資訊安全風險架構管理計畫

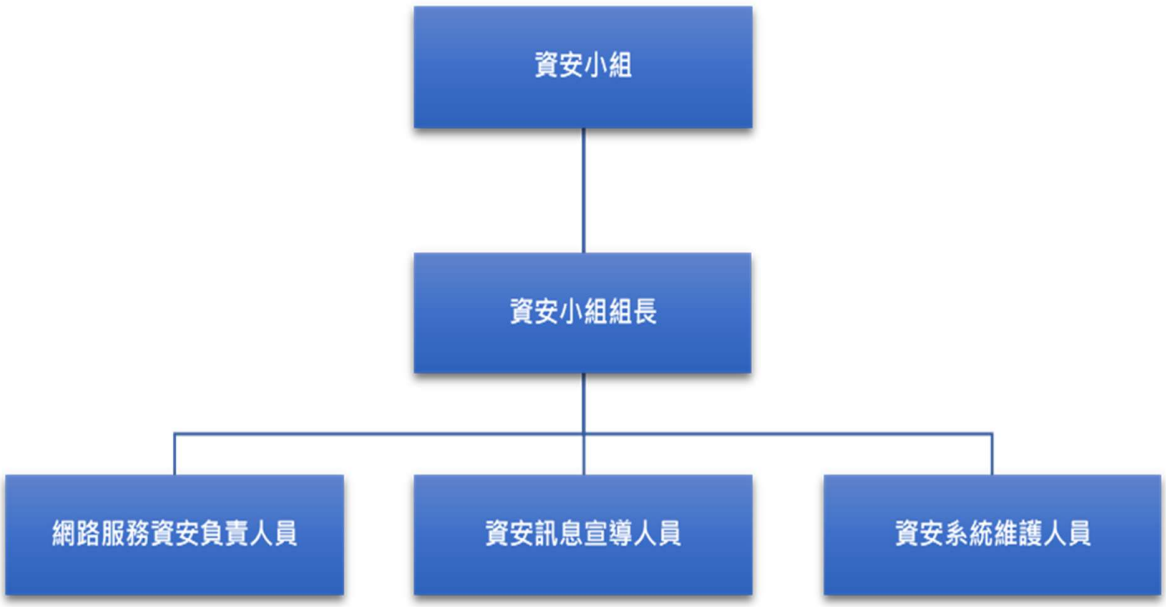
一、 資訊安全之目標

本公司以符合政府相關法令及法規等要求建立本資訊安全風險管理計畫，以保障資訊安全之機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)為目標。

二、 資訊安全風險管理架構與資訊安全政策

本公司由資訊部門成立資安小組負責統籌及執行資訊安全政策，資訊安全政策包含了以網路服務工程師與公司員工為實施對象的遵行要領。另外也對網路服務工程師安排資安相關的培訓，使網路服務工程師具有所需的資安能力，為公司的所有網路服務提供高規格的資安防護措施；在公司員工資安訓練的課程則著重提升員工的資安意識。

資訊安全工作小組的管理架構圖



針對網路服務工程師的部份，資安小組收集業界資安相關的資訊，並因應外部的資安事件，立即採取相對應的資安防護措施。另外定期安排工程師參加資安研討會，以提升網路服務的資安專業技能。針對公司的網路服務，資安小組定期安排弱點掃描與源碼掃測，確保所有網路服務都有完整的資安防護。除了內部定期的弱點掃描與源碼掃測之外，資安小組也會定期請第三方機構執行滲透測試，並取得第三方機構的測試報告及認證，確保重

2024.02.29

要資料不會外流。除了資安相關系統掃測之外，資安小組針對每個網路服務指派專屬資安負責人員，設立資安事件通報群組，以確保資安政策的落實及資安事件的應變。

針對公司員工，資安小組定期宣導資訊安全訊息，並且錄製資訊安全影片教材，供公司新人訓練使用，以提升公司員工資訊安全意識。除此之外，資安小組定期更換員工內部系統的帳號密碼，並且確保員工安裝防護軟體並定期更新。員工使用公司內部系統需要做多因子驗證才能登入使用，如果在公司外部，需要使用安全連線並且使用二次驗證才能遠端連線回公司內部。遠端連線也都有系統紀錄並通知相關人員。

除了上述內容，資安小組負責維護資訊安全系統產品或程序之有效性，每年定期進行資安預算的編列，提升公司資安管理及防護所需的技術及軟硬體，確保公司網路服務的資訊安全無虞之際，公司系統與設備都有足夠的資安防護。

三、 具體管理方案及投入資通安全管理之資源

（一）網際網路資安管控

1. 架設防火牆：確保無非預期的連線及封包流入或流出公司，竊取公司資訊。所有防火牆的設定皆透過公司內部系統控管簽核，確保防火牆設定符合資安要求。
2. 即時偵測惡意軟體：系統設定自動且強制的病毒掃描，並即時偵測是否有可疑的惡意軟體行為，確保員工工作平台安全無虞。
3. 建置入侵偵測及防護系統：自動偵測不預期的行為並且自動阻擋，再由資安人員從後台檢查狀況並採取對應的行為。
4. 追蹤網路異常情形：自動偵測不預期的行為並做阻擋，並且通報相關單位。

