資訊安全管理制度

資訊安全是本公司長期以來重視、關注的重要工作之一，為了確保各項資訊安全管理作業之有效落實，並及早發現不正當之行為以及安全漏洞或威脅，早期識別可幫助阻止不法行為並盡可能減少潛在的風險。

本公司為提升資訊安全管理已成立「E 化作業委員會」，定期於每季度針對資安進行宣導及資安改進措施報告，並定期對全體員工就資安議題及釣魚信件等資安案例說明，亦不定時以 email 通知全體員工有關防禦惡意郵件通知。

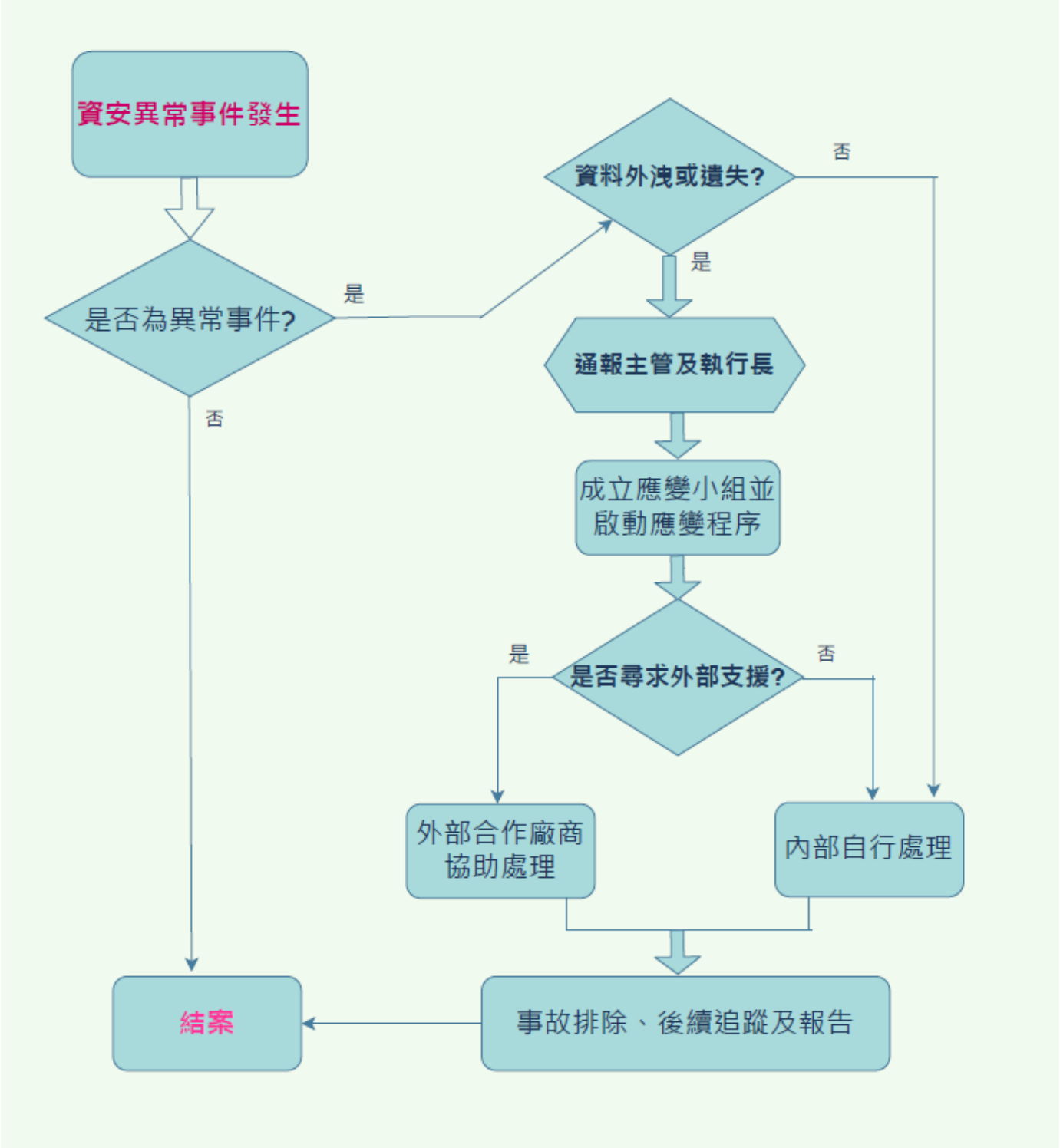
資訊安全管理措施

1. 明訂資訊安全政策：已於資訊系統管理程序中訂有資訊安全規範，明訂員工各項資訊安全的必要執行原則及措施：。

類型	項目	防範目的	相關作業說明
員工管理	•資訊安全推行及宣導	•預防降低中毒機率 •提升員工資安意識	隨時掌握政府及業界最新資安與預警訊息，定期對於員工進行國內外重大資安異常事件案例分享。
裝置控管	•防毒軟體 •非信任裝置阻檔	•預防中毒 •阻斷非組織人員存取	•系統判定符合規範之電腦才給與網路連接權限。 •非經公司許可之電腦設備嚴禁接入公司網路，如有未經許可之設備接入系統將自動進行網路封鎖。
權限管理	•雙因素身分驗證 •專案權限控管	•避免帳號冒用	•同仁登入個人電腦需通過雙因素身分驗證，以避免帳號被竊取冒用的情況發生。 •各研發專案皆有嚴格權限控管，專案成員需提出表單申請，經主管同意後由資訊管理人員設定存取權限，並定期進行一次存取權限覆核，以確保權限管理之正確性。
資料管理	•專業型儲存設備 •本地備援架構 •異地資料備份	•避免資料遺失	•專業型儲存設備具有高可用性的備援能力，專案研發資料皆有權限控管，僅允許授權成員進行存取。 •公司研發資料有完整的定期備份機制。 •採取異地存放，以確保災難發生時的復原能力。

2. 制訂資訊系統緊急應變辦法，為使資訊作業在發生天災或人為破壞後，能依序採取緊急應變措施，儘速回復各項電腦作業，以維持公司業務之運作。並規定倘若發生資安事件，應立即成立緊急狀況重大危安事故應變小組，由執行長及各部門主管依職權編組，負責資訊安全事件緊急應變處理，並由資訊部門負責執行資訊安全預防、危機通報及緊急應變處理等相關措施。

