先益電子工業股份有限公司
資安事件通報及應變作業辦法

1 、目的：

為使公司資安事件之處理有明確的相關規範，當事件發生，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衝擊，並建立事件學習機制，降低事件造成的損害。

2、適用範圍：

公司各項資訊資產之管理，均適用之。

3、名詞定義：

3.1 資訊安全事件：凡於作業環境中，資訊或資通系統之機密性、完整性、可用性，遭受影響導致異常之事件。

3.2 發現人員：指企業所有人，含正式或非正式人員（臨時員工或派駐人員），發現疑似資安事件時，皆負有即時通報之責任。

4、資安事件通報及應變：

4.1、資安事件發現

4.1.1　若發現或疑似資訊安全事件時，由發現人員依事件之人、事、時、地、物，迅速通報資訊部，並告知直屬單位主管。

4.1.2　資訊部人員依發現人員通報之資料填寫「資安事件通報單」，進行記錄及分類。

4.1.3　資訊部於收到通知後，研判是否為資訊安全事件。

（1）　若判斷為非資訊安全事件時，將判斷結果回覆發現人。

（2）　若判斷為資安事件時，則依資安事件之影響程度通知權責主管。

4.1.4　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…
系統異常	硬體設備故障，如主機故障….等 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	執行人員未遵守相關作業程序 廠商維修及維護人員未依規定執行評估及風險控管作業。 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
一般中毒	中毒，但未造成服務異常或中斷。
其他	無法歸於分類項目之事件

4.2 資安事件記錄

資訊部人員於發生資安事件時，應將資安事件發現之狀況、評估可能影響之範圍，詳細記錄於「資安事件通報單」中。提供資訊主管於評估事件等級影響及損害評估判定。

4.3 資安事件分級

4.3.1　資安主管接獲資安事件通報發生時，應先研判資安事件等級之對應。

4.3.2　資安事件等級，共分為 4 級，如下說明：

事件衝擊 等級	評估內容

4 級	機密等級資料洩漏。 核心業務系統或資料遭受嚴重竄改或毀損。 嚴重衝擊多個業務、系統運作，影響企業聲譽
3 級	內部限閱等級資料洩漏。 影響核心業務運作或相關系統中斷服務。 影響重要業務、系統運作
2 級	一般等級，非核心業務系統。 只是資料遭輕微竄改，業務運作遭影響或系統效率降低。 不影響重要業務、系統運作。
1 級	非核心業務之資產。 受到衝擊的損失程度很低，不影響業務、系統運作。

4.4 資安事件通報

4.4.1　資訊安全事件發現後，發現人員應以電話通知資訊部，並由資訊人員填寫「資安事件通報單」提交資訊主管。

4.4.2　資訊主管應視情況尋求維護廠商或公司相關人員協助判斷，並填入「資安事件通報單」中。

4.4.3　需持續向權責主管報告事件處理狀況，待事件處置完成並一切回復正常運作後，須將處置之結果，記錄於「資安事件通報單」中，再依資安事件等級逐級報告。

4.5 資安事件應變處理

4.5.1　4、3 級事件指揮官由總經理擔任，指揮官視狀況進行異常事件排除及控制。2、1 級事件指揮官由資安主管擔任。

4.5.2　資安事件等級，4、3 級事件須於 36 小時內，完成復原或損害管制；2、1 級事件須於 72 小時內復原或損害管制。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	通報對象	通報 方式	處置期限
第 4 級 （嚴重）	總經理	電話 （或任何可通訊	接獲通報後 36 小時以內

第 3 級 (重大)	總經理	手段)	接獲通報後 36 小時以內
第 2 級 (注意)	資安主管		接獲通報後 72 小時以內
第 1 級 (輕微)	資安主管		接獲通報後 72 小時以內

4.5.3 資安事件無法於評估修復完成之時間內修復

(1) 通知資安主管及權責主管，並需於一小時內釐清，發生事實、可能影響，並重新核定等級。

(2) 重新核定之範圍、損失評估與事件等級、事故分類、判斷資源申請、採取之緊急應變措施與利害關係人,補充於【資通安全事故通報單】，並評估是否聯繫相關維護廠商協助事件處理。

4.5.4 視事故類型採取應變程序因應，必要時得經權責主管同意後，進行備援或緊急應變作業。

4.6 資安事件追蹤調查

4.6.1 檢討分析相關資訊以釐清事件發生的原因與責任，並分析是否會重複發生，並審視現有資訊環境的漏洞，加以修補。

4.6.2 資訊安全事件應保留事件發生之線索。

4.6.3 為有效追蹤,檢討事件原因，應審視現有環境的漏洞,細節記錄於「資安事件通報單」。

4.7 檢討改善會議

4.7.1 若為重大等級以上資訊安全事件，於處理完畢且獲得控制後，為預防資安事件不再重複發生，須由總經理或資安主管集相關單位召開資安事件檢討會議，研析問題發生之原因。

4.7.2 依據資安事件檢討會議之結果，由系統負責人執行矯正措施，進行問題矯正的作業，以降低事件再發生的可能性。

4.8 資安事件管制

4.8.1 資安事件應列入[資安事件管制表]進行案件管制

4.8.2　資安事件管制表，連同資安事件通報單及事件軌跡資料，應定期呈主管覆核。

5、使用表單：

5.1 資安事件通報單

5.2 資安事件管制表