

德信綜合證券股份有限公司
個資事故及資通安全事件通報處理作業程序

106 年 11 月 17 日訂定

1、目的

為確保本公司發生重大個人資料損害、資訊服務異常或資通安全事件時，能迅速依通報程序進行通報相關權責人員及主管機關，並採取必要之應變措施，降低事件可能帶來之損害，爰依「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」與「證券期貨市場資通安全事件通報應變作業注意事項」，制訂本作業程序。

2、範圍

本公司施作範圍內資訊業務及各單位所保有與管理之個資事件管理。

3、組織及權責

個資管理小組之組織及權責悉依本公司「個人資料檔案安全維護計畫及業務終止後個人資料處理方法」規定辦理。

3.1 發現人

所有本公司相關人員含正式員工與非正式員工(臨時員工或第三方派駐本公司人員)，皆負有通報之責任，應立即通報單位個資管理人員，必要時並會資訊單位處理。

3.2 個資安全人員(單位主管或總經理指派之專案處理人員)

- (1)執行處理個人資料、資訊服務與資通安全事件再確認與分級。
- (2)與各部門適時聯繫，並維持互動。
- (3)負責撰寫及維護本作業程序和個資事件報告。

3.3 管理代表(總經理或其指派之專責人員)

- (1)審查本作業程序。
- (2)進行對於各項管理及處理監督作業。

3.4 個資管理小組

於必要時，負責規劃危機處理程序、蒐集個資資訊、建置個資安全措施、執行個資管理監控、查明安全事件原因、執行緊急應變措施、執行解決辦法、辦理安全事件通報等事項、研議重大個人資料事故之矯正預防措施。

3.5 支援單位

- (1)公司內部單位：協助處理相關個資、法律、人事懲處及採購等問題。
- (2)外單位：委外(第三方)廠商及司法警政等協助處理警政事件調查之單位。

4、個資事件定義

4.1 個資事件，凡於本公司中任何個人資料遭竊取、竄改、毀損、滅失或洩露者；或其他影響本公司資通安全之事件均稱之。

4.2 個資事件影響嚴重程度分級

本公司資安事件影響等級分為 3 個級別：

(1) 3 級事件：符合下列任一情形者，屬 3 級事件：

- A. 敏感資料遭洩露。
- B. 核心業務系統或資料遭嚴重竄改。
- C. 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。

(2) 2 級事件：符合下列任一情形者，屬 2 級事件：

- A. 核心業務一般資料遭洩露。
 - B. 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改。
 - C. 非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；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。
- (3) 1 級事件：符合下列任一情形者，屬 1 級事件：
- A. 非核心業務一般資料遭洩露。
 - B. 非核心業務系統或資料遭輕微竄改。
 - C. 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

4.3 資訊安全事件分類

- (1)系統面：a. 電腦病毒感染及駭客攻擊或非法入侵等事件。
b. 作業不慎致個人資料遭竊取、竄改、毀損、滅失或洩露。
- (2)人為事件：發現或疑似遭人為惡意竊取、竄改、毀損、滅失或洩露。

5、個資或資訊安全事件緊急應變作業程序

5.1 通報對象與其通報方式

- (1)疑似個資安全事件發生時，由發現人通知個資安全人員。
- (2)個資安全人員接獲通報後，應進行初步了解事故及衝擊評估，並立即填寫「個資事故通報記錄表」
- (3)個資安全人員判定事故等級後，如為 2、3 級事件應立即通報管理代表。如為 3 級事件更應立即通知個資管理小組進行因應。
- (4)對外通報受害當事人、主管機關，並視受害狀況必要時通報檢警等治安單位。

5.2 啟動緊急應變措施，控制當事人之損害

當判定事故為 3 級事件時，個資管理小組應執行：

- (1)查明損害情形，並立即進行避免當事人損害擴大的控制方式。
- (2)於「證券期貨市場資通安全通報系統」(以下簡稱通報系統)進行通報。
- (3)必要時須預先擬定對當事人及對主管機關的說明，及指定對外發言人員。
- (4)個資管理小組應緊急調度或取得支援單位之資源及人力。
- (5)如遇資通安全事件，危及人員生命或設備遭到破壞等涉及民、刑事案件時，應作好相關資料(含稽核紀錄)保全工作，通報警察或檢調單位請求處理。

