信息安全风险自查报告

### 自查时间： 年 月 日

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 一、自查单位基本情况 | | | | | | |
| 单位名称 | | |  | | 组织机构代码 |  |
| 填表联系人 | | |  | | 联系方式 |  |
| 网络安全专职  工作人员 | | | ①网络安全专职工作人员总数：\_\_\_\_\_\_\_  ②网络安全兼职工作人员总数：\_\_\_\_\_\_\_ | | | |
| 二、信息系统基本情况（可提供服务合同扫描件等） | | | | | | |
| 信息系统  数量 | | ①信息系统总数（包括自行运维和委托其他单位运维的信息系统）：\_\_\_\_\_\_\_\_个，其中  面向互联网开放系统：\_\_\_\_\_\_个  生产系统（如资产管理、制造运行）：\_\_\_\_\_个  办公系统（含OA财务系统、邮件系统）：\_\_\_\_\_\_个  ②2024年度新投入运行信息系统数量：\_\_\_\_\_\_个 | | | | |
| 互联网接入 | | ①互联网接入口总数：\_\_\_\_\_\_\_\_\_\_  □接入中国联通 □接入中国电信 □接入中国移动 □其他 | | | | |
| 门户网站 | | ①主域名：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ②在用域名数量：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ③在用互联网IP地址段：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| 三、网络安全责任制落实情况 | | | | | | |
| 网络安全主管领导 | | ①负责网络安全管理工作的单位领导：□已明确 □未明确  ②主管领导：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ③职务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ④是否本单位主要负责同志：□是 □否 | | | | |
| 负责网络安全工作的内设机构 | | ①负责网络安全管理工作的内设机构：□已明确 □未明确  ②内设机构名称：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ③负责人：\_\_\_\_\_\_\_\_\_\_\_\_\_，职务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| 网络安全责任制度建设和落实情况 | | ①网络安全事件责任制度：□已建立 □未建立  ②网络安全检查责任：□已明确 □未明确  ③2024年网络安全检查专项经费：  □已落实，\_\_\_\_万 □无专项经费 | | | | |
| 四、网络安全日常管理情况 | | | | | | |
| 人员管理 | | ①重点岗位人员安全保密协议：□全部签订 □部分签订 □均未签订  ②人员离岗离职安全管理规定：□已制定 □未制定 | | | | |
| 信息资产管理 | | ①信息资产管理制度：□已建立 □未建立  ②信息资产管理执行记录：□记录完整 □记录不完整 | | | | |
| 安全建设与  运维 | | ①是否同步规划、同步建设和同步使用安全技术措施：□是 □否  ②是否对机房重要区域出入进行审批和记录：□是 □否  ③是否记录安全运维行为（包括但不限于补丁升级、漏洞扫描、日志审计、重大事件或威胁）□是 □否 | | | | |
| 日常监测 | | ①是否实时监测重要信息系统/信息资产运行状态：□是 □否  ②是否留存6个月上的重要信息系统/信息资产日志，并定期审计：□是 □否  ③是否开展网络安全威胁监测和态势分析：□已开展 □未开展  ④是否建立内部网络安全事件通报制度：□已建立 □未建立 | | | | |
| 经费保障 | | 2024年信息化总预算（含网络安全预算）：\_\_\_\_\_\_\_万元，网络安全预算：\_\_\_\_\_\_\_万元，其中采购网络安全服务比例：\_\_\_\_\_ | | | | |
| 五、网络安全防护情况 | | | | | | |
| 网络边界  安全防护 | | ①网络安全防护设备部署（可多选）：  □防火墙 □入侵检测/防御设备 □堡垒机 □VPN设备 □应用防火墙 □其它\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ②设备安全策略配置：□使用默认配置 □根据需要配置 | | | | |
| 无线网络  安全防护 | | ①是否使用无线网络：□是 □否  ②启用安全防护策略（可多选）：  □采取身份鉴别 □采取地址过滤 □未设置防护策略  ③无线路由器使用默认管理口令情况：□存在 □不存在 | | | | |
| 电子邮件  安全防护 | | ①建设方式：□自行建设 □由上级单位统一管理  □使用第三方服务邮件服务提供商  ②启用安全防护策略（可多选）： □注册邮箱审批登记 □离职后注销邮箱 □垃圾邮件过滤□邮件病毒查杀 □其它\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| 终端计算机  安全防护 | | 终端计算机管理方式：  □分散管理  □集中统一管理（可多选）  □统一身份管理 □统一补丁升级 □统一设置程序黑白名单 | | | | |
| 漏洞修复情况 | | ①漏洞检测周期：□每月 □每季度 □每年 □不进行漏洞检测  ②2024年自行发现漏洞：\_\_\_\_个，外部漏洞风险通报：\_\_\_\_个，其中已修复漏洞：\_\_\_\_个 | | | | |
