

江苏宁沪高速公路股份有限公司

信息安全与网络安全政策

第一章 总则

第一条 为规范江苏宁沪高速公路股份有限公司（以下简称“公司”）信息安全与网络安全管理，深入贯彻《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，落实江苏交通控股有限公司相关制度要求，将信息安全风险纳入公司全面风险管理体系，完善信息安全治理机制，强化网络安全主动防控与被动响应能力，保障公司业务持续稳定运行与数字资产安全，特制定本政策。

第二条 本政策适用于公司本部及各所属单位（以下统称“各单位”）的信息化建设、运维、使用等全部业务活动。

第三条 公司要求供应商、服务商等合作伙伴在与公司开展业务合作时，严格遵守本政策相关规定，共同保障业务合作全流程的信息与网络安全。

第二章 组织与责任

第四条 公司遵循“谁主管谁负责、谁建设谁负责、谁运维谁负责、谁使用谁负责”与“属地管理”原则，建立分级管控、权责清晰的信息安全与网络安全责任体系。

第五条 公司设立网络信息安全委员会，作为公司信息安全与网络安全工作的决策机构，负责审议公司信息安全与网络安全规划、预算投入、重要制度及重大安全事件处置方案，统筹协调全公司网络与信息安全重大事项。公司董事会监督公司信息安全与网络安全风险管理，每年至少听取一次信息安全与网络安全管理及重大风险情况报告。

第六条 网络信息安全委员会下设管理办公室，办公室设在运营管理中心（信息技术部），是委员会的执行与办事机构，具体职责包括：

（一）统筹拟定公司信息安全与网络安全管理制度、标准与规范，经审定后组织落地实施；

（二）协调、监督各单位信息安全与网络安全工作落实情况，定期组织检查、考核与通报；

（三）牵头开展信息安全风险评估、网络安全等级保护测评、应急演练等专项工作；

（四）负责网络安全事件的统筹协调、处置调度与复盘管理。

第七条 公司各部门、各所属单位主要负责人是本单位信息安全与网络安全工作的第一责任人，负责本单位网络与信息系统的日常安全管理，配备专（兼）职安全管理人员，落实各项安全管理要求。公司每年年初与各所属单位、各部门签订《网络安全保护责任书》，层层压实安全责任。全体员工对其使用的账号、终端设备、访问权限及接触的数据承担个人信息安全责任，不得共享账号口令、不得违规外发或者私自留存公司数据与客户个人信息。

第三章 信息安全管理机制

第八条 公司坚持“事前主动预防、事中积极应对、事后优化整改”的原则，构建管理与技术并重、覆盖全生命周期、持续改进完善的信息安全防护体系。

第九条 网络与信息系统建设遵循“同步规划、同步建设、同步使用”的三同步原则，采购的网络安全产品须符合国家法律法规要求，操作系统、数据库、中间件、办公软件等须使用正版授权软件。

第十条 公司实施网络边界安全分级管控，专用业务网与互联网、不同业务专网之间明确边界并采取物理或逻辑隔离措施；确需跨网络进行数据交互的，须落实安全隔离、访问控制与传输加密策略，确保网络传输安全。

第十一条 公司加强机房物理环境安全管理，各单位机房须配备防火、防盗、防水、防鼠、防雷及环境监控设施，严格执行人员与设备进出机房登记制度，保障信息系统基础设施物理安全。

第十二条 各单位须建立常态化系统运维安全机制：

（一）定期开展漏洞扫描、渗透测试等安全检测工作，对发现的安全漏洞与隐患及时整改闭环，完整留存工作记录；

（二）动态排查清理“僵尸系统”，对停止运维、停止使用的信息系统、网站按规范流程及时下线退网；

（三）信息系统正式上线或对外提供服务前，须完成安全策略加固、防火墙配置、安全检测等工作，安全检查报告报运营管理中心备案认可后方可启用；

（四）运维工作使用专用设备，外部计算机或移动存储介质接入专用业务网须经病毒查杀与安全审批；

（五）主机与信息系统须安装适配的防病毒软件，定期升级病毒库并开展病毒查杀，病毒高发期加密检测频次。

第十三条 公司严格落实账号与密码安全管理：

（一）各类系统、设备的账号密码由专人负责管理，定期更新，人员岗位变动时立即完成账号权限调整与密码变更；

（二）密码设置须符合安全强度要求，具备条件的核心业务系统推行双因素身份认证登录机制。

第十四条 公司建立分级数据备份与容灾管理体系：

（一）各单位根据信息系统重要程度、恢复要求制定差异化数据备份方案，明确备份周期与保存期限，定期开展备份有效性验证；

（二）重要核心业务系统部署冗余架构，制定灾难恢复预案，保障核心业务连续性；

（三）重要系统与核心数据采用异机、异地备份方式，确保数据具备合理容灾恢复能力。

第十五条 公司推行信息系统白名单管理，各单位每年4月对当前在运及年度拟建的信息系统（含网站、APP、小程序等）进行白名单申报，提交《网络信息安全年度白名单申报表》《网络信息安全管理安全承诺书》，报运营管理中心审核备案。未纳入白名单的信息系统不得上线运行。

第十六条 公司建设全员信息安全文化，面向全体员工（含劳务派遣人员）定期开展网络安全法律法规、信息安全知识与技能培训，强化全员安全意识，提升整体安全防护能力。

第四章 信息安全与网络安全事件管理

第十七条 公司建立健全信息安全与网络安全事件应急响应机制，针对不同等级安全事件制定分级应急预案，明确处置流程、责任分工与响应时限，每年至少组织一次应急演练，持续优化预案体系。

第十八条 发生信息安全与网络安全事件时，事发单位须第一时间向运营管理中心

（网络信息安全委员会办公室）上报，同步启动对应等级应急预案，采取有效措施控制事态蔓延，组织开展系统恢复与风险处置工作。

第十九条 信息安全与网络安全事件处置结束后，事发单位须对事件发生原因、处置过程、损失影响进行全面总结评估，形成复盘报告报送运营管理中心；针对事件暴露的管理与技术薄弱环节，及时完善制度、优化防护措施，并依规追究相关人员责任。

第二十条 各单位须按要求将信息安全与网络安全事件的发生、处置全过程向公司报备，不得迟报、瞒报、漏报。

第五章 审计与考核

第二十一条 公司依法落实网络安全等级保护制度，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。同时定期聘请专业第三方机构开展信息安全专项审计，覆盖信息技术治理、合规风险管理、安全管理、运维管理等全领域。

第二十二条 运营管理中心定期对各单位信息安全与网络安全工作开展考核评价，考核结果纳入公司绩效考核体系；各单位建立自查自评机制，持续完善安全管理体系。

第二十三条 公司将信息安全内部控制有效性纳入公司内控有效性评价，通过多维度监督检查强化信息科技内控水平。

第六章 附则

第二十四条 本政策自发布之日起生效；公司至少每三年或者在相关法律法规、监管要求发生重大变化时对本政策进行评估并适时修订。本政策通过公司官方网站公开。