   資訊安全處理程序：



資安政策

依據公司的資訊系統管理程序中所列示之資訊安全規範：

1. 公司資訊資源區隔為內部區與公開區，內部區為公司內部同仁使用不對外開放，公開區為對客戶及廠商開放區，公開區僅能連上網際網路，與內部網路互不相通。
2. 使用者使用遠端存取時必須使用憑證才可登入，使用者要妥善保管憑證。
3. 使用者不得將個人登入身份識別碼與密碼交付他人使用，使用者亦不得以任何方法竊取他人的登入身份識別碼與密碼。
4. 密碼應該符合複雜化原則，使用者應負責保管及定期更換個人密碼，維持密碼的機密性。
5. 當有跡象足以顯示使用者密碼可能遭破解時，應立即更改密碼並通知所屬部門主管及資訊部門。
6. 禁止同仁安裝、使用或分享未經授權之軟體，並要求同仁遵守智慧財產權相關規定。
7. 禁止同仁私自拆換公司資訊設備。
8. 禁止並防範網路使用者以任何儀器設備或軟體工具竊取網路上的通訊。
9. 禁止蓄意傳送電腦病毒，並宣導如何防範不知情夾帶傳送電腦病毒。
10. 不得利用電子郵件或其他資訊服務散佈不實訊息、黑函或不當之言論。
11. 不得傳送匿名或冒名電子郵件。
12. 非公務往來，不得將公司文件檔案以電子郵件寄出公司。
13. 非公務需求，不得將公司內之文件以電子檔案私自以任何儲存媒體(如:磁片、硬碟、隨身碟、NoteBook、光碟、ZIP及MO等)攜出公司。
14. 禁止攜帶PC及NB個人資訊設備進入工作場所，若有公務需要可提出資訊設備採購需求。
15. 禁止私自於公司工作場所連接無線網路基地台及3G等其他連線網卡。
16. 同仁在會議室若使用非公司設備之PC及NB或測試機器需要使用到內部資源存取時，必須填寫《會議室內部存取申請表》提出申請。
17. 外部人員(客戶、廠商、顧問、兼職人員等，非公司正常人力編制)攜帶資訊設備進入公司，欲使用公司內網相關資源需求，請依規定填寫《帳號權限新增申請表》，經核管單位主管簽核後，資訊部門人員依照表單項目新增相關權限並確認，並於人員離開時，請資訊部門人員檢查相關權限是否關閉。

資安事件通報表單:

