陕西省交通运输厅

网络安全事件应急预案
（暂行）

2019年1月

陕西省交通运输厅

目 录

**[1 总则](#_Toc534206970)** [- 1 -](#_Toc534206970)

[1.1 编制目的及依据 - 1 -](#_Toc534206971)

[1.2 适用范围 - 1 -](#_Toc534206972)

[1.3 事件分级 - 1 -](#_Toc534206973)

[1.4 工作原则 - 3 -](#_Toc534206974)

**[2 组织机构与职责](#_Toc534206975)** [- 4 -](#_Toc534206975)

[2.1 领导机构及职责 - 4 -](#_Toc534206976)

[2.2 办事机构与职责 - 5 -](#_Toc534206977)

[2.2.1 厅网信办职责 - 5 -](#_Toc534206978)

[2.2.2 省交通运行监测中心职责 - 5 -](#_Toc534206979)

[2.3 厅直单位职责 - 6 -](#_Toc534206980)

**[3 监测预警](#_Toc534206981)** [- 6 -](#_Toc534206981)

[3.1 安全监测 - 6 -](#_Toc534206982)

[3.2 预警研判及发布 - 6 -](#_Toc534206983)

[3.3 预警响应 - 7 -](#_Toc534206984)

[3.3.1 I级预警响应（红色预警） - 7 -](#_Toc534206985)

[3.3.2 II级预警响应（橙色预警） - 8 -](#_Toc534206986)

[3.3.3 III级预警响应（黄色预警） - 9 -](#_Toc534206987)

[3.3.4 IV级预警响应（蓝色预警） - 9 -](#_Toc534206988)

[3.3.5 预警解除 - 9 -](#_Toc534206989)

**[4 应急处置](#_Toc534206990)** [- 10 -](#_Toc534206990)

[4.1 事件报告 - 10 -](#_Toc534206991)

[4.2 初步处置 - 10 -](#_Toc534206992)

[4.3 应急响应 - 11 -](#_Toc534206993)

[4.3.1 I级和II级响应 - 11 -](#_Toc534206994)

[4.3.2 III级响应 - 11 -](#_Toc534206995)

[4.3.3 IV级应急响应 - 13 -](#_Toc534206996)

[4.4 应急结束 - 13 -](#_Toc534206997)

[4.5 调查和评估 - 13 -](#_Toc534206998)

**[5 预防工作及应急准备](#_Toc534206999)** [- 14 -](#_Toc534206999)

[5.1 日常管理 - 14 -](#_Toc534207000)

[5.2 技术条件准备 - 14 -](#_Toc534207001)

[5.3 应急演练 - 14 -](#_Toc534207002)

[5.4 技术培训 - 14 -](#_Toc534207003)

[5.5 重要敏感时期的预防措施 - 15 -](#_Toc534207004)

**[6 保障措施](#_Toc534207005)** [- 15 -](#_Toc534207005)

[6.1 技术支持保障 - 15 -](#_Toc534207006)

[6.2 专家队伍保障 - 15 -](#_Toc534207007)

[6.3 经费保障 - 16 -](#_Toc534207008)

[6.4 责任与奖惩 - 16 -](#_Toc534207009)

**[7 附则](#_Toc534207010)** [- 16 -](#_Toc534207010)

**[8 附件](#_Toc534207011)** [- 17 -](#_Toc534207011)

[附件1：事件分类及典型事件 - 18 -](#_Toc534207012)

[附件2：网络安全事件处置流程图 - 20 -](#_Toc534207013)

[附件3：应急处置工作联络表 - 21 -](#_Toc534207014)

[附件4：网络安全事件应急技术条件准备内容 - 22 -](#_Toc534207015)

# **1 总则**

## 1.1 编制目的及依据

为建立健全陕西省交通运输厅网络安全事件应急工作机制，规范应急工作流程，提高应急处置精细化专业化水平，增强应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，依据《中华人民共和国网络安全法》、《国家网络安全事件应急预案》、《交通运输部网络安全事件应急预案》、《陕西省网络安全事件应急预案》等法规和政策，制定本应急预案。