| 六、网络安全应急工作情况 | | | | | | |
| 网络安全应急预案 | | □已制定：2024年修订情况：□修订 □未修订  □未制定 | | | | |
| 2024年应急预案启动次数： | | | | |
| 网络安全应急演练 | | □2024年已开展，演练次数：\_\_\_\_，其中实战演练数：\_\_\_\_；  □2024年未开展 | | | | |
| 网络安全应急技术队伍 | | □本部门所属 □外部服务机构 □无 | | | | |
| 七、网络安全教育培训情况 | | | | | | |
| 培训次数 | | 2024年开展网络安全教育培训（非保密培训）的次数：\_\_\_\_\_ | | | | |
| 培训人数 | | 2024年参加网络安全教育培训的人数：\_\_\_\_\_  占本单位总人数的比例：\_\_\_\_\_％ | | | | |
| 八、近期技术检测及网络安全事件情况 | | | | | | |
| 技术  检测  情况 | 恶意代码检测 | 近半年有无开展恶意代码检测：  □有，开展恶意代码检测的系统\_\_\_\_个，发现恶意代码\_\_\_\_个  □无  *恶意代码检测：通过检测手段发现黑客历史攻击痕迹和遗留的恶意代码文件，及时发现并查杀恶意文件，阻断黑客的进一步攻击行为。* | | | | |
| 安全漏洞检测 | 近半年有无开展安全漏洞检测：  □有，发现可利用漏洞\_\_\_\_个，已整改\_\_\_\_个  □无  *安全漏洞检测：基于漏洞数据库，通过扫描手段对指定的远程或者本地计算机系统进行安全脆弱性检测，发现可利用漏洞。* | | | | |
| 渗透测试 | 近半年有无开展渗透测试：  □有，开展渗透测试系统\_\_\_\_个。渗透测试过程中，发现高危安全问题\_\_\_\_个，已整改\_\_\_\_个；发现中危安全问题\_\_\_\_个，已整改\_\_\_\_个  □无  *渗透测试：通过模拟黑客攻击行为，从攻击者的角度发现系统存在的隐性安全漏洞和网络风险，深层次探索企业安全中的脆弱环节，提升企业安全能力建设。* | | | | |
| 网络安全  事件情况 | | 2024年，发生网络安全事件：\_\_\_\_\_\_\_\_\_次，外部主管单位通报的网络安全事件件：\_\_\_\_\_\_次。其中：勒索病毒：\_\_\_\_次，数据泄露：\_\_\_\_次，网页被篡：\_\_\_\_\_次，其他事件：\_\_\_\_次 | | | | |
| 网络安全风险评估情况 | | ①2024年是否开展网络等级保护测评工作：  □有，开展系统\_\_\_\_个 □无 ②2024年是否开展密码应用安全性评估工作： □有，开展系统\_\_\_\_个 □无 ③2024年是否开展网络安全风险评估工作： □有，开展系统\_\_\_\_个 □无 | | | | |
| 九、数据安全防护情况 | | | | | | |
| 数据安全防护情况 | | ①企业存储数据量：\_\_\_\_\_\_\_\_\_\_\_TB，  其中，用户隐私数据\_\_\_\_\_\_TB，企业生产经营数据\_\_\_\_\_\_TB  ②是否形成企业统一的数据资源台账：  □台账管理工具：\_\_\_\_\_\_\_\_\_\_\_\_ □否  ③是否定期更新数据资源台账：  □更新频率：\_\_\_\_\_\_\_\_\_ □否  ④是否制定数据分类分级的操作指南，内容包括分类分级流程设计、分类分级方法、分类分级规则等：  □是，文件名称为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  □否  ⑤是否形成数据分类清单和重要数据、核心数据目录：  □是，重要数据数量\_\_\_\_\_\_\_TB，核心数据数量\_\_\_\_\_\_\_TB  □否  ⑥是否对数据分类分级工作进行动态更新：  □是，每年一次 □是，每季度一次 □否 □其他，\_\_\_\_\_\_\_\_\_\_\_  ⑦采取数据安全保护措施（多选）：  □存储加密 □传输加密 □数据脱敏 □数据备份  □数字水印 □其它\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ⑧是否开展数据安全风险自查，内容包括：（可多选）  □数据库账号管理 □数据备份 □数据审计 □接口测试  □其他：\_\_\_\_\_\_\_\_\_\_\_  □否 | | | | |
| 十、信息技术外包服务机构情况（包括参与技术检测的外部专业机构，多个单位可以自行增加；可提供服务合同扫描件等） | | | | | | |
| 外包服务机构1 | | 机构名称 | |  | | |
| 服务内容 | | □系统集成 □系统运维 □风险评估  □安全检测 □安全加固 □应急支持  □数据存储 □数据分析 □灾难备份  □安全监测 □流量清洗 □其他 | | |
| 保密协议 | | □已签订 □未签订 | | |
| 十一、互联网敏感信息自查情况（包括真实IP、开放端口、证书信息、whois信息、源代码、网络架构图、网络拓扑图、邮箱、密码、通讯录等暴露在互联网上的内部敏感信息）（可另附页） | | | | | | |
| 自查情况 | | 敏感信息类型 | | 相关链接与简要描述 | | |
|  | 源代码泄露 | https://www.xxx.com/xxx/xx疑似本单位xx系统源代码托管在互联网代码平台，通过该系统反查xx公司承接开发工作，所涉及人员x名，目前处置情况xx... | | | | |
| ... | ... | | | | |

说明：

1.评审环节会结合各申报单位自查报告进行评审，请各申报单位重视信息安全风险自查工作，如实填写自查报告。

2.申报数字化示范工厂的单位至少应满足信息安全风险自查表第一至第六点内容对应防护要求，并在评审环节提供相应证明材料供专家组审阅。