資訊安全政策

本政策適用於邁萊及集團關係企業，範圍包含各營運據點同仁及接觸集團內部資訊之委外廠商、約聘廠商及派遣廠商，使人員針對資訊安全能有所依循，以利各項業務作業順利運行，並確保各項資訊與系統獲得適當保護之安全。

第一條 資訊安全概述

資訊安全宗旨即確保企業團內所使用之「資訊」的「安全」，而資訊，泛指組織內為達成其營運目標，在過程中所建立、蒐集、處理、利用、傳輸、儲存、銷毀的數位內容及紙本文件。重要之資訊例如：公文的收發、商業機密、競爭情報、營運報表、核心技術、設計圖紙、關鍵系統程式碼、採購訂單、人事資料、財務資料和電子郵件等，都屬於資訊，且對組織營運具有重要價值及影響，因此在資訊的生命週期中，組織需要確保重要資訊的「安全」，不可因洩漏遺失、竄改或毀損，而危及組織的營運、商譽、及資本損失。因此確實及準確的保障企業內的資訊安全是當今企業極具重要之課題。

第二條 集團資訊安全治理

集團於 2024 年度已成立資訊安全組織架構，並規劃導入 ISO 27001 資訊安全管理系統設立「資訊安全管理委員會」，致力保護集團重要資訊系統與資料的機密性、完整性與可用性，且負責企業團資訊安全管理制度之推動及審核事宜。

此資訊安全組織架構會進行資訊安全全球布局及完善資訊安全管理流程，並由資訊安全權責主管擔任主委員定期報告至董事會。

第三條 資訊安全目標

（一）對於集團之機敏資料採取適當保護與防範措施，以降低資訊安全事件之風險。

（二）降低發生毀損、失竊、洩漏、竄改、濫用、以及侵權等資訊安全事件之衝擊。

（三）持續提升集團各資訊安全作業之機密性、完整性與可用性。

第四條 員工資訊安全認知

企業員工是資訊安全最重要的一環，為了提升集團同仁的資訊安全意識，會每年定期舉辦資訊安全教育訓練，告知同仁基本資訊安全概念、最新的資訊安全趨勢以及最新的駭客攻擊手法，並讓同仁培養良好的資訊安全工作習慣，如：定期備份重要工作資料、仔細檢視電子郵件的來源地址、不打開來路不明的網路連結、在接觸機敏資料或是處理財務相關事宜時更加謹慎、以及避免在個人社群媒體留下過多的個人或公司資訊等，以降低資訊安全事件發生之機率。

第五條 資訊安全管理方針

（一）資訊安全防護人人有責，為確保集團員工之資訊安全意識，應不定期參與資訊安全相關的教育訓練，並了解近期國際發生之資訊安全事件，以強化員工自身之資訊安全意識，避免受到社交工程之危害以致資訊安全事件發生。

（二）於各企業團在進行業務作業時，如涉及傳輸重要資訊或敏感資料，應有適當之資訊安全保護措施，以降低機敏資訊外漏之風險。

（三）辦公所使用之個人電腦應安裝防毒軟體，並定期進行系統更新與病毒碼更新以降低駭客攻擊之風險及勒索病毒之危害。

（四）若發生資訊安全事件應立即通報相關單位，以降低資訊安全事件所造成的後續損失。

（五）資訊安全委員會將不定期進行資訊安全評估或稽核作業，以檢視資訊安全成熟度、管理措施與程序是否合乎相關標準、法令規章或資訊安全需求，並提供建議改善以持續增進集團資訊安全管理之有效性。

第六條 本資訊安全政策每年至少評估內容乙次，檢討覆核與修訂，以符合集團組織及策略發展，並符合內外部利害關係團體之期望，進而確保資訊安全政策要求之有效性。

第七條 實施規範與法令之遵循

所有人員應遵循此資訊安全政策，若違反則須依本公司相關規定予以處分，如涉有相關刑責或法律責任者，如網安法、營業秘密法、著作權法、個人資料保護法等，將衡量酌情節追訴其法律責任。