陕西省交通运输厅

网络安全管理细则

（暂行）

2019年1月

陕西省交通运输厅

**目录**

[第一章 总则 1](#_Toc533584881)

[第二章 人员安全管理 1](#_Toc533584882)

[第一节 网络安全岗位职责 1](#_Toc533584883)

[第二节 沟通与合作 2](#_Toc533584884)

[第三节 人员录用和培训 2](#_Toc533584885)

[第四节 转岗离职管理 3](#_Toc533584886)

[第五节 第三方外包人员安全管理 4](#_Toc533584887)

[第三章 系统建设安全管理 5](#_Toc533584888)

[第一节 系统定级 5](#_Toc533584889)

[第二节 安全方案设计 5](#_Toc533584890)

[第三节 网络安全产品的采购和使用 6](#_Toc533584891)

[第四节 开发安全管理 6](#_Toc533584892)

[第五节 工程实施管理 7](#_Toc533584893)

[第六节 测试、发布管理要求 7](#_Toc533584894)

[第七节 系统交付管理 8](#_Toc533584895)

[第八节 等级测评管理 8](#_Toc533584896)

[第九节 安全服务商的选择 9](#_Toc533584897)

[第四章 系统安全运维管理 9](#_Toc533584898)

[第一节 机房安全管理 9](#_Toc533584899)

[第二节 资产安全管理 10](#_Toc533584900)

[第三节 介质安全管理 12](#_Toc533584901)

[第四节 设备安全管理 12](#_Toc533584902)

[第五节 安全监控管理 13](#_Toc533584903)

[第六节 网络环境管理 14](#_Toc533584904)

[第七节 系统安全管理 14](#_Toc533584905)

[第八节 系统变更管理 16](#_Toc533584906)

[第九节 备份与恢复安全管理 16](#_Toc533584907)

[第十节 网站安全防护管理 17](#_Toc533584908)

[第十一节 电子邮件安全管理 17](#_Toc533584909)

[第十二节 防病毒安全管理 18](#_Toc533584910)

[第十三节 网络安全事件管理 18](#_Toc533584911)

[第五章 附则 19](#_Toc533584912)

## **总则**

1. 为规范陕西省交通运输厅网络安全管理，保障信息系统安全、稳定、高效运行，依据《中华人民共和国网络安全法》、《信息安全技术信息系统安全等级保护基本要求》（GB/T 22239-2008）、《陕西省交通运输厅网络安全管理办法（试行）》及网络安全管理相关规定，结合省交通运输信息化运行实际情况，制定本细则。
2. 本细则对省交通运输厅厅直各单位网络安全管理工作提出详细管理措施，各单位应按照本细则要求执行。
3. 各单位应根据实际情况，制定包括网络安全管理部门和人员管理、系统建设安全管理、系统安全运维管理等内容的网络安全管理制度，强化网络安全管理。

## **人员安全管理**

### 第一节 网络安全岗位设置

1. 各单位应配备系统管理员，负责服务器、操作系统、应用系统、网络设备、安全设备的日常管理和维护；应配备安全管理员，定期进行安全检查，及时向本单位网络安全管理部门汇报网络安全状况及重大安全事件；应配备审计管理员，负责网络、系统、应用安全等操作行为的安全审计。

### 第二节 沟通与合作

1. 厅直各单位网络安全管理部门应定期召开工作例会，指导网络安全策略和制度在本单位的实施，推进各项网络安全工作的落实，对工作过程中的问题进行探讨解决。
2. 各单位应建立沟通与合作机制：
3. 建立与相关政府职能部门的沟通机制，及时获取网络安全信息。
4. 接受专业网络安全技术服务商的安全漏洞和网络攻击网络警告、建议和补丁，分享和交换新技术、产品、威胁或脆弱性信息，及时加固信息系统，有效抵抗网络安全威胁。
5. 与外部网络安全专家组保持联系，以获取安全建议、咨询支持及接受培训。

### 第三节 人员录用和培训

1. 网络安全人员的录用按照本单位人事部门的管理规定执行，人员应明确安全职责，并签署安全协议。从事关键岗位的人员应签署岗位保密协议。
2. 各单位应对新入职人员进行网络安全管理及规章制度等宣贯，针对新入职的网络安全管理人员还应进行专业理论与操作培训，形成培训记录，并进行考核。
3. 各单位根据各岗位工作和发展需要制定网络安全培训计划，并对培训教师、培训对象进行资格审定。
4. 各单位参应根据上级单位安排或本单位需求，由本单位网络安全管理部门审批，委派相关人员参加外部机构的网络安全培训。
5. 各单位网络安全管理部门应对网络安全管理人员定期进行考核，考核内容包括安全知识、安全技能、操作行为等。

