北京新都远景网络技术有限公司

安徽益联-丰盈云人力资源服务业财一体化管理系统-信息安全管理计划

文件编号：XDYJ-06-14

编制部门：人力资源部　编制时间：2025.02.20

版　　本：V 1 . 0　　编制时间：2025.02.20

批 准 人：孙玥　　审批时间：2025.02.20

修订记录

日期	版本	变更说明	批准人
2025.02.20	V1.0	新建	孙玥

目录

1. 总则

1.1. 目的

为确保“丰盈云人力资源服务业财一体化管理系统”项目（下称“本项目”）在全生命周期（包括设计、开发、测试、部署、运维及废止）中的信息安全，保护甲方（安徽益联科技有限公司）及最终用户的业务数据、个人信息及商业秘密免受泄露、篡改、丢失及未授权访问等风险，并满足国家法律法规、监管要求及合同约定，特制定本信息安全管理计划。

1.2. 范围

本计划适用于为本项目提供服务的所有乙方（北京新都远景网络技术有限公司）人员、供应商及合作伙伴。安全管理对象涵盖本项目所涉及的所有信息系统资产，包括但不限于：应用程序、服务器、网络设备、终端、数据（含客户CRM数据、员工个人信息、财务数据等）和技术文档及管理流程。

1.3. 依据

1. 国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）等相关标准
2. 《信息安全管理制度》
3. 合同中关于服务质量、数据保密及运维服务的要求
4. 公司内部《信息安全管理程序》及相关政策

2. 安全管理目标

保密性：确保项目数据（尤其是客户信息、员工个人敏感信息、财务数据）仅在授权范围内访问。

完整性：保障项目数据、系统配置及业务逻辑的准确与完整，防止未授权篡改。

可用性：保障系统在合同约定的服务级别协议（SLA）内（7x24小时）持续稳定运行，故障恢复时间符合合同承诺（48小时内）。

可审计性：所有关键操作和安全事件均有完整、不可抵赖的记录，满足合规审计与故障追溯要求。

合规性：满足信创（信息技术应用创新）国产化适配的安全要求及国家相关法律法规。

3. 组织与职责

3.1. 信息安全领导小组

以公司副总为组长，运维相关部门担任组员组成的信息安全小组。

组长：公司副总经理

成员：运维管理部经理、研发部经理、质量效能部经理、人力资源部经理

职责：审批本安全计划，提供资源保障，决策重大安全事项，监督计划执行。

3.2. 项目实施团队安全职责

运维管理部经理/运维项目经理：作为本项目安全第一责任人，负责安全计划的落地执行、日常安全监控、应急响应协调及安全事件报告。

研发部：负责系统开发安全（安全编码、漏洞管理）、上线前的安全测试。

运维工程师：负责系统运行环境（服务器、网络、数据库）的安全配置、漏洞修复、备份恢复及安全日志监控。

服务台专员：作为安全事件接收入口，按流程进行初步判断与上报。

服务知识专员：负责安全管理文档、应急方案、漏洞知识的整理与归档。

质量效能部：负责安全审计、检查计划执行情况，组织内部审核，监督整改闭环。

4. 安全控制措施

4.1. 人员安全

背景审查：依据合同条款中人员要求，对项目核心成员进行必要的背景审查，签署保密协议。

安全培训：所有项目成员必须接受岗前信息安全培训，内容涵盖数据保护、隐私政策、安全操作规程及应急流程，年度复训。

权限最小化：根据岗位说明书和“系统管理”模块权限，实施严格的访问控制，确保用户仅拥有完成工作所必需的最小权限。

4.2. 物理与环境安全

数据中心访问受控，有门禁、监控录像。

关键设备有冗余电源和温湿度控制。

4.3. 系统开发与获取安全

安全需求：将安全性作为需求分析的一部分，特别是针对CRM、员工管理、社保、财务管理等敏感模块。

安全编码与测试：遵循安全开发规范，对代码进行安全审查。上线前进行渗透测试与漏洞扫描，修复中高危漏洞。

信创适配安全：根据合同条款要求，若需进行国产化适配，所选用的国产基础软硬件（CPU、OS、数据库等）需通过安全认证，并进行专项安全兼容性测试。

4.4. 系统运维与访问控制

网络隔离：生产环境与测试/开发环境严格隔离。

身份认证与授权：启用强密码策略，对管理后台、数据库等高权限访问启用双因素认证（2FA）。

漏洞与补丁管理：定期（每月）对系统组件、中间件、操作系统进行漏洞扫描，在评估风险后及时安装安全补丁。

安全监控：根据合同条款中“系统监控”功能要求，部署日志审计系统（SIEM），集中收集和分析应用、系统、安全设备日志，监控异常访问和攻击行为。

数据安全：

加密：敏感数据（如身份证号、银行卡号）在存储和传输过程中进行加密。

备份与恢复：根据合同条款及档案管理要求，执行定期数据备份（包括数据库和文件），并定期测试恢复流程，确保备份有效性。

数据脱敏：测试环境使用脱敏数据。

5. 安全事件管理与应急响应

5.1. 5.1 定义与分类

明确信息安全事件分类，如：数据泄露、恶意软件感染、拒绝服务攻击、越权访问等。

5.2. 5.2 响应流程

报告：任何人员发现安全事件，须立即通过服务台报告。

初步处置：运维管理部经理根据应急预案，协调技术团队进行遏制（如隔离系统、禁用账户）。

调查与根除：查明原因，清除威胁（如删除恶意软件、修补漏洞）。

恢复：从已验证的备份中恢复受影响的系统与数据。

报告与改进：编写事件报告，报质量效能部备案。进行根本原因分析（RCA），更新安全控制措施和应急预案。

时效承诺：应急响应启动时间不超过1小时，并致力于在合同约定的48小时故障排除时限内解决安全类故障。

6. 合规性与审计

6.1. 合规性检查

定期检查系统操作是否符合《个人信息保护法》关于个人信息处理的规定。

确保系统功能变更不违反安全与隐私政策。

6.2. 审计

质量效能部每季度对项目安全控制措施的执行情况进行一次内部审计，检查范围包括：权限分配、日志审计、备份恢复测试记录、漏洞修复状态等。

审计结果向信息安全领导小组汇报，并跟踪整改直至闭环。

7. 计划评审与更新

本信息安全计划每年至少评审一次，或在发生重大安全事件、法律法规变更、技术架构重大调整时立即评审更新，以确保其持续适宜性、充分性和有效性。本计划的最新版本将提交甲方备案。