OOOO 公司

遵循性管理作業程序

ISMS-B-012

版本 1.0

中華民國 105 年 MM 月 DD 日

文件編號	ISMS-B-012	遵循性管理作業程序	文件類別	限閱
版　　次	V1.0		發布日期	105/MM/DD

1. 目的

OO 公司(以下簡稱本公司）為使資訊安全管理制度，符合相關法令、法規、契約義務、資訊安全政策目標及 CNS27001 資訊安全之要求，爰訂定遵循性控制之管理程序。

2. 範圍

適用於本公司所有資訊安全管理制度相關的法律、法規與合約。

3. 權責

3.1 軟體管理單位

負責統籌辦理軟體之需求評估及軟體管理等事項。

3.2 資訊安全推動組

3.2.1 資訊安全管理制度規劃、建立、實施、維護、審查與持續改善。

3.2.2 定期呈報資訊安全管理委員會，有關資訊安全管理制度相關的法律、法規與合約異動狀況。

3.3 內部稽核分組

負責或協助遵循性查核活動執行。

3.4 本公司所有同仁、資訊系統服務使用者及委外人員

遵守本公司適用的法令、法規、契約義務、資訊安全政策目標及 ISO 27001 標準要求。

4. 定義

4.1 電腦軟體

係指商業套裝或自行開發之電腦程式及電腦程式存放電子媒體。

4.2 軟體管理

係指關於軟體之增置、登記、管理、盤點、減損、移轉與使用宣導等事項。

4.3 資訊安全管理適用法規

本公司資訊安全管理適用之外部法令、法規、主管機關要求與本公司內部規定。

5. 作業內容

5.1 識別適用法規

5.1.1 資訊安全推動組應識別資訊安全管理適用法令、法規，並依據【資訊安全管理作業程序】維護「外來文件一覽表」，以供相關同仁參閱。

5.1.2 資訊安全推動組應鑑別公司所需遵循的法律、法規及合約要

求，並根據蒐集到的法律、法規、標準、合約、保密書或切結書加以識別，並對其資料內容進行適用性評鑑，將識別出適用的法律、法規、標準、合約、保密書或切結書填寫於「資訊安全法令及法規現況一覽表」。

5.1.3 資訊安全推動組應依據適用之法規要求，執行紀錄管理，紀錄管理依據【資訊安全管理作業程序】與【通訊與作業管理作業程序】規範辦理。

5.1.4 本公司同仁應遵守智慧財產權與資訊安全相關之要求。

5.1.5 業務資料之蒐集或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾業務目的之必要範圍，資料處理作業依據個人資料保護法、【資訊資產管理作業程序】、【存取控制管理作業程序】規範保護與控管資料，避免資料未經授權外洩與資訊處理設施的誤用。

5.1.6 合約、保密書或切結書蒐集範圍：

5.1.6.1. 採購合約書。

5.1.6.2. 委外合約書。

5.1.6.3. 員工之保密書合約書。

5.1.6.4. 委外保密切結書。

5.1.6.5. 其他有關資訊安全作業之保密要求事項規範。

5.1.7 法律、法規、標準蒐集範圍：

5.1.7.1. 個人資料保護法。

5.1.7.2. 個人資料保護法施行細則。

5.1.7.3. 勞動基準法

5.1.7.4. 電子簽章法。

5.1.7.5. 著作權法。

5.1.7.6. 通訊保障及監察法。

5.1.7.7. 刑法：

5.1.7.8. 妨害電腦使用罪。

5.1.7.9. 無故入侵電腦罪。

5.1.7.10. 無故取得、刪除或變更電磁記錄罪。

5.1.7.11. 干擾電腦罪。

5.1.7.12. 製作專供電腦犯罪之程式罪。

5.1.7.13. ISO/CNS 27001 標準。

5.1.7.14. PCI DSS 標準。

5.2 軟體管理

5.2.1 電腦軟體(以下簡稱軟體)使用之權利及義務，依著作權法、智慧財產權、主管機關管理要求、版權規定及議定之契約協議辦理，且嚴禁使用任何非法或未經授權使用之軟體。

5.2.2 為尊重智慧財產權，於本公司內部一律使用合法軟體，並禁止使用非法軟體、禁止下載與散播非法音樂、影片及未經授權使用之軟體，不得使用來路不明之軟體，亦不得測試來路不明之軟體。

