凱銳光電股份有限公司

資訊安全政策

一、 資訊安全綜合管理計劃

1. 核心目的:

為強化本公司資訊安全管理，確保資訊資產的機密性、完整性及可用性，維持資訊系統的穩定性，並符合相關法規與合約之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2. 發展藍圖與執行願景:

1. 資訊安全政策願景：

(1)維持資訊系統持續運作。

(2)防止駭客、病毒等入侵及破壞。

(3)落實日常維運。

(4)強化資訊安全基本觀念。

2. 遵循資訊安全政策方向，本公司確立以下目標：

(1)建立資訊安全委員會及「資訊管理程序」，以加強資訊安全的管理系統。

(2) 確保本公司關鍵核心系統維持一定水準的系統可用性。

(3) 保護本公司業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

(4) 定期進行內部稽核，確保相關作業皆能確實落實。

(5) 辦理資訊安全教育訓練，推廣員工資訊安全之意識與強化其對相關責任之認知。

3. 年度資訊安全實施計畫

為確保資訊安全目標的落實，公司制定年度計畫，包含待辦事項、資源配置、負責人員、完成時程及成效評估方式。同時，依照「監督與量測管理辦法」，對計畫進行持續監督與成效追蹤，確保有效執行。

4. 資安工作小組的報告流程

(1)定期於審查會議期中，由資安工作小組進行資訊安全目標的成效評估與量測。

(2)將量測結果報告於資訊安全委員會~~的~~召集人。呈現詳細數據分析，以供委員會決策參考，並優化資訊安全策略。

5. 網路安全政策指導方針

(1)遵守客戶協議的網路安全管理流程及「網路及系統安全管理辦法」，以確保系統的穩定運行。

(2)辨識並管理對網路安全活動至關重要的資產，並與客戶協議適當的安全處理方式。

(3)確保產品與作業流程符合安全標準，開發安全可靠的產品。

(4)定期進行網路安全稽核，以確保所有流程和開發活動都符合 4.2.1 條文的要求。

(5) 提供員工網路安全技能培訓，確保符合安全要求。

二、 資訊安全責任概述

1. 資訊安全委員會負責建立並定期審核資訊安全政策。

2. 資安工作小組需按照既定標準和程序實施該政策。

3. 公司員工和外包服務供應商都必須遵循相關的安全管理程序，以支持資訊安全政策。

4. 所有員工都有義務報告資訊安全事件和任何識別出的漏洞。

5. 對於違反資訊安全的行為，將根據情節的嚴重性追究相應的民事、刑事或行政責任，或依據公司規定處罰。

三、 政策評估與審核

為保持與當前政府法規、技術創新和業務變化的一致性，本政策需每年在管理審查會議中至少進行一次審查。這有助於保障公司的長期穩健發展和資訊安全實踐的能力。

四、 資訊安全實施規則

1. 本公司及其子公司在取得公司敏感資訊或個人資料時，應承擔保密責任並妥善使用該資料，同時遵守國家法律和公司的資訊安全條例。

2. 若因疏忽造成資料外洩或發生資訊安全事件，需承擔相應的法律後果。

3. 本政策需經資訊安全委員會的審核和召集人的批准後方能執行，其修改也需遵循同樣的程序。

五、 資訊安全具體管理項目

1. 鑒於當前網路安全風險如釣魚信件、網路攻擊、勒索軟體等，公司已部署諸如防火牆和入侵預防系統等網路安全設備，以及資訊資產管理系統來提供防護。

2. 定期對核心系統進行維護，包括對網域控制、電子郵件系統、ERP 系統等進行安全檢查，包括弱點掃描和修補、備份和恢復測試、安全演練和業務持續性演練，旨在預防和減少資安風險及其可能造成的損失。

六、 資訊安全事件處理流程