公司制定個人資料保護政策與其內容及實施情形之說明

本公司針對個人資料保護政策與其內容及實施情形依序說明如下：

本公司為上櫃公司，客戶大多為公家機關、金融機構及國內大型上市櫃公司，而本公司國內外供應商大多為長期合作之原廠，故本公司針對重大或有需要專案時，會與客戶或廠商須簽具保密切書，以確保雙方隱私權保護無虞。為維護個人資料適當安全的措施，本公司故訂定「國眾電腦股份有限公司個人資料保護實施辦法」，由總公司及各子公司執行辦理。其制定目的：為確保本公司保有個人資料檔案之安全，加強對個人資料之保護與管理能力，降低營運風險，並創造可信賴之個人資料保護及隱私環境，依個人資料保護法施行細則第九條，辦理個人資料安全維護事項，目前實施情形係尚無接受經證實侵犯客戶隱私或遺失客戶資料的投訴事件。

並於114年8月11日經審計委員會及董事會決議通過「國眾電腦股份有限公司消費者權益保護政策及申訴程序」，為關懷及善盡對顧客的權益保障，並建立重視消費者保護之企業文化，以落實針對產品與服務之顧客健康與安全、行銷或標示之把關。本公司之子公司未訂定消費者權益保護政策者，應適用該政策及申訴程序。另外，該政策係參考 GRI 及 SASB 等相關國際準則及國內法規訂定。以為使「消費者權益保護」成為公司整體共同遵循之價值體系與行為準則，本公司由總經理親自督導推動消費者權益保護之相關事宜，並由企業永續發展委員會負責規劃與執行。

最後，本公司亦積極申請 ISO/IEC 27701 中，預計於114年底前完成安排第三方驗證。ISO/IEC 27701:2019 是一項隱私資訊管理標準（PIMS），是 ISO/IEC 27001（資訊安全管理） 的擴充版本，專門用於管理個人可識別資訊（PII, Personally Identifiable Information）。這個標準幫助組織遵循如 GDPR（歐盟通用資料保護規則）、CCPA（加州消費者隱私法）等全球隱私法規的要求。

🧩 標準架構：
ISO 27701 延續 ISO 27001 的管理體系架構，並額外新增與隱私管理相關的控制措施與指引：
第 5–8 章：擴充 ISO 27001 的條款，新增隱私要求。
附錄 A：針對「PII 控制者（Controller）」的控制措施。
附錄 B：針對「PII 處理者（Processor）」的控制措施。
👥關鍵角色定義：
角色說明：
PII 控制者決定個人資料處理目的與方式（例如：收集用戶資料的公司）。
PII 處理者依控制者的指示進行資料處理（例如：雲端服務商、外包公司）。
🎯核心目標：
將 ISO 27001 的資訊安全管理擴展至隱私資料管理。
協助組織符合隱私法規（如 GDPR）。
建立明確的隱私角色與責任分工（控制者 vs 處理者）。
與資訊安全風險管理整合，提升整體資料保護能力。
☑ 認證資訊：
組織需先擁有 ISO/IEC 27001 認證，才能進行 ISO/IEC 27701 的認證。
認證涵蓋：隱私風險評估流程。
控制者與處理者的角色職責。
隱私影響評估（PIA）。
第三方資料處理管理等。
⚙與 ISO 27001 的整合對照：

ISO/IEC 27001	ISO/IEC 27701 補充內容
ISMS：資訊安全管理系統	PIMS：隱私資訊管理系統
CIA：機密性、完整性、可用性	增加資料隱私與保護需求
附錄 A：通用控制措施	附錄 A & B：針對隱私的專屬控制措施

📝導入 ISO 27701 的好處：
支援組織合規性（如 GDPR、CCPA、LGPD 等）。
增加客戶、合作夥伴的信任度。
強化資料保護與風險管理能力。
可透過認證展現隱私治理能力，提升市場競爭力。