ISO 27001:2022 條文釋義
(資訊安全-資訊安全管理系統-要求)

資深顧問師 彭至賢 (Sam Peng)

ISO27001/BS10012/ISO9001主導稽核員

PMP&APMP國際專案管理師

TTQS國家訓練品質計畫評核委員

Mobile: 0952-695460

E-mail: sam@safelink.com.tw

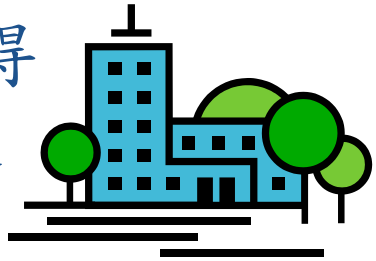
SafeLink 博創資訊科技股份有限公司

ISO 27001:2022 標準條文

1. 範圍
2. 引用標準
3. 用語和定義
4. 組織背景
5. 領導
6. 規劃
7. 支援
8. 運作
9. 績效評估
10. 改善

1. 範圍

- 本標準規定於組織全景內建立、實作、維持及持續改善資訊安全管理系統之要求事項。
- 本標準亦包括依組織需要之安全風險鑑及處理的要求事項。
- 本標準敘述之要求事項為通用的，旨在適用於所有組織，不論其型式、規模或性質。當組織宣稱符合本標準時，不得排除本標準第 4 節至第 10 節所規定之任何要求事項。



2. 引用標準

- 下列標準因本標準所引用，成為本標準之一部分。下列引用標準適用最新版(包括補充增修)。

- ISO/IEC 27000 ，資訊技術-安全技術-資訊安全管理系統-概述和詞彙。

3. 用語和定義

- 就本標準而言，適用 ISO/IEC 27000 中的術語和定義。

4. 組織背景

- 4.1 了解組織及其背景
- 4.2 瞭解利害關係方的需求與期望
- 4.3 決定資訊安全管理系統的範圍
- 4.4 資訊安全管理系統

4.1 了解組織及其背景

- 組織應決定與其目的有關且影響達成其資訊安全管理系統預期成果能力者之內部及外部議題。
- 備考：
  - 決定此等議題，是指建立ISO 31000：2018[5]條款5.4.1 中考慮的組織外部和內部背景。

4.2 瞭解利害關係方的需求與期望

該組織應確定：

- a) 與資訊安全管理系統相關的利害關係各方;
- b) 這些利害關係方的相關要求;
- c) 將如何經由資訊安全管理系統滿足前述相關要求。

備考：利害關係方的要求可以包括法律和法規要求以及合約義務。

4.3 決定資訊安全管理系統的範圍

- 組織應決定資訊安全管理系統之邊界及適用性，以建立其範圍。
- 在決定此範圍時，組織應考慮：
  - a) 4.1 中提到的外部和內部議題；
  - b) 4.2 中提到的要求；
  - c) 組織履行之活動與其他組織履行之活動間的介面及相依性。
- 範圍應以文件化資訊提供。

4.4 資訊安全管理系統

- 組織應根據以下要求建立、實施、維護和持續改進資訊安全管理系統，根據本標準的要求，包括所需的過程及其相互作用。

5. 領導

- 5.1 領導力和承諾
- 5.2 政策
- 5.3 組織角色、責任和權限

5.1 領導力和承諾

- 最高管理層應通過下列方式展現對資訊安全管理系統的領導能力和承諾：
  - a) 確保資訊安全政策和資訊安全目標的建立並與組織的策略方向相容；
  - b) 確保將資訊安全管理系統要求整合到組織的流程中；
  - c) 確保資訊安全管理系統所需的資源可取得；
  - d) 傳達有效資訊安全管理和符合資訊安全管理系統要求的重要性；
  - e) 確保資訊安全管理系統實現其預期結果；
  - f) 指導和支援人員為資訊安全管理系統的有效性做出貢獻；
  - g) 促進持續改進；和
  - h) 支援其他相關的管理角色，在適用於他們的職責領域展現他們的領導力。

