愛派司生技股份有限公司
資訊安全維護計畫

目錄 頁次

愛派司生技股份有限公司
資訊安全維護計畫

一、依據及目的

本計畫依據「上市上櫃公司資訊安全管控指引」與本公司「資訊安全政策」訂定。

二、適用範圍

本程序管理之範圍包括人員、應用系統、硬體設備及網路設施等四部分。

1. 人員

涉及公司資訊作業或資料使用之全體員工、承包商、顧問、臨時雇員、客戶、第三方人員皆應遵循。

2. 應用系統

資訊作業或資料使用之軟體、程序、服務、系統。

3. 硬體設備

各式主機、工作站、伺服器及個人電腦。

4. 網路設施

公司辦公室之區域網路，及連接辦公室與電腦機房、網際網路之數據專線及相關網路設施。

三、核心業務重要性及非核心業務說明

1. 核心業務及重要性

本公司之核心業務及重要性如下表：

核心業務	業務失效影響說明	最大可容忍中斷時間
郵件伺服器	無法即時傳遞郵件與溝通	12 小時
ERP系統	影響公司經營的運作	12 小時
伺服器主機	1. 無法掌握營運狀況 2. 營運動作缺少紀錄	12 小時

註：各欄位定義說明。

(一)核心業務名稱：該項業務內各項作業程序的名稱。

(二)重要性說明：說明該業務對公司之重要性，例如對公司財務及信譽上影響、對民眾影響、對社會經濟影響、對其他公司業務運作影響、法律遵循性影響或其他重要性之說明。

(三)最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

2. 非核心業務及說明

本公司之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
防火牆	對外網路中斷或無管制連線	24 小時
網域伺服器	無法正確連線提供服務	12 小時

3. 每年定期鑑定核心業務

判定是否符合核心業務要素:

(一)數據管理：保護數據免受未經授權的訪問和損害，數據洩露導致法律問題、損害企業聲譽並影響業務持續性。

(二)基礎設施維護：確保網絡、硬體和軟體的安全性和正常運行。基礎設施故障導致業務中斷，影響公司的運營能力和盈利能力。

4. 鑑別應遵守之法令及契約要求

(一)法令遵守

(1) 確認遵守相關的資訊安全法律、法規和規範，包括但不限於個人資料保護法、電子通信交易法、資訊安全管理系統等。

(2) 定期與外部諮詢顧問進行交流，以確保法令遵守的即時性。

(二)契約要求鑑別

(1) 尊重與客戶、供應商、員工等相關方的所有契約要求，並確保其在進行資訊系統運作時能夠完全遵守。

(2) 當簽訂新的契約或更新現有契約時，視情況諮詢外部顧問進行審查，以確保契約的合規性。

5. 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。

(一)弱點掃描

(1) 定期對核心資通系統進行弱點掃描。

(2) 掃描評估使用最先進或公認的弱點掃描工具，抑或是委託專業的資安團隊執行。

(3) 發現任何弱點時，應立即評估其影響程度並優先處理，盡快修補弱點。

(4) 修補工作應由資安團隊或視情況委外負責執行。

(5) 修補完畢後，再次進行弱點掃描。

(二)滲透測試

(1) 定期對核心資通系統進行滲透測試。

(2) 評估使用最先進或公認的滲透測試方式，抑或是委託專業的資安全團隊執行。

(3) 當發現滲透破口時，應立即評估其影響程度並優先處理，盡快修補破口。

(4) 修補工作應由資安團隊或視情況委外負責執行。

(5) 修補完畢後，再次進行滲透測試

(三)源碼掃描安全檢測

(1) 擁有或掌控之核心資通系統程式原始碼，進行新增、變動等，經編譯後上線之核心資通系統，需進行安全檢測。

(2) 使用商業或開源的靜態應用安全測試(SAST)工具對源碼進行掃描。

(3) 對檢測發現的安全問題，高中危漏洞必須修復，低危漏洞建議修復。

(四)資通安全威脅偵測管理機制(SOC)

依據上市上櫃公司資通安全管控指引第十章第 37 條，評估本公司規模大小與面對之風險，暫時使用網路通訊設備(防火牆等)之監控偵測機制。

四、資訊安全政策及目標

1. 資訊安全政策

為建構及保護本公司所有資通系統之相關資訊資產，包括實體環境、軟硬體設施、網路、雲端、資料、資訊、人員等安全，免於因內部或外在之威脅，遭受破壞、遺失、洩密或不當控制等資通安全風險，特制訂本政策。

