OOOO 公司

資訊安全政策

ISMS-A-001

版本 1.0

中華民國 105 年 MM 月 DD 日

文件編號	ISMS-A-001	資訊安全政策	文件類別	普通
版　　次	V1.0		發布日期	105/MM/DD

文件編號	ISMS-A-001	資訊安全政策	文件類別	普通
版　　次	V1.0		發布日期	105/MM/DD

1. **目的**

OO 公司（以下簡稱本公司）為確保電子商務資訊系統服務正常且安全穩定的運作，規範本公司電子商務資訊服務作業之資訊安全管理制度最高指導方針及昭示管理階層之支持，以建立安全、可信賴之電子商務服務體系，期使資訊安全管理持續穩健的運作，提昇整體資訊安全管理，以確保資訊服務作業之機密性、完整性、可用性及符合相關法規之要求，並維持業務持續運作，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範圍內之相關作業與人員。

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. 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；等同本公司所謂之資訊安全管理制度。

4.3 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。

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

4.5 完整性(Integrity)：確保資訊與處理方法的正確性與完整性。

4.6 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。

5. 作業內容

5.1 為達成本公司之任務目標及最高管理階層對資訊安全之期許與要求，資訊安全政策訂為：

5.1.1 確保本公司電子商務資訊系統服務相關資訊之機密性，防止敏感資訊及消費者個人資料免於因內部或外部、蓄意或意外之各種威脅與破壞，致業務資訊遭受竄改、揭露、破壞或遺失等風險。

5.1.2 確保本公司電子商務資訊系統服務相關資訊之完整性與可用性，以正確執行作業與各項業務服務，以保護本公司所管理資訊資產之安全。

5.2 為達成上述資訊安全政策目的，將相關目標訂定如下：

5.2.1 建立資訊資產風險評鑑機制，每年至少進行一次風險評鑑，

並進行風險處理，使資訊資產受到適當之保護，防止未經授權或因作業疏忽對資產所造成之損害。

5.2.2 確保所有資訊安全事件或可疑之安全弱點，皆依適當通報程序反應，並予以適當調查及處理。

5.2.3 確保核心服務作業系統達到全年的可用性要求，每年至少進行一次營運持續計畫之檢討、測試及檢核。

5.2.4 確保資訊安全管理運作持續正常，每年定期實施資訊安全教育訓練，並視情況實施不定期教育訓練。

5.2.5 確保相關資訊安全措施或規範符合政策與現行法令之要求，每年至少進行一次資訊安全內部稽核。

5.3 為督導全體同仁落實遵循資訊安全管理工作規範，每年持續進行適當之資訊安全教育訓練，以建立「資訊安全，人人有責」觀念，並使全體同仁瞭解資訊安全之重要性，藉此提高資訊安全之運作能量，進而促使全體同仁遵守資訊安全規定，因此，本公司資訊安全政策聲明為：

「資訊安全，人人有責」

5.4 資訊安全管理事項

資訊安全管理涵蓋 14 項管理領域事項，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、破壞等情事發生，對本公司帶來各種可能之風險及危害。管理事項如下：

5.4.1 資訊安全政策訂定與評估。

5.4.2 資訊安全之組織。

5.4.3 人力資源安全管理。

5.4.4 資產管理。

5.4.5 存取控制安全。

5.4.6 密碼學。

5.4.7 實體及環境安全。

5.4.8 運作安全。

5.4.9 通訊安全。

5.4.10 資訊系統獲取、開發及維護之安全。

5.4.11 供應者關係。

5.4.12 資訊安全事故管理。

5.4.13 營運持續管理之資訊安全層面。

5.4.14 遵循性。

5.5 管理原則

5.5.1 本公司高階主管應宣示落實資訊安全之決心，以確保本公司資訊安全措施之實施，責成相關單位與人員成立資訊安全委

員會、資訊安全推動組及專責人員，並配置資訊安全責任與進行有效之資源管理。

5.5.2 資訊安全委員會、資訊安全推動組及專責人員等成員因故無法參與各項資訊安全活動時得由其代理人暫代之。

5.5.3 資訊安全委員會、資訊安全推動組與專責人員及本公司各單位主管，應透過適當的標準和程序以實施本政策。

5.5.4 資訊安全委員會應建立及審查此政策，定期召開管理審查會議，以確保本政策符合現行需求。

5.5.5 資訊安全推動組應定期提供員工資訊安全訓練課程，提昇人員資訊安全認知。

5.5.6 應考量相關法律規章及營運要求，進行資訊資產之資訊風險評估，確定資訊作業安全需求，建立作業標準程序，採取適當資訊安全措施，確保資訊資產安全。

5.5.7 依人員角色及職能為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導活動，確保同仁皆知悉資訊安全要求。

5.5.8 資訊資產存取權限之賦予，應業務需求並考量最小權限、權責區隔及獨立性審查。

5.5.9 建立資訊安全事故管理程序，以確保事故妥善回應、控制與處理，並訂定業務持續計畫並定期演練，以確保資訊系統或服務持續運作。

5.5.10 依據個人資料保護法與智慧財產法之相關規定，審慎處理及保護個人資訊與智慧財產權。

5.5.11 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實。

5.5.12 本公司之各單位及所有員工、各連線使用單位、簽約廠商及委外廠商都應遵循並落實本政策之規定與相關要求。

5.5.13 本公司所有委外廠商皆須簽署保密協議書，並遵循本政策以及相關程序之規定，不得未經授權使用或濫用本公司之各類資訊資產。

5.5.14 違反本政策與資訊安全相關規範，依相關法規或本公司人事規定辦理，並視情節追究其民事、刑事及行政責任。

5.6 管理審查與核准

5.6.1 本政策應至少每年評估審查一次，以反映相關法令、技術及營運業務等最新發展現況，並予以適當修訂，以確保資訊安全實務作業確實遵守資訊安全政策和作業之可行性及有效性。

5.6.2 本政策經資訊安全管理委員會核准，於公告日施行，並以書

面、電子或其他方式通知經所有員工及提供資訊服務之廠商，修正時亦同。

6. **相關資料**

6.1【資訊安全管理作業程序】

6.2【資訊安全組織管理作業程序】

7. **附件**

無