文件編號：Doc. No.：3-RM02-16-01				版次 Rev.	E
文件名稱：資訊安全事件緊急應變計畫暨處理作業辦法 Title：				頁次 Page No.	1/9
版次 Rev.	制定/修訂內容 Change Description	制定/修訂日 Date	部門 Dept.	建立者 Initiator	核准者 Approved
A	初版發行	10/15/2004	管理資訊部	江信毅	廖德銘
B	修訂 7.0 附件	04/23/2012	管理資訊部	梁維萍	廖德銘
C	修訂 3.5.2、4.1、4.3、4.4、5.2.4、7.0	06/09/2014	管理資訊部	李　奇	梁維萍
D	修訂 2.0、3.1、3.2、5.1、7.0	04/15/2015	管理資訊部	李　奇	徐育宏
E	修訂 4.1、4.3、4.6、7.0	04/27/2016	管理資訊部	陳俊生	李　奇

目 錄

1.0 目的

為利公司於遭遇資訊安全事件時，能迅速通報及緊急應變處置，並在最短時間內回復，以確保公司各項業務之正常運作，特訂定本辦法。

2.0 組織架構及職掌

2.1 組織架構

資訊安全小組(以下簡稱資安小組)，負責督導各單位執行資訊安全預防及危機通報、緊急應變處理等相關工作。由管理資訊部主管擔任小組召集人，成員包括管理資訊部相關負責人員，共分三個組：安全預防組、危機處理組、稽核組。

2.2 職掌

2.2.1 安全預防組：負責確定影響範圍並作損失評估、執行解決辦法、訂定系統安全等級、簽辦及訂定資訊安全攻防演練計畫等事項。

2.2.2 危機處理組：負責規劃危機處理程序、蒐集資訊安全資訊、建置資訊安全措施、執行資訊安全監控、查明資安事件原因、執行緊急應變措施、辦理資安事件通報等事項。

2.2.3 稽核組：負責訂定相關之稽核計畫或作業程序、內部及外部稽核作業、培訓資訊安全技術等事項。各單位負責資訊安全危機事項之通報及配合資安小組處理相關事宜。

(組織架構、負責人及職掌，請參考 Notes AP 新竹廠 MI 報告管理系統 發佈最新的 資訊安全管制 -資訊安全小組組織架構、負責人及職掌；資訊安全小組名冊，請參考 Notes AP 新竹廠 MI 報告管理系統 所發佈最新的 資訊安全管制 - 資訊安全小組名冊；各單位資訊安全緊急連絡人名冊,請參考 Notes AP 新竹廠 MI 報告管理系統 所發佈最新的 資訊安全管制 - 各單位資訊安全緊急連絡人名冊)

3.0 安全防護機制

3.1 資安小組規劃建置資訊系統及網路安全整體防護環境，含系統存取控管機制、建構防火牆軟硬體、虛擬私人網路（VPN）、病毒掃描機制、、頻寬管理、系統內部安全漏洞檢測（更新、補強）、儲備必要之備份資料、程式或異地備援、重要文件資料檔案採取加密方式儲存等防護工具或措施。並制訂資訊安全管理政策及制度等相關措施，定期實施安全稽核、網路監控、人員安全管理等機制，以強化資訊安全整體防護能力，降低安全威脅及災害損失。

