OOOO 公司

資訊安全組織管理作業程序

ISMS-B-002

版本 1.0

中華民國 105 年 MM 月 DD 日

1. 目的

為有效推動與辦理 OO 公司(以下簡稱本公司) 電子商務資訊系統服務之資訊安全之各項工作，特成立資訊安全組織，以擬定本公司電子商務資訊系統服務資訊安全發展之方向及策略，進而使資訊安全管理制度持續穩健的運作。

2. 範圍

適用於本公司電子商務資訊系統服務之資訊安全組織管理相關作業。

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。

3.2 資訊安全推動組

本公司電子商務資訊系統服務之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。

4. 定義

無。

5. 作業內容

5.1 資訊安全組織架構

5.1.1 本公司設資訊安全管理委員會，負責本公司資訊安全管理相關事項之討論與決議。

5.1.2 本公司設資訊安全推動組，資訊安全推動組包含資訊安全工作分組、內部稽核分組、資訊安全文件管理分組，成員由資訊安全管理委員會核定，若考量人力因素，得由外部廠商協助辦理。

5.1.3 資訊安全推動組依據資訊安全管理委員會決議與【資訊安全管理作業程序】進行本公司電子商務資訊系統服務之資訊安全管理制度規劃、建立、實施、維護、審查與持續改善。

5.1.4 資訊安全管理委員會

5.1.4.1. 召集人一名：由本公司最高主管或指定之代理人擔任。

5.1.4.2. 副召集人數名：由本公司最高主管指派。

5.1.4.3. 小組委員數名：召集人就相關部門指派主管或指定人員擔任。

5.1.5 資訊安全推動

5.1.5.1. 推動專員一名：由召集人指派任命。

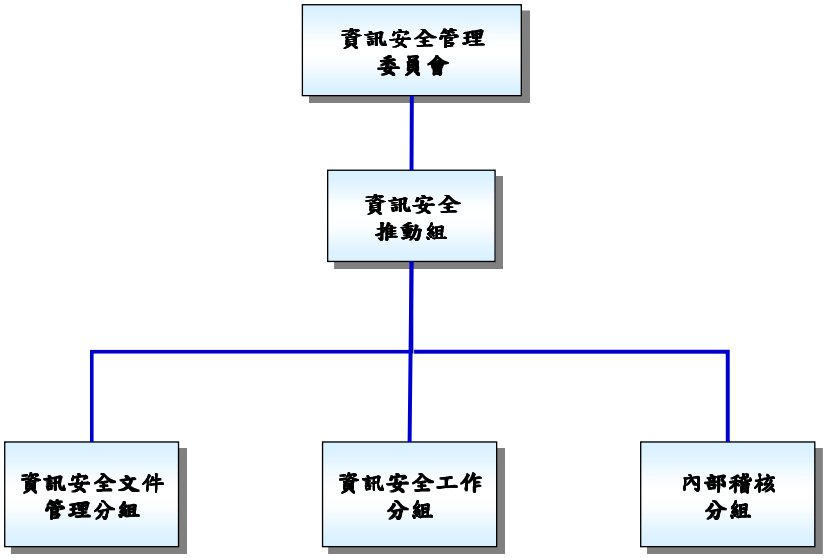
5.1.6 資訊安全工作分組、內部稽核分組

5.1.6.1. 成員數名，由各部門指派相關人員擔任。

5.1.7 資訊安全文件管理分組

5.1.7.1. 文件管理員一名：由推動專員指派任命。

5.1.8 資訊安全組織架構如后：



5.2 資訊安全管理委員會工作項目

5.2.1 制定、審查及核准資訊安全政策。

5.2.2 審查資訊安全政策目標與確認控制措施的有效性。

5.2.3 提供資訊安全所需的資源。

5.2.4 資訊安全特定角色職責指派。

5.2.5 維護資安全認知。

5.2.6 協調資訊安全相關工作。

5.3 資訊安全推動組工作項目

5.3.1 制定、審查及核准資訊安全政策。

5.3.2 審查資訊安全政策目標與確認控制措施的有效性。

5.3.3 提供資訊安全所需的資源。

5.3.4 資訊安全特定角色職責指派。

5.3.5 維護資安全認知。

5.3.6 協調資訊安全相關工作。

5.3.7 確認資訊安全風險及實施風險處理。

5.3.8 辦理資訊安全管理制度之獨立稽核。

5.3.9 持續改善資運安全管理制度。

5.4 資訊安全工作分組工作項目

5.4.1 資訊安全管理工作規劃與執行。

5.4.2 執行資訊安全風險及實施風險處理。
5.4.3 協調及支援資訊安全管理制度之安全措施。
5.4.4 執行資訊安全推動組之交辦決議事項。
5.4.5 資訊安全事故之預防、監控、預警及處理。
5.4.6 資訊安全事故通報流程之規劃與監督。
5.4.7 資訊安全教育訓練規劃與執行。
5.4.8 依據【資訊安全事故管理作業程序】、【業務持續管理作業程序】辦理，執行資訊事件通報處理與業務持續管理項目。
5.4.9 評估資訊由監控所收到的資訊、審查資訊安全事故及建議適當的動作，以回應已識別的資訊安全事故，並要時應請資訊安全推動組尋求專家建議。

