等保二级管理制度&建设&运维资料

1. 制度类
2. 提供网络安全工作总体方针和安全策略，阐明机构工作安全总体目标、原则、范围、安全框架等
3. 提供安全管理制度制定和发布管理文档，说明制度发布的流程（制定、发布程序、发布范围、论证审定、修订）、格式要求、版本编号等内容
4. 提供岗位职责文件、部门职责文件、人员配备文档（安全主管、安全管理员<不可兼任系统运维工作>、数据库管理员、审计员、系统管理员、机房管理员、应用管理员等）
5. 提供审批管理制度（系统接入、系统变更、物理访问、其他系统管理涉及到的需审批事项），对提出申请-上报-审批-批准的详细流程规定性文档
6. 提供人员安全管理文档，明确录用人员资格审查（身份、安全背景、专业资格或资质）等内容
7. 提供人员离岗（离岗人员物品、工作资料、身份证明、离岗保密责任）管理制度
8. 提供安全意识教育与岗位技能培训文档，内容涉及培训周期、培训方式、培训内容、考核方式等
9. 提供安全责任和惩戒措施文档，内容涉及人员所需承担的责任和违反相关规定所进行的不同程度的惩处
10. 外部人员访问管理文档，对外部人员可访问区域、受控区域访问的申请审批、接触资料信息等进行保密等内容进行规定
11. 工程实施制度，规定单位内系统建设时的具体实施流程、人员行为准则等内容
12. 供应商监督、评审、考核管理制度，规定考核标准、考核方式、考核内容等
13. 提供机房安全管理制度（物理访问、物品进出入、管理、维护、巡检等内容）
14. 提供办公环境保密性管理制度（人员离开座位退出电脑登录界面且锁定界面、不在桌面放置敏感文件等）
15. 提供介质管理制度，对介质的使用、存储、管理、物理传输过程中的人员选择、打包、交付等进行规定
16. 配套设施、软硬件维护方面的管理制度，对设施设备负责维护的人员职责、维修服务的申请审批、维护维修过程的监督控制、设备带出维修的数据清除或加密、带有存储介质的设备的报废或重用前的数据擦除等内容进行规定
17. 网络和系统安全管理制度，对安全策略、账户管理（远程运维账户开通审批、管理、监控）、配置管理（配置变更申请、审批、更改后的配置库更新等）、日志管理（日志审计策略的开启、保存时间、定期分析）、日常操作（运维工具使用申请授权、外部系统接入、内部系统外联等的审批和监控）、升级与打补丁、口令更新等进行规定
18. 恶意代码防范管理制度（设备接入前的恶意代码检测、定期的病毒查杀、防恶意代码软件的使用、定期分析汇报等）
19. 提供密码管理制度（管理员、用户密码长度、复杂度、更换周期、更换需进行记录等）
20. 变更管理制度（变更前的申请审批、方案制定、方案论证审批、执行、变更过程记录、中止变更并从失败中恢复的程序等）
21. 备份与恢复管理制度和策略文档（备份信息的备份方式、备份频度、备份介质、存储时间、数据备份文件命名规则、定期恢复验证等）
22. 安全事件报告和处置管理制度（不同<至少包括造成系统中断和信息泄露方面>安全事件的报告相应流程、安全事件的现场处理、事后报告、恢复总结、相关人员职责等）
23. 应急预案框架（启动应急预案条件、应急组织构成、应急资源保障、事后教育和培训等）
24. 应急预案（机房供电线路故障、空调故障、消防系统故障、人为破坏、系统中断、病毒感染、黑客攻击等方面的具体应急处置处理流程）
25. 记录类&报告类
26. 机房建设、验收文档（针对防雷、抗震、电力通信线缆布放、建筑材料耐火程度等方面）
27. 提供系统维护手册和系统操作手册（包括机房ups、空调、消防、网络设备、安全设备、服务器、应用系统、数据库等）
28. 提供安全管理制度收发登记记录（网上发布流程，需要实际查看，纸质印发则需提供收发文登记记录）
29. 提供安全管理制度定期修订和评审记录（至少每年对信息安全体系整体进行修订一次，内容涉及不适用、修改、废除、新增等方面）
30. 审批事项更新记录（至少每年对内部审批事项、审批部门、审批人进行一次排查，有变化时更新并记录）
31. 提供内部网络安全信息会议记录（部门内和部门间的信息安全会议，主要涉及会议内容、会议时间、地点、参与人员、讨论结果等）
