友达信息安全政策与治理方针

友达信息安全政策

「保护公司智慧财产，全面提升资安意识，共创赢(盈)的契机」为本公司信息安全之核心理念。本公司高度重视信息安全，视其为企业永续发展的重要基石，以保护客户、公司及利害关系人之重要信息资产为目标，持续强化整体资安治理与防护能力。

友达信息安全承诺

本公司承诺持续精进信息安全治理，并致力于：

- 持续完善信息安全管理系统，提升信息资产整体防护能力
- 确保信息资产之机密性、完整性与可用性，涵盖客户数据、个人资料及公司自有资料
- 持续监控并有效响应信息安全威胁与事故，降低对营运及利害关系人之冲击
- 落实全体员工之信息安全责任与当责文化，强化资安意识与日常遵循
- 强化供应链与合作伙伴之信息安全要求，共同维护信息生态系统之安全

资安治理架构

本公司由董事会层级之永续暨风险管理委员会统筹监督信息安全风险，并透过专责治理机制将资安纳入企业整体风险管理架构中。同时设立信息安全委员会负责审议资安政策与策略，并由信息安全长领导专责单位及跨部门团队推动各项资安工作，确保资安治理由上而下有效落实。

标准遵循与认证

本公司参考国际标准（包含但不限于ISO/IEC 27001）建置信息安全管理系统（Information Security Management System, ISMS），透过制度化、文件化及系统化之管理机制，持续强化信息安全管理能力与营运韧性，规划资安策略与行动方案，确保资安管理与公司整体营运发展方向一致，并取得相关认证（包含但不限于ISO/IEC 27001）。

法规遵循与隐私保护

本公司遵循相关信息安全与个人资料保护法规（包含但不限于GDPR），并制订隐私权政策，说明个人资料搜集、处理、利用及当事人权利保障机制。

风险管理与防护机制

本公司透过系统化风险评鉴机制，定期识别与分析资安风险，并将其纳入企业整体风险管理流程中，以确保重要资产受到适切保护。同时透过多层次防护策略，包含系统防护、弱点管理、事件侦测与响应机制等，持续强化资安防御能力与应变效率。

访问控制与数据保护

为确保数据安全，本公司依最小权限原则（Least Privilege）管理使用者访问权限，并导入多项管理与技术控制措施（包含但不限于多因子验证、传输与储存加密机制），确保信息于全生命周期皆受到妥善保护。

资安事件管理与通报机制

本公司建立资安事件应变程序，涵盖事件侦测、通报、分析、遏止与复原等流程，以降低事件冲击。于发生重大资安事件时，将依相关法规及契约要求，于适当时限内通知相关利害关系人及主管机关。

营运韧性与持续营运

本公司建置营运持续计划（BCP）及灾难复原机制（DR），透过备援设计、数据备份、复原机制与定期演练，确保关键系统及业务于灾害发生时可于可接受时间内恢复运作。

资安文化与员工责任

本公司致力推动全员资安文化，透过教育训练、倡导活动与制度规范，强化员工对信息安全之认知与遵循，并落实资安共责与当责之管理理念。

供应链与生态系安全

本公司将资安管理延伸至供应链与合作伙伴，要求供货商及合作伙伴遵循信息安全相关规范，并透过评估、契约条款及定期管理机制，共同提升整体资安防护水平，建立安全且可信赖的产业生态系。

系统开发与技术安全

本公司于系统开发生命周期（SDLC）中导入资安要求，包括安全设计、程序代码检视、弱点扫描及渗透测试，并落实系统变更与漏洞修补管理，以降低系统风险。

绩效、持续改善与稽核

本公司订定资安绩效指标（如弱点修补率、事件响应时效、训练完成率等），定期监控与检讨，以确保资安管理之落实与持续改善。本公司透过内外部稽核机制，定期检视信息安全管理制度之有效性，并由管理阶层进行审查，持续精进资安治理与控制措施。

持续合作与产业参与

本公司积极参与产业资安合作与人才培育，透过跨组织交流与专业合作，共同强化整体社会之资安韧性。

數位長 謝忠賢

Version 1, July 2026