  備考：本標準中提及的「營運」可廣義地解釋為指對組織存在的目的至關重要的活動。

5.2 政策

- 最高管理階層應建立包含下列事項之資訊安全政策：
  - a) 適合組織的目的；
  - b) 包括資訊安全目標 (見6.2)，或提供設定資訊安全目標的框架；
  - c) 包括承諾滿足與資訊安全相關的適用要求；
  - d) 包括對持續改進資訊安全管理系統的承諾。

    資訊安全政策應：
  - e) 以文件化資訊提供；
  - f) 在組織內進行溝通；
  - g) 適用時，提供給關注方。

5.3 組織角色、責任和權限

- 最高管理階層應確保資訊安全相關角色之責任及權限已指派並傳達。
- 最高管理階層應指派下列責任及權限。
  - a) 確保資訊安全管理系統符合本標準之要求事項。
  - b) 向最高管理階層報告資訊安全管理系統之績效。
- 備考：最高管理階層亦可指派報告組織內資訊安全管理系統績效之責任及權限。

6. 規劃

- 6.1 應對風險和機會的行動
- 6.2 資訊安全目標和實現目標的規劃
- 6.3變更規劃

6.1 應對風險和機會的行動

- 6.1.1 一般要求
- 6.1.2 資訊安全風險評鑑
- 6.1.3 資訊安全風險處理

6.1.1 一般要求

- 於規劃資訊安全管理系統時，組織應考量 4.1 所提及之議題及 4.2 所提及之要求事項，並決定需因應之風險及機會，以達成下列事項。
  - a) 確保資訊安全管理系統達成其預期成果。
  - b) 預防或減少非所欲之影響。
  - c) 達成持續改善。
- 組織應規劃下列事項。
  - d) 因應此等風險及機會之行動。
  - e) 執行下列事項之方法。
    - 1) 將各項行動整合及實作於其資訊安全管理系統過程之中。
    - 2) 評估此等行動之有效性。

6.1.2 資訊安全風險評鑑

- 組織應定義及應用資訊安全風險評鑑過程於下列事項中。
  - a) 建立及維持包括下列準則之資訊安全風險準則。
    - 1) 風險接受準則。
    - 2) 履行資訊安全風險評鑑之準則。
  - b) 確保重複之資訊安全風險評鑑產生一致、有效及適於比較之結果。
  - c) 識別資訊安全風險。
    - 1) 應用資訊安全風險評鑑過程，以識別資訊安全管理系統範圍內與漏失資訊之機密性、完整性及可用性相關聯之風險。
    - 2) 識別風險擁有者。
  - d) 分析資訊安全風險。
    - 1) 評鑑若6.1.2 c) 1)中所識別之風險實現時，可能導致之潛在後果。
    - 2) 評鑑6.1.2 c) 1)中所識別之風險發生的實際可能性。
    - 3) 決定風險等級。
  - e) 評估資訊安全風險。
    - 1) 以6.1.2 a)中所建立之風險準則，比較風險分析結果。
    - 2) 訂定已分析風險之風險處理優先序。
- 組織應保存關於資訊安全風險評鑑過程之文件化資訊。

6.1.3 資訊安全風險處理

- 組織應定義並應用資訊安全風險處理流程，以：
  - a) 考慮風險評結果選擇適當的資訊安全風險處理選項；
  - b) 對所選定資訊安全風險處理選項，決定所有必須實作之控制措施；
    - 備考1：組織可依要求設計控制措施，或由任何來源識別之。
  - c) 比較上述6.1.3 b)中所決定之控制措施與附錄A中者，並確認未忽略必要之控制措施；
    - 備考 2：附錄A包括控制目標及控制措施之詳細清單。本標準之使用者參照附錄A以確保未忽略必要之控制措施。
    - 備考 3：控制目標隱含於所選定之控制措施中。附錄A中所列之各項控制目標及控制措施並未盡列，故可能需要額外之控制目標及控制措施。
  - d) 產生包含以下內容的適用性聲明：

    -必要的控制措施 (見6.1.3 b 和 c)；

    -將其納入的理由；

    -是否實施了必要的控制措施;以及

    -排除任何附錄A控制措施的理由。
  - e) 制定資訊安全風險處理計畫；以及
  - f) 獲得風險擁有者對資訊安全風險處理方案的核准，並接受剩餘的資訊安全風險。
  - 組織應保存關於資訊安全風險處理過程之文件化資訊。
    - 備考 4：本標準中的資訊安全風險評鑑和處理過程符合ISO 31000 [5]中提供的原則和通用指南。