（二）資料存取管控

1. 系統密碼每季更新：由系統控制強制網路服務工程師及公司員工更換密碼，避免因為人為失誤而忘記密碼更新。
2. 嚴格控管存取權限：存取權限由公司內部系統控管並經過簽核，確保權限僅授權給負責的主管及必要的操作人員。
3. 系統控管遠端登入資訊：遠端登入公司平台經過安全連線，並且使用多因子驗證，確保公司以外的人無法登入或是竊取連線資訊。另外登入不論成功失敗都有訊息通知，以確保沒有非預期的登入行為。
4. 內部資訊系統導入多因子驗證：內部系統導入多因子驗證，避免帳號密碼外流導致不預期的登入。

（三）資料備份及還原演練

1. 每日進行異地備份：確保公司重要資料不會因為機房或是伺服器毀損造成公司嚴重損失。
2. 舉行資料還原演練：每半年施行資料還原演練，確保災難發生都可以將公司重要資料安全回復。

（四）資訊安全訓練及宣導

1. 每年定期安排網路服務工程師參加資安研討會：定期收集資安研討會資訊，及安排網路服務工程師參加，並且進行內部報告以提升資安團隊的專業能力。
2. 每季針對公司員工進行資安宣導：定期提供資安相關資訊給全公司員工並且錄製資安影片用作新人訓練教材。
3. 定期舉行釣魚信件攻擊演練，以提升員工的資安意識。

（五）更新資安軟體及硬體

1. 定期檢查防火牆更新：系統自動檢查, 收到通知手動更新
2. 定期檢查防毒軟體更新
3. 定期檢查入侵偵測及防護系統更新
4. 定期檢查防釣魚軟體更新
5. 定期檢查垃圾信件過濾軟體更新
6. 定期檢查弱點掃描系統更新
7. 定期檢查系統備份軟體與磁帶更新

（六）系統維運

1. 每週執行弱點掃描：所有網路服務每週執行弱點掃描，並且將中級以上弱點安排處理。設置通報系統，將一定時間沒有處理的弱點向資安負責人員通報。
2. 定期執行源碼掃測：所有網路服務在上伺服器前經過源碼掃測，確保資安相關漏洞皆有更新與修補。
3. 每年委託外部資安檢核機構執行滲透測試：委託外部資安機構針對公司對外營運的伺服器及內部員工使用的伺服器執行滲透測試，並取得外部資安機構的測試報告及認證，確保重要資料不會外流。

執行情形：

截至 2023 年 12 月 31 日止執行情形如下，並於 2024 年 2 月 29 日向董事會報告：

一、資安小組編制

資安小組組長一名，網路服務資安負責人員五名，資安訊息宣導人員兩名，資安系統維護人員三名。

二、資訊安全例行性防護措施

- 網路服務指定專屬資安負責人員，以確保資安政策的落實
- 設立資安事件通報群組，收集業界資安相關的資訊，以確保快速針對資安事件採取應變措施
- 定期檢視公司內外服務及工作環境的資安保護措施及相關的軟硬體更新
- 定期宣導資訊安全訊息及進行釣魚信演練，以提升公司員工資訊安全意識
- 定期更換員工內部系統的帳號密碼，定時更新員工作業系統及防護軟體
- 使用多因子驗證 保護公司內部系統，使用 VPN 保護從公司外部進來的連線
- 每年定期進行資安預算的編列，提升公司資安管理及防護所需的技術及軟硬體

三、2023 年已完成的資安相關項目

- 2023 年無發生重大的資安事件
- 防禦系統阻擋的可疑事件數：5574 次 (2022 年為 347 次)
    - 入侵防禦系統 (IPS) 阻擋 5559 次可疑事件 (2022 年為 345 次)
    - 端點偵測及回應系統 (EDR) 阻擋 15 次可疑活動 (2022 年為 2 次)
    - 可疑事件的次數增加主要原因為
        - 上線的服務及伺服器持續增加，佈建的偵測系統也隨之增加，因此有更多的可疑事件回報
        - 偵測系統根據以往的可疑事件新增及調整防護規則，因此偵測到更多的可疑事件
- 已於 12 月加入台灣資安主管聯盟，成為該聯盟會員，共享業界資安情報
- 執行網路服務及內部系統的弱點掃描：每週執行，持續進行中
- 委託第三方資安公司進行滲透測試已於 1 月完成測試
- 執行企業資料的異地備份：每日執行，持續進行中
- 資料還原演練：
    - 系統資料 4 月演練完成

- 程式碼資料 11 月演練完成

- 資安宣導已完成五次，最近一次宣導：11 月
- 郵件社交工程演練已完成四次，最近一次演練：10 月
- 訓練及培養資安人員的專業知識及技能：8 人次，共 100.5 小時
  - CYBERSEC 2023 臺灣資安大會：32 小時
  - TWCERT/CC 資安事件通報與 IoC 應用實務課程：5 小時
  - TWCERT/CC 企業資安演練：5 小時
  - CheckMarx 客戶經驗分享會：5 小時
  - 昕奇雲端: 全面防護！零信任時代下，雲端資安怎麼做：5 小時
  - DEVCORE Conference 2023：39.5 小時
  - 2023 AWS 台灣雲端高峰會 - 資安工作坊：3 小時
  - AWS TechFest：資安攻防入門實戰營：6 小時