本公司應採取以下措施：

(一)恪遵法令訂定相關資訊安全管理規章，對本公司資訊資產提供適當的保護措施，以確保其機密性、完整性、可用性及法律遵循性。

(二)定期評估各種人為及天然災害對本公司資訊資產之影響，並訂定重要資訊資產及關鍵性業務之防災對策及災變復原計劃，以確保本公司業務持續運作。

(三)督導本公司同仁落實資訊安全防護工作，建立「資訊安全、人人有責」觀念，提升各業務部門及人員對資訊安全之認知。

(四)要求本公司同仁以及連結本公司資通系統或提供服務之往來廠商，應確實遵守本公司資訊安全相關規定，如有違反者，視其情形分別依本公司規定懲處或依契約罰責辦理外，情節嚴重者另將受相關法律之追訴。

2. 資訊安全目標

(一)量化型目標

(1) 知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。

(2) 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%。

(二)質化型目標

(1) 適時因應法令與技術之變動，調整資訊安全維護之內容，以避免資訊系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。

(2) 達成資訊安全責任等級分級之要求，並降低遭受資訊安全風險之威脅。

(3) 提升人員資安防護意識、有效偵測與預防外部攻擊等。

3. 資訊安全政策及目標之核定程序

(一)資訊安全政策由公司資安長簽核，經主管會議討論後由總經理核定。

(二)資訊安全政策及目標之宣導

(1) 公司之資訊安全政策及目標應每年透過教育訓練、內部會議、郵件宣告等方式，向公司內所有人員進行宣導。

(2) 公司應每年向利害關係人（例如 IT 服務供應商、與公司連線作業有關單位）進行委外廠商資安查核。

五、資訊安全推動組織

組別	單位職稱	工作職掌
資訊安全長	資安長	督導資訊安全相關事項
資訊規劃組	資安專員	1. 資訊安全政策及目標之研議。 2. 訂定公司資訊安全相關規章與程序制度文件，並確保其內容合乎法令及契約之要求。 3. 依據資訊安全目標擬定公司年度工作計畫。 4. 其他資訊安全事項之規劃。 5. 傳達公司資訊安全政策與目標。 6. 辦理資訊安全內部稽核。 7. 每年定期於經管會議，提報資訊安全事項執行情形。

資安防護組	資深專員	1. 資訊安全技術之研究、建置及評估相關事項。 2. 資訊安全相關規章與程序制度之執行。 3. 資訊及資訊業務之盤點及風險評估。 4. 資料及資訊業務之安全防護事項之執行。 5. 資訊安全事件之通報及應變機制之執行。 6. 其他資訊安全事項之辦理與推動。

六、專職人力及經費配置

1. 人力及資源配置

(一)公司依「資訊安全責任等級分級辦法」之規定，屬資訊安全責任等級 D 級，最低應設置資訊安全兼辦人員 1 人，其分工如下，公司現有資訊安全專責人員名單及職掌應列冊，並適時更新。

(1) 負責資訊系統分級、內部資訊安全稽核、防護基準及教育訓練業務。

(2) 負責資訊安全防護設施建置及資訊安全事件通報及應變業務之推動。

(二)本公司應加強資訊安全人員之培訓，並提升其管理能力；若資訊安全人力或經驗不足，得洽請相關學者專家、專業公司或機構提供顧問諮詢服務。

(三)負責重要資訊設備之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

(四)各單位主管應負責督導所屬人員之資訊安全作業，防範不法及不當行為。

(五)專業人力資源之配置情形應每年定期檢討，並納入資訊安全維護計畫持續改善機制之管理審查。

2. 經費配置

(一)資訊安全長於規劃配置相關經費及資源時，應考量公司之資訊安全政策及目標，並提供建立、實行、維持及持續改善資訊安全維護計畫所需之資源。

(二)各單位於規劃建置資訊系統時，應一併規劃資訊系統之資安防護需求，並於整體預算中合理分配資訊安全預算所佔之比例。

(三)各單位如有資訊安全資源之需求，應由資訊安全長視整體資訊安全資源進行分配，並經資訊安全長核定後，進行相關之建置。

(四)資訊安全經費、資源之配置情形應每年定期檢討，並納入資訊安全維護經費、資源之配置情形應每年定期檢討。

七、資訊及資訊系統之盤點

公司每年辦理資訊及資訊系統資產盤點，依管理責任指定對應之資產管理人。

八、資訊安全風險評估

1. 公司應每年針對資訊及資訊設備資產進行風險評估。
2. 公司應每年依據「資訊安全責任等級分級辦法」之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估。
3. 公司應定期評估評估導入 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，以維持公司

