豐謙建設股份有限公司

資訊安全管理辦法

113.10.29

1 目的：

1.1 為落實資訊安全的管理，確保公司營運，免於受到內部及外部的刻意或意外的威脅，有效管理資訊及資訊設備使用安全，特訂立資訊安全管理辦法。

2 範圍：

2.1 有關資訊安全之事項，除另有規定外，悉依本辦法辦理。

3 資訊安全風險管理架構：

3.1 本公司資訊安全之權責單位為管理部之資訊專職人員，負責訂定公司資訊安全政策、規劃暨執行資訊安全防護與資訊安全政策推動，並執行相關之資訊安全作業。

3.2 為落實資訊安全管理，公司應設置資訊安全組織，成員應包含資安主管及至少一名資安專責人員，負責推動、協調及督導下列資訊安全管理事項：

3.2.1. 資訊安全政策之核定及督導。

3.2.2. 資訊安全責任之分配及協調。

3.2.3. 資訊資產保護事項之監督。

3.2.4. 資訊安全事件之檢討及監督。

3.2.5. 其他資訊安全事項之核定。

3.3 定期執行資安政策之評估與審查，以反映管理政策、政府法令、公司業務等之最新發展現況，確保資訊安全管理制度的可行性及有效性。

4 資訊安全政策及管理方案：

4.1 本公司資訊安全設施與管理方式：

4.1.1. 伺服器機房安全管理

- 出入機房皆有進出人員記錄，且由資訊人員陪同。
- 機房設有獨立空調，控制溫度使伺服器維持正常運作。
- 為防斷電時造成系統毀損或資料流失，主機房配置不斷電系統因應斷電時有足夠時間做存檔與正常關機。

4.1.2. 網路安全管理

- 設有防火牆設備，阻擋外來惡意威脅。

- 監控分析防火牆資訊報告。
- 對電子郵件嚴格控管，寄出及接收之郵件均經過郵件主機掃毒，且確保郵件無法夾帶病毒檔。

4.1.3. 存取權限管理

- 同仁使用各資訊系統(含遠端存取連線)，需向公司提出系統權限申請，經主管核准後，由資訊提供使用者帳號與密碼，並依其申請項目逐項設定使用權限。
- 各單位主機須限制外部人員以管理者權限帳號登入使用系統，如有設備保管人以外人士使用或維護設備的需求時，須經授權同意後由資訊單位人員授權開啟權限。
- 設有伺服器及個人電腦資訊系統身分驗證、登入登出之存取紀錄。
- 公司內各資訊系統、電腦帳號均由資訊單位統一管理，規定設置適當密碼強度、字數，且必須文數字、特殊符號混雜，並定期啟動必須更改密碼通知。
- 同仁離職或留職停薪一經確認，即由資訊進行帳號刪除或暫時停權作業。

4.1.4. 病毒及威脅偵測防護管理

- 伺服器主機及同仁電腦均設有防毒軟體，病毒碼會進行自動更新與即時偵測，防止惡意病毒入侵。
- 防毒軟體對於偵測到的病毒，會進行隔離及刪除，並發出系統警告通知至資訊人員電子信箱，以利資訊人員採取因應措施。
- 伺服器主機及同仁電腦均設有威脅偵測機制，進行行為監控分析及防護，包含存取資源紀錄、重要行為、重要資料異動、偵測攻擊與未授權之連線、功能錯誤及管理者行為，存有每月異常行為紀錄。

4.1.5. 備份及備援管理

- 針對重要資訊與檔案採用日備份機制，由本地端儲存設備自動備份作業，以便在發生系統失效或資料錯誤時，可迅速地回復

正常作業，及還原正確資料。

- 各項系統設定檔、伺服器檔案及資料庫資料均採週期自動雲端備份機制。
- 定期執行人工備份，以驗證備份之可靠性及資訊之完整性。

4.2 資訊安全管理之執行：

4.2.1. 硬體：防火牆、UPS 不斷電系統、電腦及相關設備定期更新。

4.2.2. 軟體：防毒軟體、威脅偵測機制、雲端備份系統、相關軟體定期更新。

4.2.3. 人員：資安宣導與教育訓練、內部稽核定期查核、每日確認機房設備狀況、檢視防火牆資訊報告、權限設定狀況、防毒軟體更新及偵測報告、威脅偵測機制狀況、資料備份狀況。