6.2 資訊安全目標和實現目標的規劃

- 組織應在相關部門及層級建立資訊安全目標。
- 資訊安全目標應：
  - a) 與資訊安全政策保持一致；
  - b) 可以量測 (如果可行)；
  - c) 考慮適用的資訊安全要求，以及風險評估和風險處理的結果；
  - d) 受到監控；
  - e) 被傳達；
  - f) 適時更新；
  - g) 作為記錄的文件化資訊提供。
- 組織應保存關於資訊安全目標之文件化資訊。
- 於規劃如何達成資訊安全目標時，組織應決定下列事項將做什麼;
  - h) 待辦事項；
  - i) 將需要哪些資源；
  - j) 誰將負責；
  - k) 何時完成；和
  - l) 結果之評估方式。

6.3 變更規劃

- 當組織確定需要對信息安全管理體系進行變更時，應以預先規劃的方式進行變更。。

7. 支援

- 7.1 資源
- 7.2 能力
- 7.3 認知
- 7.4 溝通
- 7.5 文件化資訊

7.1 資源

- 組織應決定並提供建立、實施、維護和持續改進資訊安全管理系統所需的資源。

7.2 能力

- 組織宜採取下列措施。
  - a) 決定於組織控制下執行工作，影響其資訊安全績效人員之必要能力。
  - b) 確保此等人員於適當教育、訓練或經驗之基礎上能勝任。
  - c) 於適當時，採取取得必要能力之行動，並評估所採取行動之有效性。
  - d) 保存適切之文件化資訊，作為勝任之證據。
- 備考：適用之行動可能包括，例：對現有員工提供訓練、指導或重新指派，或是雇用或委外勝任人員。

7.3 認知

- 組織控制下執行工作之人員，應認知下列事項。
  - a) 資訊安全政策。
  - b) 其對資訊安全管理系統有效性之貢獻，包括改善之資訊安全績效的益處。
  - c) 未遵循資訊安全管理系統要求事項之可能後果。

7.4 溝通

- 組織應決定，相關於資訊安全管理系統之內部及外部溝通或傳達的需要，包括下列事項。
  - a) 關於溝通什麼；
  - b) 何時溝通；
  - c) 與誰溝通；
  - d) 如何溝通。

7.5 文件化資訊

- 7.5.1 一般要求
- 7.5.2 制訂和更新
- 7.5.3 文件化資訊之控制

7.5.1 一般要求

- 組織之資訊安全管理系統應包括下列內容。
  - a) 本標準要求之文件化資訊。
  - b) 由組織所決定對資訊安全管理系統有效性，必要之文件化資訊。

  備考：各組織之資訊安全管理系統文件化資訊內容，可能因下列因素而異。
    - 1) 組織規模，以及其活動之型式、過程、產品及服務。
    - 2) 各過程及其互動之複雜度。
    - 3) 人員之能力。

7.5.2 制訂和更新

- 於制訂及更新文件化資訊時，組織應確保適切之下列項目：
  - a) 標識和描述（例如標題、日期、作者或參考文獻編號）；
  - b) 格式 (例如語言、軟體版本、圖形) 和媒體 (例如紙張、電子)；和
  - c) 合宜性及適切性之審查及核准。

7.5.3 文件化資訊之控制

- 應控制資訊安全管理系統及本標準要求之文件化資訊，以確保下列事項。
  - a) 其於需要處及需要時為可用及適用。
  - b) 其受適切保護 (例：防止漏失機密性、不當使用或漏失完整性)。
    為控制文件化資訊，組織應於適當時，闡明下列活動。
  - c) 派送、存取、檢索及使用。
  - d) 儲存及保存，包括可讀性之保存。
  - e) 變更之控制 (例:版本控制)。
  - f) 留存及屆期處置。
- 於適當時，應識別及控制由組織所決定對資訊安全管理系統之規劃及運作為必要之外部來源的文件化資訊。
- 備考：存取意謂關於文件化資訊僅可檢視之許可、或檢視及變更文件化資訊之許可及權限的決策等。