## 1.2 适用范围

本预案适用于陕西省交通运输厅厅机关及厅直各单位主管和运行维护的，涉及行业管理及服务的国家关键信息基础设施、重要业务应用系统及基础网络运行环境发生网络安全事件的应急处置工作。

## 1.3 事件分级

网络安全事件（分类见附件1）分为四级: 特别重大（I级）、重大（II级）、较大（III级）、一般（IV级）。

### 1.3.1 符合下列情形之一的，为特别重大网络安全事件（I级）：

（1）重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

（2）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

（3）其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

### 1.3.2 符合下列情形之一，且未达到特别重大网络安全事件的，为重大网络安全事件（II级)：

（1）重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

（2）国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

（3）其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

### 1.3.3 符合下列情形之一，且未达到重大网络安全事件的，为较大网络安全事件（III级)：

（1）陕西省交通运输厅政府网站发生信息内容安全事件，造成反动信息、煽动性信息、谣言等小范围传播，对国家安全、社会稳定和政府形象造成较严重损害的。

（2）重要信息系统的重要敏感数据发生一定范围丢失或被窃取、篡改，对国家安全、社会稳定、行业运行造成较严重损害的。

（3）在陕西省交通运输厅开展重大灾害及紧急突发事件应急处置期间，因遭受网络攻击、设备故障、灾害等，导致重要信息系统服务中断4小时以上，并对陕西省交通运输厅开展应急处置工作的应急保障造成严重影响，或平时中断24小时以上，对政府形象造成严重损害的。

（4）其他对政府形象、重要业务运行和公众出行等造成严重影响的网络安全事件。

### 1.3.4 除上述情形外，对单位形象、公众利益构成一定威胁，并造成一定影响的网络安全事件，为一般网络安全事件（IV级）。

## 1.4 工作原则

（1）坚持统一领导，注重分类分级响应的原则。网络安全事件应急处置工作在陕西省交通运输厅网络安全和信息化领导小组（简称“厅领导小组”）统一领导下，各相关部门和单位密切配合、协同作战、分工负责，按照事件类型和级别，分类分级开展网络安全事件应急响应处置工作。

（2）坚持快速反应，有效控制事件影响的原则。发挥一线运行维护队伍直接作用和现场处置的临机决断作用，强调第一时间快速反应，做好先期初步处置，及时有效控制事态，切实防止扩大蔓延，最大程度地减少危害和影响。

（3）坚持预防为主，预防和应急相结合的原则。加强网络安全态势感知和日常监测预警，提升情报研判、风险评估和发现防范能力，切实做好预警响应和应急准备工作，严控苗头性风险、严控事件影响范围。

（4）坚持“谁主管谁负责，谁运行谁负责”的原则。落实网络安全运行和监管责任，明确运行和管理责任，充分发挥各方面的力量共同做好网络安全事件的预防和处置工作。

# **2 组织机构与职责**

## 2.1 领导机构及职责

在厅领导小组的领导下，厅网络安全和信息化厅领导小组办公室（简称“厅网信办”，设在厅科技处）统筹组织协调网络安全事件应对工作，建立健全跨部门联动处置机制。必要时（发生III级及以上网络安全事件），成立陕西省交通运输厅网络安全事件应急指挥部（简称“厅指挥部”），总指挥由厅领导小组主管领导担任，成员由厅领导小组相关成员担任，根据事件实际情况，吸纳事件涉及的部门、单位主要负责人进入厅指挥部参与应急处置工作。

厅指挥部负责统一指挥网络安全事件应急处置工作，组织建立应急指挥体系，决定启动应急响应并开展重大决策部署，协调处理重大事项。

## 2.2 办事机构与职责

陕西省交通运输厅网络安全应急管理工作由厅网信办承担，省交通运行监测中心负责应急管理具体工作。厅直各单位应明确网络安全工作负责人和应急联络人，人员调整时及时上报厅网信办（见附件3）。

