招商局公路网络科技控股股份有限公司

信息安全政策

第一章总则

第一条 招商局公路网络科技控股股份有限公司（以下简称“本公司”）严格遵循《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规要求，制定《招商局公路网络科技控股股份有限公司信息安全政策》（以下简称“本政策”），将信息安全风险纳入公司全面风险管理体系，深化主动预防与被动响应机制建设，完善信息安全管理体系，持续提升公司信息系统安全等级，进一步保障客户权益与公司数字资产安全。

第二条 本政策适用于本公司及各所属公司（以下简称“本公司”）的全部业务活动。

第三条 本公司要求供应商等合作伙伴在与本公司开展业务活动时遵守本政策的相关规定。

第二章组织与责任

第四条 本公司以国家网络安全法律法规要求为基本遵循，贯彻“全员参与、合法合规、管理先导、风险管控、技术支撑、重点防护、监督审计、持续改善”的工作原则，制定并落实《数字化工作管理制度》《数字化运维管理制度》《网络安全管理制度》等内部制度与管理办法，持续建设覆盖边界安全、物理与环境安全、应用安全、运维安全、管理安全及安全测试等全方

位的信息安全体系，实现安全能力的统一规划与规范管理。

第五条 本公司建立并持续完善信息安全管理体系。依据“谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”原则，逐级细化分解网络安全责任并严格落实。本公司设立信息化工作领导小组，由公司总经理、信息化副总经理、首席数字官、信息化工作职能部门及各职能部门负责人组成，为信息化日常管理工作的决策机构，负责审议公司信息化规划、预算与投资，审定发布公司信息化标准，以及审定本公司信息安全政策及重大信息安全事件的报告。

第六条 本公司信息化工作领导小组下设信息化工作小组，负责督促指导所属公司的信息化重点项目，考核所属公司信息化工作，协调信息安全工作及日常管理工作。

第七条 本公司各所属公司设置独立的信息化工作职能部门或信息化工作专职岗位，负责本公司信息化基础设施（设备）、基础软件、应用系统及终端设备的运行维护、服务支持及管理，以及本公司信息安全管理与审计。公司本部与各所属公司负责人为信息安全的第一责任人，第一责任人需督促本单位及员工做好网络安全保护工作。本公司每年年初与各所属公司、部门签订《网络安全保护责任书》。

第三章信息安全管理机制

第八条 本公司及各所属公司建立并持续优化系统运行维护与应用支持管理服务体系。遵循“事前主动预防、事中积极应对、事后优化整改”的原则，坚持管理与技术

并重，确保系统持续、稳定、安全、高效地运行。本公司通过常态化风险评估、分层防御部署、常态化威胁检测、标准化应急响应和漏洞修复机制，持续提升公司整体信息安全防护水平。

第九条 本公司监控并应对信息安全威胁。网络出口处应当部署相关设备检测和阻止攻击行为、恶意代码、垃圾邮件，净化网络信息。

第十条 本公司建设信息安全文化。面向全体员工（含劳务派遣员工），定期开展数据安全保护相关培训，强化员工信息安全意识。

第十一条 本公司严格落实系统备份、恢复管理。各应用信息系统的管理单位应制订可行的备份方案和灾难恢复方案，以保障在出现系统故障或数据丢失等影响业务正常运行的情况时恢复系统，减少和避免信息资产损失。

第十二条 本公司严格落实系统容灾管理。重要系统应制定合理的设备冗余和容灾方案，以保障当部分设备发生故障时能够支持业务和系统连续运行；重要系统和数据应进行异机备份或用备份设备进行备份，以保障系统和数据具备合理容灾性能。

第十三条 本公司已针对不同等级的信息安全事件，制定分级应急响应预案，并每年至少开展一次应急演练工作，要求相关人员必须参加培训与演练，总结并优化保障计划。

第四章数据安全管理机制

第十四条 本公司各数据库服务器责任单位应制定数据备份方案，并按方案进行备份，方案报主管部门备案。应用人

员要对自己本地计算机的信息安全负责，做好各自的信息备份工作。

第十五条 本公司应制定涉密电子信息保密管理办法，对涉密电子信息按公司保密制度进行密级划分并按密级进行管制。员工有责任和义务保护所接触到的含有公司密级文档、敏感资料（包括第三方数据）的电子文档、纸质文档和数据，终端设备上如承载有保密数据，须依照《招商公路保密管理规定》有关要求管理及使用。未经批准禁止任何人将公司信息系统中的电子数据提供给无关人员、外单位人员；未经批准禁止任何人复制、转移、查看、发布、打印公司涉密信息。

第十六条 本公司对外提供技术类电子数据与涉密电子文档时，均须按审批权限完成流出审批，并与客户签收凭证一并备案存档。

第十七条 本公司各类计算机、数字存储设备经报废、送外维修、外借、出售等方式转出公司时，员工有责任将所需数据备份，并对存储的保密、受限、敏感信息进行不可恢复性删除。

第十八条 本公司涉密信息不得在非涉密网络上存储、传输、处理。

第五章信息安全审计与评估

第十九条 本公司基于公司内控自评价、网络安全等级保护组织外部机构开展外部审计，落实信息安全审计管理要求。在信息安全等级保护工作方面，公司按年度开展网络安全等级保护测评工作，做到定期测评、定期发现、定期整改。同时，公司依照监管要求，定期聘请专

业第三方机构实施信息技术管理工作审计，覆盖信息技术治理、信息技术合规风险管理、安全管理、运维管理等信息技术管理各个方面。

第二十条 本公司结合监管要求及公司内部管理规定，定期通过审计、评估、调查等多种审计形式，对公司信息技术管理工作进行监督检查，并将信息技术内部控制有效性纳入公司内控有效性评价，通过多种角度强化信息科技内控水平。

第六章附则

第二十一条 本政策依据国家法律法规及行业规范制定。当出现特定场景下与国家法律、行政法规、规范性文件冲突时，以国家法律、行政法规、规范性文件为准。

第二十二条 本政策由董事会战略与可持续发展委员会负责制定、解释和修订。

第二十三条 本政策自发布之日起实施。