未受到適當控制，但有初步計畫與認知。 ▪ 已實施保護的機制，威脅來源必須花費一段時間（可能是數天）進行資料收集，即能接觸到關鍵資訊。

低	▪ 弱點已受到適當控制，矯正措施正執行且有認知。 ▪ 威脅來源必須花費長時間（可能需一個月以上）的資料收集，突破各層防護，才能接觸到關鍵資訊。

六、資通安全防護及控制措施

本公司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。

網路安全包括網路資源管理、防火牆與特殊連線安全控制以及無線上網等。公司通過強化內部網路基礎建設及網路服務的相應保護措施，提升網路資料傳輸安全，降低風險，減少遭受網路攻擊的傷害。網路資源管理及安全管理如下：

1、網路資源管理應關閉網路設備不使用的服務與功能，降低安全的風險；評估建立網路監控系統的必要性，及時瞭解網路運作情況，及早發現網路失效的情形或潛在風險。

2、網路安全管理

(1)依實際情況，設置適當的防火牆(Firewall)於公司的內部網路與外部網際網路接界處，防止外部未經授權進人公司內部網路。

(2)依業務需求，進行防火牆規則的適當設定；防火牆規則的設定須經過部門主管核准。

(3)定期就防火牆規則進行檢視。

(4)在資訊系統委外廠商必須以遠端登人方式進行系統維修的情況下，只在需要時才可啟動遠端登入連線，並採取管制或監控措施。

(5)不定期委由外界專家或自行評估網路系統安全並進行安全修補，提高安全防禦能力。

(6)針對開發外界連線的資訊系統，依照資料及系統的重要性，採取資訊加密、身份識別、電子簽章（若可行）等不同安全等級的技術或措施，降低資訊及系統受到入侵、破壞、篡改、刪除及未經授權存取的安全風險。

(7)無線網路架設與使用須經過審慎的安全評估。

(8)無線網路卡與無線基地台（Access Point） 間使用加密通訊協定。

3、電腦安全

本部分包含各式電腦（含伺服器及個人電腦、筆記型電腦等）系統與設備的保護、防毒軟體、存取安全、帳號密碼管理等，主要針對電腦系統進行安全保護措施，提高系統運作穩定性與持續可用能力，降低被攻擊的風險。

(1) 電腦系統與實體設備保護

A.公司所使用的各式電腦（含伺服器、個人電腦、筆記型電腦等）的系統應及時進行安全修補。

B.公司所使用的各式電腦軟體及版權，集中由資訊單位管理。

C.任何電腦均應設定螢幕保護裝置程式並設定密碼保護，防止他人未經授權使用電腦。

D.使用任何電腦設備時，必須注意其電源使用不可超過電源負載量。

E.廠商維護電腦主機設備時應有公司資訊單位人員陪同。

F.公司的任何電腦設備發生故障，資訊單位應酌情考量記錄，以供未來分析查考。

(2) 防毒軟體

A.所有電腦系統（伺服器、個人電腦、筆記型電腦等）均應安裝防毒軟體，實施並自動更新病毒庫。

B.所有電腦系統實施自動定期病毒掃描。

(3) 存取安全

A.每位電腦系統使用者（包含系統管理者），應賦予獨立的通行帳號；帳號應業務需求，賦予使用者最低能滿足作業的許可權。

B.當發生職員離職或調動的情況，需立即取消或調整其帳號許可權。

C.定期審查帳號及使用權限情況，確保符合現狀。

(4) 密碼安全管理

A.所有通行帳號的登錄LOG IN 應設立獨立密碼，密碼設定避免使用容易猜測的字串（例如生日、地名或密碼與帳號相同）。

B.輸人密碼時，電腦螢幕不得明白顯示所輸人的密碼。

C.保存密碼的檔案應予以加密。

D.設定強制使用者定期更新密碼的要求，更新密碼週期視公司情況而定，原則上不宜超過 6 個月。

E.設定使用者密碼輸人錯誤達3 次後，系統自動將帳號暫時鎖定。

F.在帳號第一次啟用後，強制使用者更新密碼，預設密碼設定的有效期限（視系統而定）。

G.制定並強制使用密碼內容至少包含：密碼長度至少6 個字元、密碼同時包含英文字母與數字。

4、應用系統管理

(1) 本部分包含電子郵件、及時通訊軟體、資料備份、異常事件處理常式等，主要針對公司日常運作的應用系統使用安全，降低不當操作所造成的傷害，提升在事件發生時的應變與處理能力。