穩健之資訊安全。

九、資訊安全防護及控制措施

公司依據資訊安全風險評估結果、自身資訊安全責任等級之應辦事項，採行相關之防護及控制措施如下：

1. 資訊及資訊設備之管理

(一)公司同仁使用資訊及資訊設備須遵守相關管理規範。

(二)公司同仁使用資訊及資訊設備時，應留意其資訊安全要求事項，並負對應之責任。

(三)公司同仁使用資訊及資訊設備後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

(四)非公司同仁使用公司之資訊及資訊設備，應確實遵守公司之相關資訊安全要求，且未經授權不得任意複製資訊。

(五)對於資訊及資訊設備，應方便識別並以文件記錄及實作成可被接受使用之規則。

2. 存取控制與加密機制管理

(一)網路安全控管

(1) 公司之防火牆由公司自行管理，區域劃分如下：

A. 外部網路：對外網路區域，連接外部廣網路 (Wide AreaNetwork,WAN)

B. 內部區域網路 (Local Area Network, LAN)：公司內部單位人員及內部伺服器使用之網路區段。

(2) 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

(3) 公司應定期檢視防火牆政策是否適當，並適時調整規則。

(4) 公司內部網路之區域應做合理之區隔，使用者應經授權並在授權之範圍內存取網路資源。

(5) 對網路系統管理人員或資訊安全主管人員的操作，均應建立詳細的紀錄。

(6) 使用者應依公司規定之方式存取網路服務。

(二)資訊業務權限管理

(1) 公司之資訊業務應設置通行碼管理，且通行碼之要求需被滿足：

A. 通行碼長度應為 8 碼(含)以上。

B. 使用者每 90 天應更換一次通行碼。

(2) 使用者辦理資訊業務前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

(3) 資訊使用者無繼續辦理資訊業務時，應立即停用或移除使用者 ID，資訊業務管理者應定期清查使用者之權限。

(三)特權帳號之存取管理

(1) 資訊設備之特權帳號應經正式申請授權才能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

(2) 資訊設備之特權帳號不得共用。

(3) 對於特權帳號，應指派與該使用者日常公務使用之不同使用者 ID。

(4) 資訊設備之管理者每年應清查系統特權帳號並劃定特權帳號逾期之處理方式。

(四)作業與通訊安全管理

(1) 防範惡意軟體之控制措施

A. 公司之主機及個人電腦應安裝防毒軟體，並進行軟、硬體之必要更新或升級。

B. 管理者應每年定期針對管理之設備進行軟體清查。

C. 使用者不得私自使用已知或有嫌疑之惡意網站。

D. 使用者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(2) 遠距工作之安全措施

公司不開放遠距工作，為特殊狀況得以申請使用。

(3) 電子郵件安全管理

A. 使用者使用電子郵件時應提高警覺，並使用純文字模式瀏覽，避免讀取來歷不明之郵件或含有巨集檔案之郵件。

B. 電子郵件原則不得傳送機密性或敏感性之資料，如有業務需求者應依相關規定進行加密或其他之防護措施。

C. 不得利用公司所提供電子郵件服務從事侵害他人權益或違法之行為。

D. 使用者應確保電子郵件傳送時之傳遞正確性。

E. 應配合公司辦理電子郵件社交工程演練，並檢討執行情形。

(4) 資訊安全需求分析，每年須定期審視，其應包括：

A. 系統及資料之存取控制方式，尤其是機敏資料存取控制。

B. 建立系統及相關設備適當之監控措施，包含身分驗證存 取紀錄（如：失敗登入、非作 業時間登入、多位使用者使用 同一來源 IP 登入成功等）、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，並針對日誌建立適當之 保護機制。

C. 系統應經由使用者代碼及密碼授權管制方式，確保處理的有效性及資料的真實性。

D. 應保護系統避免未經授權的竄改或是修改。

E. 資料應定期複製備份。

F. 除了定期複製備份外，對於版本更新、重大處理及大量資料異動等情形，均應先行備份再予處理，以確保資料安全。

G. 應視各單位之要求，對高敏感性的資料，在傳輸或儲存過程中以加密方法保護。

H. 建立遠端存取系統之管控機制，如：建立安全的遠距連線機制（如：VPN、VDI）、採多重身分驗證、採加密連線、採最小授權原則、留存完整使用 者操作稽核軌跡、監控與警示 異常操作行為、執行安全性漏洞更新等安控措施，並教育居家辦公者應對網路風險保持警覺等。

