延宇資訊股份有限公司

「資訊安全暨隱私資訊管理系統」
安全事件管理程序書

機密等級：一般

編號：YAN-ISMS-02-11

版本編號：2.1

修定日期：2022/04/26

使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

本文件歷次變更紀錄：

版次	修訂日	修訂者	說明	核准者
1.0	2020/01/31	梁維志	新增	楊文欽
2.0	2021/11/08	梁維志	因應導入 ISO 27701，修訂相關規範。	楊文欽
2.1	2022/04/26	梁維志	因外部稽核發現點修訂資訊安全、個資安全事件通報與應變作業流程	楊文欽

本程序書由資訊安全執行小組（個人資料保護推動執行小組）負責維護。

本資料為延宇資訊股份有限公司專有之財產，非經書面許可，不准透露或使用本資料，亦不准複印，複製或轉變成任何其他形式使用。

目錄：

1　目的 2

2　適用範圍 2

3　權責 2

4　名詞定義 3

5　作業說明 3

6　相關文件 7

附件：資訊安全、個資安全事件通報與應變作業流程 8

1　目的

1.1 確保延宇資訊股份有限公司（以下簡稱本公司）於資訊安全暨個資安全事件發生時，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　適用範圍

2.1 本公司資訊業務之資訊安全暨個資安全事件管理。

3　權責

3.1 資訊安全暨隱私保護委員會：審核本公司「安全事件通報與應變作業流程」，並督導資訊安全事件之管理作業。

3.2 資訊安全執行小組及個人資料保護推動執行小組：研擬資訊安全事件通報流程。

3.3 發現人員：所有人員（含：本公司人員、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。

3.4 權責單位：資訊安全、個資安全事件處理之權責單位，須執行資訊安全、個資安全事件之分析及處理。

3.5 資安長、個資管理代表：督導資訊安全、個資安全事件通報、處理及分析作業。

3.6 緊急處理組(資訊安全執行小組、個人資料保護推動執行小組)：

3.6.1　確定事件影響範圍，並評估損失。

3.6.2　協助資訊安全、個資安全事件之通報、處理及分析作業。

3.7 支援單位：

3.7.1　內部單位：協助處理相關法律、人事懲處及採購等問題。

3.7.2　委外廠商：協助處理資訊安全、個資安全事件。

4　名詞定義

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

4.2 內部危安事件：發現（或疑似）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（或疑似）電腦病毒感染事件、駭客攻擊（或非法入侵）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（主幹寬頻）中斷事件等。