3.2 資安小組執行即時偵防、監測預警工作時，藉由持續運作之監測工具以掌握最新的預警訊息，並適時對單位內發布警告訊息及控制發展趨勢，以降低受損程度。

3.3 各單位應依本辦法規定辦理資訊安全管理工作。

3.4 資訊安全事件定義及分類：

3.4.1 內部危安事件：發現遭人為惡意破壞毀損、作業不慎等危安事件時。

3.4.2 外力入侵事件：

（1） 病毒感染事件。

（2） 駭客攻擊（或非法入侵）事件。

3.4.3 天然災害或重大突發事件：

（1） 天然災害：颱風、水災、地震。

（2） 重大突發事件：火災、爆炸、核子事故。

3.5 資訊安全事件等級：

3.5.1 影響等級，分為三級：

（1） 『A』級：系統停頓，業務無法運作。

（2） 『B』級：業務中斷，影響系統效率。

（3） 『C』級：業務短暫停頓，可立即修復。

3.5.2 損害等級，分為四級：

（1） 第一級：機房主要設備嚴重損害（影響等級「A」級）。

（2） 第二級：主機或網路嚴重損害（影響等級「B」級）。

（3） 第三級：資料庫損害（影響等級「B」級）。

（4） 第四級：單純應用程式（或檔案）損害（影響等級「C」級）。

3.5.3 外在破壞性

（1） 1＝低（容易）。

（2） 2＝中（不易）。

（3） 3＝高（困難）。

3.5.4 對資訊設備依賴度

（1） 1＝低（使用系統設備不得停機三日以上）。

（2） 2＝中（使用系統設備不得停機一日以上）。

（3） 3＝高（使用系統設備不得停機四小時以上）。

3.5.5 安全等級評估方式：

安全等級＝外在破壞性 x 對資訊設備依賴度。

（1） 7－9為『A』級，高級。

（2） 4－6為『B』級，中級。

（3） 1－3為『C』級，普級。

4.0 危機通報作業處理程序

4.1 各單位於確認發生資訊安全事件時，應向資安小組反應，並由資安小組立即填報「資訊安全事件通報單」；如果無法確認是否屬資訊安全事件時，可先洽詢資安小組研判。

4.2 資安小組接獲資訊安全事件通報後，通知危機處理組處理。

4.3 各單位資安事件處理完畢，系統恢復正常運作後，亦透過「資訊安全事件通報單」，通報該資安事件解除。

4.4 如發生災損，有關處理單之災害損失評估內容包括如下：作業影響情況、設備或系統損害情況、作業延誤情況、資料受損項目、估算資訊系統作業及資料回復所需時間、備援中心設備及人員支援狀況等。

4.5 資安小組於資訊安全事件影響等級「C級」時，由危機處理組依需要召集相關單位召開緊急會議或立即處理；若影響等級達到「A級」或「B級」時，由危機處理組立即通知資安小組召集人，並即刻召集相關單位召開緊急應變會議處理該資安事件。

4.6 公司資訊安全事件危機通報緊急應變作業流程如 7.0 附記。

5.0 緊急應變作業處理程序

5.1 緊急應變優先順序：公司如遇發生重大資訊安全事件或其他災害涉及資訊安全事件時，有關緊急應變優先順序處理原則請依下表辦理；並依本計畫暨程序暨相關規定執行應變處置事宜。

優先順序：

5.1.1 資訊網路體系

公司對外網路、公司內部網路。

5.1.2 本部對外服務體系

防火牆、郵件伺服器。

5.1.3 本部對內服務體系

內部 DNS、防毒主機、內部網站。

5.1.4 其他一般體系

ERP、HRP、MES、Workflow。

5.2 各級損害緊急應變程序：

5.2.1 第三、四級：系統負責人先緊急復原該系統，並研判問題所在，以確定系統異常原因。

5.2.2 第二級：系統負責人應儘可能先備份系統的所有現況，找尋其它可行替代運作方案，並邀集主管、維護廠商或相關人員處理該事件及研判問題所在。

5.2.3 第一級：機房人員應儘速通知相關系統負責人及主管處理該事件(必要時得關閉所

有網路連線)，並連絡維護廠商或相關技術支援單位協助。

5.2.4 上述各項傷害，若系統負責人評估損害會因網路或系統開機持續擴大，應立即中斷網路連線或關機。

5.3 資訊安全事件分類緊急應變程序：

5.3.1 內部危安事件：發現（或疑似）遭人為惡意破壞毀損、作業不慎等危安事件時，應迅速查明事件影響狀況、受損程度等，啟用備份資料、程式或啟動備援計畫相關措施，期儘速回復正常運作。

5.3.2 病毒感染事件：病毒入侵後，立即聯絡防毒合約維護廠商協助掌握電腦病毒感染最新動態，隔離病毒，避免疫情擴散；同時儘速取得所需病毒清除程式，並按病毒修護程序，完成病毒清除及修護復原工作。

5.3.3 駭客攻擊（或非法入侵）事件：

（1） 發現（或）被入侵時，立即隔離受入侵系統及拒絕入侵者任何存取動作，如切斷入侵者之實體連線或調整防火牆設定等，以阻絕駭客進一步入侵，並迅速啟動備援系統或程序。

（2） 全面檢討網路安全措施、修補安全漏洞或修正防火牆之設定等具體改善補救措施，以防止類似入侵或攻擊情事再度發生。

（3） 紀錄入侵情形、被駭統計分析及損失評估等資料，以供防護與預警之參考，並向主管機關或檢警單位反映

5.3.4 天然災害或重大突發事件應變程序：

（1） 如遇颱風、水災、地震等天然災害或火災、爆炸、核子事故、重大建築災害等重大意外事件，應迅速攜帶重要資料及程式等離開現場，或儲存於防火保險櫃等設施內，以利爾後系統重置復原。

（2） 如遇資訊網路系統骨幹（主幹頻寬）中斷事件，應立即聯繫線路租用及網路維護廠商查明障礙點、影響區間及範圍，啟動應變機制，緊急調撥備援系統或替代路由，實施流量控管，執行搶修作業。

6.0 復原追蹤鑑識

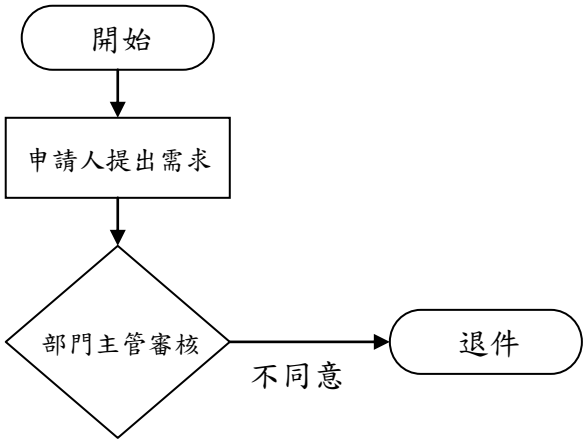
6.1 受損單位資訊系統執行災難損害回復處理步驟，實施災後復原重建工作。

6.2 受損單位執行災後復原工作，首先檢驗資訊安全環境及硬體設備是否可以正常運作，並執行環境重建、系統復原及掃描作業，其步驟包含軟硬體設備重新取得建置、重置作業系統及應用系統，以及運轉測試等；並俟運作正常後即進行安全備份檔案下載、資料回復、資料重置等相關事宜。