(五)確保實體與環境安全措施

(1) 通訊機房(機櫃)之管理

A. 通訊機房(機櫃)應進行實體隔離。
B. 公司人員或來訪人員應申請及授權才可以進入通訊機房(機櫃)，其管理者應定期檢視授權人員之名單。
C. 人員進入管制區應隨時注意身分不明或可疑人員。
D. 僅於必要時，得准許外部支援人員進入通訊機房(機櫃)。
E. 人員及設備進出通訊機房(機櫃)應留存記錄。

(2) 通訊機房(機櫃)之環境控制
A. 機房(機櫃)之空調、電力得建立備援措施。
B. 機房(機櫃)得安裝安全偵測及防護措施，包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統，以減少環境不安全所引發之危險。
C. 各項安全設備應定期執行檢查、維修，並應定時針對設備之管理者進行適當之安全設備使用訓練。

(3) 辦公室區域之實體與環境安全措施
A. 應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
B. 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。
C. 機密性及敏感性資訊，不使用或下班時應該上鎖。
D. 機密資訊或處理機密資訊之資訊業務應避免存放或設置於公眾可接觸之場所。
E. 顯示存放機密資訊或具處理機密資訊的業務地點，其通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。
F. 資訊或資訊業務相關設備，未經管理人授權，不得被帶離辦公室。

(六)資料備份
(1) 重要資料應進行資料備份，其備份之頻率應滿足復原時間點之目標要求，並執行異地存放。
(2) 確認重要資料備份，而非直接於覆寫回原資訊設備。
(3) 敏感或機密性資訊之備份應加密保護。
(4) 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

(七)電腦使用之安全管理
(1) 電腦作業系統，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能。
(2) 禁止私自安裝點對點檔案及分享軟體或未經合法授權之軟體。
(3) 連網電腦應隨時配合更新作業系統、應用程式漏洞及修補程式或防毒碼等。
(4) 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞及修補程式或防毒碼等。
(5) 下班時應關閉電腦及螢幕電源。
(6) 如發現資安問題，應主動依循公司之通報程序通報。

(八)行動設備之安全管理

(1) 機密資料不得由未經許可之行動設備存取、處理或傳送。
(2) 機敏會議或場所不得攜帶未經許可之行動設備進入。

(九)電子郵件之安全管理

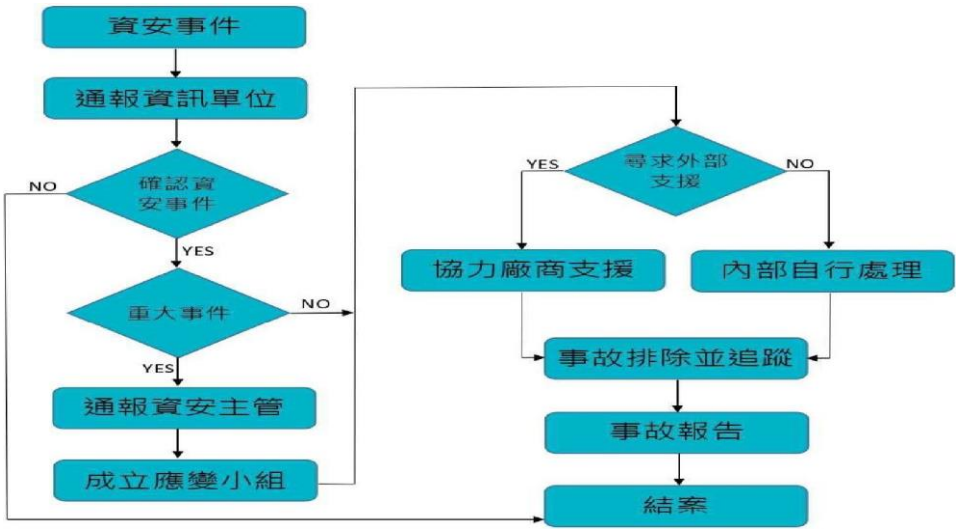
(1) 電子郵件接收後應自行管控其安全性。
(2) 敏感性資訊如有電子郵件傳送之必要，須經加密處理後傳送。
(3) 為防範假冒本公司員工名義發送電子郵件，並達到身分辨識及不可否認的目地，必要時應以電子簽章方式發送電子郵件。
(4) 對來路不明的電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞；並應通知電子郵件系統管理者處理。
(5) 禁止發送電子郵件騷擾他人，導致其他使用者之不安與不便。
(6) 禁止發送匿名信，或偽造他人名義發送電子郵件。
(7) 電子郵件服務器，需具備過濾機制(目前防火牆功能有具備)。

