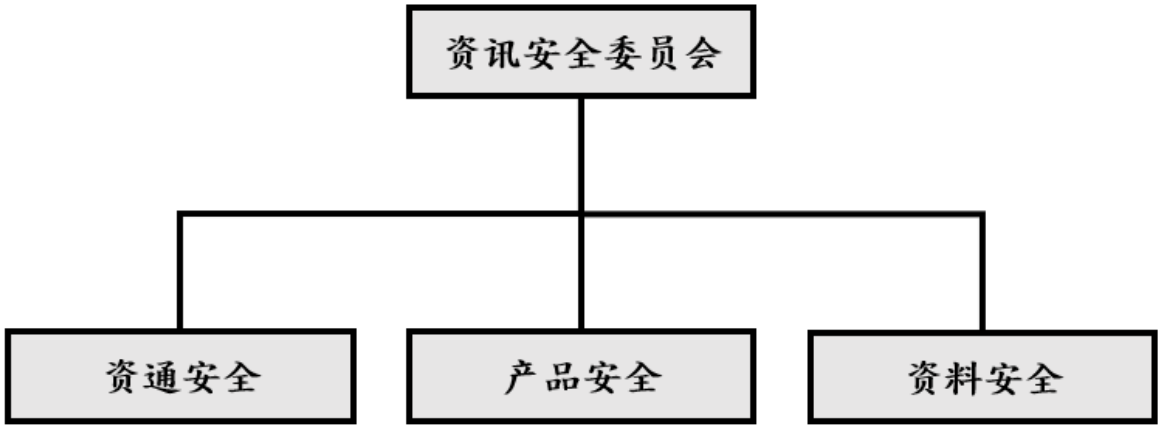
资讯安全风险管理政策

• 资讯安全风险管理架构

为管理资讯安全风险之目的，联发科技股份有限公司 (以下简称「联发科技」) 成立资讯安全委员会，由共同营运长及公司执行副总经理暨财务长担任召集人，定期检讨资通安全、产品安全、以及资料安全的执行状况，并定期向董事会报告资讯安全检查情形。资讯安全委员会每半年至少召开一次，并得视资安风险管理需要随时召开会议，资讯安全委员会召集人代表资讯安全委员会，每年向董事会报告一次。

- 资通安全：涵盖资通安全管理、规划、督导及推动执行。
- 产品安全：涵盖产品安全框架规划与导入，产业合规、程序制定、教育训练、威胁模型、测试规范、漏洞管理等。
- 资料安全：涵盖制定、执行及讨论智权资讯管理规范。



- **资讯安全策略**

1. 为有效落实资讯安全管理，联发科技应依据 ISO/IEC 27001 的 Plan-Do-Check-Act (PDCA) 循环运作模式，建立与实施资讯安全管理制度 (Information Security Management System, 以下简称 ISMS)[1]，并参考美国国家标准技术研究院资通安全框架 (National Institute of Standards and Technology Cybersecurity Framework, 以下简称 NIST CSF)，将资讯安全控管机制整合入平日作业流程。

2. 联发科技应维护资讯的机密性 (Confidentiality)、完整性 (Integrity) 与可用性 (Availability)，以降低资讯未经授权使用、遭受破坏或外泄的风险，并符合政府资讯安全相关法令、规定与政策要求。

3. 为维护客户对产品安全之信心，联发科技应建立有效的控管措施，以确保产品无安全性或隐私性漏洞隐忧，包括但不限于安全需求及架构分析、威胁分析、代码扫描、安全事件应变及漏洞管理。

4. 联发科技应建置「多层次资安侦测与防御 (Defense in Depth)」，主动积极建立事前安全防护；当资讯安全事件发生时，能迅速作必要的应变处置，降低可能带来的损害，强化资讯安全韧性。

5. 联发科技应透过教育训练，强化同仁对资讯安全的认知，建立「资讯安全，人人有责」的概念。

[1] 本公司已于 2022 年导入 ISO 27001 资讯安全管理系统标准，并持续取得 ISO27001 认证，最新证书之有效期为 2025 年 12 月 6 日至 2028 年 12 月 5 日。

- **供应商资讯安全要求**

联发科技之供应商应遵循联发科技资讯安全政策，并与联发科技签订必要之资讯安全合约及保密约定。

- **资讯安全控制措施**

联发科技应参考 NIST CSF，制定资讯安全防护及控制措施。

治理 (Govern)	**识别 (Identify)**	审视业务环境及关键资源与服务，发展符合日常营运的风险管理策略，包括制定资讯安全规范、建置资产管理系统。
	保护 (Protect)	制定并实施相应的防御措施，强化关键资源与服务，包括身分与存取管理 (Identity Access Management, IAM)、防毒软体、端点防护与系统修补管理。
	侦测 (Detect)	建置即时侦测资讯安全事件与告警的机制，包括电子邮件防护系统、入侵侦测系统、资讯安全监控中心 (Security Operations Center, SOC) ，并定期检测资讯系统架构。
	回应 (Respond)	设有应变小组 (Cyber Security Incident Response Team, CSIRT) 负责资讯安全事件应变处置，包括事件调查、鉴识与提出改善方案。资讯安全通报与处理皆应依相关资讯安全规范执行。
	复原 (Recover)	制定资料备援计划。若遭遇资讯安全事件影响营运，能在最短的时间内回复正常。