6.3 當危機解除後，受損單位應將災害應變處置復原過程之完整紀錄（如事件原因分析及檢

討改善方案、防止類似事件再次發生之具體方案、稽核軌跡及蒐集分析相關證據等資料)，予以建檔管制，以利爾後查考使用。

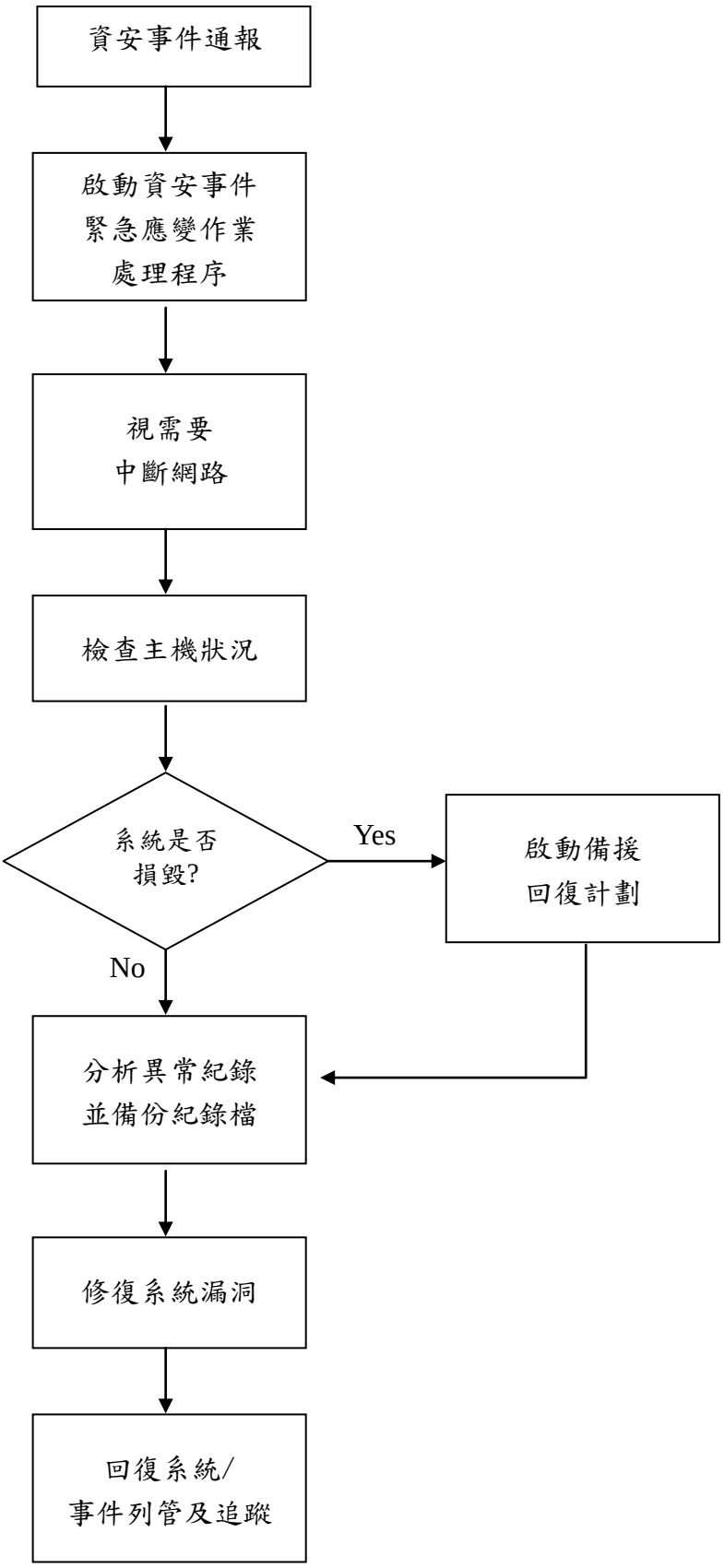
6.4 受損單位如有需要，應保留事件發生之線索，經洽資安小組同意後，向檢警單位申請追蹤鑑識、偵查支援，藉研析稽核紀錄或入侵活動偵測等相關資料，以釐清事件發生的原因與責任；並找出防護系統之漏洞，尋求補強保護方法，避免事件再度發生。



7.0 附記

3-QM01-02-01-F04-01 F

- 資訊安全事件危機通報緊急應變作業流程



- 表單 3-RM02-16-01-F09-01 資訊安全事件通報單

- Notes AP
  MI 作業需求申請
  新竹廠 MI 報告管理系統