### 第四节 转岗离职管理

1. 各单位网络安全人员可根据需要，向主管领导提出人员岗位转岗申请，由业务部门考核通过后，经主管领导批准，报人事部门，并通知系统管理员修改岗位调整人员的安全访问权限。
2. 各单位应对网络安全管理离职人员做好以下事项：
3. 立即终止离职人员的所有资源访问权限。
4. 及时收回各种相关证件（门禁卡等）、保密文件、钥匙、软硬件设备等。
5. 网络安全管理人员离职按照各单位人事部门相关规定执行离职流程。

### 第五节 第三方外包人员安全管理

1. 各单位应对第三方外包服务提供商的技术能力、经营管理能力和发展能力等资质进行审查。
2. 对外包服务商的选择应满足业务需要，明确责任范围及服务目标，评估外包服务网络安全风险，并声明相关网络安全责任与义务。
3. 第三方外包人员（如向系统提供服务的软、硬件维护人员，业务合作伙伴、评估人员等）应在访问各单位资源前取得相关授权，并签署保密承诺书（协议）。
4. 第三方人员对重要区域（如访问主机房、重要服务器或设备、保密文档等）的访问，应提出书面申请，经网络安全管理部门批准后由专人全程陪同或监督，并记录备案（记录第三方人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息）。
5. 各单位应对外包服务提供商提供的各项服务目标的执行情况进行监督，形成外包服务工作报告机制。
6. 各单位应制定外包服务商服务审核和评价指标，定期召开外包服务工作评审会议，对外包服务商提交的服务报告进行评审，评审内容包括安全事件、操作问题等处置情况，并形成外包服务商评价报告。

## **系统建设安全管理**

### 第一节 系统定级

1. 各单位应依据国家网络安全等级保护相关制度和《信息安全技术网络安全等级保护定级指南》（GA/T 1389-2017），确定本单位信息系统的安全保护等级,并依据网络安全等级保护定级流程，开展定级工作。
2. 新建系统定级应分析系统覆盖的业务范围，结合对业务发展趋势的预测，在工程可行性研究阶段以专家评审的方式确定安全保护等级。
3. 改建、扩建系统定级应根据改建、扩建后的系统服务范围、业务信息和系统服务需求等方面的变化情况，综合评定系统安全需求，确定是否变更安全保护等级。
4. 应撰写书面定级报告，组织相关部门和安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定后，报公安部门备案，备案完成后10日内将备案结果报厅网信办。

### 第二节 安全方案设计

1. 新建信息系统可行性研究报告报审前，应采取专家评审的方式确定安全保护等级，并严格按照所定级别设计安全建设方案。安全设计方案编写应在本单位网络安全管理部门和业务使用部门的参与下完成。安全方案设计应根据等级划分情况，统一考虑网络安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。
2. 各单位应组织相关业务部门和安全技术专家对安全方案进行论证，对安全保护等级第三级及以上系统的安全设计方案进行专项评审。

### 第三节 网络安全产品的采购和使用

1. 各单位的网络安全产品、密码产品的采购原则上应使用国产产品，网络安全产品的使用应符合国家的有关规定，密码产品的使用应符合国家密码主管部门的要求。
2. 各单位重要信息系统应采用省厅密钥管理与安全认证中心的密钥身份认证系统所提供密钥及身份认证服务。
3. 对于信息系统的信息化产品采购遵照国家招投标法采购流程执行，明确提出产品参数。

### 第四节 开发安全管理

1. 各单位组织开展信息系统软件外包开发时，应与软件开发单位签订协议（如软件开发协议和软件开发安全协议、保密协议），明确知识产权的归属和安全、保密方面的要求，明确软件开发单位的责任、规范开发过程中的安全行为、确保开发环境要求、软件质量要求、明确开发后的服务承诺等内容。
2. 各单位应对软件开发过程进行监督，在软件安装之前应组织第三方机构开展软件安全测评工作，并提供检测报告。

### 第五节 工程实施管理

1. 系统建设过程中，各单位网络安全管理部门应对系统建设实施工作进行监督管理。
2. 在工程实施阶段，应与工程实施单位签订安全相关协议，约束工程实施单位的工程实施行为，并明确工程实施过程的控制方法（如内部阶段性控制或外部监理单位控制）和规范实施参与人员的各种行为准则。

