文件名稱：資訊安全管理手冊

文件編號：HENGS-IM-1-001

制定單位： 資訊部

機密等級：□機密 ■一般

NO	制(修)訂日期	頁次	版次	制(修)訂內容摘要
1	2025.06.19	11	1	新制定。

1. 目的

1.1 做為聚恆科技股份有限公司(以下簡稱本公司)資訊安全管理系統(以下簡稱 ISMS)相關管理辦法以及作業程序之參考依據。同時引用 ISO/IEC 27001國際標準，建立制度化、文件化及系統化的管理機制，並依循 PDCA 之持續改善流程，持續監督及審查管理績效，確保 ISMS 有效運作，降低本公司所可能面臨之資安風險，並達到以下之目標：

1.1.1 建立、落實及維護資通安全管理政策。

1.1.2 全面導入資通安全管理制度。

1.1.3 培訓資通人員在資通安全領域之專業能力。

1.1.4 強化資通安全環境及資通安全應變能力。

1.1.5 達成資訊安全目標之量測指標。

1.2 確保本公司各項資訊資產之機密性、完整性及可用性，並符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意料外的威脅，以滿足本公司各關注方之需求與期望。

2. 適用範圍

2.1 本公司ISMS 所涵蓋範圍內皆適用。

2.2 資訊安全管理範疇涵蓋 4 大控制主題，用以避免因人為疏失、蓄意或天然災害等因素，導致資訊不當使用、洩漏、竄改或破壞等情事發生，而對本公司造成各種可能之風險與危害，各類控制主題如下：

2.2.1 組織控制。

2.2.2 人員控制。

2.2.3 實體控制。

2.2.4 技術控制。

3. 資訊安全政策與目標

3.1 ISMS簡介

ISMS著眼於管理本公司在營運上所可能遭遇之資訊安全風險，並以「規劃(Plan)-執行(Do)-檢查(Check)-行動(Action)」之模式來建置與維護，確保此制度有效運作，所有作業均佐以適當文件記載或紀錄予以說明，包括：

3.1.1 組織全景。

3.1.2 領導作為。

3.1.3 規劃。

3.1.4 支援。

3.1.5 運作。

3.1.6 績效評估。

3.1.7 改善。

3.2 資訊安全政策

3.2.1 為落實執行本公司ISMS，確保其運作之有效性，並持續監督管理，維護重要資通系統之機密性、完整性與可用性，使其免於遭受內、外部的蓄意或意外之威脅，特訂定本政策。

3.2.2 本政策旨在提供公司員工從事資通作業之明確指導原則，所有員工皆有義務積極參與推動，以確保本公司之資料、系統、設備及網路能安全維運，達到營運持續的目標。

3.2.3 本公司資訊安全政策如下：

3.2.3.1 落實安管措施，強化服務品質

全體員工應落實ISMS之各項管理措施，確保業務資料之機密性、完整性及可用性，避免因外在威脅或內部弱點，而遭到洩漏、破壞或遺失等風險，並應選擇適切的控制措施，將所有可能風險降至可接受範圍，並持續進行監控、稽核與審查，以強化服務品質，提升服務水準。

3.2.3.2 加強資安訓練，確保營運持續

因應資通安全威脅情勢的不斷變化，每年持續進行適當的資通安全教育訓練，使員工了解資通安全的重要性，並敦促其遵守資通安全規定；而全體員工亦應確實參與訓練課程，提高資通安全意識，建立「***資安防護做得好，駭客攻擊無處找***」的觀念，強化資通安全緊急應變能力，降低資通安全風險，達成營運持續之目標。

3.2.3.3 制定應變流程，迅速災害復原

應制定重要資訊資產及關鍵業務之營運持續運作計畫，並定期進行相關緊急應變流程的演練，確保資通系統失效或重大災害發生時，能夠迅速完成復原，確保關鍵業務能持續運作，並將損失降至最低。