5　作業說明

5.1 資訊安全、個資安全事件之管理

5.1.1　應建立資訊安全、個資安全事件之處理作業程序，並賦予相關人員必要責任，以便迅速有效處理資訊安全、個資安全事件。

5.1.2　除正常應變計畫（如：系統及服務之回復作業），資訊安全、個資安全事件之處理程序，應視需要納入下列事項：

5.1.2.1 導致資訊安全、個資安全事件原因之分析。

5.1.2.2 防止類似事件再發生之補救措施。

5.1.2.3 電腦稽核軌跡及相關證據之蒐集。

5.1.2.4 與受影響之使用者進行溝通及說明。

5.1.3 電腦稽核軌跡及相關證據應以適當方法保護，以利下列管理作業：

5.1.3.1 作為研析問題之依據。

5.1.3.2 作為研析是否違反契約或資訊安全規定之證據。

5.1.3.3 作為與委外廠商協商如何補償之依據。

5.1.4 處理資訊安全事件。相關作業程序應注意下列事項：

5.1.4.1 考量單位資源，於最短的時間內，確認回復後之系統及相關安全控制是否完整及正確。

5.1.4.2 向管理階層報告處理情形，並檢討、分析資訊安全、個資安全事件。

5.1.4.3 限定僅授權之人員可使用回復後正常作業之系統及資料。

5.1.4.4 緊急處理步驟應詳實記載，以備日後查考。

5.2 通報程序

5.2.1 疑似資訊安全、個資安全事件發生時，發現人員應依事件歸屬通報權責單位，並副本告知資安長、個資管理代表。

5.2.2 權責單位於收到通知後，研判是否為資訊安全、個資安全事件。若：

5.2.2.1 判定為非資訊安全、個資安全事件時，則將結果回覆予發現人員。

5.2.2.2 判定為資訊安全、個資安全事件時，初估事件處理時間，並通知資安長、個資管理代表。

5.2.2.3 如為個資安全事件時，由資安長決定是否通報客戶，如需通報客戶時，應向相關顧客實施通報。

5.2.2.4 資訊安全、個資安全事件等級區分為：

5.2.2.4.1 一般事件：

5.2.2.4.1.1 非屬密級或敏感之核心業務資料遭洩漏。

5.2.2.4.1.2 非核心業務系統或資料遭竄改。

5.2.2.4.1.3 非核心業務運作遭影響或停頓。

5.2.2.4.1.4 個資遺失、內部未經授權存取個資未造成個資外洩。

5.2.2.4.2 重大事件：

5.2.2.4.2.1 密級或敏感公務資料遭洩漏。

5.2.2.4.2.2 核心業務系統或資料遭竄改。

5.2.2.4.2.3 核心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。

5.2.2.4.2.4 個資遭人竊取。

5.2.3 權責單位於發生資訊安全、個資安全事件時，應立即填具

「YAN-ISMS-04-22 資訊、個資安全事件通報單」。

5.2.4 決策處理：

5.2.4.1 當事件影響較低、衝擊性較小，或僅涉及單位內部、受損程度輕微時（如：電腦病毒感染），由權責單位自行處理，並將處理後狀況通知單位主管、資安長及個資管理代表。

