OOOO 公司

資訊安全管理作業程序

ISMS-B-001

版本 1.0

中華民國 105 年 MM 月 DD 日

1. 目的

制訂○○股份有限公司（以下簡稱本公司）電子商務資訊系統服務之資訊安全管理制度作業規範，依過程導向（規劃、建立、實施、維護、審查與持續改善）的管理循環，建立完善的資訊安全管理框架，達成資訊安全管理目標，降低資訊作業風險，進而保障資訊系統服務使用者之權益。

2. 範圍

適用於本公司資訊安全管理制度及電子商務資訊系統服務之相關作業。

3. 權責

3.1 資訊安全管理委員會

本公司資訊安全管理階層決策組織。

3.1.1 制定、審查及核准資訊安全政策。

3.1.2 審查資訊安全政策目標與確認控制措施的有效性。

3.1.3 提供資訊安全所需的資源。

3.1.4 資訊安全特定角色職責指派。

3.1.5 維護資安全認知。

3.1.6 協調資訊安全相關工作。

3.2 資訊安全推動組

本公司資訊安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資訊安全相關議題於資訊安全管理委員會提報。

3.2.1 資訊安全工作分組

3.2.1.1. 資訊安全管理工作規劃與執行。

3.2.1.2. 執行資訊安全風險及實施風險處理。

3.2.1.3. 協調及支援資訊安全管理制度之安全措施。

3.2.1.4. 執行資訊安全推動組之交辦決議事項。

3.2.1.5. 資訊安全事故之預防、監控、預警及處理。

3.2.1.6. 資訊安全事故通報流程之規劃與監督。

3.2.1.7. 資訊安全教育訓練規劃與執行。

3.2.2 內部稽核分組

3.2.2.1. 擬定資訊安全管理制度稽核計畫及執行稽核活動。

3.2.2.2. 確認資訊安全管理制度之落實與遵行情形。

3.2.3 資訊安全文件管理分組

3.2.3.1. 依據【資訊安全管理作業程序】辦理，執行文件管理。

3.2.3.2. 協助文件之納管、編號、發行、保存與註銷。

3.2.3.3. 文件管制紀錄歸檔納管。

3.3 本公司所有主管及同仁(含工讀生等非正式員工)、資訊系統服務使用者及委外人員

3.3.1 配合資訊安全管理制度活動。

3.3.2 遵守相關資訊安全管理制度規範。

4. 定義

4.1 資訊安全(information security）：避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織和軟硬體功能等，以保護本公司資訊資產的機密性、完整性、可用性之安全；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。

4.2 資訊安全管理系統（Information Security Management System, ISMS）：為整體管理系統的一部份，以營運風險導向（作法）為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全；等同資訊安全管理制度。