### 第六节 测试、发布管理要求

1. 各单位应建立系统测试环境，用于生产环境发布前进行的集成测试。完成集成测试之后，应及时清除所有测试数据。
2. 系统测试时应由专人负责系统测试管理，对测试过程（包括测试前、测试中和测试后）提出文档化要求，并按照安全管理要求完成系统测试工作。
3. 系统发布前应委托第三方测试机构根据设计方案或合同要求，对信息系统进行独立的安全性测试。
4. 系统验收时应根据安全设计方案或合同要求制订安全验收方案，详细记录验收结果，形成验收报告，并组织对系统安全验收报告进行审定。

### 第七节 系统交付管理

1. 各单位应制定系统交付安全管理制度，系统建设单位应提供详细的交付清单，系统接收单位根据交付清单对所交接的设备、软件和文档等进行清点。
2. 系统建设单位应提交系统建设过程中的文档（如系统建设方案）和指导用户进行系统运行维护的文档（如服务器操作规程书）以及系统培训手册等文档。
3. 系统建设单位应签署服务承诺书，保障系统运行维护，并对系统运维技术人员进行培训。

### 第八节 等级测评管理

1. 各单位网络安全管理部门负责本单位信息系统等级测评的管理工作，应选择具有国家相关技术资质和安全资质的测评单位对所属信息系统进行等级测评，测评单位应出具公安部门认可的测评报告。
2. 新建信息系统应在试运行期间完成等级测评，安全保护等级第三级系统应按规定每年至少开展一次等级测评，并依据测评结果完成系统整改工作。
3. 当系统发生重大变更时，应对系统重新进行等级测评；若系统安全保护级别发生变化，应及时调整备案级别并完成相应整改工作，使其满足等级保护要求。各单位应根据测评结果，对发现的问题进行安全整改，并通过测评。

### 第九节 安全服务商的选择

1. 各单位应按照国家有关规定选择安全服务商，并与选定的安全服务商签订安全协议，明确约定的安全责任。

## **系统安全运维管理**

### 第一节 机房安全管理

1. 各单位应指定专人定期对机房供配电、空调、温湿度控制等设施进行维护管理，定期对基础设施进行检查，并形成检查记录，发现设备故障应及时组织人员进行维修。
2. 各单位应监测机房环境参数、重要节点连通情况和各业务系统运行状况，出现异常情况时，及时上报并组织力量排查处置。
3. 各单位应建立机房进出管理机制，并对人员和设备的进出情况形成记录，未经授权，禁止人员和设备进出机房。
4. 各单位应加强机房的日常防火管理，保证机房配备的气体灭火系统、火灾探测器和喷淋系统等灭火设施。机房及周边区域严禁烟火，禁止明火作业。机房设备应标识固定的标签注明责任部门、重要程度等信息。机房设备专机专用，不得自行配置或更换。

### 第二节 资产安全管理

1. 各单位应对信息化资产进行分类管理，明确资产责任部门，形成信息化资产清单，内容包含资产名称、资产所属系统、资产厂商、资产责任部门、资产用途、保修期限等。
2. 信息化资产分类标准如下：

|  |  |  |
| --- | --- | --- |
| **资产大类** | **资产细类** | **对应信息系统** |
| **系统硬件** | 服务器  存储设备  负载均衡设备  新风机  视频监控系统  环境监控系统  配电柜  精密空调  机房专用UPS电源  … | 主机系统、存储系统、备份系统、机房专用设备等 |
| **网络、安全设备** | 交换机  路由器  光端机  集线器  防火墙  入侵检测和防护设备  网络审计设备  负载均衡设备  防病毒设备  漏洞扫描设备  防篡改设备  网络设备组件  网络接入设备  … | 网络系统、安全系统 |
| **操作系统软件** | 操作系统软件  中间件软件  其他系统软件 | 主机系统 |
| **应用系统软件** | 自行开发的应用软件  外购的商品化应用软件  外购终端软件 | 应用系统 |
| **数据库系统软件** | 开发的数据库  外购的数据库  备份软件 | 数据库系统 |
| **信息和数据** | 各类信息和数据 | 各类信息和数据 |

1. 依据《GB/T 20984-2007信息安全风险评估规范》，资产的价值分为1～5个等级，等级越大，资产的价值越高；资产的价值评定依据描述如下：
2. 1级（很低）：对其承载的业务系统基本上没有或仅有极小的影响或损害。
3. 2级（低）：对其承载的业务系统带来一定的损失或破坏。
4. 3级（中等）：对其承载的业务系统带来严重的损失或破坏。
5. 4级（高）：对其承载的业务系统带来极其严重的损失或破坏。
6. 5级（很高）：对其承载的业务系统带来灾难性的损失或破坏。各单位应编订资产的命名规范，按照该命名规范制作信息化资产标签。资产标签应包括如下内容：名称、型号、位置、所属系统、购置日期等。
7. 各单位应每年组织一次信息化资产核查。在资产核查时，根据信息化资产清单对相关资产进行逐一核对。针对核心资产重点管理，增加核查次数，扩大核查规模。
8. 各单位应建立备品备件管理机制，对备品备件的采购计划、更换流程、使用等进行安全管理。