5.2.4.2 處理過程中如發現造成之影響大於原先判定事件，權責單位應立即向資安長、個資管理代表報告，重新執行事件分析辨識。

5.2.5 有關是否啟動營運持續運作計畫，依「營運持續運作管理程序書」辦理。

5.3 危機處理程序

5.3.1 本公司資訊安全、個資管理代表危機處理包括事前建置安全防護機制、事中主動預警與緊急應變，以及事後復原追蹤鑑識偵查等步驟。說明如下：

5.3.1.1 事前建置安全防護機制：

5.3.1.1.1 建置資訊安全暨隱私資訊管理系統及整體防護架構。

5.3.1.1.2 彙整及備妥資資訊安全暨隱私資訊管理相關文件。

5.3.1.2 事中主動預警與緊急應變：

5.3.1.2.1 事件辨識：辨識事件之歸屬及採取之對策，如內部資安事件、外力入侵事件、天然災害或重大突發事件等，並

決定處理的方法與程序。

5.3.1.2.2 事件控制：依據各類事件危機處理之程序，進行事件傷害控制，降低影響的程度及範圍。

5.3.1.2.3 問題解決：事件處理權責單位或負責人須將問題解決。必要時，應向資訊安全執行小組、個人資料保護推動執行小組提出建議方案。

5.3.1.2.4 恢復作業：問題解決後，系統需恢復至事件發生前之正常運作狀態。

5.3.1.3 事後復原追蹤鑑識偵查：

5.3.1.3.1 後續追蹤之精神乃係檢討相關資訊安全、個資安全事件是否會重複發生，並審視現有環境漏洞，透過研析相關資料，以釐清事件發生之原因與責任。

5.3.1.3.2 受損單位依復原程序實施災後復原重建。

5.3.1.3.3 重大資訊安全事件、隱私資訊安全應保留事件發生之線索，如有需要得向檢警單位申請數位鑑識（電腦、網路鑑識）。

6 相關文件

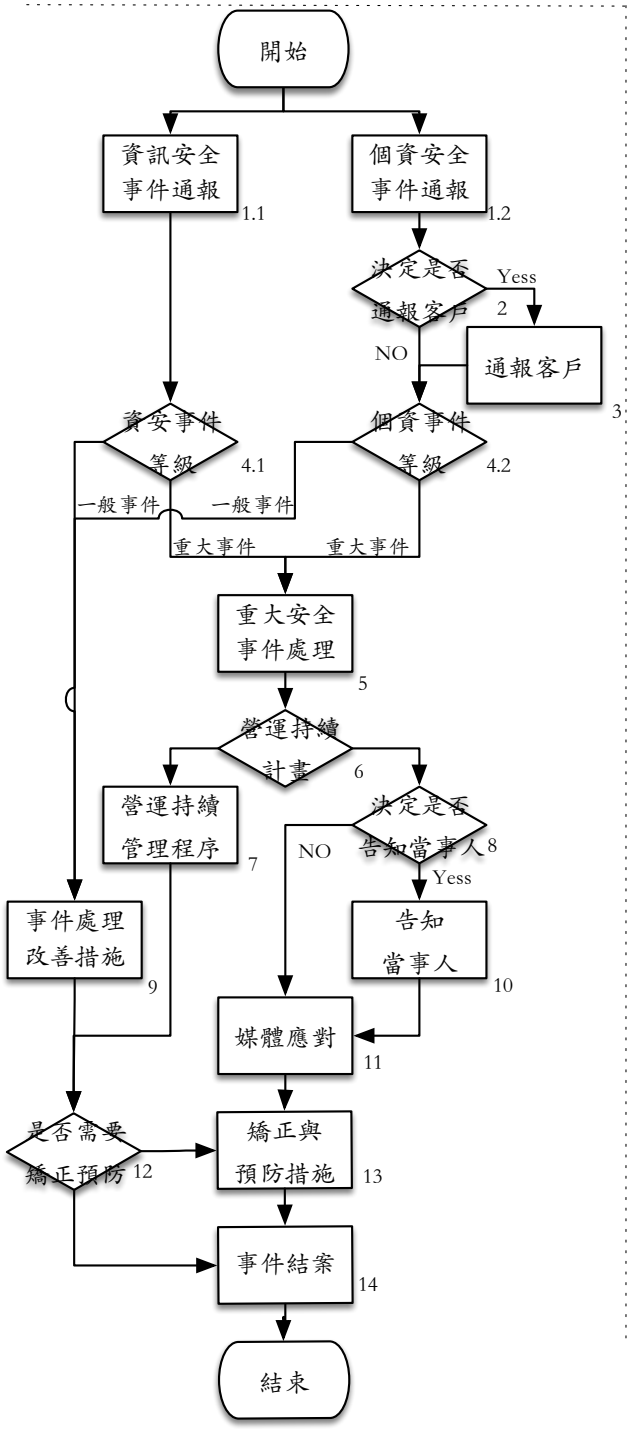
6.1 資訊安全、個資安全事件通報與應變作業流程(附件)

6.2 YAN-ISMS-04-22 資訊、個資安全事件通報單

附件：資訊安全、個資安全事件通報與應變作業流程

1　流程圖：

流程



說明

1 察覺資訊/個資安全事件
1.1 資訊安全事件通報（向資訊通報）
1.2 個資安全事件通報（向個資小組通報）
2. 由資安長決定是否通報客戶
2.1 如需要通報客戶，執行步驟 3
2.2 如不需要通報客戶，執行步驟 4.2
3. 依客戶合約規定執行通報客戶
4.資安/個資事件等級分級，並填寫資訊/個資安全事件通報單
4.1 經判斷為一般事件者，直接執行步驟 9
4.2 經判斷為重大事件者，執行步驟 5
4.3 向資安長/召集人請示是否向檢警單位報案
5 重大安全事件處理
5.1. 進行資訊/個資安全事件之證據蒐集
6. 判斷是否啟動營運持續計畫
6.1. 啟動營運持續計畫，執行步驟 7
6.2. 如為個資事件，執行步驟 8
7. 參考營運持續作業管理程序，並啟動營運持續管理程序
8. 由資長安決定是否告知當事人
9.1. 如決定不告知當事人，執行步驟 9
9.2. 如決定告知當事人，執行步驟 8
9. 事件處理改善措施
10. 告知當事人
11. 媒體應對
11.1. 個資事故發生後，應注意媒體報到，如輿論關注，需對外說明及澄清，應由發言人適時招開記者會說明，或呈請公司同意後，發佈新聞稿
12. 決定是否需要實施矯正預防措施
12.1 如需要執行矯正預防措施，執行步驟 11
12.2 如不需執行矯正預防措施，執行步驟 12
13. 執行矯正預防措施
13.1 依照矯正與預防措施程序，進行該事件之排除或執行預防措施
13.2 資安事故需重新檢討事故發生之原因並擬定改善計畫
13.3 必要時，得重新進行風險評估及個人資料管理機制之設計
13.4 將事故檢討及改善計畫，製作個資事故處理報告，送交個資小組備查
14. 事件結案，必要時依相關法規究責