4.3 適用性聲明

描述與組織之 ISMS 相關且對其適用之各項控制目標與控制措施的已文件化聲明。

4.4 資訊安全管理制度文件

為保護組織內資訊資產安全所建立、文件化、實作及維持的程序。

4.5 資訊安全管理制度紀錄

遵循安全要求與資訊安全管理制度有效運作的證據。

4.6 資訊安全管理制度稽核

資訊安全管理制度之獨立資訊安全檢查，以決定各項活動及相關結果是否與計畫的安排相符及此等安排是否有效執行及達成目標。

4.7 機密性(Confidentiality)：確保只有經授權的人才可以存取資訊。

4.8 完整性(Integrity)：確保資訊與處理方法的正確性與完整性。

4.9 可用性(Availability)：確保經授權的使用者在需要時可以取得資訊及相關資產。

4.10 文件

適用於管理制度相關之政策、作業流程管理辦法、標準作業細則及表單等書面資料，均屬之。

4.11 外來文件

非本公司訂定之文件，該文件內容會適用本公司管理制度之文件內容依據或補充規範者。

4.12 紀錄：

執行適用管理制度之相關控制時所需之各項表單、各式紀錄或報告。

4.13 資產（asset）：對組織有價值的任何事物。

4.14 資訊資產：對組織有價值的任何事物，如資訊、人員、軟體、硬體、服務與建築與保護類設施等皆屬之。

4.15 重要資產：指資產價值 C+I+A 綜合所得 12 分(含)以上且可用性(A)為 4 之資產。

4.16 弱點

是指資訊資產內部可能遭受威脅利用之處。

4.17 威脅

危及資訊資產的外在因素，如天然災害、惡意攻擊等。

4.18 風險

威脅利用弱點對資訊資產所造成影響之可能性。

4.19 外部議題

評估組織的外部情況可包括，但不侷限於下列：

4.19.1 無論是國際、國家、區域抑或地方的文化、社會、政治、法令、規章、財務、技術、經濟、天然及競爭環境。

4.19.2 對組織的目標具有衝擊影響之主要推動者及趨勢。

4.19.3 與外部利害相關者的關係，及其感知及價值觀。

4.20 內部議題

評估組織的內部全景可包括，但不侷限於下列：

4.20.1 治理、組織之結構、角色及可歸責性。

4.20.2 政策、目標，以及可達成政策及目標的策略。

4.20.3 由資源及知識（例如：資金、時間、人員、過程、系統及技術）的觀點所瞭解的能力。

4.20.4 資訊系統、資訊流及決策過程（正式及非正式兩者）。

4.20.5 與內部利害相關者的關係，及其感知及價值觀。

4.20.6 組織的文化。

4.20.7 組織所採用的標準、指導綱要及模型。

4.20.8 契約關係之形式及範圍。

4.21 風險評鑑

風險分析與風險評估的整個過程。

4.22 風險評估

把預估的風險和已知的風險準則進行比較的過程，以決定風險的顯著性。

4.23 風險分析

系統性的使用資訊，以識別緣由與估計風險。

4.24 風險值

依據資訊資產之價值、風險及風險之影響程度所計算出之等級或數值。

4.25 可接受之風險

考量在可供選擇的控制目標與控制方式、成本與有限資源分配下，所決定之可容忍風險程度。

4.26 風險管理

藉由協調各項活動以指導與控管組織之有關風險。

4.27 風險處理

選擇與實作措施的過程藉以修正風險。

4.28 殘餘風險

資訊資產於實施風險處理後所剩餘的風險。

4.29 資訊安全稽核

係一種有系統且獨立的資訊安全檢查，以決定各項活動及相關結果是否與所計畫的安排相符，此等安排是否予以有效執行，以及是否可以達成目標。

4.30 內部稽核

由內部稽核小組針對作業程序之安全控制、保護措施、風險評估、營運持續計畫等，進行定期查核，以確保其成效。

4.31 外部稽核

由外部單位進行資訊安全、個資保護稽核。

4.32 矯正措施

為避免不符合資訊安全管理制度之事件重複發生，所採取之措施，即消除不符合事項之原因，以防止再發生。

4.33 預防措施

為預防潛在不符合資訊安全管理制度要求之事件發生所採取之措施，即消除潛在風險之原因，以防止其發生。

5. **作業內容**

5.1 資訊安全管理制度建立與管理

5.1.1 資訊安全推動組應依據本公司電子商務資訊系統服務之營運活動與所面臨的風險及 CNS27001 指導規範之『規劃—執行—檢查—行動』(PDCA)模式，建立、實作、運作、監視、審查、維持與持續改善文件化的資訊安全管理系統。

5.1.2 資訊安全管理制度係管理本公司重要的資訊資產，以『規劃—執行—檢查—行動』(PDCA)模式來建置與維護，確保此制度有效運作，所有活動都有適當的文件記載或紀錄說明之，包括：

5.1.2.1. 定義資訊安全政策
5.1.2.2. 說明資訊安全管理系統的範圍
5.1.2.3. 評鑑風險
5.1.2.4. 訂定控管目標與機制
5.1.2.5. 實施風險處理計畫
5.1.2.6. 撰寫適用性聲明書
5.1.2.7. 實施與操作
5.1.2.8. 監控、定期審查及稽核
5.1.2.9. 執行矯正與預防措施作業程序

5.1.3 【資訊安全政策】為本公司資訊安全管理最高指導原則，其制定應考量組織特性與組織風險全景、法令、法規要求，建立資訊安全各項作為原則，並由資訊安全管理委員會所核准，並依據 5.1.4 風險管理程序審視資訊安全管理制度範圍內資訊資產之風險，並實施各項風險控制機制，以保障資訊資產之機密性、完整性與可用性。

5.1.4 依據本公司電子商務資訊系統服務之業務需求、組織風險全景、組織文化、資訊資產、應用技術等特性，將資訊安全管理制度範圍與驗證範圍分別訂定於【資訊安全政策】與「適用性聲明書」中，並由資訊安全管理委員會核准並維護其適切性；各措施的機制分別列述於下列文件：