(2) 電子郵件使用安全

A.明確規定員工禁止利用公司電子郵件從事工作業務以外的活動，並宣導員工不開啟來路不明的電子郵件。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。

B.以業務及個人工作需要，對員工電子郵件內容及大小進行規範和限制（以公司實際情況而定）。

C.開啟郵件過濾及防毒機制，以過濾垃圾及可能含有病毒的郵件。

(3) 即時通訊軟體使用安全

安裝與使用即時通訊軟體（如MSN、SKYPE ）等，必須按業務實際需要進行審慎評估。定期由資訊人員實施員工電腦合法性軟體檢查作業，並針對軟體安裝、電子郵件、即時通訊軟體、個人行動裝置及可攜式媒體等進行檢查及管控。

(4) 資料安全與備份

A.不定期進行備份資料復原測試，以確保備份資料的有效性。

B.任何資料存儲媒體（硬碟、磁片、光碟等）進行報廢時，須徹底將其內資料銷毀， 直至無法解讀；資訊單位執行資料存儲媒體銷毀作業前需填製「銷毀計畫申請表」及製作「銷毀清冊」經權責主管審查及核准後，由稽核人員於銷毀時逐項勾稽確認，以確保機敏性資料確實刪除。

C.應用系統的重要資料至少维持2套以上的備份。

D.實體的機密資料，如紙張檔、重要合約等，宜妥善存放與保管。

E.針對機敏性資料之處理及儲存建立適當之防護措施，依業務不同需求採取實體隔離、專用電腦作業環境、存取權限、資料加密、傳輸加密、資料遮蔽或以人員管理及處理。

(5) 異常事件處理常式及災害複原計劃

A.公司需依實際情況，針對常見的資安事件與異常情況，擬定異常事件處理常式，以增加處理實效，並降低異常事件發生的傷害。

B.按企業持續經營的原則，評估並理清重大業務衝擊威脅事件，據以制定災害復原計劃。

5、人員安全

(1) 本部分人員安全包含人員安全管理、認知教育與事件通報等，其主要目的為提升企業內部人員的安全意識以及對資安危機的瞭解，將有助於降低因安全意識不足所造成資安事件發生的機會。

(2)人員安全管理

A.對公司的資訊單位人員的職責進行明確定義。

B.公司負責資訊安全相關工作或處理機密資訊的人員，需簽署保密協定。

C.各種資訊安全工作，需有 2 人及以上瞭解，以應付緊急情況的需要。

(3)安全認知訓練

A.資訊安全事件應立即公告公司員工（如最新電腦病毒威脅）

B.定期提供員工適當的資通安全認知或教育訓練（依實際情況而定）

C.以實際情況，酌情考量將資通安全要求納人員工手冊中。

七、資通系統或資通服務委外辦理

委外的管理需充分注意並儘量降低因委外所造成的資安問題發生的機會，資訊委外（如電腦設備維護、系統開發等）應與委外廠商簽訂契約，並將保密條款納人其中，電腦系統資訊委外業務完成後，應要求委外廠商提供詳細的系統檔及手冊；委外廠商人員如有派駐公司情況，派駐的委外人員的電腦系統使用權限應予以適當控管。

資訊單位應與委外廠商確認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。公司於委外關係終止或解除時，資訊單位應確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料。

八、資通安全事件通報應變及情資評估因應

公司應確實遵循主管機關對資訊系統、資訊安全等相關法令規定，避免在資料處理上發生違法情形。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。

各部門發生資安事件時，應第一時間通報資訊專責人員，並遵循資訊專責人員指示之應變處置，後續由資訊部及各業務主管聯合判定事件影響及進行損害評估，內部通報由資訊專責人員執行、外部主管機關之通報由財務部及業務部依相關業務通知外部受影響機關。

本公司由資訊部判斷本公司是否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，如：所屬產業資安資訊分享與分析中心(ISAC)、臺灣電腦網路危機處理暨協調中心(TWCERT/CC)。

九、資通安全之持續精進及績效管理機制

本公司由資訊部每年至少一次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。資訊專責人員不定期檢核內部及委外廠商之資安情形，並針對發現事項擬訂改善措施，且追蹤改善情形。

十、訂定與修訂

本作業程序經董事會通過後施行，修正時亦同。

本作業程序訂定於中華民國 111 年 12 月 23 日。