怡利電子工業股份有限公司

資訊安全政策及管理方案

一、資訊安全風險管理架構

為促進本公司資訊安全管理制度執行之有效性，已成立「資訊安全委員會」，由總管理處主管擔任召集人，每年定期或視需要召開會議，審查資訊安全管理相關事宜，使制度能有效達成既定之目標，增進業務運作之安全。

本公司資訊安全權責單位為資訊室，設置資訊安全主管 1 人，以及資訊安全人員 1 人。資訊安全由資訊部門主管擔任，主要任務為負責協助與執行資訊安全相關作業，對資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置，對於資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。資訊安全人員由資訊人員任，負責規劃及執行各項資訊安全作業，主要任務為負責資訊安全管理制度之規劃、執行、監控與改善資及處理資訊安全事件。

本公司於 112 年取得 TISAX 汽車資訊安全評估交換機制管理系統 Level 3 認證，113 年 10 月 24 日取得更新認證，於 116 年 6 月 20 日到期。

最近一次內部稽核已於 113 年 4 月 12 日完成，內部稽核 13 件發現事項，已全部完成矯正處理。

本年度管理審查會議合計召開 1 次，已於 113 年 5 月 10 日完成。主要內容為檢討資訊安全政策、內外部關注者議題、 稽核結果報告、風險評鑑與持續改善機會有關之決策。資訊安全治理報告已於民國 113 年 7 月 30 日提報董事會。

二、資訊安全政策

目的:

本公司為強化資訊安全管理，確保本公司所屬之資訊資產的機密性、完整性及可用性，以提供資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特訂定資訊安全政策規範。

願景與目標:

1. 資訊安全及原型品保護政策願景：

   強化人員認知、避免資料外洩

   落實日常維運、確保服務可用

2. 依據資訊安全及原型品保護政策願景，擬定資訊安全及原型品保護目標如下：
   - 辦理資訊安全及原型品保護教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。
   - 保護本公司業務活動及原型品資訊，避免未經授權的存取與修改，確保其正確完整。
   - 定期進行內部稽核，確保相關作業皆能確實落實。
   - 確保本公司關鍵核心系統維持一定水準的系統可用性。
3. 應針對上述資訊安全及原型品保護目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本公司”監督與量測管理辦法”IS-I15 辦理。
4. 資訊工作小組應於管理審查會議中，針對資訊安全及原型品保護目標有效性量測結果，向資訊安全委員會召集人進行報告。
5. 網路安全政策：
   - 我們將遵循 ISO 21434 等國際網路安全標準或與客戶約定的網路安全管理流程來維護我們的管理體系。
   - 我們應遵守上述公司層面的一般政策。

- 應識別與管理具有價值且與網路安全活動相關的資產，並由客戶與本公司協議適當的處理方式。
- 我們將開發安全產品作為我們的核心價值，因此我們將確保採取必要的活動。在功能安全和資訊安全的技術解決方案存在權衡時，應優先考慮功能安全的危害和技術解決方案，以最小化對資訊安全屬性的影響。我們也應考慮與其他團隊的相依性，例如 IT 安全團隊、研發團隊、工程團隊等。
  當產品同時具有功能安全性和網路安全相關性時，將在整個產品開發週期中指派來自這兩個領域的專業人員。這些專業人員可能包括來自兩個領域的經理和架構師。
- 我們將定期對流程進行網路安全稽核，以確保流程和開發活動符合第一條的要求。
- 我們將確保員工具備良好的網路安全技能或計劃和安排適當的培訓。
- 及時與客戶/供應商合作，對高優先級的威脅場景進行風險處理，並與客戶/供應商討論已識別的風險和漏洞。相關處理與識別程序，應遵循”風險評鑑與管理辦法”IS-I04 辦理。

責任:

1. 建立及審查此政策。
2. 資訊工作小組透過標準和程序以實施此政策。
3. 所有人員和委外服務供應商均須依照相關安全管理程序以維護資訊安全政策。
4. 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

審查:

1. 本政策應至少每年於管理審查會議審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本公司永續運作及資訊安全實務作業能力。

實施:

1. (含子公司)因業務需求取得本公司機敏性資訊或個人資料時，應負起資料保密責任及妥善運用，並遵守國家相關之法令及本公司之相關資訊安全規定。
2. 若因疏失造成資料外洩或資安事件，應負相關法律責任。
3. 本政策經「資訊安全委員會」進行會審後，由召集人核定後實施，修訂時亦同。

三、 資訊安全具體管理方案

1. 經由ISO27001資訊安全管理制度的實施，可以有效減少資安事件的發生，對風險管理具有一定的成效，綜合評估成本與效益後，目前暫無承保資安險的急迫性與必要性。
2. 已實施的ISO27001:2013標準14個領域及相關控措施。
   - 資訊安全政策
   - 資訊安全組織
   - 人力資源安全
   - 資產管理
   - 存取控制
   - 密碼學
   - 實體及環境安全
   - 運作安全
   - 通訊安全
   - 系統獲取開發及維護
   - 供應者關係
   - 資訊安全事故管理
   - 營運持續管理之資訊安全層面
   - 遵循性
3. 目前常見的網路惡意攻擊、勒索軟體等資安風險議題，已有投入網路資安設備的建置進行防護，如防火牆的入侵預防系統(IPS)設置，威脅偵測應變服務(MDR)。
   - 於112年10月完成集團三地重要伺服器佈署。
   - 監控期間112年10月~113年6月事件摘要:總計偵測到553筆異常事件。分析後有7筆為高風險惡意軟體行為。該7筆事件皆由MDR服務自動阻擋，未有擴散產生危害之狀況。

4. 每年都會針對核心系統，如網域控制站、電子郵件、ERP系統、資料庫、文件主機等...進行弱點掃描，弱點修補、備份還原演練、資安事件演練、營運持續演練，有效的預防資安風險的發生，如果風險發生時可以有效的控制災害並減少損失。已於113年3月完成上述所有項目的演練。