## 2.2.1 厅网信办职责

负责网络安全应急协调工作，组织落实厅指挥部任务部署，协调涉事单位研判事件等级，向厅领导小组提出启动和终止I 级、II 级、III级响应工作建议，必要时，可视情况提出事件等级及响应措施的调整建议，组织制定III级事件应急工作方案，协调III级事件处置，督促检查IV级事件处置，对接交通运输部科技司（简称“部科技司”）和省委网络安全和信息化领导小组办公室（简称“省委网信办”），建立应急联络机制，组织开展应急演练和事件调查评估等。

## 2.2.2 省交通运行监测中心职责

负责为厅领导小组提供处置建议；负责监督指导涉事单位开展预警监测、安全事件及时处置和应急演练工作，提供网络安全处置措施建议；开展省交通网络安全监测预警，对接省、部监测体系，及时协调相关单位获取预警信息，协调跨部门、跨行业的监测信息共享事宜；完成厅网信办安排的其他网络安全应急管理工作。

## 2.3 厅直单位职责

负责研判IV级事件及应急工作方案制订；开展网络安全事件应急处置和应急演练；负责落实厅应急处置工作要求，提出应急处置工作建议，参与制定事件应急工作方案并承担具体处置工作；开展网络安全预警监测工作；做好应急技术和设备保障，组织调度系统开发单位参与应急处置工作；定期开展网络安全技术培训和应急演练；开展事件调查评估等。

# **3 监测预警**

## 3.1 安全监测

各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作，建立安全预警监测机制，并纳入以省交通网络安全监测预警平台为核心的监测体系，及时发现、及时通报，实现安全监测信息共享。

## 3.2 预警研判及发布

网络安全事件预警，是指依据国家级或部省级网络安全机构、专业网络安全技术服务机构等发布的可靠风险信息或汇总监测信息，判断有安全事件发生可能后，或在重要敏感时期，为可能发生的较大网络安全事件，发出提醒或告警的行为。预警信息包括事件类别、预警级别、起始及终止时间、可能影响范围、应采取措施等内容。

预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应网络安全事件级别I级（特别重大）、II级（重大）、III级（较大）、IV级（一般）。

红色预警由国家网络安全应急办组织研判、确定和发布，橙色预警由省网络安全应急办组织研判、确定和发布。

厅网信办组织对可能为III级的安全事件风险进行研判，认为需立即采取防范措施的，及时报厅领导小组，由厅领导小组发布本厅的黄色及以下级别预警。由厅网信办向省委网信办和部科技司及时汇报事件详情和处置进展。

各单位对可能为IV级的安全事件风险进行研判，立即采取防范措施，并发布蓝色预警，如有需要，及时上报厅网信办。

## 3.3 预警响应

## 3.3.1 I级预警响应（红色预警）

接上级网络安全部门发布的I级预警后，厅领导小组立即组织相关领导、机构和人员到位，按照上级部署要求开展预警响应工作，全面做好应急准备，对于业务连续性不强、存在安全隐患的非重要网络和信息系统，采取关停、断网等措施，集中技术力量、设备和工具确保重要网络与信息系统的安全运行，与省委网信办和部科技司保持24 小时沟通协调，发现问题立即上报网络安全部门。

涉事单位相关人员紧急进入待命状态，保持24小时联络通畅，发现问题立即上报省交通运行监测中心；系统运行维护单位加强监测分析和信息搜集工作，实行7×24小时值班制，协调技术支持队伍、基础条件保障单位、落实应急设备及人员等必备条件，做好风险管控和应急准备工作。

## 3.3.2 II级预警响应（橙色预警）

接上级网络安全部门发布的II级预警，在厅领导小组的指导下，厅网信办组织加强监测和情报搜集工作，重要信息随时报告，配合上级网络安全部门预警响应工作，省交通运行监测中心及时指导涉事单位做好数据备份，并根据业务工作实际，制定并实施网络与信息系统限制使用方案。与省委网信办和部科技司保持24小时沟通协调，发现问题立即上报。

涉事单位相关人员进入待命状态，保持24小时联络通畅，发现问题立即上报省交通运行监测中心；系统运行维护单位加强监测分析和信息搜集工作，实行7×24小时值班制，协调技术支持队伍、基础条件保障单位、落实应急设备及人员等必备条件，做好风险管控和应急准备工作。