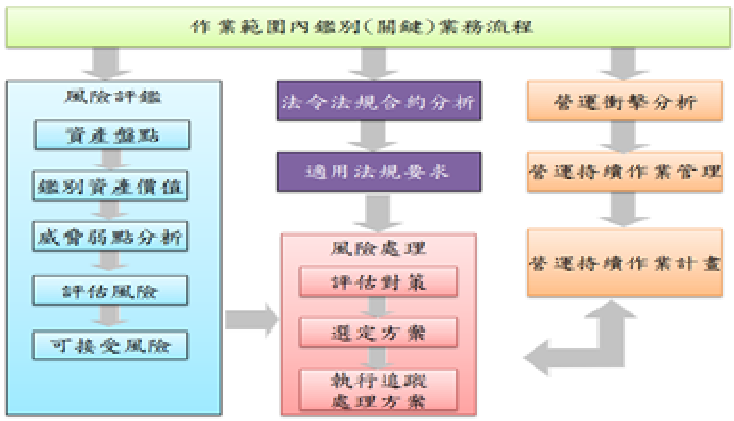
5.1.4.1. 【資訊安全政策】
5.1.4.2. 【資訊安全管理作業程序】
5.1.4.3. 【資訊安全組織管理流程】
5.1.4.4. 【資訊資產管理作業程序】
5.1.4.5. 【人力資源安全管理作業程序】
5.1.4.6. 【實體與環境安全管理作業程序】
5.1.4.7. 【通訊與作業管理作業程序】
5.1.4.8. 【存取控制作業程序】
5.1.4.9. 【資訊系統獲取、開發及維護管理作業程序】
5.1.4.10. 【供應商管理作業程序】
5.1.4.11. 【資訊安全事故管理作業程序】
5.1.4.12. 【業務持續管理作業程序】
5.1.4.13. 【遵循性管理作業流程及程序】

5.1.5 依據CNS27001 國際標準要求與附錄A之控制目標與控制措施及本公司所建立之系統文件，提出「適用性聲明書」來佐證系統之完整性與可用性。

5.1.6 風險管理程序

5.1.6.1. 資訊資產風險評鑑及風險處理之流程與主要作業項目

與程序，以下圖表示



5.1.6.2. 風險評鑑時機

5.1.6.2.1. 風險評鑑作業每半年定期執行，並由資訊安全推動組決定評鑑範圍。

5.1.6.2.2. 如遇組織變更、作業流程變更、資訊資產異動或發生重大資訊安全事故、資訊安全管理範圍有變動、營運系統架構重大改變等，資訊安全推動組得針對特定範圍內之資訊資產進行風險評鑑。

5.1.6.3. 資訊安全風險評鑑作業規劃

進行風險評鑑之前應就以下關鍵事項進行先期規劃，以確保風險評鑑作業之有效性。

5.1.6.3.1. 識別組織全景與利害相關方及定義風險評鑑範圍。

5.1.6.3.1.1. 識別組織全景與關注方之需求與期望，並將上述資料識別分析結果彙整於「利害相關方與相關議題調查表」。

5.1.6.3.1.2. 風險評鑑的範圍、評鑑的主體(如業務流程、資訊系統、單位等)。

5.1.6.3.1.3. 風險評鑑範圍之相關業務單位之資訊安全有關之事物、計畫、關係人（組織）、會影響資訊安全管理制度之內部及外部議題。

5.1.6.3.1.4. 風險評鑑範圍之相關業務之描述及其環境、現行已知之資訊安全現況（如對於資訊安全的要求、現行資訊安全控制等資訊）。

5.1.6.3.1.5. 風險評鑑範圍各業務依全公司運作觀點之關鍵優先次序。

5.1.6.3.1.6. 風險評鑑範圍之相關業務之業務目標。

5.1.6.3.1.7. 風險評鑑範圍之相關業務近中程發展計畫對業務之主要可能變化。

5.1.6.3.1.8. 風險評鑑範圍之相關業務的關係人（如內部往來單位、外部往來機關、委外服務、服務對象、

客戶、使用者等）及其對於資安的要求。

5.1.6.3.1.9. 風險評鑑範圍之相關業務須遵循的法規標準或合約規範。

5.1.6.3.1.10. 風險評鑑範圍內已發生過之資訊安全事故與事件以及障礙維修等資訊，並參考外部已發生過之資訊安全事故。

5.1.6.3.1.11. 風險評鑑範圍內其他應特別考量的內、外部的資源、慣例、限制與衝擊影響、功能特性及組織要求等因素。

5.1.6.3.2. 定義並維護「威脅弱點清單」及「威脅弱點衝擊影響判定表」之威脅、弱點、風險內容及衝擊影響等評估準則及風險計算原則並參考上述之資訊進行威脅、弱點之評選，以確保風險評鑑各項結果資料的可比較性、重複性及完整性。

5.1.6.4. 風險評鑑方法

5.1.6.4.1. 依據「資訊資產清冊」之各項資產進行風險評鑑作業並紀錄於「風險評鑑清冊」;「風險評鑑清冊」於完成作業後應轉呈風險擁有者確認，於核定後再轉呈資訊安全委員會核准。

