資訊安全風險管理架構及112年具體管理方案

為強化資訊安全之風險管理，成立資訊安全執行小組，建置資訊安全風險管理架構、訂定資訊安全政策及具體管理方案，並定期檢討資訊安全政策，以確保資訊安全。

壹、資訊安全風險管理架構及組織

- 資訊安全執行小組定期檢討資訊安全管理政策及相關辦法。
- 各單位成員皆依相關辦法確實執行。
- 日常營運時定期進行伺服器等設備之檢核，以即時發現問題。
- 進行資訊安全風險評估，配合稽核單位查核以確保作業之正確性及有效性。
- 遇有錯誤、漏洞與風險立即進行改善，以建構資訊安全之持續改善管理循環。
- 資訊安全執行小組由管理處處長為召集人，資管課經理為總幹事，資訊安全執行小組每年依公司風險管理程序評估資安風險並於董事會報告資訊安全執行情形。

貳、資訊安全風險管理機制

執行資訊機房、電腦資訊檔案安全、網路安全、郵件安全管理、資訊系統控制存取等管理。

參、資訊安全政策:

一、目標

為促使本公司各項資訊安全管理制度能貫徹執行、永續運作及監督管理，維護重要資訊系統的機密性、完整性與可用性，特制定此一資訊安全政策，來強化資訊安全管理，提供安全、有效之資訊服務，建立安全可信賴之資訊作業環境，確保資料、系統、設備及網路之持續運作之目標。

二、範圍

本政策適用於本公司所有單位、人員及資訊資產(包括置於本公司辦公大樓、廠區的資訊設施)。本資訊安全政策旨在讓全體公司同仁有一明確指導原則，以保障本身權益，並有效了解、實施與維持資訊安全管理，達成資訊營運的目標。

三、原則及標準

(一)、維持資訊系統持續運作

1. 重要系統資源與廠商簽訂維護合約，維持系統的正常運作。
2. 登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由資管課系統管理人員設定賦予權限之帳號與密碼，並定期更新。
3. 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以便發生災害或儲存媒體失效時，可迅速回復正常作業。
4. 規劃災難復原計劃，使損失降至最低。

(二)裝置防火牆以防止非法入侵、破壞或竊取資料，以避免網站遭到非法使用，保障使用者的權益，防止駭客、病毒等入侵及破壞。

(三)維護實體環境安全

1. 電腦機房進出的進行安全管制，避免人為的破壞。
2. 電腦機房維持穩定的電壓及適當的溫濕度，確保硬體設備運作正常。

(四)防止人為意圖不當及不法使用

1.避免未經授權者竄改資訊，保護資訊完整。

2.登入各作業系統時，依各級人員執行任務所必要之系統存取權限，由資管課系統管理人員設定賦予權限之帳號與密碼，並定期更新。

3.落實遵守資訊安全有關法律及規定，避免使用非法軟體。

4.隨身碟限於公務用，禁止使用於私人用途，使用時應嚴防資訊外洩或中毒。

(五)資訊安全事件應依程序通報反映，並在最短期間內採行應變措施，事件處理後須檢討改進。

(六)加強資安訓練，提升資安智能

針對全公司同仁，進行一年兩次的資訊安全教育訓練及宣導，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

(七)為確保資訊安全管理制度之有效性，各單位人員凡違反資訊安全管理制度相關程序規範者，依相關人事規定審議懲處。

(八)本政策應不定期評估檢討，以反映政府法令、技術發展及業務需求等，以落實資訊安全作業。

四、資訊安全之目標：

建立安全及可信賴之電腦化作業環境，確保本公司資料、系統、設備及網路安全，以保障公司利益及各單位資訊系統之永續運作。

資訊安全之範圍：

1.人員定期執行資訊安全宣導作業，強化同仁資安認知及法令觀念。

2.電腦系統安全管理。

3.網路安全管理。

4.系統存取管制。

5.系統發展及維護安全管理。

6.資訊資產安全管理。

7.實體及環境安全管理。

8.資訊系統永續運作計畫管理。

9.資訊安全稽核。

肆、建立資訊安全通報及啟動緊急應變程序

因資訊安全事件（包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等），致電腦系統無法運作或影響執行效率時，相關人員應視其狀況嚴重程度及影響層面，循序向各權責主管通報以及啟動緊急應變程序，主要分成下面步驟，分別說明如下：