## 3.3.3 III级预警响应（黄色预警）

在厅领导小组指导下，厅网信办牵头，省交通运行监测中心做好预警响应工作，实行24小时值班，保持通信联络畅通，实施每日信息汇报机制，各部门和涉事单位逐级上报相关信息；厅网信办及时联系专家及有关单位开展形势研判、研究防范措施及应急方案、协调调度应急资源，指导系统运行维护单位做好预防工作。

涉事单位开展网络安全风险评估和检查评估工作，制定并落实风险控制方案，对短期内难以解决的安全问题制定管理控制措施，最大限度的降低风险，做好安全防护设备、备用设备和应急物资的应急准备工作。

## 3.3.4 IV级预警响应（蓝色预警）

由涉事单位组织做好预警响应工作，保持通信联络畅通，密切关注事态发展，收集、汇总监测信息，重要信息及时向省交通运行监测中心汇报。

涉事单位针对预警信息制定整改方案和管理措施，并严格落实。

## 3.3.5 预警解除

预警发布单位根据实际情况，确定是否解除预警，及时发布预警解除信息。

# **4 应急处置**

## 4.1 事件报告

网络安全事件发生后，第一发现（接报）人应立即报告本单位网络安全管理机构，接报后涉事单位应根据事件类型迅速组织开展初步处置，控制事态，经合理分析判断后，认为可能为IV级及以上事件的，应及时将事件情况向省交通运行监测中心汇报（处置流程见附件2）。

## 4.2 初步处置

1.当确定网页上出现反动信息、煽动性言论、谣言等内容的安全事件发生时，应于第一时间切断相应服务器网络连接，并保留证据。

2.对信息窃取事件及信息破坏事件，应立即核实关联的信息系统，暂时关闭相关系统对外服务，并保留证据。

3.对网络服务异常事件，应立即核查访问量、软硬件设备配置及运行等情况，分析评估服务异常原因，并保留证据。

4.对有害程序事件，应首先将发现被感染的主机或计算机从网络上隔离开来，立即分析评估有害程序感染范围和破坏程度，并保留证据。

5.对设备设施故障事件，应立即核查故障设备情况，如果能够自行恢复，应立即用备件替换受损部件；如不能自行恢复的，立即与设备供应商联系，请求派维护人员前来维修，并分析评估事件影响。

6.对灾害性事件，应在确保人员安全的前提下，按照各类灾害应急方法予以科学处置。

## 4.3 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I级为最高响应级别。

厅网信办组织相关涉事单位、省交通运行监测中心、网络安全专家对网络安全事件开展事件研判，初判为III级及以上网络安全事件的，应立即向厅领导小组汇报，并根据事件研判，由厅领导小组决策启动III级应急响应；初判为IV级网络安全事件的，由涉事单位启动应急响应。

## 4.3.1 I级和II级响应

Ⅰ级和II级响应由上级网络安全部门启动，厅领导小组在上级网络安全部门的统一指挥下，开展应急处置工作。厅领导小组成员进入应急状态，保持24小时联络畅通，根据需要，厅领导小组有关成员赶赴现场，成立现场厅指挥部，在上级网络安全部门统一指挥、协调下，实施应急处置工作。

## 4.3.2 III级响应

（1）启动指挥体系

厅领导小组决定启动III级响应后，向省委网信办、部科技司报告事件情况，成立厅指挥部，厅指挥部成员保持24小时联络畅通。厅网信办组织涉事单位、省交通运行监测中心、网络安全专家等研究对策，提出处置方案建议，为厅指挥部决策提供支撑。

（2）掌握事件动态

跟踪事态发展。初步处置后，涉事单位应及时将事态发展变化情况和处置进展情况上报厅网信办。

检查影响范围。省交通运行监测中心、涉事单位及时掌握信息系统运行情况及事件影响情况，厅网信办汇总相关信息，及时报厅指挥部。

及时上传下达。厅网信办负责掌握事件动态发展情况，及时报送省委网信办和部科技司，并组织省交通运行监测中心将省委网信办、部科技司和厅指挥部要求、事件处置情况等通报有关单位。

