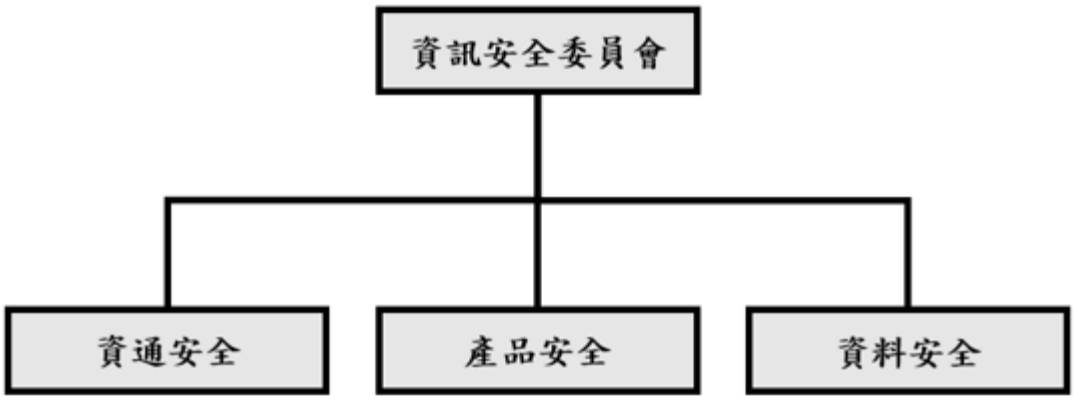
資訊安全風險管理政策

• 資訊安全風險管理架構

為管理資訊安全風險之目的，聯發科技股份有限公司 (以下簡稱「聯發科技」) 成立資訊安全委員會，由公司副總級含以上擔任召集人，定期檢討資通安全、產品安全、以及資料安全的執行狀況，並定期向董事會報告資訊安全檢查情形。資訊安全委員會每半年至少召開一次，並得視資安風險管理需要隨時召開會議，資訊安全委員會召集人代表資訊安全委員會，每年向董事會報告一次。

- 資通安全：涵蓋資通安全管理、規劃、督導及推動執行。
- 產品安全：涵蓋產品安全框架規劃與導入，產業合規、程序制定、教育訓練、威脅模型、測試規範、漏洞管理等。
- 資料安全：涵蓋制定、執行及討論智權資訊管理規範。



- **資訊安全策略**

1. 為有效落實資訊安全管理，聯發科技應依據 ISO/IEC 27001 的 Plan-Do-Check-Act (PDCA) 循環運作模式，建立與實施資訊安全管理制度 (Information Security Management System, 以下簡稱 ISMS)[1]，並參考美國國家標準技術研究院資通安全框架 (National Institute of Standards and Technology Cybersecurity Framework, 以下簡稱 NIST CSF)，將資訊安全控管機制整合入平日作業流程。

2. 聯發科技應維護資訊的機密性 (Confidentiality)、完整性 (Integrity) 與可用性 (Availability)，以降低資訊未經授權使用、遭受破壞或外洩的風險，並符合政府資訊安全相關法令、規定與政策要求。

3. 為維護客戶對產品安全之信心，聯發科技應建立有效的控管措施，以確保產品無安全性或隱私性漏洞隱憂，包括但不限於安全需求及架構分析、威脅分析、代碼掃描、安全事件應變及漏洞管理。

4. 聯發科技應建置「多層次資安偵測與防禦 (Defense in Depth)」，主動積極建立事前安全防護；當資訊安全事件發生時，能迅速作必要的應變處置，降低可能帶來的損害，強化資訊安全韌性。

5. 聯發科技應透過教育訓練，強化同仁對資訊安全的認知，建立「資訊安全，人人有責」的概念。

[1] 本公司已於 2022 年導入 ISO 27001 資訊安全管理系統標準，並持續取得 ISO27001 認證，最新證書之有效期為 2025 年 12 月 6 日至 2028 年 12 月 5 日。

- **供應商資訊安全要求**

聯發科技之供應商應遵循聯發科技資訊安全政策，並與聯發科技簽訂必要之資訊安全合約及保密約定。

- **資訊安全控制措施**

聯發科技應參考 NIST CSF，制定資訊安全防護及控制措施。

治理 (Govern)	**識別 (Identify)**	審視業務環境及關鍵資源與服務，發展符合日常營運的風險管理策略，包括制定資訊安全規範、建置資產管理系統。
	保護 (Protect)	制定並實施相應的防禦措施，強化關鍵資源與服務，包括身分與存取管理 (Identity Access Management, IAM)、防毒軟體、端點防護與系統修補管理。
	偵測 (Detect)	建置即時偵測資訊安全事件與告警的機制，包括電子郵件防護系統、入侵偵測系統、資訊安全監控中心 (Security Operations Center, SOC) ，並定期檢測資訊系統架構。
	回應 (Respond)	設有應變小組 (Cyber Security Incident Response Team, CSIRT) 負責資訊安全事件應變處置，包括事件調查、鑑識與提出改善方案。資訊安全通報與處理皆應依相關資訊安全規範執行。
	復原 (Recover)	制定資料備援計劃。若遭遇資訊安全事件影響營運，能在最短的時間內回復正常。