5.5 內部稽核分組工作項目
5.5.1 稽核管理分組負責評估資訊安全管理制度之落實與遵行情形，為任務編組，由資訊安全推動組指派人員擔任，依據【資訊安全管理作業程序】辦理，執行稽核。
5.5.2 提出稽核報告及相關建議事項予資訊安全推動組。
5.5.3 報告稽核結果與改善情況之追蹤管理。

5.6 資訊安全文件管理分組工作項目
5.6.1 依據【資訊安全管理作業程序】辦理，執行文件管理。
5.6.2 協助文件之納管、編號、發行、保存與註銷。
5.6.3 文件管制紀錄歸檔納管。

5.7 資訊安全組織人員資格要求
5.7.1 每年應針對不同工作類別之需求，參與各項資訊安全教育訓練及宣導課程。
5.7.2 擔任資訊安全職務之人員，應審慎篩選。
5.7.3 稽核人員資格要求依據【資訊安全管理作業程序】規定。

5.8 內部組織資訊安全管理
5.8.1 資訊安全推動組為資訊安全管理制度之管理權責單位，資訊安全推動組所轄各分組統籌辦理資訊安全管理制度相關事宜，並依據【資訊安全政策】，規劃與制定相關安全作業程序，由資訊安全推動組核准後實施。
5.8.2 資訊安全推動組為達成資訊安全政策目標，資訊安全推動組安全工作角色與職掌明訂於「資訊安全工作執掌表」，以執行安全作業流程及程序，維護資訊資產安全，。
5.8.3 各項資訊資產應依據【資訊資產管理作業程序】，由權責單位指派專人負責，建立資訊資產管理與使用授權程序，並依據風險評鑑結果實施必要控制措施。
5.8.4 電子商務資訊系統服務之相關人員，應依據【人力資源安全

管理作業程序】，簽署保密切結。

5.8.5 資訊安全推動組應取得各方資訊安全建議，以持續改善資訊安全管理制度。

5.8.6 資訊安全管理制度應依據【資訊安全管理作業程序】進行獨立審查，確認資訊安全管理制度落實情形，並且持續改善。

5.8.7 資訊安全推動組應依據【資訊安全事故管理作業程序】與相關權責單位建立通報管道並執行通報作業。相關權責單位與利害團體之聯繫關係及權責應詳列於「資訊安全聯絡名單」。

5.9 外部組織資訊安全管理

5.9.1 外部組織存取組織內之資訊處理設施或資訊時，應依據【資訊安全管理作業程序】評估其風險，並遵循相關資訊安全管理制度或依循標準之要求，採取適當控制措施。

5.9.2 委外合約中，應制定可滿足安全需求之合約條款，並與委外廠商簽訂、遵循保密切結書並執行保密作業。委外開發或維護之應用系統依據【資訊系統獲取、開發及維護管理作業程序】規範辦理。

5.9.3 委外服務內容變更，應審查是否影響相關資訊安全管理制度或依循標準之要求，評估其風險，採取適當控制措施。

5.9.4 委外作業規格書或徵求建議書說明文件，應包含資訊安全要求，並謹慎評估委外廠商資格。

5.9.5 委外廠商須依合約執行相關工作，應提交工作報告或維護紀錄，以監督委外作業契約履行情形及執行績效，並將評估紀錄記載於「供應、委外廠商績效評鑑表」，必要時應稽核委外廠商安全控管措施，評鑑時機可參考專案交付驗收點進行。

5.9.6 委外廠商須遵守本公司內之相關安全規定並配合資訊安全稽核活動。

5.9.7 委外人員執行業務時，應遵守本公司資訊安全相關規定，若違反時應依相關法令、本公司相關規定及契約懲處。

5.9.8 外部組織因應業務需要需存取組織內之資訊處理設施或資訊，應遵守本公司資訊安全相關規定，資訊資產管理權責單位應依據本公司資訊安全相關規定進行安全管制，並告知使用者所須遵循之權責義務，妥善使用資訊處理設施或資訊，涉及資訊資產完整性與隱密性之資訊安全管理範圍者，應簽署保密協議書，使其瞭解未遵循本公司資訊安全相關規定或有行使任何危及本公司資訊安全之行為，應依公司內相關懲處管理規範處理或訴諸適當之懲罰或法律行動。

6. **相關資料**

6.1【資訊安全管理作業程序】

6.2【實體與環境安全管理作業程序】

6.3【通訊與作業管理作業程序】

6.4【存取控制管理作業程序】

6.5【資訊安全事故管理作業程序】

6.6【業務持續管理作業程序】

6.7【資訊安全政策】

6.8【資訊資產管理作業程序】

6.9【人力資源安全管理作業程序】

6.10【資訊系統獲取、開發及維護管理作業程序】

7. **附件**

7.1 資訊安全工作執掌表

7.2 資訊安全聯絡清單

7.3 供應、委外廠商績效評鑑表