(十)網路入侵之處理

(1) 若發現網路被入侵或疑似被入侵時(如：網頁遭竄改、分散式攻擊、資料非法存取、密碼被破解等)，應立採取必要的行動。
(2) 立即拒絕入侵者任何存取動作，防止災害繼續擴大；當防護網被突破時，統一設定拒絕任何存取；或入侵者已被嚴密監 控，在不危害內部網路安全的前題下，得適度允許入侵者存取 動作，以利追查入侵者。
(3) 切斷入侵者的網路連接，如無法切斷則必須關閉防火牆；或為達到追查入侵的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的網路連接。
(4) 應全面檢討網路安全措施及修正防火牆的設定，以防範類似的入侵與攻擊。
(5) 應正式記錄入侵的情形及評估影響的層面。立即向權責主管人員報告入侵情形。並向相關緊急處理小組反應，以獲取必要的外部協助。

十、資訊安全事件通報、應變及演練相關機制

為即時掌控資訊安全事件，並有效降低其所造成之損害，公司應訂定資訊安全事件通報、應變及演練相關機制，詳資訊安全事件通報應變程序。



十一、 資訊安全情資之評估及因應

公司接獲資訊安全情資，應評估該情資之內容，並視其對公司之影響、公司可接受之風險及公司之資源，決定最適當之因應方式，必要時得調整資訊安全維護計畫之控制措施，並做成紀錄。

1. 資訊安全情資之分類評估

公司接受資訊安全情資後，應指定資訊安全專責(兼職)人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一)資訊安全相關之訊息情資

資訊安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資訊安全相關之訊息情資。

(二)入侵攻擊情資

資訊安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三)機敏性之情資

資訊安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或情資之公開提供有侵害公司、個人、其他團體之權利，或涉及公司機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四)涉及核心業務、核心資訊系統之情資、涉及關鍵基礎設施營運之核心業務、核心資訊系統之運作等內容，屬涉及核心業務。

2. 資訊安全情資之因應措施

公司於進行資訊安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資訊安全維護計畫之控制措施。

(一)資訊安全相關之訊息情資

彙整情資後進行風險評估，並依據資訊安全維護計畫之控制措施採行相應之風險預防機制。

(二)入侵攻擊情資

由資訊安全專責(兼職)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資訊安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三)機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四)涉及核心業務、核心資訊系統之情資應評估其是否對於公司之運作產生影響，並依據資訊安全維護計畫採行相應之風險管理機制。

(五)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

(1) 國家資安資訊分享與分析中心(https://www.nics.nat.gov.tw/)

(2) 台灣電腦網路危機處理暨協調中心(https://www.twcert.org.tw/)

(六)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)「企業資安事件應變處理指南」。

十二、 資訊系統或服務委外辦理之管理

公司目前如有委外辦理資訊系統之建置、維護營運或資訊服務需求，應考量對方之專業能力與經驗、委外項目之性質及資訊安全等項目後，選任適當之廠商並監督其資訊安全執行情形。

1. 徵求委外資訊服務應注意事項

(一)受託者辦理受託業務之相關程序及環境，應具備完善之資訊安全管理措施或通過第三方驗證。

(二)受託者應配置充足且經適當之資格訓練、擁有資訊安全專業證照或具有類似業務經驗之資訊安全專業人員。

(三)受託者應具備相關資訊安全維護措施。

(四)受託者接受委託業務時，若涉及國家機密者，應考量受託業務所涉及國家機密之機密等級內容，並相關公告或契約文件中，註明受託者辦理該項業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家業務人員及可能接觸該國家機密人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

(五)前點適任性查核得在必要範圍內就下列事項查核，查核前應經當事人書面同意：

(1) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案者。

(2) 曾任公務人員因違反相關安全保密規定，受懲戒處分、記過以上行政懲處者。

(3) 曾受到外國政府、大陸地區或香港、澳門官方之利誘、脅迫，從事不利國家安全或重大利益情事者。

(4) 其他與國家機密保護相關之具體項目。

2. 監督受託者資訊安全維護情形應注意事項

(一)受託者應提供該資訊系統之受託業務包括客製化資訊系統開發者，受託者應提供該資訊系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(二)受託者執行受託業務，違反資訊安全相關法令或知悉資訊安全事件時，應於1小時內通知委託公司及採行之補救措施。