8. 運作

- 8.1 運作之規劃及控制
- 8.2 資訊安全風險評鑑
- 8.3 資訊安全風險處理

8.1 運作之規劃及控制

- 織應策劃、實施和控制滿足要求所需的過程，並通過以下方式實施第 6 章確定的措施：

  -為過程建立準則；

  -根據準則實施過程控制。
- 組織應保存文件化資訊，其程度必須具有足以達成其過程已依規劃執行之信心。。
- 組織應控制所規劃之變更，並審查非預期變更之後果，必要時採取行動以減輕任何負面效果。
- 組織應確保委外過程經確定並受控制。

8.2 資訊安全風險評鑑

- 組織應依規劃之期間，或當提議或發生重大變更時，考量在 6.1.2 a)所 建立之準則，執行資訊安全風險評鑑。
- 組織應保存資訊安全風險評鑑結果之文件化資訊。

8.3 資訊安全風險處理

- 組織應實作資訊安全風險處理計畫。
- 組織應保存資訊安全風險處理結果之文件化資訊。

9. 績效評估

- 9.1 監控、量測、分析和評估
- 9.2 內部稽核
- 9.3 管理審查

9.1 監控、量測、分析和評估

- 組織應決定下列事項。
  - a) 需要監督及量測之事項，包括資訊安全過程及控制措施。
  - b) 監督、量測、分析及評估之適用方法，以確保有效的結果。
    - 備考：所選擇之方法宜產生適於比較及可重製視為有效之結果。
  - c) 執行監督及量測之時間。
  - d) 監督及量測之人員。
  - e) 監督及量測結果應分析及評估之時間。
  - f) 分析及評估上述結果之人員。
- 組織應保存適切之文件化資訊，作為監督及量測結果的證據。
- 組織應評估資訊安全績效及資訊安全管理系統之有效性。

9.2 內部稽核

- 9.2.1 一般要求
- 9.2.2 內部稽核方案

9.2.1 一般要求

- 組織應依規劃之期間施行內部稽核，以提供資訊安全管理系統之下列資訊。
  - a) 是否遵循下列事項。
    - 1) 組織本身對其資訊安全管理系統之要求事項。
    - 2) 本標準之要求事項。
  - b) 是否有效實作及維持。

9.2.2 內部稽核方案

- 組織應計劃、建立、實施和維護稽核計劃，包括頻率、方法、職責、計劃要求和報告。
- 在建立內部稽核計劃時，組織應考慮有關過程的重要性和先前稽核的結果。

  組織應：
  - a) 定義每次稽核的標準和範圍；
  - b) 選擇稽核人員並進行稽核，以確保稽核過程的客觀性和公正性；
  - c) 確保將稽核結果報告給相關管理階層；

    保存文件化資訊作為稽核計畫及稽核結果之證據。

9.3 管理審查

- 9.3.1 一般要求
- 9.3.2 管理審查輸入事項
- 9.3.3 管理審查結果

9.3.1 一般要求

- 最高管理階層應於規劃之期間，審查組織之資訊安全管理系統，以確保其持續的合宜性、適切性及有效性。

9.3.2 管理審查輸入事項

- 9.3.2管理審查輸入事項
- 管理審查應包括對下列事項之考量：
  - a) 過往管理審查之議案的處理狀態。
  - b) 與資訊安全管理系統有關之內部及外部議題的變更。
  - c) 與資訊安全管理系統有關的利害關係方的需求和期望的變化;
  - d) 資訊安全績效之回饋，包括下列之趨勢。
    - 1) 不符合項目及矯正措施。
    - 2) 監督及量測結果。
    - 3) 稽核結果。
    - 4) 資訊安全目標之達成。
  - e) 關注方之回饋。
  - f) 風險評鑑結果及風險處理計畫之狀態。
  - g) 持續改進的機會。