### 第三节 介质安全管理

1. 介质分为一般介质和可移动介质，一般介质包括文件档案、计算机硬盘等，可移动介质是指U盘、移动硬盘、存储卡、光盘、磁带等。
2. 对于存储敏感信息的介质，应委派专人对其进行标识、登记管理，介质的使用需形成使用记录。介质的处置（销毁、再利用）应与其存储信息的敏感程度相一致。

### 第四节 设备安全管理

1. 网络安全产品的采购和使用应符合国家的有关规定，并要求设备供货方提供营业执照、产品的版权或专利证书，计算机信息系统安全专用产品销售许可证等相关材料。
2. 各单位对将要投入使用的设备，应规定安装软件，配置网络及安全策略，形成配置记录，配置完后要进行安全性检查，并更新《资产清单》。
3. 各单位应要求设备供应商提供设备操作使用说明，并指导运维人员使用。
4. 各单位应指定专人对设备进行维护，形成维护记录，必要时，请服务商提供技术支持。
5. 各单位对更新、维护后的设备功能进行测试，保证维护之后的设备能正常使用。
6. 若设备无法满足安全管理要求，设备责任部门可提出设备报废申请，按有关规定审批后，进入设备报废处理流程。
7. 各单位在设备报废前对设备中的数据进行审核，删除所有数据；删除前，应做好数据备份。设备完成报废后，更新《资产清单》。

### 第五节 安全监控管理

1. 各单位应对网络设备、主机和应用软件的运行情况、网络流量、用户行为等进行监测，形成监测记录。各单位定期对监测记录进行分析，并形成分析报告，对发现的安全问题采取必要的应对措施。
2. 各单位应制定网络设备、安全设备、主机、应用软件巡检机制，形成巡检记录。

### 第六节 网络环境管理

1. 各单位应指定专人对网络进行管理，并对所有接入网络的设备进行统一安全管理，通过网络监测、安全审计、病毒防范、网络与安全设备配置管理、身份鉴别与访问控制等措施，确保网络、应用、数据安全。
2. 各单位应组织对网络及安全设备进行巡检，检查各种网络及安全设备的运行日志，形成巡检记录。
3. 各单位应定期对网络及安全设备进行升级和更新，定期对网络系统进行漏洞扫描，发现漏洞及时修补。
4. 网络规划及建设中涉及网络安全的资料，以及重要网络通信硬件设施、网管应用软件设施及网络参数配置应定期进行备份，统一管理。
5. 外部人员因业务需要，开通网络访问控制端口等参数的操作，应由各单位授权审批后，方可接入网络。
6. 交通行业专网的安全管理按照专网运行管理办法执行。

### 第七节 系统安全管理

1. 各单位根据系统的访问控制策略，对操作系统的登录程序加以控制，并定期对主机进行安全检测、漏洞扫描，形成报告。
2. 各单位应定期对服务器进行补丁更新。在补丁更新前，应对系统数据进行备份；补丁安装完成，应重新启动操作系统，测试操作系统运行是否正常，测试信息系统程序运行是否正常，若出现运行异常情况，应立即卸载安装的补丁程序，恢复系统正常运行状态，系统补丁更新成功后，将已安装补丁程序的列表、补丁更新时间等操作内容进行记录、备案。
3. 各单位应对口令实施分级管理，依据系统应用的安全级别，确定相应的口令强度、更新频率及管控方式。
4. 各单位应将服务器口令的保管人员进行备案，泄露口令者，要追究有关人员责任。
5. 因来访人员需要而临时开通的帐户，要分配最小使用权限，在使用完毕后，应及时删除该帐号，并形成日志记录；工作人员离职时，管理员要及时更换其掌管的口令，或者注销相关帐户。
6. 各单位应定期检查帐户及口令的使用情况，如发现帐户已不再使用，或者口令超出了生存期限，应及时通知相关管理员注销该帐户或更换过期口令。
7. 各单位网络和信息系统的废止，应由业务部门以书面形式向运行单位提出数据、资料等处理要求，并将废止情况报网络安全管理部门备案。