5.1.6.4.2. 資訊資產的風險值是以資訊資產價值以及自身弱點之脆弱度、所面臨威脅發生機率及其風險衝擊影響面所構成。

5.1.6.4.3. 資訊資產鑑別（識別清查），依據【資訊資產管理作業流程及程序】執行所轄之資訊資產清查作業。

5.1.6.4.4. 資訊資產評價（評估價值），由風險擁有者針對資產之機密性、完整性、可用性，並考量組織特性與法令、法規要求所構成進行評估。評估標準依據「資訊資產評估原則表」辦理。

5.1.6.4.5. 資訊資產群組

資產在同一流程或系統，存在於相同實體、邏輯環境之特定條件下歸類為同一作業流程群組，以利進行風險鑑別作業，作業流程群組資產之資產價值取各資訊資產最高者。

5.1.6.4.6. 為確保風險評鑑一致與準確性，將針對代表各項資訊資產之資訊資產群組進行風險評鑑，資訊資產群組歸類方式可依照資訊資產性質是否相同、是否存在於相同的實體環境、是否面臨相同的弱點與威脅來進行。

5.1.6.4.7. 弱點與威脅之分析，針對各項資訊資產群組之使用及管理現狀，識別資訊資產群組所面臨之內部弱點及外在威脅。並針對資訊資產群組弱點之脆弱度及威脅之發生機率進行評分，評分標準參照「威脅弱點衝擊影響判定表」。

5.1.6.4.8. 每一資訊資產群組依據「威脅弱點清單」分析威脅脆弱點發生機率可能性，再依據「威脅弱點衝擊影響判定表」決定衝擊影響大小，進而產生風險值且可能會有一或多個風險值。

5.1.6.4.9. 計算風險值與訂定風險等級

5.1.6.4.9.1. 總風險值之計算

1. 資訊資產價值 =

   機密性評價＋完整性評價＋可用性評價

2. 風險值 =

   資訊資產價值x威脅發生可能性x脆弱點利用難易度x風險衝擊度

5.1.6.4.9.2. 訂定風險等級

將總風險值的最大值為 324 與最小值為 3 相減，再分成四等級分。即：風險等級的級距(Y)＝【總風險值最大值－總風險值最小值+1】/ 4。

1. D 等級的區間範圍=【總風險值最小值)~【總風險值最小值+Y-1】，即風險值介於 3~83 分者屬之。
2. C 等級的區間範圍=【總風險值最小值+Y】~【總風險值最小值+2xY-1】，即風險值介於 84~164 分者屬之。
3. B 等級的區間範圍=【總風險值最小值+2xY】~【總風險值最小值+3xY-1】，即風險值介於 165~245 分者屬之。
4. A 等級的區間範圍=【總風險值最小值+3xY】~【總風險值最大值】，即風險值介於 246~324 分者屬之。

5.1.6.4.9.3. 風險等級最高的至最低分別以 A、B、C、D 代表，風險等級所代表的意義說明於后：

等級	風險值	說明
A	246~324	可能影響業務的營運，得視需要在既定時間以內及時處理。
B	165~243	可能影響業務的營運，得視需要進行處理。
C	84~162	可能影響局部系統、業務運作，得視需要處

		理即可。
D	3~81	對系統或業務運作之影響有限，在既定時間以內處理或維持現行控制作業即可。

5.1.6.5. 營運衝擊分析

針對資產價值為 C+I+A 綜合所得 10 分(含)以上且可用性(A)為 4 之重要資產，彙集討論分析，再鑑別出重要系統或服務，並針對重要系統或服務分析其作業流程之關鍵程度、容許衝擊及復原需求，相關討論分析紀錄應留存，並將結果紀錄於「營運衝擊分析表(BIA)」。

5.1.6.5.1. 訂定關鍵次序

對於各項鑑別之關鍵業務營運流程，訂定重要性次序。

5.1.6.5.2. 復原目標時間 (Recovery Time Objectives, RTO)

發生業務營運中斷之事件時，將營運流程恢復至最低服務水準的運作狀態(包含技術及處理)允許花費之時間。

5.1.6.5.3. 資料復原點目標時間 (Recovery Point Objectives, RPO)

