

信息安全政策

保利物业服务股份有限公司（以下简称“保利物业”或“公司”）高度重视信息安全管理，致力于保护公司信息系统、网络设备、数据资产及相关信息存储介质的安全，防范未经授权的访问、泄露、篡改、损毁、误传及恶意攻击等风险，保障公司业务运营的连续性、稳定性和可靠性。

本政策适用于保利物业及控股子公司，并鼓励所有参股公司及供应商、承包商等商业合作伙伴共同遵守。

一、管治架构

- 建立信息安全管理机制，由相关职能部门统筹信息安全工作，推动信息安全制度建设、系统安全管理、风险识别、问题收集、检查监督及整改落实；

- 各业务部门及相关单位按照职责分工，配合开展信息安全工作，及时识别、反馈和处理信息安全问题，共同维护公司信息系统和数据资产安全。

二、具体举措

- 持续加强信息系统运维管理，规范系统账号、密码、日志、监控、备份等管理要求，保障信息系统安全、稳定运行；

- 对信息系统建设、变更、上线、测试、验收及维护实施必要的管理控制，在系统建设和变更过程中开展评估、审批、备份及风险控制，降低对业务运营的影响；

- 加强网络安全和终端安全管理，对服务器、网络环境、系统状态、防火墙、路由器、交换机、办公电脑等信息基础设施进行必要的配置、监控、维护和安全防护，防范外部非法访问及内部不当操作带来的安全风险；

- 持续开展防病毒及恶意软件防护管理，在服务器、客户端及相关终端设备上部署必要的安全防护措施，并根据需要开展病毒库更新、病毒查杀、安全测试及风险处置；

- 重视数据资产保护，按照内部管理要求开展重要数据和软件备份，防范数据丢失、损坏或不可恢复风险；

- 规范信息存储介质的领用、借阅、传递、使用、归还、处置和销毁流程，降低敏感信息或重要信息在存储、传输及处置过程中的泄露风险；

- 遵循权限最小化原则，控制信息系统访问权限及数据交换权限，防止未经授权访问、使用、披露或处理相关信息；

- 在信息系统建设、软件采购、硬件维护及外部服务过程中，按照采购及合同管理要求选择供应商或服务商，并根据业务需要在合同中明确保密、信息安全、服务范围、记录保存等相关要求；

- 定期或不定期开展信息安全检查，关注硬件设备、应用系统、防病毒软件、账号密码、存储介质、数据备份及员工信息安全行为等重点领域。对于违反信息安全管理要求、造成信息系统损害、数据泄露、数据丢失或其他不良影响的行为，本集团将按照相关法律法规及内部制度要求进行处理；

- 持续提升员工信息安全意识，要求全体员工规范使用工作电脑、电子邮件、移动存储介质、外部软件及网络资源，避免访问非法网站、使用来源不明的软件或硬件设备，防范病毒传播、数据泄露及系统损害。

本政策由董事会负责监督，将每三年一次或适时进行回顾及更新，以确保符合相关法律法规要求，并促进公司持续提升可持续发展水平。