（3）决策部署

厅指挥部组织厅网信办、省交通运行监测中心、涉事单位、网络安全专家等及时研究对策，对应急处置工作进行决策部署。

（4）处置实施

厅网信办组织指导涉事单位开展应急处置实施工作。

控制事态防止蔓延。采取各种技术措施、管控手段，最大限度地阻止和控制事态发展防止事态蔓延。

消除隐患恢复系统。根据事件发生原因，针对性制定具体的解决方案，组织实施处置，对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

调查取证。涉事单位应保护相关数据、记录、资料和现场，并在24小时内将网络安全事件报当地公安机关，配合开展调查取证工作。

信息上报。处置情况报厅网信办，厅网信办报厅领导小组。

## 4.3.3 IV级应急响应

IV 级响应由涉事单位具体负责，参照III级响应进行事件应急处置工作，处置完成后按照网络安全信息通报相关规定，及时向厅网信办汇报。

## 4.4 应急结束

网络安全事件应急处置基本完成后，风险得到控制，由厅指挥部授权厅网信办宣布I、II、III级应急处置工作结束。

## 4.5 调查和评估

事件调查和评估，原则上应在应急响应结束后30天内完成。调查评估报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

III级及以上安全事件调查评估按国家、交通运输部及省政府相关要求执行，经厅网信办审核批准后，将调查报告报厅领导小组、省委网信办和部科技司。

# **5 预防工作及应急准备**

## 5.1 日常管理

各单位负责网络安全事件预防，完善风险信息收集和管控机制，加强安全巡检、风险评估和容灾备份，及时整改安全隐患，建立与网络安全技术支撑队伍、基础条件保障单位、系统开发单位等的联络协调机制，并制定各类各级事件专项应急预案。

## 5.2 技术条件准备

各单位负责落实技术条件准备（见附件4），加强设备及系统基础信息、软硬件配置信息、技术文档、备品备件、运维记录等管理，并实施专人负责制，为合理、高效处置提供保障。

## 5.3 应急演练

厅网信办定期组织开展应急预案演练，各单位每年至少自行开展一次应急演练，模拟处置网络安全事件，提高实战能力，检验、评估和完善预案。

## 5.4 技术培训

省交通运行监测中心定期组织开展网络安全风险预警、事件处置等方面的专业技术培训。各单位每年对实施应急工作的人员至少组织两次技术培训。

## 5.5 重要敏感时期的预防措施

国家重大活动、会议等重要敏感时期，加强防范和应急准备，各单位应组织技术力量合理评估风险，提前关停不涉及重要业务运行、安全防护能力不强、应急处置难度较大的系统，对必须正常运行的重要信息系统实行7×24小时值班，实行风险管控专人负责制，确保及时处置网络安全风险隐患。

# **6 保障措施**

## 6.1 技术支持保障

各单位加强监测预警能力建设，储备必要的软硬件备品备件，建立各类事件专项应急预案，明确应急处置责任，落实到具体部门、具体岗位和个人；协调做好专业技术支撑单位联动；加强专家咨询队伍建设，充分发挥对决策咨询的支撑作用。

## 6.2 专家队伍保障

建立陕西省交通运输厅网络安全应急专家队伍，协助分析研判事件等级影响，提供专业指导和决策咨询，及时对处置结果预测、研判和评估，及时反映处置过程中存在的问题、不足，并提出改进建议。

## 6.3 经费保障

财务部门要提供必要的经费保障，协调落实应急处置工作相关经费，加大监测预警、应急演练和培训的资金投入，建立应急处置经费分级管理、分级负担的保障机制。

## 6.4 责任与奖惩

厅领导小组对在应急事件处置工作中表现突出的单位和个人给予表彰；对不落实应急预案要求，应急处置出现失职渎职，瞒报安全事件和影响，给国家和社会造成严重损失的部门和个人依照有关法律法规进行惩处。