中斷事件發生後，足以回復至運作之資料時點(如前一天、前一周等)。備份之頻率及時點必須符合 RPO 要求。

5.1.6.5.4. 資源需求

各項關鍵業務營運之環境與相關人員之要求，進行營運持續運作管理時，愈關鍵之營運業務，對於資源之需求程度愈高，必須投注較多之資源以便及時加以恢復。

5.1.6.6. 法令、合約與義務分析

資訊安全風險評鑑中，法令與合約義務，需依據「遵循性控制作業程序」辦理，並參照已識別之「資訊安全法令及法規現況一覽表」之內容辦理。

5.1.6.7. 鑑別安控機制

以前述所列之威脅、脆弱點與法令、契約義務再參照 CNS27001 之要求擬訂安控機制。

5.1.6.8. 決定風險可接受程度

由資訊安全委員會，以風險評鑑報告為基準決定風險可接受程度，並依風險不可接受程度為目標，採取相對應的安控措施以降低風險；決定之風險可接受程度應知會資訊安全推行組與風險擁有者及相關作業人員。

5.1.6.9. 各單位經風險評鑑而產生之風險等級，應需依資訊安全

委員會決定之風險可接受程度，對不符風險可接受程度之資產採取相關風險處理措施。

5.1.6.10.「風險評鑑報告」之撰寫，依據資訊資產風險值之評估結果，撰寫風險評鑑報告，提報資訊安全推動組審查。

5.1.6.11. 風險處理程序

5.1.6.11.1. 可接受風險之決定，由資訊安全推動組審查風險評鑑報告，依據風險衝擊程度、風險處理急迫性及可接受的成本與分配資源，決定可接受之風險。

5.1.6.11.2. 風險處理計畫之擬訂，依據可接受風險之決定，將資訊資產不可接受之風險進行處理，由 風險擁有者擬訂所轄資訊資產之風險處理措施，彙整成「風險處理計畫」。

5.1.6.11.3. 執行各項風險控制措施前應評估執行後風險減緩之效益，並產製風險減緩後之風險再評鑑工作底稿，以供資訊安全推動組審查。

5.1.6.11.4. 風險處理之選項可包括下列選項：

1. 決定不開始或不繼續會引起風險的活動，以避免風險。
2. 承受或增加風險以尋求機會。
3. 移除風險來源。
4. 改變可能性。
5. 改變結果(後果)。
6. 與另一團體或多個團體分攤風險(包含契約及風險資金提供)。
7. 藉由現有資訊之分析與支持而決定保留風險。

5.1.6.11.5. 選定安控目標與機制

將威脅/脆弱點、法令/契約義務與現行狀況相關必要的安控機制、服務等級與現況分析等一起考慮，以選定安控目標與機制，又因預算、人力與資源可能有所限制故會有實施的優先順序，其選定的原則為以風險等級為考慮重點。

5.1.7 適用性聲明書

適用性聲明依據風險評鑑及風險處理結果，選擇適用與不適用的 CNS27001 附錄 A 控制項目，並於「適用性聲明書」中說明其原因。

5.1.8 資訊安全風險之溝通

資訊安全風險評鑑作業時，資訊安全推動組成員及利害相關人員，應溝通對於資產價值、威脅弱點選擇、資訊安全要求與風險處理方案之選用，並利用作業說明或討論會方式統一工作方法及產出物，以確保風險值之一致性及相關人員對於風險管理有一致性的作法與標準。

5.2 資訊安全管理制度實施與運作

5.2.1 為管理風險，應依據「風險處理計畫」執行各項風險控制措施，並提報資訊安全推動組核定、追蹤及持續改善。

5.2.2 應實施與維護資訊安全政策目標、「適用性聲明書」與「風險處理計畫」所選擇控制措施或控制措施群組，並建立有效性評估方式，詳列於「控制措施有效性量測表」。

5.2.3 為有效推動與辦理資訊安全之各項工作，資訊安全推動組應依據 5.6 管理階層責任，提供所需資源。

5.2.4 資訊安全事件與事故應依據【資訊安全事故管理作業程序】規範，進行通報與處理。

5.3 資訊安全管理制度監視與審查

5.3.1 資訊安全管理制度之實施與運作情形，應依據 5.7 資訊安全管理制度內部稽核及 5.8 資訊安全管理制度管理審查，為進行資訊安全管理制度之監視與審查，以確認資訊安全管理制度有效性。

5.3.2 實施控制措施或控制措施群組，應依據「控制措施有效性量測表」之規劃週期進行有效性評估，以確認各項安全要求皆已符合，並於管理審查會議進行討論與決議。

5.3.3 風險處理計畫執行成效之評估，於下次風險評鑑作業時確認殘餘風險及風險處理計畫之執行是否達到預期目標，並於管理審查會議進行討論與決議。

5.4 資訊安全管理制度維持與改進

5.4.1 資訊安全管理制度監視與審查結果，應依據 5.9 資訊安全管理制度矯正預防，並於管理審查會議進行討論與決議。

5.5 資訊安全管理制度文件與紀錄管理

5.5.1 資訊安全管理制度文件管理

5.5.1.1. 資訊安全管理制度文件架構

類別	說明
政策（一階文件）	政策（Policy）-資訊安全最高指導文件。
程序（二、三階文件）	流程或程序（Procedure）-規範資訊安全各項作業的方式、權責及各項工作細節及標準工作方法。
表單（四階表單）	表單、紀錄（Records）、清冊-執行資訊安全各項控制作業時使用或產出。

