OOOO 公司

資訊安全事故管理作業程序

ISMS-B-009

版本 1.0

中華民國 105 年 MM 月 DD 日

1. 目的

確保 OO 公司（以下簡稱本公司）於為確保資訊安全事故發生時，能迅速依通報程序進行通報，並採取必要之應變措施，降低事件可能帶來之損害。

2. 範圍

適用於本公司資訊安全組織與資訊安全管理制度範圍內資訊安全事件通報及危機處理作業。

3. 權責

3.1 事件或事故發現者

發現疑似資訊安全異常事件或事故時，本公司同仁與委外人員皆負有即時通報之責任。

3.2 資訊安全工作分組

3.2.1 資訊安全事故通報流程之規劃。

3.2.2 確定事故影響範圍並作影響評估。

3.2.3 執行資訊安全事故偵測、預防、通報、分析及處理。

3.3 內部稽核分組

協助資資訊安全工作分組處理因應計畫、危機處理、分析報告及改善措施作業等事項。

3.4 資訊安全推動組

督導資訊安全事故偵測、預防、通報、分析及處理。

4. 定義

4.1 資訊安全事件

系統、服務或網路發生一個已識別的狀態，其指示可能的資訊安全政策違例或保護措施失效，或是可能與安全相關而先前未知的狀況等。

4.2 資訊安全事故

單一或一連串有顯著機率可能危害營運作業與威脅資訊安全之非所欲或非預期的資訊安全事件。

4.3 外部支援單位

委外廠商、司法警政及消防機關、政府網路危機處理中心（GSN-CERT/CC）、國家資通安全會報技術服務中心、台灣電腦網路危機處理暨協調中心（TWCERT/CC）、電子商務資安服務中心(EC-CERT)等等。

5. **作業內容**

5.1 資訊安全事故通報與處理程序

5.1.1 發現有可疑資訊安全事件或事故時，應向資訊安全工作分組人員進行資訊安全事故通報。

5.1.2 資訊安全工作分組人員於收到通知後需研判是否為資訊安全事故，將研判結果填寫於「資訊安全事故報告單」通知資訊安全推動組。

5.1.3 資訊安全推動組應確認「資訊安全事故報告單」之判定是否適切，如確定為資訊安全事故，則由資訊安全推動組召集資訊安全工作分組進行後續處理。

5.1.4 資訊安全工作分組依據事故嚴重程度，進行事故分級，資訊安全事故等級區分為四級：

5.1.4.1.『4』級：

5.1.4.1.1. 密級或營運或客戶資料遭洩漏。

5.1.4.1.2. 重要資訊基礎建設系統或資料遭竄改。

5.1.4.1.3. 重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

5.1.4.2.『3』級：

5.1.4.2.1. 密級或敏感資料遭洩漏

5.1.4.2.2. 關鍵業務系統或資料遭嚴重竄改。

5.1.4.2.3. 關鍵業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。

5.1.4.3.『2』級：

5.1.4.3.1. 非屬密級或敏感之關鍵業務資料遭洩漏。

5.1.4.3.2. 關鍵業務系統或資料遭輕微竄改。

5.1.4.3.3. 關鍵業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。

5.1.4.4.『1』級：

5.1.4.4.1. 非關鍵業務資料遭洩漏。

5.1.4.4.2. 非關鍵業務系統或資料遭竄改。

5.1.4.4.3. 非關鍵業務運作遭影響或短暫停頓。

5.1.5 資訊安全工作分組若判定為 2 級（含）以下之資安事故，由資訊安全工作分組進行處理，並將處理結果回覆資訊安全推動組與通報之權責單位主管。若處理過程中如發現造成之影響大於原先等級判定，應立即更正事故分級。

5.1.6 資訊安全工作分組若判定為 3 級（含）以上，應評估事故處理時間，並通知資訊安全推動組專員及資訊安全管理委員會召集人，由召集人決定是否應啟動業務持續計畫，資訊安全

推動組專員應決定是否向上級單位通報，適時尋求外部單位協助處理。

5.1.7 啟動業務持續計畫，依據【業務持續管理作業程序】規範辦理。

5.1.8 資訊安全推動組專員應負責對外說明資訊安全事故處理進度。

5.2 資訊安全事故管理

5.2.1 處理資訊安全事故時，由資訊安全推動組負責配合或支援相關單位之溝通協調，並提供資訊安全工作分組必要資源。

5.2.2 辨識資訊安全事故之根因，並採取有效對策，並應依據資訊安全事故分類，決定事故處理的方法與程序。

5.2.3 『2』級(含)以上之資安事件處理作業依照「資訊安全管理作業程序」執行，並對資安事件受影響範圍依照「矯正-復原-檢討」的順序處理，執行矯正及預防作業。

5.2.4 資訊安全工作分組應分析引發資訊安全事故之弱點、威脅與處理成本，記錄於「資訊安全事故報告單」，定期將資訊安全事故統計資訊提交資訊安全管理委員會中報告，以利資訊安全管理制度持續改善及建立從資安事件、事故中學習經驗。

5.2.5 資訊安全事故涉及違反國家訂定法律，於資訊安全事故處理過程中，應進行蒐證與證據保留，如有需要得向外部支援單位或向檢警單位協助處理。

6. **相關資料**

6.1 【業務持續管理作業程序】。

7. **附件**

7.1 資訊安全事故報告單。