# **7 附则**

（1）本预案由厅网信办负责制定、修订和解释，原则上每年评估一次，根据实际情况适时修订。

（2）厅直各单位应明确应急工作联系人，并报厅网信办备案; 应急联系人员发生变化后，应于3日内重新备案。

（3）厅直各单位负责依据本预案，建立本单位本系统的应急处置工作组织机构，结合实际情况自主合理确定事件级别，制定本单位本系统的应急预案。

（4）本预案自印发之日起正式实施。

# **8 附件**

附件：1. 事件分类及典型事件

2. 网络安全事件处置流程图

3. 应急处置工作联络表

4. 网络安全事件应急技术条件准备内容

# **附件1：事件分类及典型事件**

一、事件分类

（1）信息内容安全事件，是指因遭受网络攻击或信息发布管理不当导致的利用信息网络发布、传播危害国家安全、破坏民族团结、损害政府形象、影响社会稳定和公共利益等相关内容的网络安全事件。

（2）信息窃取事件，是指通过网络或其他技术手段，利用配置缺陷、协议缺陷、程序缺陷或使用暴力方式实施攻击，造成信息系统的数据或信息被窃取、泄露的安全事件。

（3）网络服务异常事件，是指通过网络或其他技术手段，利用配置缺陷、协议缺陷、程序缺陷或使用暴力方式实施攻击，造成信息系统运行异常、网络服务中断或网络服务欺骗。

（4）有害程序事件，是指因受到人为蓄意制造或传播的有害程序影响而导致的网络安全事件。

（5）信息破坏事件，是指通过网络或其他技术手段，假冒合法用户发布虚假信息或篡改原始信息的事件，以及因误操作、人为蓄意等原因导致信息丢失的事件。

（6）设备设施故障事件，是指因软硬件设备故障、外围保障设施故障以及人为使用非技术手段有意或无意造成信息系统被破坏的网络安全事件。

（7）灾害性事件，是指由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。

（8）其他网络安全事件。

二、典型事件

（1）常见信息内容安全事件：网页出现反动标语，破坏民族团结言论，迷信、赌博信息，谣言等。

（2）常见信息窃取事件：危险品车辆动态数据被窃取，无船承运业务许可申报信息泄露等。

（3）常见网络服务异常事件：分布式拒绝服务攻击（DDOS）事件、利用系统后门篡改服务器配置导致响应速度变慢等。

（4）常见有害程序事件：计算机、服务器或物联网设备等被植入病毒、木马、后门，被黑客控制成为僵尸网络设备，系统页面被嵌入恶意代码等。

（5）常见信息破坏事件：如向许可相对人发布被篡改的行政许可内容，企业、从业人员资质、信用、考试成绩等信息被篡改，传输错误的业务数据，蓄意删除设备日志，恶意损害或加密文件资料实行勒索等。

（6）设备设施故障事件:服务器电源故障，传输设备网卡故障、运维人员误拔网线等。

（7）灾害性事件：火灾、地震、雷击、机房坍塌等。

# **附件2：网络安全事件处置流程图**


# **附件3：应急处置工作联络表**

单位名称： （盖章）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 角色 | 姓名 | 部门 | 职务 | 手机 | 邮箱 |
|  | 应急主管领导 |  |  |  |  |  |
|  | 应急部门负责人 |  |  |  |  |  |
|  | 应急工作联络人 |  |  |  |  |  |

填表人： 联系方式： 填表时间

# **附件4：网络安全事件应急技术条件准备内容**

各单位预防网络安全事件时，应积极完善技术储备工作，储备内容应包括且不少于以下项目:

一、技术文档

技术文档至少应包括各类网络设备、服务器、计算机及其附属设备的型号、序列号等；硬件设备供应商、生产厂商的联络方式；操作系统、关键业务应用软件开发商或供应商联络方式；网络拓扑图；IP地址文档；路由器、防火墙、入侵检测等网络安全设备配置文档；服务器登录用户及原始密码文档；各类软件技术文档及其他需要保存的文档。

二、软硬件设备

至少应包括正版操作系统启动盘、安装盘，正版防病毒软件（注明安装及升级序列号），数据库管理系统软件，数据库备份软件及最近完整的数据备份存储介质，相关的设备驱动程序（含主板、网卡、显卡等）及更新到最新的服务器注册表文件；备用网线，万用表，测网仪等必要工具，备用路由器、交换机、服务器和存储等应急设备。