5.5.1.2. 資訊安全管理制度文件與紀錄機密等級，依據【資訊資產管理作業程序】辦理。

5.5.1.3. 資訊安全文件管制中心應製作「資訊安全管理制度文件一覽表」，條列出最新的資訊安全管理制度文件清單及版次，並公告於內部網站，以提供相關同仁查閱參考。

5.5.1.4. 非本公司制訂之資訊安全管理制度有關文件，如：上級主管機關規章、國際性標準等，資訊安全文件管理分組應製作「外來文件一覽表」，管控外來文件。

5.5.1.5. 資訊安全管理制度文件編號及撰寫格式標準

管理項目	作業原則
文件編號	一 ~ 三階文件編號 1 2 3 4　5　6 7 8 □□□□-□-□□□ 第 1、2、3、4 碼：ISMS 資訊安全文件代碼。 第 5 碼：文件階別，A 表一階、B 表二、三階、D 表四階。 第 6、7、8 碼：文件編號，文件編號由 001 開始，例 ISMS-A-001。 四階文件編號 1 2 3 4　5　6 7 8　9 10 □□□□-□-□□□-□□ 1~8 碼同一~三階文件編號，第 9、10 碼：流水號，由 01 開始，例 ISMS-B-001 資訊安全管理作業程序，產製的第一個表單附件「資訊安全文件標準格式」則表單編號為 ISMS-B-001-01。
紀錄編號	年度　流水號 □□□-□□□□表單使用的流水號原則上以年度+流水號編列，例：105 年度第一次填寫的紀錄，其紀錄流水號為 105-0001，以此類推。
文件目錄、內文格式	文件目錄：除一階政策外，二、三階文件架構應包含文件目的、範圍、權責、定義、作業說明、相關資料與附件。 內文格式：文件內字體、編號應有一制性。文件應註記文件名稱、文件編號、版次及其機密等級。 文件內文引用其它文件名稱標示方式採【】樣式，文件產出之附件於敍明時採「」樣式方式標明。

5.5.1.6. 資訊安全管理制度文件簽核權責

作業 / 類別	制訂/修訂/廢止	審查	決行/發布	管理
政策（一階文件）	文件負責人	資訊安全專員	資訊安全管理委員會	資訊安全文件管理分組
流程及程序（二、三階文件）	文件負責人	資訊安全專員	文件負責單位最高主管	
表單（四階表單）	隨附文件辦理審查			

5.5.1.7. 文件制訂、修訂、廢止之申請，由文件負責人填寫「資訊安全管理文件制訂、修訂及廢止申請單」，並依據資訊安全管理制度文件簽核權責由相關人員進行審查、決行與發布。

5.5.1.8. 送審文件與表單版次應一致，並附上前次版本文件與表

單，以供審查人員參閱。

5.5.1.9. 文件發布以電子型式公告於內部網站，並以電子郵件方式通知相關人員。

5.5.1.10. 執行資訊安全管理制度相關工作時，所需引用之空白表單，應與公告之版本相符。

5.5.1.11. 文件已無存在之必要，或因內部作業修訂需廢止文件時，依文件發行簽核程序辦理；文件廢止後，原文件編號不可重覆使用。

5.5.1.12. 在過時版本之紙本文件上標示「作廢」字樣以示區別，電子檔則以各管理制度之專屬資料夾保存。

5.5.1.13. 定期檢閱

資訊安全推動組應至少每年一次分批檢閱，由文件負責單位(人員)或與執行文件內容作業相關單位進行年度檢閱，檢閱時應按照「說、寫、做」一致之原則，就不適用之文件提出檢討並修正。