5.2.3 本公司軟體增置之方式如下：

5.2.3.1. 自行開發。

5.2.3.2. 購置。

5.2.3.3. 委託開發。

5.2.3.4. 授權使用。

5.2.3.5. 隨硬體設備附贈。

5.2.3.6. 他機關贈與。

5.2.3.7. 其他合法增置。

5.2.4 本公司軟體購置原則如下：

5.2.4.1. 相同之軟體集中採購。

5.2.4.2. 使用者多之軟體，採用網路版或授權使用方式。

5.2.4.3. 訓練用之軟體，採合約授權使用方式。

5.2.5 增置之軟體於正式啟用前，應由軟體管理單位確認已完成請採購程序，並登錄增置軟體於「軟體清冊」。軟體異動作業完成後，依發生之事實進行登錄，以備查。驅動程式（光碟、硬碟、磁帶、印表機、掃瞄器、數據機、多媒體、儀器等設備所用）免予登錄。

5.2.6 軟體授權證明、安裝光碟片與相關手冊文件，由軟體管理單位或軟體使用者負責保管，其職務異動或離職時，應移交其保管或使用之軟體及相關手冊文件，並辦理軟體異動登錄，如有遺失應負相關責任。不需使用之軟體得辦理繳回。

5.2.7 使用者如需使用或複製軟體，需洽詢軟體管理單位確認授權問題。

5.2.8 軟體管理單位及軟體使用者對於保管或使用之軟體如有盜賣、循私營利或其他不法情事時，違法情節提報考績委員會議處，並依法究辦。

5.2.9 軟體管理單位對使用中之軟體，應視需要查核實際使用狀況，並作為軟體增置之參考資料。

5.2.10 軟體管理單位應辦理軟體之授權與數量清點，每年至少一次，並更新「軟體清冊」。

5.2.11 軟體申請程序

5.2.11.1. 軟體使用申請者填寫資訊系統需求申請單，提出軟體安裝申請需求與詳細計畫內容。

5.2.11.2. 未依規定粘貼本公司財產標籤之電腦設備，不予提供

軟體維護服務；若遇電腦設備財產編號粘貼作業不及之情況則不在此限。

5.2.11.3. 軟體管理單位不受理未經核准之私人電腦維護安裝需求與非授權本公司使用之軟體安裝申請。

5.2.11.4. 嚴禁於本公司電腦安裝未經核准（Freeware 或 Shareware）與無合法授權之軟體，每半年會同查核單位排定軟體使用稽核，如有違反智慧財產權等相關法令規範及組織規範之情事，將由該部設備保管人員負相關責任，並依本公司相關管理辦法處理。

5.3 遵循性管理

5.3.1 資訊安全管理制度遵循性查核

資訊安全推動組應依據【資訊安全管理作業程序】規範，至少每年辦一次理資訊安全管理制度與 CNS 27001 標準遵循性審查及稽查作業。

5.3.2 應特別識別與審視，涉及個人資料之資訊

5.3.2.1. 應依個人資料保護法之規範辦理，並明確識別該資料之蒐集、處理及利用之合法性。

5.3.2.2. 需特別著重保護以防未經授權之存取與揭露並確保資訊之機密性及秘密通信之人權自由，包括時間、日期、資訊內容、通訊內容及使用者個人資料及隱私等資訊。

5.3.3 資訊安全推動組應定期辦理技術遵循性查核，以確定資訊系統及網路設備符合資訊安全管理制度與 CNS27001 標準要求，技術脆弱性檢測依據【資訊系統獲取、開發及維護管理作業程序】規範辦理。

5.3.4 資訊系統稽核工具保護

5.3.4.1. 執行技術遵循性查核，內部稽核分組需擬執行計畫，並將計畫提報於資訊安全推動組，並經同意後，始得進行。

5.3.4.2. 遵循性查核執行高風險作業時（如：滲透測試、阻斷服務攻擊、暴力破解等），應先備妥配套應變措施，防止業務中斷。

5.3.4.3. 技術遵循性查核應使用合法且安全工具，設定存取權限管制，並由授權人員於查核範圍內操作，以防止資訊處理設施的誤用。

5.3.4.4. 遵循性查核資料存取要求，依據【資訊資產管理作業程序】規範辦理，資料調閱應由資訊安全推動組授權，並會同內部稽核分組進行調閱。

6. **相關資料**

6.1【資訊安全管理作業程序】。

6.2【通訊與作業管理作業程序】
6.3【存取控制管理作業程序】
6.4【資訊資產管理作業程序】
6.5【資訊系統獲取、開發及維護管理作業程序】

7. **附件**

7.1 資訊安全法令及法規現況一覽表
7.2 軟體清冊