### 第八节 系统变更管理

1. 各单位系统变更时，应提出变更申请，制定变更方案，并对方案进行评审，审批通过后，方可实施变更。变更正式实施前需在测试环境中进行测试，并出具测试报告，保证实施的系统变更不会对现有应用造成严重影响。
2. 为保证变更的有效性和安全性，在变更实施前应进行安全测试，并制定回退方案。
3. 各单位在系统变更后，应对变更进行测试与验收，并记录测试与验收的结果。

### 第九节 备份与恢复安全管理

1. 各单位应对重要数据和系统进行备份，明确备份周期、备份方式等，对业务影响较大的关键数据要进行异地备份。
2. 各单位应定期对备份数据进行抽样检查与测试，进行备份数据恢复测试。恢复程序应定期运行，并达到预期效果。
3. 各单位发现业务系统的数据有损坏或丢失，应制订数据恢复方案，分析数据恢复操作对业务系统的影响和可能出现的问题，经审批后，实施数据恢复，并形成数据恢复记录。

### 第十节 网站安全防护管理

1. 各单位应建立以网页防篡改、域名控制、域名防劫持以及防攻击、防瘫痪、防挂马为主的防护体系，严格划分安全区域，严格设置访问控制策略，建立安全访问路径。
2. 各单位应对后台发布账号进行权限管理，按照系统管理员、操作管理员、安全审计员三员分立原则，对后台账号进行安全管理，定期对后台账号的操作行为进行审计，形成记录。
3. 信息发布时应对所发布的信息内容进行审核，加强管理，确保发布信息准确、真实，符合国家有关的各项法律法规制度，不得有危害国家安全、泄露国家秘密，侵犯国家的、社会的、集体的利益和公民的合法权益的内容出现。

### 第十一节 电子邮件安全管理

1. 各单位应按照网络安全等级保护制度的要求，督促落实电子邮件系统的定级备案工作，并对达到等级保护三级的邮件系统每年至少一次进行等级测评和安全整改，制定和完善应急响应预案，定期开展应急演练工作。
2. 各单位应定期组织清理电子邮件系统帐号，并对清理账号进行记录。各单位应对电子邮件系统设置口令强度及复杂度，并对使用人员设置口令更换周期。
3. 互联网电子邮件系统应具备防钓鱼、防窃密、防病毒、反垃圾、内容过滤、安全审计等关键安全保护措施。

### 第十二节 防病毒安全管理

1. 各单位应指定专人负责防病毒软件的升级、维护，以及对病毒事件的处理。及时更新病毒库和补丁，形成记录文件，对截获的危险病毒或恶意代码及时进行分析处理，并形成书面报告。
2. 各单位工作人员应认真学习计算机病毒防治的知识和技能，加强防范意识，自觉遵守有关计算机病毒防治规定。
3. 各单位应定期对各类终端进行全盘查杀病毒（每周至少检查一次）。当发现不可清除的病毒或异常情况时，应及时报告主管领导。
4. 各单位应在外部计算机接入网络前，对计算机进行病毒查杀。

### 第十三节 网络安全事件管理

1. 各单位应落实网络安全管理部门作为网络安全突发事件应急工作协调机构，按照《陕西省交通运输厅网络安全事件应急预案（试行）》相关规定，明确网络安全事件的分级分类以及产生的影响，并根据不同安全事件制定不同的报告和响应处置流程，确定事件响应和处置的范围、程度，以及处理方法等。
2. 各单位应在安全事件报告和响应处置过程中，分析和鉴定事件产生的原因，收集证据，记录处置过程，总结经验教训，制定防止再次发生的补救措施，形成记录文件。
3. 各单位应定期组织网络安全应急演练，模拟处置影响较大的网络安全事件，检验预案的可执行性，提高全员网络安全意识和应急处置能力。

## **附则**

1. 网络安全相关术语解释

1.网络，是指由计算机或者其他信息终端及相关设备组成的按照一定规则和程序对信息进行收集、存储、传输、交换、处理的系统。

2.网络安全，是指网络空间的安全，通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.网络安全事件，是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为：信息内容安全事件、信息窃取事件、网络服务异常事件、有害程序事件、信息破坏事件、设备设施故障事件、灾害性事件和其他网络安全事件。

4.个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

5．安全审计，是计算机网络安全审计的简称，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。代码安全审计是检查[源代码](https://baike.so.com/doc/5395725-7589481.html" \t "_blank)中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方。日志审计是记录与审查用户操作计算机及网络系统活动的过程，从而发现系统漏洞、入侵行为，是提高系统安全性的重要举措。

1. 本细则由厅网信办负责解释、修订。