(1) 資訊系統遭竄改。

(2) 系統之運作受影響或停頓。

(三)委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

(四)受託者應採取之其他資訊安全相關維護措施。

(五)公司應定期或於知悉受託者發生可能影響受託業務之資訊安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

十三、 資訊安全教育訓練

1. 資訊安全教育訓練要求

(一)資安兼任或資訊人員每人每年至少接受 6 小時以上之資安專業課程訓練。

(二)本公司同仁每年至少接受 3 小時以上之一般資訊安全教育訓練。

2. 資訊安全教育訓練辦理方式

(一)資安防護組應於每年初，考量管理、業務及資訊等不同工作類別之需求，擬定資訊安全認知宣導及教育訓練計畫，以建立員工資訊安全認知，提升公司資訊安全水準，並應保存相關之資訊安全認知宣導及教育訓練紀錄。

(二)公司資訊安全認知宣導及教育訓練之內容得包含：

(1) 資訊安全政策。

(2) 資訊安全法令規定。

(3) 資訊安全作業內容。

(4) 資訊安全技術訓練。

(三)員工報到時，應使其充分瞭解公司資訊安全相關作業規範及其重要性。

(四)資訊安全教育及訓練之政策，除適用所屬員工外，對公司外部的使用者，應一體適用。

十四、 公司員工涉及資訊安全事項之考核機制

本公司員工資訊安全意識皆納入考核，並依據員工考績管理辦法及員工獎懲管理辦法執行。

十五、 資訊安全維護計畫及實施情形之持續精進及績效管理機制

1. 資訊安全維護計畫之實施

為落實本安全維護計畫，使資訊安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與公司之資訊安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

2. 資訊安全維護計畫實施情形之稽核機制

(一)稽核機制之實施

(1) 資訊安全長應定期(至少兩年一次)或於系統重大變更或組織改造後執行一次內部稽核作業。

(2) 辦理稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

(3) 辦理稽核時，資訊安全長應於執行稽核前，通知受稽核單位，並明確將稽核資訊(包含查核期間、樣本資料區間、查核項目及樣本資訊)等提供受稽單位。

(4) 公司之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦之業務，以確保稽核過程之客觀性及公平性，應將稽核查檢表內容彙整至稽核

報告及改善追蹤報告中，並提供給相關權責主管簽核。

(5) 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資訊安全稽核計畫及稽核事件之證據。

(6) 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（例如：是否瞭解資訊安全政策及應負之資安責任、是否訂定人員之資訊安全作業程序與權責、是否定期更改密碼。

(二)稽核改善報告

(1) 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研擬改善措施、改善進度規劃，並落實執行。

(2) 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

(3) 受稽單位於判定缺失或待改善之原因後，應提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資訊安全管理制度或相關文件進行變更。

(4) 公司應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

(5) 受稽單位於執行改善措施時，應留存相關之執行紀錄，並將改善方式及其結果填寫改善報告。

3. 資訊安全維護計畫之持續精進及績效管理

(一)公司之資訊安全長應於每年定期召開資訊安全管理審查會議，確認資訊安全維護計畫之實施情形。

(二)管理審查議題應包含下列討論事項：

(1) 過往管理審查議案之處理狀態。

(2) 與資訊安全管理業務有關之內部及外部議題的變更，如法令變更、上級公司要求、資訊安全長決議事項等。

(3) 資訊安全維護計畫內容之適切性。

(4) 資訊安全績效之回饋。

(5) 資訊安全政策及目標之實施情形。

(6) 資訊安全人力及資源之配置之實施情形。

(7) 資訊安全防護及控制措施之實施情形。

(8) 內外部稽核結果。

(9) 不符合項目及矯正措施。

(10) 風險評鑑結果及風險處理計畫執行進度。

(11) 重大資訊安全事件之處理及改善情形。

(12) 利害關係人之回饋。

(13) 持續改善之機會。

(三)持續改善機制之管理審查應做成追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

(四)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。

十六、 施行

1. 本計劃經總經理通過後實施，修正時亦同。
2. 本計劃訂立於中華民國 113 年 08 月 01 日。
   第一次修訂於中華民國 113 年 09 月 20 日。