台灣典範半導體股份有限公司
資通安全之風險管理

1. 資通安全管理策略與架構

- **資訊安全政策**

  在配合本公司資訊安全政策要求，確保所屬之資訊與資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，考量適用之資訊安全要求事項，以及風險評鑑與風險處理之結果後制訂下列資訊安全政策目標：

  - 保護本公司關鍵業務資訊，避免未經授權的存取。
  - 定期評估各項人為與天然災害對本公司資訊資產之衝擊，訂定重要關鍵性資訊資產之防災對策與災難復原計劃，維持核心資訊系統持續運作確保本公司具備可供業務持續運作之資訊環境。
  - 督導本公司同仁資訊安全防護工作，建立正確資訊安全防護意識。
  - 要求本公司全體同仁以及使用本公司電腦系統之往來客戶廠商，應確實遵守本公司資訊安全相關規定，如有違反者，將受追訴相關法律責任。

- **制定資訊安全風險管理架構**

  為提升資訊安全管理， 組成資訊安全管理小組，資訊部負責主導及規劃制定資訊安全管理政策，各業務相關單位配合執行，定期實施資訊安全宣導及資安稽核，以確認資訊安全管理運作之有效性。

- **資訊安全具體管理方案及投入資源**

風險項目	因應對策
教育訓練及宣導	定期辦理資訊安全教育訓練及宣導，建立員工資管安全認知及強化資管安全意識，登入系統的身份驗證、密碼控管、存取授權管制及定期進行更新病毒碼等稽核機制。
網路威脅	針對外部威脅，網路建立 IPS、防火牆等多層次防禦，並建立防毒、郵件過濾、郵件稽核、惡意程式偵測等管控機制，以降低網路威脅。

資產管理	資管設備依規定申請出入廠、入廠之廠外設備皆依公司規範進行管制，以確認無資管外洩疑慮。
備援機制	重要服務與資料皆有建立備援與異地備份，並定期進行災害還原測試，以確保服務不中斷與資料不遺失。
存取管制	人員存取內外部系統與資料傳輸進行管制，避免資料外洩並保留行為軌跡紀錄。
文件加密	使用文件保全加密技術，保護公司內部重要機敏資料，避免未經授權機敏文件外流事件發生。
ISO-27001 推動	預計推動國際資安管理系統認證 （ISO/IEC 27001），從系統面、技術面、 程序面降低企業資安威脅，建立符合客戶需求、最高規格 的機密資訊保護服務。

公司內部應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業，以防範電腦網路犯罪與危機，維護資訊系統安全。符合一定條件者，依主管機關命令指派綜理資訊安全政策推動及資源調度事務之人兼任資訊安全長，及設置資訊安全專責單位、主管及人員。

2. 資通安全風險評估分析及其因應措施：

本公司已建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統能完全避免來自任何第三方癱瘓系統的網路攻擊。這些網路攻擊以非法方式入侵本公司的內部網路系統，進行破壞公司之營運及損及公司商譽等活動。在遭受嚴重網路攻擊的情況下，本公司的系統可能會失去公司重要的資料，生產線也可能因此停擺。本公司透過持續檢視和評估其資訊安全規章及程序，以確 保其適當性和有效性，但不能保證公司在瞬息萬變的資 訊安全威脅中不受推陳出新的風險和攻擊所影響。網路攻擊也可能企圖竊取公司的營業祕密及其他機密資訊，例 如客戶或其他利害關係人的專有資訊以及本公司員工的個資。

惡意的駭客亦能試圖將電腦病毒、破壞性軟體或勒索軟體導入本公司的網路系統，以干擾公司的營運、對本公司進行敲詐或勒索，取得電腦系統控制權，或窺探機密資訊。這些攻擊可能導致公司因延誤或中斷訂單而需賠償客戶的損失；或需擔負龐大的費用實施補救和改進措施，以加強公司的網路安全系統；也可能使公司因涉入公司對其有保密義務之員工、客戶或第三方資訊外洩而導致的相關法律案件或監管調查，而承擔重大法律責任。

過去曾經有同業因購買及安裝內含惡意軟體的設備而遭受攻擊，本公司未來也可能面臨類似的攻擊。為了預防及降低此類攻擊所造成的傷害，公司落實相關改進措施並持續更新，例如建置機台入廠掃毒機制以防止內含惡意軟體的機台進入公司；強化網路防火牆與網路控管以防止電腦病毒跨機台及跨廠區擴散；依電腦類型建置端點防毒措施；導入先進的解決方案以偵測與處理惡意軟體；設計開發資安強化個人電腦供員工使用；設計開發雲端應用安全政策；導入新技術加強資料保護；加強釣魚郵件偵測；建立一個整合的自動化資安維運平台，並定期執行員工警覺性測試及委託外部專家執行資安評鑑。雖然本公司持續加強資訊安全防護措施，但仍無法保證公司免於惡意軟體及駭客攻擊。

此外，本公司需要分享高度敏感及機密的資訊給部分其雇用提供公司及其全球關係企業服務的第三方廠商，以使其能提供相關服務。儘管公司在和第三方服務廠商簽訂之服務合約中，要求其遵守保密及／或網路安全規定，但不能保證每個第三方服務廠商都將嚴守這些義務。由上述服務廠商及／或其承攬商所維護的內部網路系統及外部雲端運算網路（例如伺服器），亦會有遭受網路攻擊的風險。若本公司或其服務廠商無法及時解決這些網路攻擊所造成的技術性問題，或確保公司(及屬於本公司客戶或其他第三方)的數據完整性及可用性，或控制住公司或其服務廠商的電腦系統，皆可能嚴重 損及本公司對客戶和其他利害關係人的承諾，而公司營運成果、財務狀況、前景及聲譽亦可能因此遭受重大不利影響。

3. 重大資通安全事件：

截至目前為止，無發生重大資安事件。