二階文件

文 件 類 別	程序書
文 件 名 稱	資安事件應變處置及通報作業程序
文 件 編 號	GP-MP-047

制 修 訂 記 錄		
版次	發行日期	制 修 訂 要 點
A	113/09/19	新制定

核 准	審 查	主 辦	文件發行章

一、 目的

本程序旨在為公司處理資訊安全事件提供明確的規範。當事件發生時，可依照既定的通報程序迅速通報，並採取必要的應變措施，以降低事件可能帶來的影響，此外，通過事件的處理與檢討，建立學習機制，減少未來類似事件造成的損害。

二、 適用範圍

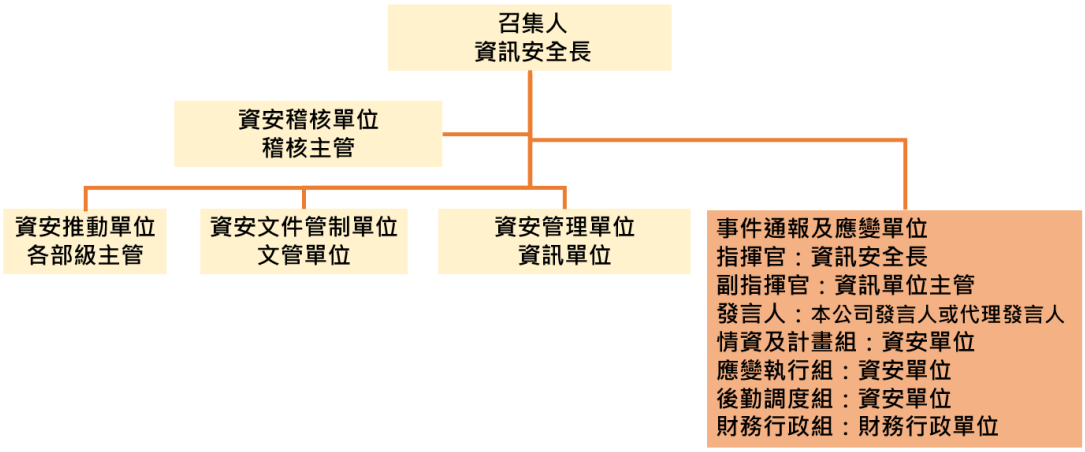
用於全體員工、承包商、合作夥伴及其他訪問公司資訊資產的第三方，涵蓋公司所有資訊系統、網路、資料及相關資產

三、 名詞定義

1. 資訊安全事件:系指在作業環境中，資訊或資通系統的機密性、完整性或可用性遭受破壞的任何事件。
2. 發現人員: 包括所有公司成員，無論是正式員工還是非正式人員（如臨時員工或派駐人員），均負有發現並即時通報疑似資訊安全事件的責任。

四、 資訊安全管理組織

資訊安全管理組織



五、 資訊安全管理組織權責

職稱	權責說明
召集人	由本公司資訊安全長擔任，負責協調各部門制定及執行資訊安全政策和目標，並進行相關管理作業。召集人需主持會議，公告及宣導資安議題，並在管理階層或董事會報告資安執行情況。
資訊安全專責主管	由召集人指派的專人擔任，主要負責本公司內資訊安全管理。專責主管需掌握並回報資訊安全狀況，針對外部資安管控要求進行應對，並處理相關事件。
資訊安全稽核單位	由稽核室指定專人擔任，除負責資安推動委員會的稽核外，還需評估及執行本公司內外部的資訊安全稽核任務，以確保資安工作符合規範。
資訊安全推動單位	由相關單位部門主管擔任，負責配合資安推動委員會的要求，積極推動及執行本公司內部的資安管理工作，確保資安目標與決策相一致。
資訊安全文件管制單位	由文件管理部門擔任，負責管理與控制資訊安全相關文件的存檔與版本，並提供最新版本給相關部門使用。
資訊安全管理單位	由本公司資安負責部門擔任，負責日常資訊安全管理、紀錄、因應及維護，確保資安管理工作的持續性。

六、 事件通報及應變單位權責

成員責任	權責說明
事件指揮官	資訊安全長兼任，負責總覽全局，指導各單位協同處理，並直接聯繫本公司發言人。
副指揮官	事件指揮官的助手，負責協助處理通報應變小組的各項事務。
發言人	本公司指定的發言人，負責對外發布事件相關訊息，並定期更新通報計畫。
情資及計畫組	由資訊安全專責人員或外聘專家組成，負責收集與分享安全事件情報，並研擬應變策略和計畫。
應變執行組	由資訊安全專責人員或外聘專家組成，負責執行搶救與損害控制工作，並協助系統恢復。完成後對漏洞修補進行審查。
後勤調度組	由資訊安全專責人員或外聘專家組成，負責確保相關資料的保存，並協助進行事件原因分析，提出改善建議。
財務行政組	由財務行政單位組成，負責事件相關的預算調撥及行政支援。

七、 資安事件應變處置及通報作業程序

1. 資安事件發現：當發現或懷疑發生資訊安全事件時，發現人員應根據事件情況，迅速通報相關的資訊安全管理單位，並告知其直屬主管。

1.1 資訊安全管理單位：在收到「資安事件通報單」後，將依據發現人員提供的資料進行記錄與分類。

1.2 研判資訊安全事件: 資訊安全管理單位收到通知後，將進行事件研判，以確定是否為資訊安全事件，若判斷為非資訊安全事件，將結果回覆給發現人員; 若確認為資訊安全事件，將依事件的影響程度通知相關權責單位的主管，以進一步處理。

