

啓基科技資訊安全政策聲明

1 目的

- 1.1 為維護本公司資訊安全理念，對於本公司所儲存或傳遞之資訊應作周全保護與防範，以杜絕毀損、失竊、洩漏、篡改、濫用與侵權等資訊安全風險。本公司制訂資訊安全政策，依循 ISO/IEC 27001:2022 及 TISAX 等國際資安標準規範，落實 Plan-Do-Check-Act(PDCA)循環運作模式，作為全體同仁遵循之準則，以確保各項資訊媒體之安全。
- 1.2 本公司資訊安全目標為「機密」、「完整」、「可用」及「法律遵循」。各相關部門應依公司資訊安全政策及整體目標，建立與推動適當之資訊安全指標及控制措施，定期評估其執行成效，並依評估結果採取必要之改善措施，以持續維持及提升資訊安全管理制度（Information Security Management System，以下簡稱「ISMS」）之有效性。各單位應至少每年檢視所屬資訊安全指標之適切性，並依程序提報資訊安全委員會核定及更新相關指標紀錄。

2 適用範圍

2.1 適用廠區

本資訊安全政策適用於本公司及經核定納入資訊安全管理範圍之所屬相關企業與廠區。

2.2 適用人員

本公司內部所有正式員工、約聘員工、派遣員工、臨時僱員等公司所聘用之人員以及訪客及供應商等。

2.3 適用標準與要求

本政策依循包含但不限於 ISO/IEC 27001:2022、TISAX 管理要求之適用資訊安全標準、規範及要求，並應遵循適用之法令、法規、客戶契約及其他與資訊安全相關之要求。

2.4 供應商

供應商於提供服務過程中如涉及存取、處理、儲存或傳輸本公司資訊，應遵循本公司資訊安全政策、ISMS 相關規範、契約及工作說明書所定之資訊安全要求，並配合本公司採取必要的資訊安全防護措施，以維護資訊之機密性、完整性及可用性。

3 資訊安全政策聲明

為使本公司 ISMS 有效運作，並保障本公司適用範圍內各營運據點之資訊資產安全，特頒佈本政策聲明，作為全公司資訊安全之最高指導原則。

3.1 落實資訊安全，保護營業秘密

所有資訊作業應確保資訊資產之機密性、完整性及可用性。應針對核心營業秘密選擇適切之保護措施，降低未經授權之存取、竄改、破壞或不當揭露。本公司應依資訊資產之機密等級及相關程序，對資訊資產之保管、儲存、使用、傳送、移轉、返還、報廢及銷

毀採取適當之保護措施。資訊資產之檢視、使用、存取及異動，應限於取得適當授權之人員，並依業務需要及核准權限辦理。本公司應依業務需求及資訊安全風險，適當區隔相關工作職掌，並依人員職責及業務需要授予完成工作所需之必要權限。所有人員不得於本公司資訊資產上安裝、使用或下載非法或未經授權之軟體。

3.2 強化產品資安，符合客戶與市場要求

支支援產品生命週期各階段之安全性，建立並實施產品安全開發、維護及支援流程，將產品安全要求融入產品需求定義、設計、實作、測試、發行、更新及事件管理等階段，以提升產品安全品質、確保流程之透明度、可追溯性及品質控制。詳細作法依產品安全相關程序辦理。

3.3 法規遵循、永續發展與持續營運

本公司應遵循包含但不限於資訊安全相關法令、客戶合約義務及適用之國際標準與管理要求，並依營運衝擊分析及風險評鑑結果，建立資訊作業持續營運及災害復原計畫，以因應可能造成資訊作業中斷、營運影響、生產中斷、財務損失或其他重大影響之資訊安全事件、駭客攻擊或入侵、惡意程式感染、未經授權存取、資訊外洩、網路或資訊系統異常，以及其他與資訊安全相關之事故、危機及緊急狀況。當發生上述情況時，應依相關計畫執行通報、應變及復原作業，以降低對關鍵業務之影響，並於最大可容忍中斷時間內恢復運作。