<table>
<tr><td colspan="8">資　通　安　全　事　件　通　報　單</td></tr>
<tr><td colspan="8">事件通報單位聯絡資料</td></tr>
<tr><td>通 報 人</td><td colspan="2"></td><td>單位名稱</td><td colspan="4"></td></tr>
<tr><td>電　　話</td><td colspan="2"></td><td>電子郵件</td><td colspan="4"></td></tr>
<tr><td colspan="8">事件通報事項</td></tr>
<tr><td>事件發生時間</td><td colspan="2">___年___月___日___時___分</td><td>填報日期</td><td colspan="4">___年___月___日___時___分</td></tr>
<tr><td>事件樣態</td><td colspan="4">□資通安全事件 □個人資料事件 □重大緊急事件
□其他事件_____</td><td>管制編號</td><td colspan="2"></td></tr>
<tr><td>事件說明</td><td colspan="7"></td></tr>
<tr><td rowspan="3">設備資料
(發生事件之資通系統的詳細資訊)</td><td>IP 位址</td><td colspan="2"></td><td>Web 位址</td><td colspan="3"></td></tr>
<tr><td>設備廠牌、機型</td><td colspan="2"></td><td>作業系統/版本</td><td colspan="3"></td></tr>
<tr><td>已裝置之安全機制</td><td colspan="5"></td></tr>
<tr><td rowspan="3">資通安全事件影響等級
(以 C, I, A 最高級別為事件等級)</td><td>機密性衝擊
(單選)</td><td colspan="6">□國家機密資料遭洩漏(4 級)
□密級或敏感公務資料遭洩漏(3 級)
□核心業務(含關鍵資訊基礎設施)一般資料遭洩漏(2 級)
□非核心業務一般資料遭洩漏(1 級)
□無資料遭洩漏(無需通報)</td></tr>
<tr><td>完整性衝擊
(單選)</td><td colspan="6">□關鍵資訊基礎設施系統或資料遭嚴重竄改(4 級)
□核心業務系統或資料遭嚴重竄改；抑或關鍵資訊基礎設施系統或資料遭輕微竄改(3 級)
□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(2 級)
□非核心業務系統或資料遭竄改(1 級)
□無系統或資料遭竄改(無需通報)</td></tr>
<tr><td>可用性衝擊
(單選)</td><td colspan="6">□關鍵資訊基礎設施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(4 級)
□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；抑或關鍵資訊基礎設施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 級)
□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(2 級)
□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(1 級)
□無系統或設備運作受影響(無需通報)</td></tr>
<tr><td>資通安全事件等級判定</td><td colspan="3">□0 級 □1 級 □2 級□3 級 □4 級
(3 級及 4 級須呈核至管理代表以上管理階層)</td><td colspan="4">□通報國家資通安全應變中心</td></tr>
<tr><td>破壞程度</td><td colspan="7">□服務中斷 □資料庫毀損 □資料遭竊取及竄改 □系統當機 □軟硬體故障 □病毒感染
□個資被竊取、竄改、毀損、滅失或洩漏 □其他_____</td></tr>
<tr><td>事件影響範圍及損失評估</td><td colspan="7"></td></tr>
</table>

事件之應變與處置			
損害控制及 復原作業之歷程			
系統服務終止 紀錄(必填)	□系統維持運作，無須終止服務。 □系統需終止服務(起迄時間：　年　月　日　時　分 ~　年　月　日　時　分)， 總停機時間：　日　時　分。		
期望支援項目			
事件調查及 處理作業之歷程	□另填寫「矯正及預防處理單」將此問題列管並防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施(預防措施)，及預定完成時程和成效追蹤機制納入管制。		
完成損害控制或 復原作業之時間	____年____月____日____時_____分		
承辦單位	會辦單位	執行秘書	召集人

實際與預計投入資通安全管理之資源

✧ 已投入之資通安全管理資源

1. 資安會議：每半年召開 TQM E 化委員會會議。
2. 防毒防護：防火牆、自動更新病毒碼等，確保最佳防護機制。
3. 備援機制建置：建構備份管理機制與系統，確保資料之安全機密性與可用完整性。
4. 資安案例分享與強化資安意識：不定時，隨時接獲可疑案件即進行分析與宣導。
5. 投入人力如：每日各系統狀態檢查、每週定期備份及備份媒體異地存放之執行、不定期資安宣導、每年系統災難復原模擬演練、每年對資訊循環之內部稽核、外部會計師或台積電稽核等。
6. 資安專職人員：業已聘僱專職資安人員負責資安架構設計、資安維運與監控、資安事件回應與調查、資安政策檢討與修訂。

✧ 預計投入之資通安全管理資源

1. 每週/每月 Log 分析，分析是否有大量惡意外部攻擊及潛藏威脅事件。若有，將會立即優先處理，保護企業內部環境，減少外部惡意攻擊。
2. 針對過時作業系統升級，如 Win7 or Centos7 or Win2008R2 以下版本。避免遭受橫向或外部攻擊。造成破口產生，危害企業環境。
3. 每年七月實施演練災難還原演練計畫，每年演練形式及主題方式不同。如:2024 年以 AD/Exchange 為主題，進行相關災難演練還原計畫。
4. Log Server 導入，將重要主機 Log 存放在 Log Server 同時可即時查看到相關資訊，減輕資安人員分析並減少異常事件產生。如:AD 帳號大量登入異常失敗、Web Server 遭受大量外部 IP 連線攻擊等。
5. 不定期與 IT 同仁開會，確認現行架構或環境內有無潛藏風險，並做相關的因應處置並回報給主管，以利後續相關進行處理。
6. 不定期資安講座，提升同仁資安意識。
7. 每 6 個月進行一次主機的弱點掃描，除修補高風險以上漏洞外，也要確認作業系統是否已 EOS/EOL，若作業系統已 EOS/EOL 會建議請主機管理者升級到新版本，避免遭受弱點攻擊。

本公司資訊部門執行作業依規定程序均能落實執行，風險評估結果尚屬良好，近來資安攻擊事件頻傳，本公司積極加強資訊安全維護措施，建立員工資安觀念提升資安意識，降低公司營運風險。最近年度並無因重大資通安全事件之情形。