



信息安全政策

目的

广合科技致力于保证信息的保密性、可用性和完整性。秉承“改进信息安全技术，提升信息安全意识，严守信息安全策略，降低信息安全风险”的信息安全方针，在 2026 年 1 月发布广合科技《信息安全政策》作为核心指导原则，为各方利益相关者筑牢可信、安全、可持续的数字基石。

适用范围

本政策适用于广州广合科技股份有限公司及各子公司。

我们的原则与立场

（1）广合承诺

广合科技承诺严格遵守信息安全国家和行业相关法律法规以及所有客户保密合约，通过信息安全风险评估，不断改进信息安全技术和完善信息安全策略。

广合科技承诺加强对各级员工信息安全教育，降低信息安全风险，杜绝重大信息泄密事件发生。遵守 ISO 27001 信息安全标准，以达到利益相关方的期望作为重点工作目标之一。

（2）信息安全治理

由总经理领导，信息中心、人力资源中心、市场营销中心、财务中心、品质中心、设备设施中心、工程技术中心、研究院等相关部门的最高负责人组成信息安全管理小组，负责对广合科技的信息安全进行监督与评审，并制定战略和协调各部门信息安全工作落地。

职能部门需依据职责，在日常运营中履行信息安全保护责任，确保信息安全保护工作落地。

所有员工都对信息安全保护负有责任，包括但不限于信息安全事件报告和遵守保密协议。

（3）数据保护

采用包括但不限于双链路冗余网络架构、网关防火墙、终端防病毒、入侵态势感知平台、服务器冗余备份与端到端加密等技术，确保数据传输与存储的稳定、完整与保密，实现实时威胁监控与快速响应。

实行信息分级分类管理、严格的审批流程与最小权限控制等管理手段，确保机密信息仅限授权专职人员访问。

定期进行升级防火墙和杀毒软件、扫描病毒、检查服务器硬件和软件、核查数据完整性等日常维护，确保终端安全和数据完整性。

（4）信息安全风险监控与持续改进

按照《信息安全技术 信息安全风险评估规范》（GB/T 20984-2022）等国内国际认可的标准制定信息安全风险管理程序，定期识别信息安全风险并持续改进。

定期开展安全漏洞扫描和攻防演练，及时发现并修复潜在安全风险，持续增强整体安全应对能力。

定期进行内部审计和 ISO 27001 管理体系评估，验证对政策和标准的遵守情况，并推动内部信息安全系统和管理体系的持续改进。

（5）员工意识与培训

定期开展覆盖全体员工的信息安全培训与考核，强化员工保密和数据操作规范的认知。

（6）供应商信息安全管理

供应商必须与公司签署保密协议，并每年完成信息安全培训。所有供应商来访须提前登记备案，由对应采购人员全程陪同，严禁进入未经授权的信息安全区域。

所有供应商在接入公司系统前必须签署保密协议，接受堡垒机进行的行为监督，并通过公司信息安全资质审查和定期审核。明确供应商数据保护责任，确保其数据保护能力的符合性与改进情况。

（7）客户信息安全管理

客户资料的传输与存储由专职人员管理，信息中心落实访问授权、密码策略及备份机制，确保客户隐私数据在全生命周期内可控。

政策发布与审查

本政策经广合科技集团总经理审核通过，并对执行情况进行持续监督。本政策发布后，信息安全管理小组与 ESG 办公室依据外部环境、法律法规等因素变化，进行政策审查与修订，修订稿经集团总经理审议批准后发布。