本公司響應永續發展政策，於資訊設備及相關服務之採購、使用、維護及汰換過程，依公司永續、採購及相關管理規範，適度考量資源使用效率、節能、環境影響及設備生命週期等因素。

3.4 資安教育訓練，全員參與

本公司應依公司教育訓練計畫及程序辦理資訊安全教育訓練與宣導，並依人員職務、業務需求及資訊安全風險，規劃適當之教育訓練主題。訓練主題包含但不限於資訊安全通識、社交工程防範及資訊安全事件通報與應變等內容，並應教導新進人員了解資訊安全政策、資訊安全事件的處理與應變程序及相關規範；必要時，應評估教育訓練及宣導之有效性。

3.5 資安事件通報、應變與必要揭露

本公司應建立正式之資訊安全事件通報程序及管道。公司員工及與本公司有業務往來之外部單位及其人員，發現或疑似發生資訊安全事件、安全弱點或違反資訊安全政策與規範之情事時，應即時通報本公司。相關權責單位將依事件影響範圍進行必要的應變處理，並於必要時向受影響之內外部單位揭露相關資訊。

疑似資訊安全事件發生時，應立即以電子郵件寄送至 security.issues@wnc.com.tw，或向資訊安全事件通報受理窗口通報，並說明事件發生時間、現象及可能來源，以協助判斷

是否屬於資訊安全事件及其可能影響之資訊作業範圍。

資訊安全事件應依相關程序辦理分級、應變、處理、追蹤及結案；如涉及客戶、合作廠商、主管機關或其他外部利害關係人，應依相關法令、契約及公司程序辦理必要之對外通報、處理進度通知及資訊揭露，並由投資人與公共關係部主管擔任對外發言窗口，統一辦理對外資訊發布。

資訊安全事件應依其影響範圍及程度分為下列三級；如事件情形同時符合一個以上等級，應以較高等級認定：

3.5.1 嚴重資訊安全事件：造成公司重大損害或影響，並達法規要求之資訊安全事件。

3.5.2 重大資訊安全事件：影響公司生產、出貨或直接影響公司商譽之資訊安全事件。

3.5.3 一般資訊安全事件：非屬直接影響生產、出貨或公司商譽之資訊安全事件。

資訊安全事件之負責單位接獲通報後，應立即依相關程序進行回應與處理，並於規定時間內完成。重大資訊安全事件應由緊急應變小組召集相關單位，於4小時內完成相關處理；一般資訊安全事件應於16小時內完成相關處理。若一般資訊安全事件無法於規定時間內解決，該負責人應立即向其直屬主管報告，並考量將事件升級為重大資訊安全事件。資訊安全事件確認後，應依事件等級及影響範圍，於24小時內通知受影響之內部單位；如涉及客戶、合作廠商、主管機關或其他外部利害關係人，應依相關法令、契約及公司程序，由權責單位辦理必要之資訊通報、處理進度通知及資訊揭露。資訊安全事件處理過程，應對受影響之內部及外部利害關係人提供適當、及時且必要之資訊。事件處理完成後，應依相關紀錄檢討事件原因、類型及影響範圍，採取改善及減緩措施，以降低事件再發生之可能。

3.6 資安事件檢討與持續改善

資訊安全事件處理完成後，應依相關紀錄檢視事件發生原因、事件類型及影響範圍，研擬並執行適當之改善措施，以降低事件再發生之可能，並持續提升 ISMS 及資訊安全事件處理之有效性。事件檢討所產出之 Lesson Learned，應依相關程序回饋至資訊作業持續營運及災害復原計畫，並視需要納入後續營運持續（BCP）或災害復原演練之情境、應變程序及改善事項，以強化本公司對資訊作業中斷及其他緊急狀況之應變與復原能力。