9.3.3 管理審查結果

- 管理審查之輸出應包括與持續改善機會有關之決策，以及任何對資訊安全管理系統變更之需要。
- 組織應保存文件化資訊，以作為管理審查結果之證據。

10. 改善

- 10.1 持續改進
- 10.2 不符合及矯正措施

10.1 持續改進

- 組織應持續改善資訊安全管理系統之合宜性、適切性及有效性。

10.2 不符合及矯正措施

- 不符合項目發生時，組織應有下列作為。
  - a) 對不符合項目反應，並於適當時採取下列作為。
    - 1) 採取行動以控制並矯正之。
    - 2) 處理其後果。
  - b) 藉由下列作為，評估對消除不符合項目之原因的行動之需要，使其不再發生且不於他處發生。
    - 1) 審查不符合項目。
    - 2) 決定不符合項目之原因。
    - 3) 決定是否有類似之不符合項目存在，或可能發生。
  - c) 實作所有所需行動。
  - d) 審查所有所採取矯正措施之有效性。
  - e) 若必要時，則對資訊安全管理系統進行變更。
- 矯正措施應切合遇到之不符合項目。
- 組織應保存文件化資訊，以作為下列事項之證據。
  - f) 不符合項目之本質及後續採取之所有行動。
  - g) 所有矯正措施之結果。

附錄A. 資訊安全控制措施參考

- 5. 組織面控制措施
- 6. 人員面控制措施
- 7. 實體面控制措施
- 8. 技術面控制措施

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.1 資訊安全政策
    - 控制措施：資訊安全政策和特定主題之政策應被定義、獲管理層核准、發布、傳達給相關人員及相關的利害關係者並取得其認可，並於計劃的時間間隔和發生重大變化時進行審查。
  - 5.2 資訊安全的角色與職責
    - 控制措施：應根據組織的需要，定義和分配資訊安全的角色與職責。
  - 5.3 職務的區隔
    - 控制措施：相互衝突的職務和責任領域應被區隔。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.4 管理階層責任
    - 控制措施：管理階層應要求所有人員按照組織已制定的資訊安全政策、特定主題之政策及程序運用資訊安全。
  - 5.5 與權責機關的聯繫
    - 控制措施：組織應與有關之權責機關建立並保持聯繫。
  - 5.6 與特殊利害關係者的聯繫
    - 控制措施：組織應與特殊利害關係者或其他專家安全論壇和專業協會建立並保持聯繫。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.7 威脅情資
    - 控制措施：應蒐集和分析與資訊安全威脅有關的資訊以產出威脅情資。
  - 5.8 專案管理的資訊安全
    - 控制措施：資訊安全應融入專案管理之中。
  - 5.9 資訊和其他相關資產的清查盤點
    - 控制措施：應開發和維護資訊和其它相關資產（包括擁有者）的清冊。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.10 資訊和其它相關資產之可被接受的使用
    - 控制措施：應識別、文件化和實施有關處理資訊和其它相關資產之可被接受的使用及程序之規則。
  - 5.11 資產歸還
    - 控制措施：人員和其他適當的利害關係者應在其聘僱、合約或協議變更或終止時歸還其擁有的所有組織資產。
  - 5.12 資訊分類
    - 控制措施：資訊應根據組織基於機密性、完整性、可用性及相關利害關係者的資訊安全需要進行分類。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.13 資訊標示
    - 控制措施：應根據組織採用的資訊分類方案發展和實施一套適當的資訊標示程序。
  - 5.14 資訊傳輸
    - 控制措施：組織內部以及組織與其他各方之間的資訊傳輸規則、程序或協議，應適用於所有類型的傳輸設施。
  - 5.15 存取控制
    - 控制措施：應基於營運和資訊安全要求，建立和實施對資訊和其它相關資產之實體面和邏輯面的存取控制規則。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.16 身份管理
    - 控制措施：應管理身份的完整生命週期。
  - 5.17 驗證資訊
    - 控制措施：驗證資訊的分配和管理應由一個管理過程管控，包括適當處理驗證資訊的建議人員。
  - 5.18 存取權限
    - 控制措施：應根據組織的特定主題政策和存取控制規則來提供、審查、修改和移除對資訊和其它相關資產的存取權限。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.19 供應商關係的資訊安全
    - 控制措施：應識別和實施過程和程序，以針對使用供應商產品或服務相關的資訊安全風險進行管理。
  - 5.20 供應商協議內的資訊安全要求
    - 控制措施：應建立相關的資訊安全要求，並根據供應商關係的類型與每個供應商達成協議。
  - 5.21 管理資通技術(ICT)供應鏈的資訊安全
    - 控制措施：應定義並實施流程和程序，以管理與ICT產品和服務供應鏈相關的資訊安全風險。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.22 供應商服務之監控、審查及變更管理
    - 控制措施：組織應定期監控、審查、評估並管理供應商資訊安全實務和服務交付的變更。
  - 5.23 使用雲端服務之資訊安全
    - 控制措施：應根據組織的資訊安全要求建立獲取、使用、管理和退出雲端服務的流程。
  - 5.24 資訊安全事故管理規劃與準備
    - 控制措施：組織應透過定義、建立並溝通資訊安全事故管理過程、角色和職責，以規劃並準備對資訊安全事故的管理。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.25 資訊安全事件的評定與決策
    - 控制措施：組織應評定資訊安全事件並決定是否將其歸類為資訊安全事故。
  - 5.26 對資訊安全事故的回應
    - 控制措施：應依照文件化程序回應資訊安全事故。
  - 5.27 從資訊安全事故中學習
    - 控制措施：從資訊安全事故中獲得的知識應用強化與改善資訊安全控制措施。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.28 證據的蒐集
    - 控制措施：組織應建立並實施與資訊安全事件相關之證據的識別、蒐集、獲取及保存程序。
  - 5.29 中斷期間的資訊安全
    - 控制措施：組織應規劃如何於中斷期間將資訊安全維持在適當的水準。
  - 5.30 為營運持續性做好資通技術(ICT)的準備
    - 控制措施：應基於營運持續性目標和 ICT 持續性要求來規劃、實施、維護並測試 ICT 準備情形。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.31 識別法令法規、監管與合約要求
    - 控制措施：資訊安全相關的法令法規、監管與合約要求，以及組織滿足這些要求的方法，應被識別、文件化並與時俱進。
  - 5.32 智慧財產權
    - 控制措施：組織應實施適當的程序，以保護智慧財產權。
  - 5.33 紀錄之保護
    - 控制措施：應保護紀錄免遭遺失、破壞、偽造、未經授權的存取和未經授權的發布。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.34 隱私與個人可識別資訊(PII)的保護
    - 控制措施：組織應根據適用的法令法規、監管與合約要求，識別並滿足有關維護隱私和保護PII的要求。
  - 5.35 資訊安全之獨立審查
    - 控制措施：組織管理資訊安全的方法及其實施，包括人員、流程與技術，應按規劃的間隔時間或發生重大變更時進行獨立審查。