2. 資訊安全事件之分類

類別	事件狀況
天然災害	如：火災、地震、水災、颱風…等。
機房設施失效	如：不斷電系統、電力或冷氣空調失效等。
系統異常	1. 硬體設備故障，如主機故障，硬體障…等。 2. 系統、軟體異常，如資料庫服務、ERP系統異常…等。
網路異常	網路中斷，如網路無法連接、對外網路無法連接…等。
駭客入侵	駭客攻擊致系統損壞或中斷，如 加密勒索、挖礦病毒、DDoS攻擊。
人員操作失當	1. 執行人員未遵守相關作業程序。 2. 廠商維修及維護人員未依規定執行評估及風險控管作業。 3. 人為蓄意破壞、無意疏失、洩漏機敏資料或違反資安規範之行為。
電腦或週邊失效	個人電腦設備、硬體、軟體、作業系統、電力、網路失效，或週邊設備故障。
設備失竊	設備遭竊。
其他	無法歸於分類項目之事件。

3. 資安事件紀錄

3.1 資訊安全管理單位在發生資安事件時，應詳細記錄相關資訊。包括資安事件發現的狀況、可能影響的範圍、損失評估、支援申請以及採取的應變措施等，並將這些內容詳細記錄在「資安事件通報單」中。

3.2 將記錄資料提供給[應變執行組]，以便其評估事件等級、影響範圍及進行損害評估判定。

4. 資安事件分級

等級\ 事件衝擊	評估內容
4 級	1. 機密等級資料洩漏 2. 核心業務系統或資料遭受嚴重竄改或毀損 3. 嚴重衝擊多個業務、系統運作，影響本公司聲譽，無法於時效復原
3 級	1. 內部限閱等級資料洩漏 2. 影響核心業務運作或相關系統中斷服務 3. 影響之重要業務、系統運作，可於時效內復原
2 級	1. 一般等級，非核心業務系統 2. 只是資料遭輕微竄改，業務運作遭影響或系統效率低 3. 不影響重要業務、系統運作
1 級	1. 非核心業務之資產 2. 受到衝擊的損失程度很低，不影響業務、系統運作

5. 資安事件通報: 發現資訊安全事件後，發現人員應立即以電話通知資訊安全管理單位，並由通報單位或資訊安全管理單位填寫「資安事件通報單」，提交給[應變執行組]。

5.1 ［應變執行組］ 應根據情況，尋求維護廠商或本公司相關人員的協助，以進行事件判斷，並將相關信息填入「資安事件通報單」中。

5.2 過程中需持續向權責主管報告進展情況，待事件處置完成並恢復正常運作後，應將處置結果記錄於「資安事件通報單」中，並根據事件等級逐級報告。

5.3 若資安事件涉及利害關係人（或主管機關/情資共享機構），應依照與各利害關係人制定或要求的通報機制進行通報。

5.1.1 通知利害關係人並記錄通報過程的軌跡。

5.1.2 根據與利害關係人的合約/契約進行事件等級評估。

5.1.3 視利害關係人的要求或具體情況，召開雙方資安防護會議。

6. 資安事件應變處理

6.1 4 至 3 級事件，指揮官由指揮官（召集人）擔任 ；2 至 1 級事件，指揮官由副指揮官擔任(指揮官應視狀況完成緊急應變小組配置，進行異常事件排除及控制)。

6.2 4 至 3 級資安事件須於 **36 小時**內；2 至 1 級資安事件須於 **72 小時**內（完成復原或損害管制)。

6.3 資訊安全事件通報對象、通報方式及處置期限如下表所示:

資訊安全事件等級	指揮統籌	通報方式	處置期限
第 4 級(嚴重)	指揮官	電話(或任何可通訊手段)	接獲通報 36 小時以內
第 3 級(重大)	指揮官		接獲通報 36 小時以內
第 2 級(注意)	副指揮官		接獲通報 72 小時以內
第 1 級(輕微)	副指揮官		接獲通報 72 小時以內

7. 資安事件應變處理

如遇資安事件無法在預定修復時間內完成修復

7.1 應立即通知資訊安全管理單位（資訊單位），並在一小時內釐清事實、可能影響，並重新核定事件等級。

7.2 將重新核定的範圍、損失評估、事件等級、事故分類、資源申請判斷、採取的緊急應變措施以及涉及的利害關係人，補充記錄於【資安事件通報單】中，並評估是否需要聯繫相關維護廠商協助處理事件。

7.3 事故類型採取應變程序必要時，經權責主管同意後，可進行備援或緊急應變作業。

7.4 資安事件等級為 4 級指揮官應成立重大資安事件緊急應變小組，並照上市上櫃公司資通安全管控指引「第三十四條」的規定，啟動重大資安事件通報，並依相關規定進行重大訊息通報。

八、事件追蹤調查

1. 事件發生後，應對相關資訊進行檢討分析，以釐清事件的原因和責任，同時評估是否存在重複發生的風險。對現有資訊環境中的漏洞進行審視和修補，以防止類似事件再次發生。
2. 資訊安全事件的相關線索應妥善保留，以便未來追蹤和分析。
3. 為了有效追蹤並檢討事件的原因，應仔細審視現有環境中的漏洞，並將詳細資訊記錄於「資安事件通報單」中。

九、 檢討改善會議

1. 若發生重大等級以上的資訊安全事件，應在事件處理完畢並得到控制後，由事件指揮官召集相關單位，或委由副指揮官主持檢討會議，深入分析事件發生的原因，以預防類似事件再次發生。
2. 根據檢討會議的結果，由系統負責人執行矯正措施，進行問題的修正作業，旨在降低事件再次發生的風險。
3. 資訊安全事件應納入《資安事件管制表》進行案件管理，並與《資安事件通報單》及事件軌跡資料一同定期提交主管覆核。

十、 附件

1. 資安事件通報單----------GP-MP-04701A
2. 資安事件管制表----------GP-MP-04702A