4 資訊安全管理目標

本公司資訊安全管理目標，係指透過客觀且可量化之資訊安全指標，定期評估資訊安全控制措施之有效性，以掌握 ISMS 之運作情形。

各單位應至少每年一次檢視所屬資訊安全指標之合適性，並將檢視結果提報管理審查會議核定；經核定後，依程序更新資訊安全指標彙總表，作為下一年度資訊安全指標。

5 資訊安全責任

本公司建立資訊安全管理組織，明定資訊安全委員會、資訊安全單位、各部門、使用者及資訊作業供應商之責任，以確保 ISMS 有效運作及落實執行。

5.1 資訊安全委員會

資訊安全委員會負責資訊安全管理政策、策略及 ISMS 之審查與核定，並執行下列事項：

- 5.1.1 界定 ISMS 之適用範圍，並研議、審查資訊安全政策、策略及相關管理規範。
- 5.1.2 指定相關人員執行資訊安全風險評鑑，審查風險評鑑結果與風險處置對策，並核定資訊資產分類、可接受風險水準、適用控制措施及所需資源。
- 5.1.3 核定各單位資訊安全指標，並檢視其達成情形。
- 5.1.4 審查 ISMS 之內部查核結果、矯正及預防措施之執行進度，並追蹤改善情形。
- 5.1.5 審視客戶合約等利害關係人之資訊安全要求，並確認相關要求以納入 ISMS 之管理。
- 5.1.6 審查資訊安全事件及其處理情形，必要時核定相關改善或處置措施。
- 5.1.7 核定資訊作業持續營運計畫、營運衝擊分析結果及所需投入之資源。
- 5.1.8 召開或參與 ISMS 管理審查會議，評估資訊安全政策、策略、目標及 ISMS 之適切性、充分性與有效性，並決議持續改善事項及 ISMS 之變更需求。

5.2 資安執行小組

資安執行小組應依資訊安全委員會之決議，推動及執行 ISMS 相關管理作業，並彙整執行成果及改善狀況提報資訊安全委員會審查。

- 5.2.1 執行資訊安全風險評鑑，並規劃風險處置對策。
- 5.2.2 協助資訊安全委員會規劃及訂定各項控制措施與處理程序。
- 5.2.3 推動及執行 ISMS 各項控制措施與處理程序。
- 5.2.4 彙整及分析 ISMS 之各項資訊安全指標。
- 5.2.5 執行內、外部資安查核改善事項及矯正預防措施。
- 5.2.6 規劃及實施資訊安全教育訓練。
- 5.2.7 識別適用之資訊安全相關法令規定。
- 5.2.8 執行 ISMS 內部自行查核，並追蹤不符合事項之改善情形。

5.3 緊急應變小組

- 5.3.1 重大資訊安全事件發生時，召集相關成員，統籌事件評估、應變、協調、聯絡、層報及調查作業。
- 5.3.2 領導緊急應變處理計畫之執行，並協調資源之調派使用。

- 5.3.3 掌握事件資訊、進行決策與層報，並依事件影響範圍通知受影響之內部及外部單位，包含客戶及合作廠商。
- 5.3.4 召集相關資訊業務人員，發展、維護、更新及執行各項資訊業務災害復原程序。
- 5.3.5 協調內部相關單位及外部廠商，確保支援設備及所需資源充足，並取得緊急所需之額外資源。
- 5.3.6 負責災害現場之損害評估、現場指揮、災後協調及原營運場所復原工作。
- 5.3.7 協助各單位於災後檢視、確認及改善相關架構，並檢視公司資訊安全架構及提出改善建議。

5.4 資安查核小組

5.4.1 資安查核小組組長

- 5.4.1.1 召開資安查核小組會議
- 5.4.1.2 協調及分派 ISMS 自行查核工作

5.4.2 資安查核小組組員

- 5.4.2.1 擬定 ISMS 自行查核計畫
- 5.4.2.2 執行 ISMS 自行查核
- 5.4.2.3 撰寫 ISMS 自行查核報告
- 5.4.2.4 追蹤不符合事項之改善執行情形