ISO 27001:2022控制措施 → 5.

- 5.組織面控制措施
  - 5.36 資訊安全政策、規則與標準之遵循性
    - 控制措施：應定期審查對組織資訊安全政策、特定主題之政策、規則與標準的遵循情形。
  - 5.37 文件化的作業程序
    - 控制措施：資訊處理設施的作業程序應文件化並讓需要的人員可取用。

ISO 27001:2022 控制措施 → 6.

- 6. 人員面控制措施
  - 6.1 篩選
    - 控制措施：根據適用的法令法規、道德規範，及適度的營運要求、要存取的資訊分類和感知到的風險，對所有將成為員工的候選者於加入組織之前及持續執行的基礎上進行背景核查。
  - 6.2 聘僱條款與條件
    - 控制措施：聘僱合約協議應敘明人員和組織對資訊安全的責任。

ISO 27001:2022 控制措施 → 6.

- 6. 人員面控制措施
  - 6.3 資訊安全認知、教育與培訓
    - 控制措施：組織人員和相關的利害關係者應接受與其工作職能相關的適當資訊安全認知、教育與培訓，以及定期更新的組織資訊安全政策、特定主題之政策及程序。
  - 6.4 懲處程序
    - 控制措施：應正式制定並傳達懲處程序，以對違反資訊安全政策的人員和其他相關的利害關係者採取行動。

ISO 27001:2022 控制措施 → 6.