3.3 資訊安全目標

3.3.1 依據本公司之資訊安全政策，擬定資通安全目標如下：

3.3.1.1 防範本公司各項資訊設備遭受病毒或惡意程式感染。

3.3.1.2 確保所提供之服務能夠維持一定水準之可用性與完整性。

3.3.1.3 辦理資通安全教育訓練(含外訓)，提升員工資通安全意識。

3.3.1.4 每年定期進行內部稽核作業，確保相關規範皆能落實。

3.3.2 本公司應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間，以及結果評估方式。

3.3.3 資訊安全目標之有效性量測結果應於相關會議中報告。

3.3.4 資訊安全目標之調整應依據本政策 6.2 辦理。

4. 組織全景

4.1 瞭解組織及背景

本公司應依據 ISO 45001 / ISO 9001 確認與業務相關，且可能影響 ISMS 預期成果之各項內部及外部議題，詳細作業程序描述於『組織規劃與利害關係人管理程序（HENGS-QM-2-026）』。

4.2 瞭解利害關係人的需求及期望在決策本公司 ISMS 之範圍前，應依據『組織規劃與利害關係人管理程序（HENGS-QM-2-026）』確認下列事項：

4.2.1 與ISMS 相關之利害關係人。

4.2.2 相關利害關係人之需求或期望。

4.2.3 在4.2.2 之事項中，有哪些將透過ISMS 因應。

4.3 確認ISMS 的範圍

本公司依據『組織規劃與利害關係人管理程序（HENGS-QM-2-026）』將下列事項納入考量後，確認 ISMS 的範圍，並將其採文件化之方式記錄下來。

4.3.1 於4.1中所提及的內部與外部議題。

4.3.2 於4.2中所提及之利害關係人的要求事項。

4.3.3 本公司與其它組織執行活動間之介面與相依性。

4.4 詳細之ISMS組織架構、執掌與權責等，詳述於『資訊安全編組與權責（HENGS-IM-3-002）』。

5. 領導作為

5.1 領導與承諾

本公司資訊安全長(以下簡稱資安長)掌管公司相關職責指派及資源分配，為標準所定義之公司內最高管理階層(Top management)，為使ISMS推動順利，應負有以下所列責任：