5.5 追蹤不符合事項之改善執行情形

- 5.5.1 各部門及使用者應遵守本公司資訊安全政策、ISMS 相關規範及所屬業務之資訊安全要求。
- 5.5.2 各部門及使用者應配合 ISMS 之執行，包括資訊安全教育訓練、查核及相關改善事項。
- 5.5.3 發現疑似資訊安全事件、安全弱點或違反資訊安全政策與規範之情形時，應依相關程序進行通報。
- 5.5.4 各部門及使用者應配合資訊安全事件之處理及改善作業。

5.6 資訊作業供應商

- 5.6.1 遵循本公司資訊安全政策、ISMS 相關規範及契約要求。
- 5.6.2 配合委外作業資訊安全風險評鑑及相關安全要求。
- 5.6.3 於服務期間遵守契約規範，長期服務者應依合約及工作說明書要求，定期提交服務水準報告予業務負責人審核備查。
- 5.6.4 人員或作業內容異動時，事先通知並取得本公司核准。
- 5.6.5 服務中止或結束時，返還本公司資訊資產並移除相關存取權限。

6 資訊安全管理制度 (ISMS)

6.1 一般要求

本公司依 ISO/IEC 27001:2022 之要求建立、紀載、實施及維護 ISMS，以確保資訊資產及資訊系統獲得適當保護，並持續改善 ISMS 之有效性。

6.2 運作方式

本公司採用 PDCA 循環模式運作 ISMS，透過規劃(Plan)、執行(Do)、查核(Check)及改善(Act)，持續維持 ISMS 之有效運作。

6.2.1 規劃與建立 (Plan)

依據本公司整體策略與目標，藉由成立資訊安全委員會，控制潛在之威脅及漏洞，規劃風險評鑑、設計與建置控管機制，以建立 ISMS。

6.2.1.1 針對 ISMS 範圍內之資訊資產建立及維護，作為資訊資產管理及風險評鑑之依據。

6.2.1.2 依資訊資產之機密性、完整性及可用性評估資產價值。

6.2.1.3 依現有控制狀況評估資訊資產之弱點及所面臨之威脅，並考量其可能造成之影響。

6.2.1.4 綜合資訊資產價值、弱點及威脅進行風險評鑑，量化資訊資產所面臨或潛在之風險程度，作為選擇控制措施之依據。

6.2.1.5 對高於可接受風險水準之風險事項，應列入風險改善計畫，並依風險評鑑結果選擇適當之控制措施；可接受風險水準、控制措施及所需資源，應經資訊安全委員會核定。

6.2.2 實施與運作 (Do)

依據評估規劃之結果，建立或修正應有之管控機制。

6.2.2.1 維護 ISMS 範圍內之各類資訊資產，並建立及更新資訊資產清冊。

6.2.2.2 明確劃分資訊資產之保管責任，並指定適當之資訊資產擁有者、保管者及使用
者。

6.2.2.3 依資訊資產之機密性、完整性及可用性，落實資訊資產分類及相關保護要求。

6.2.2.4 依資訊安全委員會核定之可接受風險水準，執行風險處理及風險改善計畫。

6.2.2.5 對高於可接受風險水準之高風險項目，指定風險項目管理擁有者及改善負責人，並執行風險改善計畫。

6.2.2.6 依 ISO 27001 適用性聲明書實施適用之控制措施。

6.2.2.7 依 ISMS 相關政策、管理程序及作業規範執行資訊安全管理作業。

6.2.2.8 各單位資訊資產清冊管理人員每半年檢視所負責之資訊資產清冊；各單位主管覆核資訊資產分類及清冊內容是否更新至目前現況。

6.2.2.9 ISMS 運作所產生之文件、表單及紀錄，應依文件管制作業程序辦理管制、保存期限及核閱權限管理。

6.2.3 監督與稽核 (Check)