4.3 個人資訊安全管理：

4.3.1. 敏感性或具保密需求之資料應採檔案加密，存放辦公室固定電腦為主，並注意實體隔離，勿存放於隨身儲存設備中。

4.3.2. 若需公務電腦資料攜回家中處理，應先將隨身儲存設備中之敏感性或具保密需求資料刪除，以維安全。

4.3.3. 同仁經由網際網路下載檔案或使用隨身碟(USB)應立即進行病毒掃描，確認安全無毒後才可使用。

4.3.4. 電腦系統之安全設定應由資訊單位統一管理，如防毒軟體等，使用者不得擅自更改設定或安裝不符合規定之軟體。

4.3.5. 各網路磁碟之使用人，應善盡資料管理之行為，定時將不必要、重覆性的資料移除，以確保資料空間之利用。

4.4 定期對公司同仁進行資訊安全宣導，提高同仁資安危機意識。

5 業務永續運作計畫之規劃與管理

5.1 將資安管理事件影響與因應納入公司年度報告。

5.2 已加入「台灣電腦網路危機處理暨協調中心TWCERT/CC」會員，收集資安情資，內部宣導。

5.3 發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

5.4 稽核室依照公司內部控制之資訊循環作業控制重點，定期進行資訊安全稽核作業檢視，確保正常運作並持續改善。

5.5 每季定期向資安主管報告資通安全執行情形，確保運作之適切性及

有效性。

5.6 本公司資安事故之通報與處理，應遵守下列程序之規範：

5.6.1. 資安事件之真實性確認。

5.6.2. 通報資訊及資安主管。

5.6.3. 依重大程度判定是否向總經理呈報。

5.6.4. 自行進行事件處理或尋求外部支援。

5.6.5. 資安事件之記錄與報告歸檔。

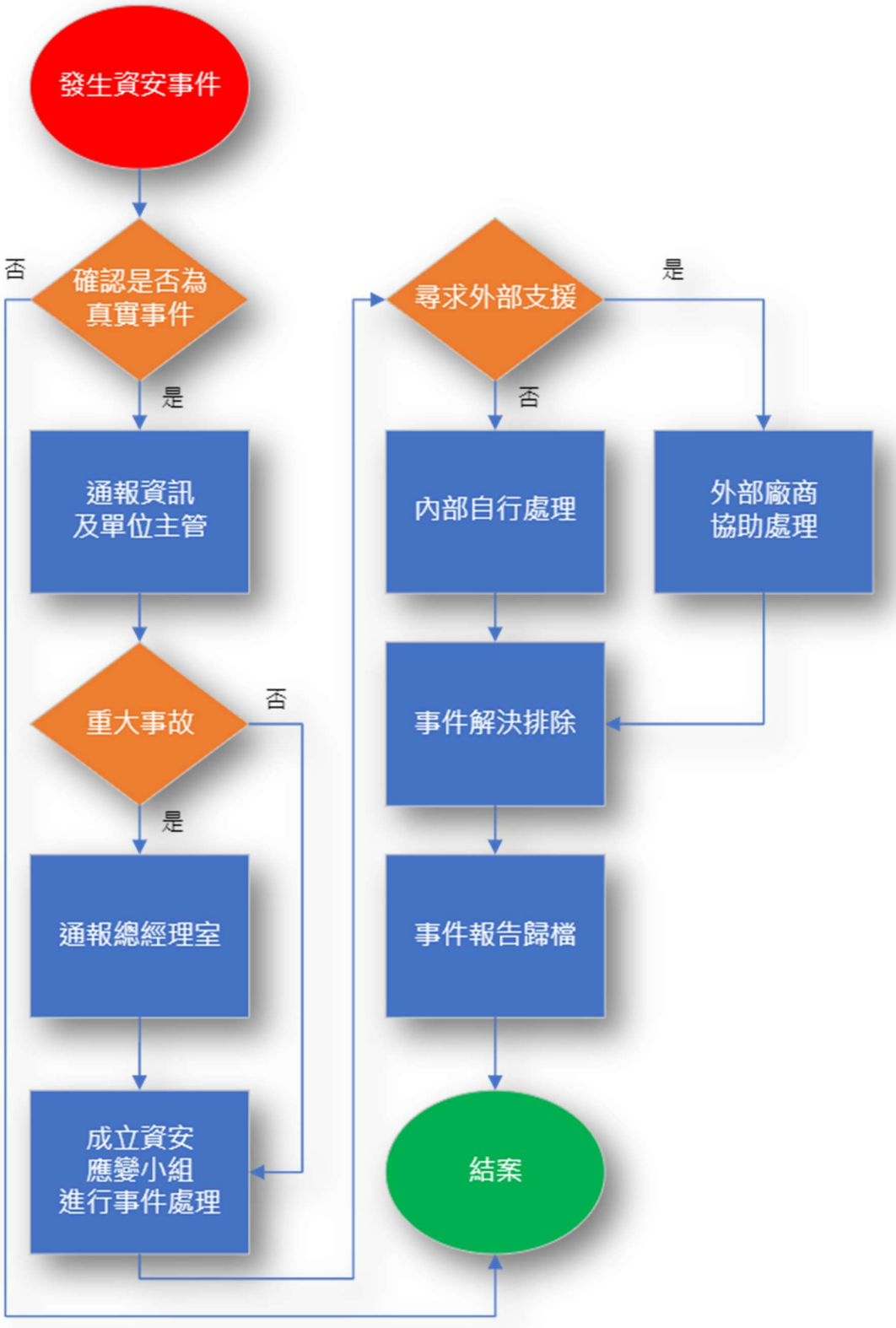
6 附件

6.1 圖表1 資安事件流程圖

7 本辦法之訂定及修正應經審計委員會同意，並提報董事會通過。

本辦法訂定於民國112年3月15日。

本辦法修定於民國113年10月29日。


發生資安事件
確認是否為
真實事件
否
是
通報資訊
及單位主管
重大事故
否
是
通報總經理室
成立資安
應變小組
進行事件處理
尋求外部支援
是
否
內部自行處理
外部廠商
協助處理
事件解決排除
事件報告歸檔
結案

圖表 1