資訊安全管理及執行情形

資通安全風險管理架構及管理政策

本公司設有資訊管理部，負責資通安全管理相關業務，並訂有資訊作業流程與管制程序，資安管理部分包含資安環境規劃、資安設備架設與維護、電腦防毒/防駭、資料備份等。資安管理管制作業如下:

1.記錄公司資訊系統、伺服主機、UPS、網路線路等運作情形與管制資訊機房人員進出狀況，以作為問題稽查追蹤使用。
2.為避免造成公司網路之干擾與安全性問題，禁止同仁未經申請核可情況下，私自架設 Wireless AP / Router 設備進行測試，以避免異常流量造成網路擁塞，影響其它同仁的網路使用權；經核可安裝者，架設後不可開啟 DHCP、不可與公司架設之 Wireless AP 頻道衝突且需設定加密功能。
3.公司所有連外網路專線、ADSL 均需受資訊單位管理；若因特殊需求欲架設獨立連外線路，需經資訊單位審核與最高主管核准方可使用。
4.資訊單位將透過網管系統與設備監控或側錄使用者的網路使用行為(包含 Internet、Email、IM 等)，若發現員工藉此傳遞公司機密資料或進行傷害公司行為，皆提報最高主管懲處並依法究辦。
5.公司所有網路連接，皆需透過 802.1x、Mac address 驗證，有線網路僅允許公司配發，且合法授權之設備可使用；若有無線網路需求之員工及外賓，使用者及受訪者需填寫 Wireless 申請單，並由最高主管核准。
6.各使用者有其使用代碼及密碼，依不同的職務及工作範圍設定不同的工作權限，以防止資料的存取、刪除、修改、新增、確認等所造成的錯誤及機密資訊外洩或被篡改之風險。

2024 年辦理資訊安全執行情形如下：

1. 於 2022 年 8 月導入網路 802.1x、Mac address 驗證，不論公司內、外部人員使用網路均需經過驗證，大幅提升網路使用安全。
2. 所有新進人員必需進行資訊安全管理課程訓練，課後並經學習測驗，提升其危機意識與資訊安全觀念。2024 年截至 9 月 30 日止，已有 37 人參與共計 74 小時的教育訓練。
3.已將資訊安全課程導入線上學習(AS E-Learning)課程，讓全體員工可以隨時上線學習。