監督 ISMS 各項作業之落實執行，並評估及稽核其有效性。

6.2.3.1 資訊安全指標應為客觀且可量測之指標，涵蓋機密性、完整性及可用性，並訂定指標內容、目標值、量測週期、資訊來源及負責人員。

6.2.3.2 各單位應依各項指標之量測週期，蒐集資料並進行統計、分析及評估，計算資訊安全指標值，保存相關紀錄並經單位主管核定。

6.2.3.3 資訊安全指標彙整權責人員應彙整各單位指標及相關紀錄，於管理審查會議中說明指標達成情形及分析評估結果。

6.2.3.4 各單位至少每年檢視資訊安全指標之適切性；經管理審查會議核定後，更新資訊安全指標彙總表，作為後續年度指標。

6.2.3.5 各單位資訊資產清冊管理人員應每半年檢視資訊資產清冊之完整性、正確性及現況；各單位主管應覆核資訊資產分類及清冊更新情形。

6.2.3.6 風險評鑑執行人員應每半年執行風險評鑑，並將現有控制狀況、利害關係人要求及內外部議題納入評估。

6.2.3.7 管理階層應依規劃之期間執行 ISMS 內部稽核，確認控管目標、控制措施及相關程序符合適用標準、法令規章及資訊安全需求。

6.2.3.8 應依紀錄及追蹤資訊安全事件之處理狀況；事件處理完成後，應依相關紀錄檢視事件發生原因、類型及影響範圍，並重新檢視 ISMS 是否有不足之處。

6.2.3.9 應執行資訊安全監控中心 (Security Operations Center, SOC) 之日常維運，持續監督及量測資訊安全管理與技術防護之運作情形，包括資安系統管理、監控、疑似異常行為分析、告警及相關紀錄檢視。管理面與技術面之監督及量測應同步進行，並依監控及分析結果追蹤異常、評估風險，必要時協同相關單位辦理資訊安全事件之回應、分析、處置、減緩及改善。

6.2.4 維護與改進 (Act)

根據監督稽核之結果與建議，執行矯正措施，改善並執行應有之控管機制，以持續維護 ISMS 之運作。

6.2.4.1 持續改善

6.2.4.1.1 透過內部及外部第三方稽核結果、資訊安全事件分析、矯正措施及管理審查，持續增進 ISMS 之有效性。

6.2.4.1.2 資訊安全事件處理完成後，應依相關紀錄檢視事件發生原因、事件類型及影響範圍，並重新檢視 ISMS 是否有不足之處，並採取必要之改善措施。

6.2.4.1.3 如有需要，應提出改善方案或新增控制措施，並依相關程序呈管理審查會議核定。

6.2.4.2 矯正措施

6.2.4.2.1 對 ISMS 建置及運作過程所發現之不符合事項，應識別不符合事項及其原因。

6.2.4.2.2 評估所採取之措施，以避免不符合事項不再重複發生。

6.2.4.2.3 決定並執行必要之矯正措施。

6.2.4.2.4 紀錄矯正措施之執行結果，並審查其有效性。

6.2.4.3 管理審查

6.2.4.3.1 資訊安全委員會至少每半年執行一次管理審查，以確保 ISMS 之適切性、充分性及有效性。

6.2.4.3.2 管理審查應考量下列事項：前次管理審查之後續追蹤、可能影響 ISMS 之內部或外部環境之改變、ISMS 執行之回饋、來自利害關係人之回應或要求事項、風險評鑑結果與風險處理計畫之狀態，以及其他持續改進之建議。