5.3 查明事實：

應由個資安全人員調查個資或資安事故的受害情形、原因及歸屬系統或作業的弱點或疏漏，並擬定對受害當事人之因應措施。

5.4 執行因應措施：

除立即進行避免當事人損害擴大的控制方式外，對所擬定受害當事人之因應措施，應指派專人分工執行，確保事故之妥善解決。

個資或資安事故如涉及相關法律責任、訴訟的事件，應注意相關的系統證據、軌跡資料及相關紀錄的保存以確保能進行後續事件的處理。

5.5 公告及通知當事人

- (1)通知方式以書面、電話、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但耗費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他足以使公眾得知之方式為之。

(2)通知內容應有當事人事故事實、所為因應措施及諮詢專線。

5.6 防止事故再次發生之矯正及預防措施

個資安全人員應提出或審查相關的矯正及預防措施針對個資事故發生的真正原因進行矯正並預防其再發生。

遇有重大個人資料事故者，除應即通報金管會外；所研議之矯正預防措施，並應經公正、獨立且取得相關公認認證資格之專家、進行整體診斷及檢視。

5.7 重大事故後續處理，如需有持續觀察或矯正、預防作業需要時間較長者，本公司應由個資安全人員進行相關審查及監控，確保所有控管事項均被完整執行。事故結案需由管理代表覆核，以確保事故已被完整結案。

6、證券期貨市場資通安全事件通報應變作業注意事項

6.1 適用時機

發生重大影響客戶權益或正常營運之資訊服務異常事件，以及資通安全事件時。

6.2 通報管道

(1)於「證券期貨市場資通安全通報系統」(以下簡稱通報系統)進行通報，通報系統接獲事件通報，自動以簡訊、電子郵件方式同時通知主管機關證期局及相關單位。

(2)前項相關單位：證交所、期交所、櫃買中心、集保結算所、證券商公會、期貨商公會、投信投顧公會等。

(3)本公司、相關單位及主管機關證期局應建立通報聯絡窗口，變更時應及時更新，以確保通報流程順利運行。

6.3 通報作業

(1)初步通報

本公司於發生影響客戶權益或正常營運之資訊服務異常事件或資通安全事件，應於知悉事件 30 分鐘內至通報系統，辦理事件初步通報。

(2)正式通報：

於查明事件後，應儘速辦理事件正式通報，並至通報系統填報。

(3)解除通報：

事件處理完成後，應辦理事件解除通報，並至通報系統填報。

(4)因網路或電力中斷等事由，致無法於通報系統完成前述通報作業時，先行以電話方式向主管機關證期局及相關單位辦理事件通報，待網路通訊恢復正常後，仍須至通報系統補登錄通報資訊。

