智新資通股份有限公司

文件名稱：資訊安全事故管理程序			
文件編號：ISMS-2-017	版本：A	頁次：1/5	發行日期：2023/01/07

版本修訂紀錄表

文件版本	制/修訂日期	修訂重點內容	修訂人員
A	2023/01/07	初稿	潘彣昕

智新資通股份有限公司

文件名稱：資訊安全事故管理程序			
文件編號：ISMS-2-017	版本：A	頁次：2/5	發行日期：2023/01/07

1. 目的：

確保於資訊安全事件發生時，能迅速依程序進行通報，並採取必要之應變措施與建立事件學習機制，以降低事件所造成之損害。

2. 範圍：

本公司軟體開發之相關資訊資產之資訊安全事件管理。

3. 權責：

3.1. 發現人員：所有人員（含：本單位人員、約聘僱人員與委外駐點人員），發現疑似資訊安全事件時，皆負有即時通報之責任。

3.2. 系統、網路管理員：資訊安全事件處理之權責單位，須執行資訊安全事件之分析及處理。

3.3. 管理代表：督導資訊安全事件通報、處理及分析作業。

4. 名詞釋義：

4.1. 資訊安全事件：凡於作業環境中，導致資訊資產之機密性、完整性、可用性遭受影響之事件。

4.2. 內部危安事件：發現（疑似）遭人為惡意破壞毀損、作業不慎等事件。

4.3. 外力入侵事件：發現（疑似）電腦病毒感染事件、駭客攻擊（非法入侵）等事件。

4.4. 天然災害：颱風、水災、地震等。

4.5. 突發事件：火災、爆炸、重大建築災害及資訊網路系統骨幹中斷事件等。

4.6. 核心系統或服務：影響軟體開發作業之資訊服務。

5. 作業內容：

5.1. 資安弱點識別

本公司與相關資安論壇、國家資通安全會報保持聯繫，並不定期向原廠及委外維護廠商提出諮詢，以獲取威脅情資，並進一步採取適切控制措施。

5.2. 事件通報作業

5.2.1. 為建全通報體系，應建立並維護相關服務廠商之「委外廠商服務人員名冊」。

5.2.2. 當系統異常事件發生時，需依”異常事件分級”要求進行通報作業。

5.2.3. 若異常事件需尋求外部支援時，依「委外廠商服務人員名冊」進行通報。

5.2.4. 資訊安全事件造成同仁生命安全或設備遭到破壞等涉及民事或刑事案件時，應通報檢調單位請求支援並協助處理。

5.2.5. 每次異常事件發生時， 須將異常事件記錄於「資訊安全事件報告單」。

5.3. 事件辨識作業

5.3.1. 記錄人員應紀錄異常事件發生狀況、異常事件處理方式及發生原因。

5.3.2. 由記錄人員根據異常事件影響程度不同，進行分級、通報

5.3.3. 資訊安全事件等級分為三個級別，由重至輕分別為「三級」、「二級」及「一級」。

5.3.3.1. 三級事件

符合下列任一情形者，屬三級事件：

(1) 極機密等級資料遭洩漏。

(2) 核心業務系統或資料遭嚴重竄改。

(3) 核心業務運作遭影響或系統停擺，無法於可容忍中斷時間內回復正常運作。

三級事件需於網路/系統負責人發現或接獲通知30分鐘內通知管理代表及主任委員，處置結果需呈主任委員審核。

5.3.3.2. 二級事件

符合下列任一情形者，屬二級事件：

(1) 機密等級資料遭洩漏。

(2) 核心業務系統或資料遭輕微竄改。

(3) 核心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。

(4) 非核心業務運作遭影響或系統停擺，不可於可容忍中斷時間內回復正常運作。

二級事件需於網路/系統負責人發現或接獲通知2小時內通知管理代表，處置結果需呈主任委員審核。

5.3.3.3. 一級事件

智新資通股份有限公司

文件名稱：資訊安全事故管理程序			
文件編號：ISMS-2-017	版本：A	頁次：4/5	發行日期：2023/01/07

符合下列任一情形者，屬一級事件：

(1) 內部使用資料遭洩漏。

(2) 非核心業務系統或資料遭竄改。

(3) 非核心業務運作遭影響或短暫停頓。

一級事件需於4小時內通知管理代表，處置結果需呈管理代表審核。

5.3.4. 事件負責人員應依資訊安全事件狀況協調設備(系統)管理人員辦理事件辨識作業，並將辨識結果紀錄在「資訊安全事件報告單」之資安事件辨識作業欄位中。

5.4. 事件緊急應變作業

5.4.1. 處理事件負責人應依資訊安全事件辨識結果，針對異常狀況協調資訊單位採取緊急應變措施，並將應變方法與注意事項紀錄在「資訊安全事件報告單」。

5.4.2. 緊急應變措施應以隔離或停止事件發生之設備、系統、環境及存取權限或連線為原則。

5.5. 事件排除作業

5.5.1. 負責人應依資訊安全事件發生之原因，協調資訊單位進行事件排除作業。

5.5.2. 為避免事件排除作業造成重要資料或鑑識證據之遺失，應於事件排除作業前完成重要設定檔、資料與鑑識記錄檔之備份。

5.5.3. 備份作業完成後，應確認備份資料之有效性與可用性，以避免備份失敗導致資料毀損。

5.5.4. 事件排除作業除需移除資訊安全事件原因外，應依事件發生原因加強防護，並將加強防護的措施紀錄在「資訊安全事件報告單」作為往後資訊安全日常管理的參考，以避免相同事件再次發生。

5.6. 系統復原作業

5.6.1. 資訊安全事件排除後，若有需要應由網路/系統管理員進行系統復原作業。

5.6.2. 事件負責人應於系統復原3天內，加強監視系統運作，確認系統屬於正常作業。

5.7. 事故矯正措施

5.7.1. 採取矯正措施時，應使用適切的資料來源，以分析檢討異常情況發生之原因，針對應

智新資通股份有限公司

文件名稱：資訊安全事故管理程序			
文件編號：ISMS-2-017	版本：A	頁次：5/5	發行日期：2023/01/07

改善事項確實檢討改進，並期能避免相同異常事件的再發生。

5.7.2. 單位主管審閱異常事件發生狀況及影響程度，依情況嚴重度給予處理。

5.7.3. 若為一、二級異常事件，可即時解決，且影響程度不大，記錄異常事件處理情形，呈請管理代表簽名結案。

5.7.4. 若為三級異常事件，重大之異常事件，可能造成法律訴訟、或影響公司營運及形象，或長期重複發生之異常事件，需進行後續處理及改善追蹤，應依「資訊安全矯正措施管理程序」研擬預防與矯正對策。

5.8. 事件檢討與學習

5.8.1. 資訊安全事件處理過程應由事件負責人填寫「資訊安全事件報告單」，並保存所有事件分析及處理紀錄。

5.8.2. 資訊安全事件處理結果，應定期彙整，描述事件發生原因、過程、處理方式、改善與注意事項等，做為內部資安宣導及事件預防之參考資訊，原則上，由事件負責人於事件處理結案後，以郵件公告方式及於年度資安通知訓練時進行宣導。

5.8.3. 若具有標準化之需要時，須採取適當的管制措施，如新增或變更作業程序。

6. 相關文件：

6.1. 資訊安全矯正措施管理程序(ISMS-2-004)

7. 使用表單：

7.1. 資訊安全事件報告單　　(ISMS-2-017-01)

7.2. 委外廠商服務人員名冊　　(ISMS-2-011-02)