6.2.4.3.3 管理審查應評估 ISMS 之改善方案及變更需求，包括資訊安全政策及資訊安全目標之變更需求。

6.2.4.3.4 管理審查結果應予詳實紀錄並妥善保存。

6.3 ISMS 文件及紀錄管制

6.3.1 文件管制

6.3.1.1 ISMS 相關文件應依文件分類及編號規則建立，並明確規範文件之編寫、核發、修訂、保存及分發方式。

6.3.1.2 ISMS 文件新增、修訂或作廢時，應由權責單位辦理審查並經權責主管核准後始生效。

6.3.1.3 文件修訂時，應識別文件版次及修訂內容；文件版次應依文件管制作業程序之規定管理，並詳實記載修訂內容。

6.3.1.4 ISMS 文件之發行及取用應依權限進行管制，確保使用單位取得有效版本。紙本文件改版時，應依文件管制作業程序回收舊版並換發新版；作廢文件如因法規、技術或知識保存等需求留存，應清楚標示「作廢」以資識別。無須留存之舊版文件及含有資訊資產之儲存媒體，應依其機密等級、媒體類型採取適當之

資料清除、消磁、破壞、碎紙或其他銷毀方式；其中紙本或文件類銷毀方式，參考 ISO 21964 Level 4 及 Level 3 辦理。涉及事業廢棄物之銷毀，應依事業廢棄物儲存清運管制程序辦理。

6.3.1.5 外來文件應予以識別、申請、保存及管制；其原始電子檔案或紙本由 DCC 存檔保管。

6.3.1.6 文件應妥善保存並防止機密內容外洩。作廢文件之回收、銷毀及相關紀錄，應依文件管制作業程序及本政策 6.3.1.4 辦理；因法規、技術或知識保存等需求而留存之舊版文件，應加蓋「作廢章」或以其他適當方式清楚標示，以避免誤用。

6.3.2 紀錄管制

6.3.2.1 ISMS 運作所產生之表單及紀錄，應依文件管制作業程序之文件編號、版次、保存及取用等相關要求辦理。

6.3.2.2 文件之分發、回收、借閱及銷毀，應依文件管制作業程序辦理，並留存必要之文件管制紀錄；相關紀錄之保存、查閱及取用，應依文件管制要求辦理。

7 管理階層責任

7.1 管理階層承諾

為確保 ISMS 有效運作，管理階層應：

7.1.1 核定、宣導及督導資訊安全政策，並確保資訊安全責任獲得適當分配及協調。

7.1.2 透過資訊安全管理組織，推動、協調及督導資訊安全管理事項。

7.1.3 確保資訊安全目標與公司資訊安全政策方向一致，並定期檢視其達成情形。

7.1.4 依資訊資產暨風險評鑑管理程序核定可接受風險水準，並依風險評鑑結果核定控制項目及所需資源。

7.1.5 管理階層應督導資訊風險評鑑及 ISMS 內部稽核之執行，並由資訊安全委員會執行 ISMS 管理審查。

7.1.6 資訊安全委員會至少每半年執行一次管理審查，檢視 ISMS 之適切性、充分性及有效性。

7.2 資源管理

管理階層應提供建立、實施、運作、監視、審查、維持及改善 ISMS 所需之資源，並確保資訊安全相關人員履行其職責。

資訊安全教育訓練及宣導應依教育訓練程序書辦理。

7.3 有效溝通

本公司應依內外部議題及利害關係人之需求與期望，決定 ISMS 相關之內部及外部溝通事項，並確保資訊安全政策、目標、責任及相關要求獲得適當宣導與傳達。

8 內部稽核

- 8.1 本公司每年至少執行一次 ISO 27001 ISMS 內部稽核；如發生重大資訊安全事件、重大缺失或其他必要情形，得依內部品質稽核程序執行不定期稽核。稽核應確認 ISMS 及其控管目標、控制措施與相關程序之符合性及有效性。
- 8.2 內部稽核應依內部品質稽核程序所定之稽核計畫、範圍、準則及方法辦理。
- 8.3 內部稽核發現不符合事項，應識別其原因，評估及決定必要之矯正措施，並紀錄及審查矯正措施之有效性。
- 8.4 內部稽核結果及改善情形應提供資訊安全委員會審查，並作為 ISMS 持續改善及管理審查之依據。