7、附件

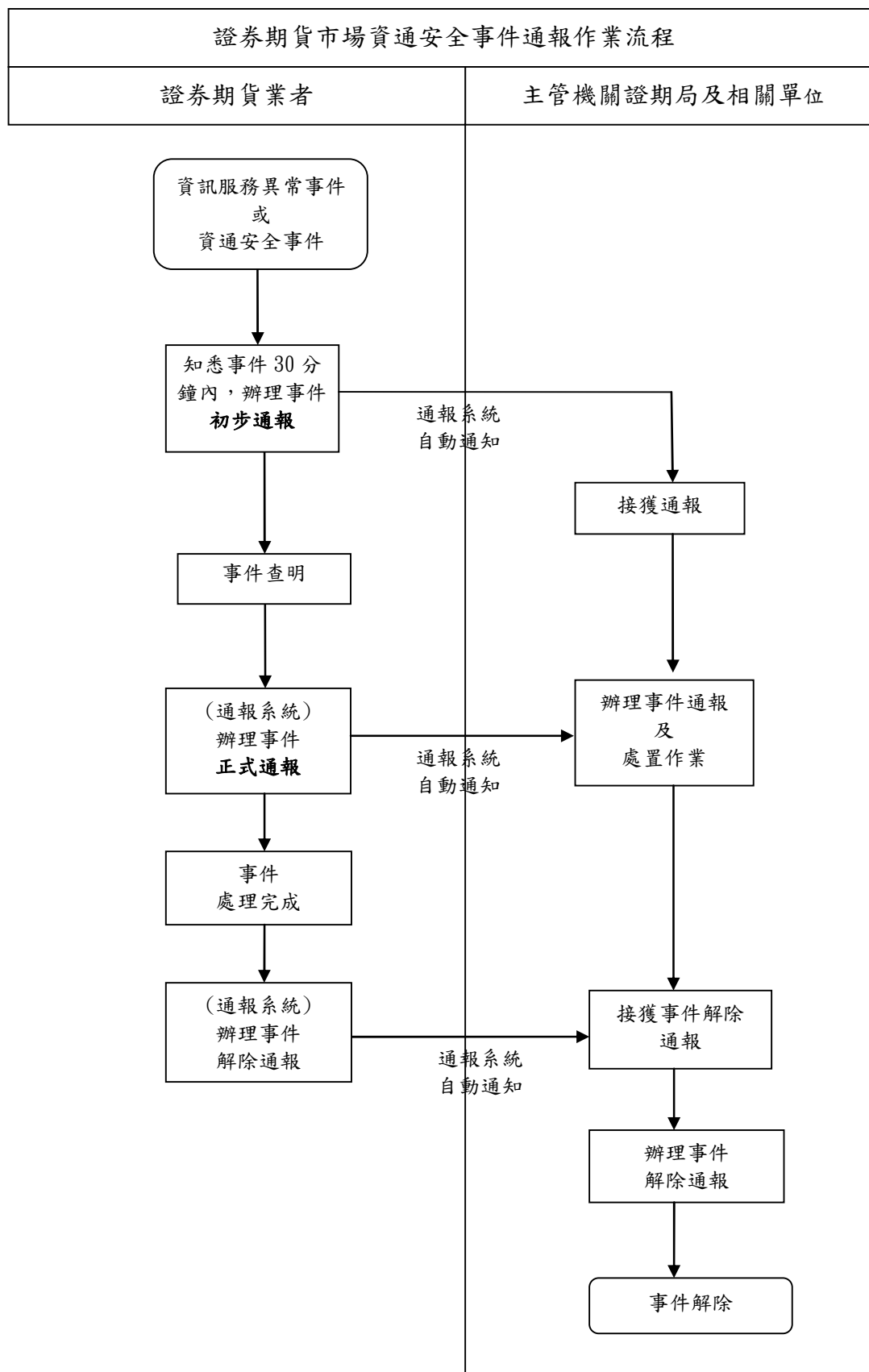
證券期貨市場資通安全事件通報作業流程如附件 1。

證券期貨市場資安事件影響等級如附件 2。

個資事件通報、處理記錄表如附件 3。

8、本作業程序經董事長核定後實施，修正時亦同。

附件 1：證券期貨市場資通安全事件通報作業流程



註：如因網路或電力中斷等事由，致無法於通報系統通報，請先行以電話方式通報

附件 2：證券期貨市場資安事件影響等級

證券期貨市場資安事件影響等級分為 3 個級別：

（一） 3 級事件：符合下列任一情形者，屬 3 級事件：

1. 敏感資料遭洩漏。
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頓，無法於可容忍中斷時間內回復正常運作。

（二） 2 級事件：符合下列任一情形者，屬 2 級事件：

1. 核心業務一般資料遭洩漏。
2. 非核心業務系統或資料遭嚴重竄改；抑或核心業務系統或資料遭輕微竄改。
3. 非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；抑或核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

（三） 1 級事件：符合下列任一情形者，屬 1 級事件：

1. 非核心業務一般資料遭洩漏。
2. 非核心業務系統或資料遭輕微竄改。
3. 非核心業務運作遭影響或系統停頓，於可容忍中斷時間內回復正常運作。

附件 3 個資事件通報、處理記錄表

德信綜合證券股份有限公司

個資事故通報記錄表				
權責單位填寫	事件編號		通報時間	年 月 日 時
	通報人員姓名		聯絡電話	
	部門			
	遭受損害之個資範圍與敘述			
	單位主管簽核		個資保管人	

個資安全人員填寫(單位主管或總經理指派之專案處理人員)	個資事故評鑑分類			
	事故等級	☐ 3 級事件 ☐ 2 級事件 ☐ 1 級事件		
		影響範圍(包括系統、人員、組織)：		
		可能影響之當事人範圍與人數：		
	事件處理單位	☐ 個資安全人員 ☐ 個資管理小組 ☐ 其他 _____		
個資小組簽核		個資安全人員		

德信綜合證券股份有限公司

個資事故處理記錄表				
事件處理單位填寫	事件處理人員		處理開始時間	年 月 日 時
			處理結束時間	年 月 日 時
	是否需(或已)通報主管機關、執行單位或媒體 ☐ 是 ☐ 否			
	是否需向社會大眾公告 ☐ 是 ☐ 否			
	通知個資事故當事人之通報對象、內容、方式及時機：			
	事件診斷調查	個資事故相關採證程序之記錄、證據保存方式及負責人員：		
		個資事故根因分析結果：		
		損失：		
主管簽核		會辦單位		

個資管理小組填寫	矯正預防措施	個資事故之新增控制措施：		
	檢討暨改善與後續追蹤			
	總經理		結案日期	年 月 日 時