5.1.1 確保已建立資訊安全政策及資訊安全目標，並與本公司的營運策略方向一致或相容。

5.1.2 確保將ISMS 要求事項與公司業務流程整合。

5.1.3 確保ISMS 所需資源的可用性。

5.1.4 傳達有效之ISMS 與符合ISMS 要求事項的重要性。

5.1.5 確保ISMS 達到預期效果。

5.1.6 指揮與支援所需人力，以促進ISMS 的有效性。

5.1.7 持續改善。

5.1.8 支持其他相關管理角色的職責，以展現領導權。

5.2 政策

5.2.1 本公司資安長負有審核資訊安全政策之責，並應確認資訊安全政策符合以下事項：

5.2.1.1 適合本公司的目標。

5.2.1.2 包含資訊安全目標。

5.2.1.3 包含滿足適用之資訊安全要求事項的承諾。

5.2.1.4 包含持續改善ISMS 的承諾。

5.2.2 同時應確保資訊安全政策符合下列要求：

5.2.2.1 以文件化資訊提供。

5.2.2.2 在組織內進行傳達。

5.2.2.3 在需要的時候，提供給利害關係人。

5.3 角色、責任及權限

5.3.1 本公司資安長應指派人員，賦予相關資訊安全管理責任及權限，並確保其責任及權限已被傳達。

5.3.2 受指派人員應確保ISMS 符合ISO/IEC 27001 標準的要求事項，並向資安長報告ISMS 之執行成效。

5.3.3 本公司人員之職務、執掌及權限說明詳見『資訊安全編組跟權責（HENGS-IM-3-002）』。

6. 規劃

6.1 因應風險及機會之行動

6.1.1 一般要求

6.1.1.1 本公司在規劃ISMS 時，應將4.1 所提及的相關議題，以及4.2 中提及的要求事項

納入考量，來確認需要因應的風險與機會，以：

6.1.1.1.1 確保ISMS 能達到預期的結果。

6.1.1.1.2 防止或減少意外的影響。

6.1.1.1.3 持續改善。

6.1.1.2 本公司應規劃以下事項：

6.1.1.2.1 因應風險及機會的行動。

6.1.1.2.2 將各項行動整合及實作在 ISMS 流程中的方式。

6.1.1.2.3 評估所採取之行動有效性的方法。

6.1.2 資訊安全風險評鑑

本公司之資訊安全風險評鑑流程訂定於『資訊安全風險評估管理程序書（HENGS-IM-2-001）』中，包含下列各項要求：

6.1.2.1 建立資訊安全風險準則，包括：

6.1.2.1.1 風險接受準則。

6.1.2.1.2 執行資訊安全風險評鑑的準則。

6.1.2.2 確保重複的資訊安全風險評鑑，能夠產出一致、有效，且可比較的結果。

6.1.2.3 識別資訊安全風險，包括：

6.1.2.3.1 應用資訊安全風險評鑑流程，識別 ISMS 範圍內與喪失資訊之機密性、完整性及可用性相關聯的風險。

6.1.2.3.2 識別風險擁有者。

6.1.2.4 分析資訊安全風險，包括：

6.1.2.4.1 評估當 6.1.2.3.1 所識別之風險發生時，可能導致的潛在後果（衝擊）。

6.1.2.4.2 評估6.1.2.3.1 所識別之風險發生的可能性（機率）。

6.1.2.4.3 判定風險等級。

6.1.2.5 評估資訊安全風險，包括：

6.1.2.5.1 以6.1.2.1 所建立之風險準則，比較風險分析結果。

6.1.2.5.2 針對已分析風險，訂定風險處理優先順序。

6.1.3 資訊安全風險處理

本公司之資訊安全風險處理流程訂定於『資訊安全風險評估管理程序書（HENGS-IM-2-001）』中，包含下列各項要求：

6.1.3.1 依據風險評鑑結果，選擇適當的風險處理項目。

6.1.3.2 針對選定的風險處理項目，決定所有必要的控制措施。

6.1.3.3 將6.1.3.2 決定的控制措施與 ISO/IEC 27001 附錄A進行比對，並確認沒有遺漏任何必要的控制措施。

6.1.3.4 產出『適用性聲明書（HENGS-IM-1-002）』，並確認其中已列明 ISO/IEC 27001 附錄 A 中所有控制措施，且說明適用或排除的衡量理由。

6.1.3.5 制定風險處理計畫，並由風險擁有者確認風險處理計畫之適切性，以及對於殘餘風險之可接受性。

6.2 資訊安全目標及達成規劃

本公司應於年度管理審查中討論下一年度之資訊安全目標，並於次年度進行組織全景分析時，評估是否需要調整，研討過程應做成會議紀錄，使資訊安全相關人員知悉；訂定資訊安全目標時，應將下列事項納入考量：

6.2.1 與資訊安全政策一致。

6.2.2 可量測（若可行）。

6.2.3 考量適用的資訊安全要求事項，以及風險評鑑與風險處理的結果。

6.2.4 受監測。

6.2.5 被傳達。

6.2.6 適時更新。

6.3 變更規劃

當本公司決定需要對 ISMS 進行變更時，應依據『變更作業管理程序書（HENGS-IM-2-002）』執行變更。

7. 支援

7.1 資源

本公司在建立、實作、維持及持續改善ISMS 的過程，應決定並提供下列工作之必要資源：

7.1.1 提供建立及維持 ISMS 所需的人力與設備。

7.1.2 提供實作 ISMS 之必要協助。

7.1.3 確定各項管理程序可配合本公司之營運需求。

7.1.4 識別並提出法令、法規的要求，以及於各項契約上所註明之安全責任與義務。

7.1.5 正確應用所有實施的控制措施，以維持適當之安全管理。

7.1.6 在需要時進行審查，並針對審查結果提出妥適的因應措施。

7.1.7 必要時改善ISMS 之作業流程，以確保其有效性。

7.2 能力

本公司應依據『教育訓練管理程序（HENGS-QM-2-004）』，確保員工有能力執行被要求的工作，並符合各項安全要求，且應確認：影響資訊安全績效之人員，在本公司的規範下執行工作的必要能力。