- 6. 人員面控制措施
  - 6.5 聘僱終止或變更後之責任
    - 控制措施：應定義、執行並與相關人員和其他利害關係者溝通在聘僱終止或變更後仍然有效的資訊安全責任和義務。
  - 6.6 機密性或保密協議
    - 控制措施：反映組織對資訊保護所需的機密性或保密協議，應由人員和其他相關的利害關係者所識別、文件化、定期審查及簽署。

ISO 27001:2022 控制措施 → 6.

- 6. 人員面控制措施
  - 6.7 遠距工作
    - 控制措施：當人員遠距工作以保護在組織場域外存取、處理或儲存的資訊時，應實施安全措施。
  - 6.8 資訊安全事件通報
    - 控制措施：組織應提供一種機制，供人員可透過適當管道及時通報觀察到或可疑的資訊安全事件。

ISO 27001:2022 控制措施 → 7.

- 7. 實體面控制措施
  - 7.1 實體安全邊界
    - 控制措施：應定義安全邊界並將其用於保護包含資訊和其它相關資產的區域。
  - 7.2 實體進出管制
    - 控制措施：安全區域應受到適當的進出管控和存取管制點的保護。
  - 7.3 辦公室、空間與設施的保護
    - 控制措施：應設計並實施辦公室、空間與設施的實體安全。

ISO 27001:2022 控制措施 → 7.

- 7. 實體面控制措施
  - 7.4 實體安全監控
    - 控制措施：應持續監控場域以避免未經授權的實體取用。
  - 7.5 對抗實體與環境威脅的保護
    - 控制措施：應設計並實施對抗實體與環境威脅的保護，例如自然災害和其它對基礎設施蓄意或無意的實體威脅。
  - 7.6 在安全區域內工作
    - 控制措施：應設計並實施在安全區域內工作的安全措施。

ISO 27001:2022 控制措施 → 7.

- 7. 實體面控制措施
  - 7.7 桌面淨空與螢幕淨空
    - 控制措施：紙本和可移除式儲存媒體的桌面淨空規則及資訊處理設施的螢幕淨空規則應被定義和適當執行。
  - 7.8 設備安置與保護
    - 控制措施：設備應被安全放置並受到保護。
  - 7.9 駐外資產的安全
    - 控制措施：駐外資產應受到保護。

ISO 27001:2022 控制措施 → 7.

- 7. 實體面控制措施
  - 7.10 儲存媒體
    - 控制措施：儲存媒體應按照組織的分類方案與處理要求，於其獲取、使用、運輸和處置的整體生命週期中受到管理。
  - 7.11支援之公用設施
    - 控制措施：應保護資訊處理設施免受因支援之公用設施故障而導致的電力失效和其它中斷。
  - 7.12 佈纜之安全
    - 控制措施：應保護傳輸電力、資料或支援資訊服務的佈纜免受攔截、干擾或破壞。

ISO 27001:2022 控制措施 → 7.