9 ISMS 之管理審查

9.1 審查頻率與召集

資訊安全委員會每半年召開一次管理審查會議；必要時，得召開臨時會議，或以公文書審方式辦理。會議由資訊安全委員會召集人召集。

9.2 審查內容

管理審查應依 ISMS 及相關程序，檢視資訊安全政策、策略、ISMS 相關規範、資訊安全目標及其執行情形，並審查下列事項：

- 9.2.1 前次管理審查之後續追蹤；
- 9.2.2 可能影響 ISMS 之內部或外部環境之改變；
- 9.2.3 ISMS 執行之回饋，包括資訊安全指標達成情形、ISMS 查核結果、資訊安全事件及改善措施等；
- 9.2.4 來自利害關係人之回應或要求事項；
- 9.2.5 風險評鑑結果及風險處理計畫之狀態；
- 9.2.6 其他持續改進之建議。

管理審查亦應檢視資訊安全政策、策略、ISMS 相關規範、資訊安全目標及其執行情形，並評估 ISMS 之適切性、充分性及有效性。資訊安全指標之統計、分析及評估結果，應由資訊安全指標彙整權責人員於資訊安全委員會中說明；指標未達目標值時，應辦理矯正措施。

9.3 審查輸出

管理審查結果應包括資訊安全政策、目標或 ISMS 之變更需求、持續改善事項、風險處理或控制措施調整，以及所需資源之決議。

9.4 審查決議與紀錄

管理審查應依審查結果決定資訊安全持續改善、ISMS 變更需求及資源提供方式與範圍。會議過程應留存紀錄，經核准後妥善保存，並依資訊資產機密等級予以保護。

10 ISMS 之改善

10.1 改善措施之啟動

本公司應依資訊安全事件、風險評鑑結果及資訊安全指標達成情形，識別改善需求，並依相關程序採取矯正措施或風險改善措施。

10.2 改善措施之執行

風險改善措施完成後，應依資訊資產暨風險評鑑管理程序重新評估風險，並依評估結果持續執行風險辨認及降低風險措施，直到風險降至可接受水準為止。內部稽核所發現之不符合事項，應依內部品質稽核程序辦理稽核、改善追蹤及確認；內、外部稽核所發現之不符合事項，應依矯正與預防措施程序完成原因分析、執行矯正措施及必要之預防措施，並由權責人員追蹤改善執行情形及確認其有效性；未完成或成效未確認者，應持續追蹤至改善完成。

10.3 改善措施之矯正

資訊安全指標未達目標值所採取之矯正措施，應依資訊安全指標管理程序說明原因、執行矯正措施，並追蹤處理情形及改善結果；必要時填寫矯正措施單。

10.4 改善措施之追蹤

改善措施之執行結果應予紀錄及追蹤，並依相關程序確認改善措施之有效性。資訊安全指標未達目標值時，應依資訊安全指標管理程序填寫矯正措施單，追蹤負責單位之處理情形及矯正措施；資訊安全事件之改善措施，則應依資訊安全事件管理辦法確認是否已降低事件影響及再發生之可能，並作為資訊安全委員會管理審查及 ISMS 持續改善之依據。

11 罰則

11.1 本公司人員（包含正式員工、約聘人員、派遣員工、臨時僱員等）應嚴格遵守本政策及相關資訊安全規範。如有違反資安規定或造成公司資產損害之情事，將依本公司員工獎懲通則予以處分；情節重大涉及違法者，本公司將依法追究其民事與刑事責任。

11.2 訪客、供應商及外部合作單位人員如有違反本政策或契約所定資安要求之情事，將依相關合約條款、工作說明書或法律規定辦理，本公司並得終止合作或追究損害賠償責任。

12 審查與發布實施

本資訊安全政策聲明經權責主管審查及核准後，應依文件管制作業程序辦理文件發布、分發及管制，確保使用人員取得適用且有效之文件版本。

本公司應依教育訓練程序辦理資訊安全政策、資訊安全事件及相關規範之教育訓練與宣導；新進人員應接受相關資訊安全政策及規範之教育。