7.2.1 員工在適當的教育、訓練或經驗之基礎上能勝任工作。

7.2.2 提供必要的教育訓練及技術支援，並評估其有效性。

7.2.3 保留所有教育訓練及有效性評核紀錄，作為員工勝任的證據。

7.3 認知

在本公司的管理下，人員執行工作應有下列認知：

7.3.1 遵循資訊安全政策。

7.3.2 對於ISMS 能有效實施的貢獻，包括資訊安全績效改善後的益處。

7.3.3 未遵循ISMS 要求事項的可能影響。

7.4 溝通或傳達

本公司應依據『溝通管理程序（HENGS-QM-2-029）』，進行相關於ISMS 的內部及外部溝通或傳達，並包含其事項、時間、對象及方式。

7.5 文件化資訊

7.5.1 一般要求

本公司之ISMS 文件化資訊應包括：

7.5.1.1 ISO/IEC 27001 標準中所要求的文件化資訊。

7.5.2 本公司對 ISMS 有效性所制定之必要的文件化資訊。制定及更新本公司於制定及更新文件化資訊時，應依據『文件與紀錄管理程序（HENGS-QM-2-001）』進行，並應確保下列事項：

7.5.2.1 識別及描述。

7.5.2.2 格式及媒體。

7.5.2.3 合宜及適切的審查與核可機制。

7.5.3 文件化資訊控管

本公司在控管相關文件化資訊時，應確保下列事項：

7.5.3.1 在被需要的時間及地點都為可用及適用的。

7.5.3.2 受到適切的保護。

7.5.3.3 已訂定派送、存取、檢索及使用等管控措施。

7.5.3.4 已制定儲存及保存(包括可讀性)的相關規劃。

7.5.3.5 已訂定變更的管理程序。

7.5.3.6 已制定留存及屆期失效的處置方式。

7.5.3.7 為規劃及實作本公司 ISMS，應識別及引用必要之外部來源的文件化資訊，而所引用之外部文件應妥適管理。

8. 運作

8.1 運作規劃及控制

8.1.1 本公司應依據下列方式來規劃、實作及控制所需程序，以建立ISMS：

8.1.1.1 資訊安全目標。

8.1.1.2 資訊安全要求。

8.1.1.3 風險管控措施。

8.1.1.4 風險處理計畫。

8.1.2 本公司應制定各種必要之程序文件，以規劃、建立、實作、監控及持續改善 ISMS，並確保這些文件化之程序足以達成所規劃的 ISMS 目標。

8.1.3 本公司應依據『變更作業管理程序書（HENGS-IM-2-002）』管理規劃的變更，並審查非預期變更的後果，必要時應採行適切的措施，以減輕任何負面的影響。

8.1.4 當有作業委外之行為發生時，本公司應依據『資訊作業委外管理程序書（HENGS-IM-2-003）』辦理，以確保所有委外作業的過程、產品或服務都在本公司的控制下進行。

8.2 資訊安全風險評鑑

本公司應依據『資訊安全風險評估管理程序書（HENGS-IM-2-001）』所規定的時間或狀況來執行資訊安全風險評鑑，並遵照所建立之作業程序，留存資訊安全風險評鑑的所有必要紀錄。