5.5.2 資訊安全管理制度紀錄管理

5.5.2.1. 執行資訊安全管理制度相關工作時，所填寫之表單、紀錄，保存規範須考量組織需求與法令法規要求，若無特別相關規定，至少須保存一年。

5.5.2.2. 資訊安全管理制度表單及紀錄之銷毀，依據【資訊資產管理作業程序】辦理。

5.5.3 文件保護

5.5.3.1. 各部門依文件之特性與類別，給予不同之保護程度。例如：檔案櫃上鎖。

5.5.3.2. 專供現場使用之文件須放置於作業現場。

5.5.3.3. 密級以上(含)之文件不得私自影印。

5.5.3.4. 限閱以上(含)文件不使用時須加以歸檔存放，並予以適當保護。

5.5.3.5. 限閱以上(含)等級之書面文件須存放於檔案櫃或其他安全區域內。

5.5.3.6. 員工離職須將所保管之限閱以上(含)文件列入移交。

5.5.3.7. 未經書面核准，任何員工不得將限閱以上(含)文件攜出辦公場所。

5.5.3.8. 各單位主管可依文件（含限閱以上）之重要性自行決定保管方式。

5.6 管理階層責任

5.6.1 為有效推動與辦理資訊安全之各項工作，由管理階層成立之資訊安全管理委員會，規範資訊安全組織運作方式與工作職

責，以昭示管理階層對資訊安全之重視及支持，進而使資訊安全管理制度能持續並穩健的運作。

5.6.2 資訊安全推動組為支持資訊安全管理制度建立、實施、維護、審查與持續改善，依據 5.8 資訊安全管理制度管理審查進行審查，確認相關控制措施支援營運要求，並確保被指定責任的人員，有能力履行被要求之工作，並提供適當的教育訓練與控制，人員教育訓練依據【人力資源安全管理作業程序】辦理。

5.7 資訊安全管理制度內部稽核

5.7.1 稽核頻率

每半年定期辦理資訊安全內部稽核作業，並視需要採取針對組織、營運業務、資訊安全事件及資訊系統的重大變更等特定目的之不定期稽核。

5.7.2 稽核人員要求

為確保稽核過程的客觀性與獨立性，避免稽核自身工作。稽核人員需有資訊安全制度稽核的經驗。

5.7.3 稽核計畫

應事前規劃並編製資訊安全稽核計畫，以作為執行稽核指導綱要，內容應包括：稽核依據、範圍、程序、人員、項目、預定時程等，由資訊安全推動組核准後執行。稽核計畫格式可參考 5.5.1.5.資訊安全管理制度文件編號及撰寫格式標準。

5.7.4 稽核準則

5.7.4.1. 稽核檢查內容應依據「資訊安全管理制度稽核表」，檢查內容應符合最新 CNS 27001 之要求。

5.7.4.2. 稽核評定原則

5.7.4.2.1. 符合：

實際作業依照書面規範進行;記錄及簽核作業皆按照規定辦理；或已建立書面規範，但尚未有實際作業需求。

5.7.4.2.2. 不符合：

1. 人員雖按照規範執行作業但於過程中發生疏失。
2. 人員作業達到安全控制之目的，但尚未建立完整書面程序或紀錄。
3. 尚未規劃或執行相關安全管理規定。
4. 違反自訂之管理規範。
5. 違反個人資料保護法、CNS27001 標準之要求。

5.7.4.2.3. 不適用：

稽核範圍內作業無需使用的控制項目。

5.7.5 稽核執行

5.7.5.1. 稽核人員依稽核準則執行稽核，抽樣收集足夠之客觀證據，以研判該稽核項目是否符合管理制度要求，稽核時應保存適當的稽核軌跡與佐證資訊。

5.7.5.2. 受稽核人員應尊重及支持稽核人員，並接受調閱有關紀錄、報告及文件。

5.7.5.3. 稽核員應將稽核發現之不符合事項，填列於「資訊安全矯正與預防處理單」，經召集人確認後發出。

5.7.5.4.

5.7.6 稽核報告

5.7.6.1. 稽核人員應將稽核結果彙整後提出稽核報告。稽核報告格式可參考 5.5.1.5.資訊安全管理制度文件編號及撰寫格式標準。

5.7.6.2. 受稽核單位於接獲稽核報告後，稽核計畫中所要求之時限內將該組之缺失分析原因及擬採行之矯正與預防措施填列於「資訊安全矯正與預防處理單」內，且經主管核定後回覆稽核人員，並進行後續追蹤。