32. 提供与网络安全职能部门、各类供应商、业界专家、安全组织的沟通合作记录（如会议记录、服务工单、培训记录、考核记录等）
33. 提供系统日常运行（系统运行日志有无异常、设备CPU占用比、内存使用率、）、系统漏洞（定期杀毒、漏洞扫描）、系统备份（备份方式、备份介质、存储数据、保管人、检查人等）检查记录
34. 与录用人员签署的保密协议，内容涉及保密内容、保密期限、违约责任、人员签字等
35. 培训计划：针对不同岗位制定的不同的培训计划和适用所有人员培训计划，培训内容涉及基础安全知识、具体岗位操作等方面
36. 培训记录（培训时间、内容、参与人员、培训结果）
37. 人员进出入受控区域（物理机房、办公环境、其他受控区域）的审批和登记记录
38. 外部人员接入受控网络访问系统前的申请、审批、登记备案、离场权限清除规定性文档
39. 外部人员接入受控网络访问系统前的书面申请审批记录和开设账户登记备案记录
40. 外部人员离场后的权限清除记录
41. 提供系统建设的整体安全规划和安全设计方案（密码技术或应用）
42. 对系统整体安全规划和安全设计方案的合理性和适用性进行论证审定的记录
43. 系统中使用到的安全产品采购证明和合格证明（国家规定销售产品）
44. （若使用到则提供）密码产品和服务的合格证明（国家密码管理主管部门备案允许销售的产品）
45. 产品采购前的选型测试记录，定期对产品采购名单进行更新的记录
46. 自行软件开发：
47. 实际开发环境和运行环境是否物理隔离
48. 软件安装之前的安全检测（恶意代码检测和源代码审计报告）
49. 开发人员处于受控环境（接受相关人员和部门的监督和检查）
50. 外包软件开发
51. 软件交付前的恶意代码检测记录
52. 开发单位提供的软件设计文档和使用指南
53. 提供工程实施方案，内容涉及系统建设的时间限制、进度控制、质量控制
54. 系统建设的阶段性工程文档（实施方和内部管理人员提供的工作周报、月报、阶段性测试验收记录等）
55. 提供工程测试验收方案（参与测试验收的部门、人员、测试依据、测试内容、测试具体安排）
56. 测试验收报告（测试内容、测试结果、测试参与部门或人员的盖章和签字）
57. 系统正式上线前的安全性测试验收记录（针对系统密码技术和密码应用方面）
58. 系统交付清单（系统所涉及到的软件、硬件、软件开发、使用说明、运维手册等）
59. 开发单位对内部运维人员进行培训的培训记录（若由开发单位负责运维则需提供开发单位对内部使用人员进行培训的培训记录）
60. 在系统发生重大变更或级别变化时的等级保护测评报告（若未发生过则无需提供）
61. 提供机房巡检（UPS、空调、线路、供电设备、消防设备、监控设备、网络设备、安全设备、服务器、数据库）记录
62. 物品带出受控区域申请审批记录
63. 资产清单（资产名称、所处位置、重要程度、责任人、责任部门等）
64. 介质归档、使用、查询登记记录（若目前不涉及相关工作则提供未登记的表格即可）
65. 漏洞扫描或渗透测试报告（详细记录扫描设备、应用的基本信息）
66. 对漏扫和渗透中发现的问题进行整改的整改记录
67. 管理员角色和权限划分表
68. 系统账户管理流程和各环节中的记录（账户申请、审批、增加、修改、删除等）
69. 运维操作日志（巡检记录、参数设置、修改等方面）
70. 日志、监控记录定期分析审计报告
71. 各设备和应用的恶意代码检测记录、恶意代码库升级记录和分析报告
72. 数据、业务信息、配置（网络拓扑、安装软件组件、软件版本和补丁、各设备参数信息等）备份记录
73. 密码更换记录
74. 变更方案（变更原因、类型、过程）和变更方案审批记录
75. 安全事件报告记录（原因、证据、现场处理、补救措施、经验教训等，若未发生过安全事件则提供记录表格即可）
76. 定期的应急预案演练记录（时间、演练操作内容、演练结果等）、培训记录（培训对象、培训内容、培训结果等）
77. 定期对应急预案进行修订的修订记录
78. 合同类
79. 提供设备供应商、等级测评机构签订的服务合同或安全责任书
80. 提供外包（系统运维、设备运维、安全服务等）运维服务商合同或协议（运维范围、工作内容、等级保护服务能力、安全责任）