- 7. 實體面控制措施
  - 7.13 設備維護
    - 控制措施：應正確維護設備，以確保資訊之可用性、完整性與機密性。
  - 7.14 設備的汰除或再使用之安全
    - 控制措施：應核查包含儲存媒體的設備，以確保於汰除或再使用之前已移除或安全覆蓋任何敏感資料和授權軟體。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.1 使用者端點設備
    - 控制措施：應保護透過使用者端點設備儲存、處理或可存取的資訊。
  - 8.2 特權存取權限
    - 控制措施：應限制並管理特權存取權限的分配和使用。
  - 8.3 資訊存取限制
    - 控制措施：應根據已建立的特定主題之存取控制政策限制對資訊和其它相關資產的存取。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.4 程式源碼的存取
    - 控制措施：應適當管理對程式源碼、開發工具和軟體庫的讀寫存取。
  - 8.5 安全認證
    - 控制措施：應根據資訊存取限制和特定主題的存取控制政策，實施安全認證技術與程序。
  - 8.6 容量管理
    - 控制措施：應根據當前和預期的容量要求監控和調整資源的使用。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.7 防範惡意程式
    - 控制措施：應透過適當的使用者意識，實施並支持防範惡意程式的保護。
  - 8.8 技術漏洞的管理
    - 控制措施：應獲取有關資訊系統在使用中的技術漏洞資訊，並且應評估組織對此類漏洞的暴露程度並應採取適當的措施。
  - 8.9 組態管理
    - 控制措施：應建立、文件化、實施、監控和審查硬體、軟體、服務和網路的組態，包括安全組態。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.10 資訊刪除
    - 控制措施：當不再需要時，應刪除儲存於資訊系統、裝置或任何其它儲存媒體中的資訊。
  - 8.11 資料遮蔽
    - 控制措施：應根據組織關於存取控制與其它相關的特定主題政策以及營運要求使用資料遮蔽，並將法律要求納入考量。
  - 8.12 預防資料洩漏
    - 控制措施：資料洩漏的預防措施應應用於處理、儲存或傳輸敏感資訊的系統、網路及任何其它裝置。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.13 資訊備份
    - 控制措施：資訊、軟體和系統的備份副本應按照議定的特定主題備份政策進行維護和定期測試。
  - 8.14 資訊處理設施的備援
    - 控制措施：資訊處理設施的實施應具有足以滿足可用性要求的備援。
  - 8.15 日誌存錄
    - 控制措施：記錄活動、例外、錯誤和其他相關事件的日誌，應被生成、儲存、保護和分析。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.16 活動監控
    - 控制措施：應監控網路、系統和應用程式的異常行為，並採取適當行動以評估潛在的資訊安全事故。
  - 8.17 時脈同步
    - 控制措施：組織使用的資訊處理系統之時脈應與核准的時間源同步。
  - 8.18 特權的公用程式之使用
    - 控制措施：應限制並嚴格管控能夠竄越系統和應用程式控制的公用程式之使用。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.19 運作中系統上的軟體安裝
    - 控制措施：應實施程序和措施以安全地管理運作中系統上的軟體安裝。
  - 8.20 網路安全
    - 控制措施：應保護、管理和管控網路及網路設備以保護系統和應用程式中的資訊。
  - 8.21 網路服務的安全
    - 控制措施：應識別、實施並監控網路服務的安全機制、服務水準及服務要求。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.22 網路區隔
    - 控制措施：資訊服務、使用者與資訊系統的群組應於組織的網路中區隔。
  - 8.23 網頁過濾
    - 控制措施：應管理對外部網站的存取，以減少曝露於惡意的內容。
  - 8.24 密碼學的使用
    - 控制措施：應定義並實施有效使用密碼學的規則，包括密碼學的金鑰管理。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.25 安全之開發生命週期
    - 控制措施：應建立並運用軟體和系統的安全開發規則。
  - 8.26 應用程式安全要求
    - 控制措施：於開發或獲取應用程式時，應識別、明訂並核准資訊安全要求。
  - 8.27 安全系統架構與工程原則
    - 控制措施：應建立、文件化、維護工程安全系統的原則並將其運用於任何資訊系統開發活動。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.28 安全編碼
    - 控制措施：軟體開發應採用安全編碼原則。
  - 8.29 開發與驗收的安全測試
    - 控制措施：應於開發生命週期中定義並實施安全測試流程。
  - 8.30 委外開發
    - 控制措施：組織應指導、監控並審查與委外系統開發相關的活動。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.31 區隔開發、測試與正式環境
    - 控制措施：應區隔並保護開發、測試與正式環境。
  - 8.32 變更管理
    - 控制措施：資訊處理設施和資訊系統的變更應依循變更管理程序。
  - 8.33 測試資訊
    - 控制措施：應適當地選擇、保護並管理測試資訊。

ISO 27001:2022 控制措施 → 8.

- 8. 技術面控制措施
  - 8.34 於稽核測試期間對資訊系統的保護
    - 控制措施：稽核測試與其它涉及評鑑運作中系統的保證活動，應於測試人員和適當的管理人員之間進行規劃並同意。

Q&A 問題與討論

～如有任何問題，歡迎隨時來電詢問～

SafeLink

博創資訊科技股份有限公司

臺中市西屯區國安一路208巷6號

TEL：886-4-25250535

http://www.safelink.com.tw/

E-mail: sam@safelink.com.tw