5.7.6.3. 稽核報告需連同相關稽核資料，呈送召集人覆核，於覆核完成後交付內部稽核分組列管。

5.7.7 稽核技巧與工具

執行資訊安全稽核時，事件紀錄需包含下列資訊：

5.7.7.1. 系統面：

5.7.7.1.1. 使用者識別碼。

5.7.7.1.2. 登入及登出系統之日期及時間。

5.7.7.1.3. 記錄使用者端(Client)的識別資料或其位址。

5.7.7.2. 作業面：

5.7.7.2.1. 工作日誌（操作紀錄）。

5.7.7.2.2. 異常紀錄。

5.7.7.2.3. 維護紀錄。

5.7.7.3. 執行資訊安全稽核或個資保護稽核時，對於相關系統之存取，應予以監督並留下紀錄，以備日後查考。

5.7.7.4. 系統稽核工具（例如 IDS 等）之存取應由授權人員於授權範圍內操作，並留有存取、操作紀錄，以防止任何可能的誤用或破解。

5.7.7.5. 系統稽核工具應存放於獨立系統及安全的地點內，防止不當操作造成其他系統之損害。

5.8 資訊安全管理制度管理審查

5.8.1 管理審查會議召開時程：

5.8.1.1. 資訊安全推動組每半年應召開一次管理審查會議，必要時得召開臨時會議，相關會議討論與決議事項，應依據權責層級向上呈報。

5.8.2 管理審查會議審查內容應包含：

5.8.2.1. 過往管理審查之議案的處理狀態。

5.8.2.2. 與資訊安全管理制度有關之內部及外部議題的變更。

5.8.2.3. 資訊安全績效之回饋，包括下列之趨勢。

5.8.2.3.1. 不符合項目及矯正措施。

5.8.2.3.2. 監督及量測結果。

5.8.2.3.3. 稽核結果。

5.8.2.3.4. 資訊安全目標之達成。

5.8.2.4. 關注方之回饋。

5.8.2.5. 風險評鑑結果及風險處理計畫之狀態。

5.8.2.6. 持續改善之機會。

5.8.3 管理審查會議之結論應包含：

5.8.3.1. 資訊安全管理制度之有效性改進措施。

5.8.3.2. 風險評鑑與風險處理計畫之更新。

5.8.3.3. 為因應可能影響資訊安全管理制度之內部或外部議題，必要時，會影響資訊安全與個資保護之流程應予修訂，包括：

5.8.3.3.1. 營運需求。

5.8.3.3.2. 安全需求。

5.8.3.3.3. 影響既有營運需求之營運過程。

5.8.3.3.4. 法令或法規要求。

5.8.3.3.5. 合約的各項義務。

5.8.3.3.6. 風險等級及/或風險可接受程度。

5.8.3.3.7. 管理審查決議事項追蹤。

5.8.3.4. 資源需求。

5.8.3.5. 資訊安全控制措施與個資保護措施的有效性如何量測之改進。

5.8.3.6. 資訊安全之管理目標與控制措施之有效測量的評估結果。

5.8.4 管理審查紀錄

管理審查為資訊安全管理制度重要之活動，審查紀錄應依資訊安全管理制度紀錄管理要求辦理。

5.9 資訊安全管理制度矯正預防

5.9.1 矯正及預防執行時機

5.9.1.1. 內部、外部稽核、自行發現之不符合或效能改善事項

時，應提出矯正及預防措施，並填寫於「資訊安全矯正與預防處理單」。

5.9.1.2. 受查部門應應分析問題發生之原因及影響程度，決定優先順序與處理時限，評估措施時須考慮成本效益及可行性，提出矯正與預防措施時，得區分為暫時性對策及永久性對策。

5.9.1.3. 資訊安全推動組應視情況，將永久性對策之預防措施及其風險納入風險評鑑之作業程序或作業模版。

5.9.1.4. 矯正與預防措施之執行狀況，應由受查部門應依據「資訊安全矯正與預防處理單」確實執行，並於「資訊安全矯正與預防處理單」留存追蹤紀錄。

5.9.1.5. 由內部稽核分組負責內部稽核作業所發現之不符合事項的追蹤，並依各缺失部門所提之改善時程追蹤執行狀況。

5.9.1.6. 配合資訊安全委員會之管理審查作業，資訊安全推動組應配合管理審查作業之頻率週期，彙整相關矯正及預防措施呈報資訊安全委員會，進行管理審查。

6. 相關資料

6.1 【資訊安全政策】

6.2 【資訊資產管理作業程序】

6.3 【資訊安全事故管理作業程序】

6.4 【人力資源安全管理作業程序】

7. 附件

7.1 適用性聲明書

7.2 利害相關方與相關議題調查表

7.3 風險評鑑清冊

7.4 資訊資產評估原則表

7.5 威脅弱點清單

7.6 威脅弱點衝擊影響判定表

7.7 營運衝擊分析表(BIA)

7.8 風險評鑑報告

7.9 風險處理計畫

7.10 控制措施有效性量測表

7.11 資訊安全管理制度文件一覽表

7.12 外來文件一覽表

7.13 資訊安全管理文件制訂、修訂及廢止申請單

7.14 資訊安全管理制度稽核表

7.15 資訊安全矯正與預防處理單