【STEP 1】啟動應變處理程序、且同時執行通報

確認為資安事件後，判斷資安事件影響等級，由輕至重分為「１」、「２」、「３」及「４」個級，執行通報，且同時啟動應變處理程序，聯絡中華國際資安團隊。

【STEP 2】確認災害狀況及影響作業程度

中華國際資安團隊確認確認資安原因、影響等級、可能影響範圍，並保留入侵或相關證據，並且進行資安分析。

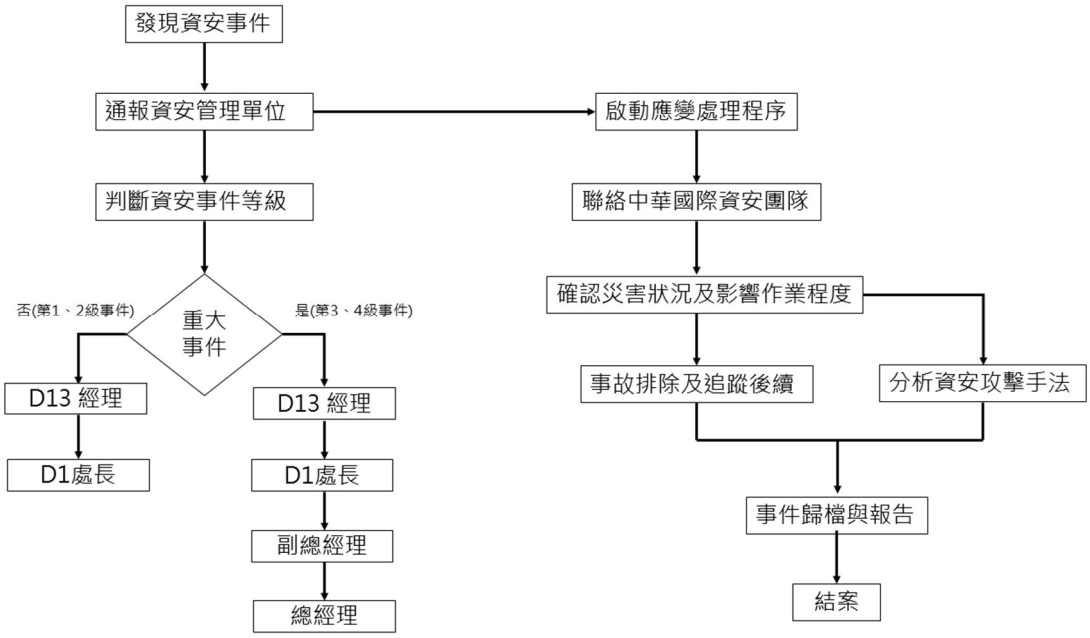
【STEP 3】事故排除及後續追蹤

原因確認後，進行事故排除，並且全面檢查討論安全措施、修補安 全弱點、修正防火牆設定等具體改善措施，以防止類似入侵或攻擊再度發生。

【STEP 4】事件歸檔

將相關完整記錄(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、蒐集分析相關證據等資料)，且建檔管制，以利爾後查考使用。

資通安全事件通報及應變作業流程，詳圖如下所示。



伍、112 年度具體管理方案及投入資通安全管理之資源之說明。

一、具體管理方案

(一)一年兩次資安教育宣導及不定期於 EIP 公告相關資安新聞。

(二)隨身碟使用管制，申請 USB 使用需填寫隨身碟申請單經主管通過後才能使用，並且只能使用公司配發隨身碟。

(三)個人電腦、相關系統密碼登入複雜度提升。

(四)電腦更新由 WSUS SERVER 自動派送且更新。

(五)每年執行災難復原演練確保系統因相關因素故障可及時復原上線使用。

(六)針對 ISO27001 所認證的範圍進行整機備份。

二、投入資通安全管理之資源:

(一)資通安全威脅偵測管理(SOC)監控服務。

(二)全域(個人電腦、伺服器虛擬機)導入 MDR(Managed Detection and Response)

(三)每年對外網站及 ISO27001 驗證範圍系統執行弱點掃描或者滲透測試。

(四)每年執行社交工程演練(初測、複測)。

(五)全域(個人電腦、伺服器虛擬機)安裝防毒軟體。
(六)總部中鋼防火牆 VDOM 設備有 IPS(入侵偵測防禦)。
(七)建置 WinMatrix IT 資源管理系統落實資訊資產與資訊安全政策管理。
(八)通過 ISO27001:2013 驗證。(經第三方 BSI 驗證通過，有效期至 115 年)
(九)伺服器主機維運(漏洞、更新檢查修補修正)
112 年度以上各項目公司共投入新台幣 230 萬元。