8.3 資訊安全風險處理

本公司應依據『資訊安全風險評估管理程序書（HENGS-IM-2-001）』，實作資訊安全風險處理計畫，並遵照作業程序之規定，留存資訊安全風險處理的所有必要紀錄。

9. 績效評估

9.1 監督、量測、分析及評估

本公司應依據『內部稽核管理程序（HENGS-QM-2-21）』進行 ISMS 績效評估，該作業程序中應詳細說明下列事項：

9.1.1 需要監督及量測的事項，包括資訊安全流程與控制措施。

9.1.2 監督、量測、分析及評估的方法，並確保結果的有效性。

9.1.3 應執行監督及量測的時間。

9.1.4 應執行監督及量測的人員。

9.1.5 應針對監督及量測的結果進行分析與評估的時間。

9.1.6 應執行分析及評估這些結果的人員。

9.2 內部稽核

本公司應依據『內部稽核管理程序（HENGS-QM-2-21）』進行內部稽核，並提供文件化資訊，以確定 ISMS 是否：

9.2.1 符合本公司所制定之要求事項。

9.2.2 遵循ISO/IEC 27001 標準的要求。

9.2.3 有效的實作及維持。

9.3 管理審查

本公司應依據『管理審查程序（HENGS-QM-2-003）』進行管理審查，以確保ISMS 持續的合宜性、適切性及有效性。

10. 改善

10.1持續改善

本公司應依據『矯正與預防措施管理程序（HENGS-QM-2-024）』，持續改善 ISMS 的合宜性、適切性及有效性。

10.2不符合事項及矯正措施

當不符合事項發生時，本公司應依據『矯正與預防措施管理程序（HENGS-QM-024）針對不符合事項分析成因、採取行動及追蹤結果，以避免不符合事項再次或於別處發生。

11. 審查

11.1本政策每年應至少檢討審查一次，以反映內部資通安全需求、外在網路環境變化、政府法令法規及資通安全技術等最新發展現況，確保本公司對於營運持續及服務提供的能力。

11.2 本政策如遇到本公司發生重大變革或嚴重資安事件時，應立即實施審查，以確保其適切性及有效性。必要時應通告相關外部單位共同遵守。

12. 發行

本政策由資安長核准，並於公告日施行，發布後應公開傳達(書面、電子郵件、會議宣達或其他方式皆可)給本公司內部員工及各相關外部單位，修訂時亦同。

13. 相關文件

13.1 適用性聲明書（HENGS-IM-1-002）

13.2 資訊安全風險評估管理程序書（HENGS-IM-2-001）

13.3 變更作業管理程序書（HENGS-IM-2-002）

13.4 資訊作業委外管理程序書（HENGS-IM-2-003）

13.5 資訊資產管理程序書（HENGS-IM-2-004）

13.6 人力資源安全管理程序書（HENGS-IM-2-005）

13.7 實體及環境安全管理程序書（HENGS-IM-2-006）

13.8 存取控制管理程序書（HENGS-IM-2-007）

13.9 運作安全管理程序書（HENGS-IM-2-008）

13.10 通訊安全管理程序書（HENGS-IM-2-009）

13.11 資訊安全事件管理程序書（HENGS-IM-2-010）

13.12 營運持續運作管理程序書（HENGS-IM-2-011）

13.13 系統開發與維護管理程序書（HENGS-IM-2-012）

13.14 人員資訊作業安全管理說明書（HENGS-IM-3-001）

13.15 資訊安全編組跟權責（HENGS-IM-3-002）

13.16 防火牆運作管理說明書（HENGS-IM-3-004）

13.17 營運持續運作計畫（HENGS-IM-3-005）

13.18 文件與紀錄管理程序（HENGS-QM-2-001）

13.19 管理審查程序（HENGS-QM-2-003）

13.20 教育訓練管理程序（HENGS-QM-2-004）

13.21 內部稽核管理程序（HENGS-QM-2-021）

13.22 矯正與預防措施管理程序（HENGS-QM-2-024）

13.23 組織規劃與利害關係人管理程序（HENGS-QM-2-026）

13.24 溝通管理程序（HENGS-QM-2-029）