晋城市人民政府办公室文件

晋市政办〔2020〕82号

晋城市人民政府办公室
关于印发晋城市网络与信息安全
突发事件应急预案的通知

各县（市、区）人民政府、开发区管委会，市人民政府各委、办、局：

《晋城市网络与信息安全突发事件应急预案》已经市人民政府同意，现印发给你们，请认真贯彻执行。《晋城市网络与信息安全突发事件应急预案》（晋市政办〔2017〕110号）同时废止。

晋城市人民政府办公室

2020年12月31日

（此件公开发布）

晋城市网络与信息安全突发事件应急预案

1 总 则

1.1 编制目的

建立健全网络与信息安全突发事件应急响应机制，提高应对网络与信息安全事件能力，预防和减少网络与信息安全事件造成的损失和危害，维护国家安全和社会稳定。

1.2 工作原则

统一领导，协同配合；分级负责，职责明确；防范为主，加强监控；依法管理，规范有序；快速反应，有效应对。

1.3 编制依据

《中华人民共和国网络安全法》《中华人民共和国安全生产法》《中华人民共和国突发事件应对法》《中华人民共和国计算机信息系统安全保护条例》《网络安全等级保护条例》《国家网络安全事件应急预案》《山西省突发事件应对条例》《山西省网络与信息安全突发事件应急预案》《晋城市突发公共事件总体应急预案》《信息安全技术信息安全事件分类分级指南》（GB/Z20986-2007）等。

1.4 适用范围

本预案适用于本市行政区域内网络与信息安全突发事件的预防和应对工作。另有规定的，依照其规定执行。

1.5 事件分类

根据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）要求，网络与信息安全事件分为：有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障事件、灾害性事件和其他事件。

一、有害程序事件：计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

二、网络攻击事件：拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件、其他网络攻击事件。

三、信息破坏事件：信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

四、信息内容安全事件：指通过互联网传播法律法规禁止信息、组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

五、设备设施故障事件：软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

六、灾害性事件：指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件，包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的信息安全事件。

七、其他信息安全事件：不能归为以上6个基本分类的信息

安全事件。

1.6 事件分级

根据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）要求，网络与信息安全事件分为四级：特别重大网络与信息安全事件、重大网络与信息安全事件、较大网络与信息安全事件和一般网络与信息安全事件。

一、凡符合下列情形之一的，为特别重大网络与信息安全事件：

（一）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。

（二）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。

（三）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。

二、符合下列情形之一且未达到特别重大网络与信息安全事件的，为重大网络与信息安全事件：

（一）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。

（二）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。

（三）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。

三、符合下列情形之一且未达到重大网络与信息安全事件的，为较大网络与信息安全事件：

（一）重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

（二）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较严重威胁。

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

四、除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络与信息安全事件。

2 组织体系与职责

2.1 市网络与信息安全突发事件应急指挥部及职责

市人民政府设立晋城市网络与信息安全突发事件应急指挥部（以下简称市指挥部），统一指挥、协调全市网络与信息安全突发事件的应急处置工作。

指 挥 长：市人民政府分管网络与信息工作的副市长

副指挥长：市人民政府分管网络与信息工作的副秘书长、市大数据局局长、市委网信办主任、市应急局局长、市公安局常务副局长、晋城军分区参谋长。

成员单位：市委政法委、市委网信办、市发展改革委、市教育局、市科技局、市工信局、市公安局、市财政局、市交通局、

市文旅局、市应急局、市外事办、市市场监管局、市大数据局、市委机要保密局、市政府新闻办、市国家安全局、晋城军分区、国网晋城供电公司、中国铁塔晋城分公司、中国联通晋城分公司、中国移动晋城分公司、中国电信晋城分公司。各成员单位分管负责人为指挥部成员。根据网信突发事件实际情况，指挥长可随时增加市直有关单位为指挥部成员单位。

主要职责：统一领导、指挥、协调全市网络与信息安全事件的应急处置工作；负责对网络与信息安全事件、预防和预警工作进行及时报告和建议；决定启动与结束网络与信息安全事件应急响应；指导全市开展网络与信息安全突发事件应急处置工作；批准市指挥部办公室提请审议的重要事项；负责突发事件的信息发布；分析网络与信息安全突发事件发生原因和总结培训、演练、指导、协调评估、督导检查事件处置工作。

2.2 市指挥部办公室及职责

市指挥部办公室设在市大数据局。办公室主任由市大数据局局长、市委网信办主任担任（兼）。

主要职责：落实市指挥部指示和部署，承担市指挥部日常工作；监测汇总上报网络与信息安全事件预防和应对工作进展情况，分析研判网络与信息安全形势，做好舆情监管和引导工作，提出具体应急处置方案和措施建议；指导协调市网络与信息安全应急技术支撑队伍工作；负责协调大数据安全保障体系建设，组织实施数据安全审查和监管工作；负责统筹协调全市政务大数据

云平台系统及安全保障体系建设，承担安全等级保护、应急协调等相关工作；办理市指挥部交办的其他事项。

2.3 市指挥部成员单位及职责

市指挥部成员单位根据相关法律法规和各自职责，做好网络与信息安全突发事件日常监管和预防预警工作。事件发生时，根据以下职责分工承担相应的工作任务：

市委网信办：负责网络与信息安全事件舆论引导和管理工作；通知相关部门或网站及时删除危害国家安全和社会稳定的有害信息；指导重点新闻网站开展网络安全事件的预防、监测和应急处置工作；负责统筹协调全市网络安全保障体系建设和全市信息安全防护工作，指导推进全市政府部门、重点行业网络安全保障工作。

市大数据局：负责全市大数据基础设施统筹规划、协调建设、管理运维；负责组织全市电子政务外网规划和建设、运维管理；协调基础电信运营企业为信息系统的正常运行提供基础网络保障，确保网络与信息安全应急指挥系统通信的联络畅通；配合有关部门监测发现网络与信息安全事件，并按有关规定具体实施管控措施。

市委政法委：负责协调指导各相关部门做好网络安全领域反邪教工作，协调处理重大突发事件等。

市发展改革委：按有关规定负责网络与信息安全应急基础设施建设有关事宜。

市教育局：负责全市学校的应急宣传教育工作；负责教育城域网和校园网络信息安全应急协调工作。

市科技局：负责科研等非经营性网络突发事件应急协调工作。

市工信局：指导电信管理部门做好基础信息网络的安全防范工作；组织协调电信行业开展处置恢复工作。

市公安局：负责监督、指导和检查社会领域各网络与信息系统运营单位开展网络与信息安全突发事件的预防和应对工作；开展网络安全监测，发现并通报网络攻击、病毒木马传播、地下黑产等网络安全事件，发布预警信息；依法打击网络与信息安全事件中的违法犯罪行为；依法打击邪教组织的违法犯罪活动等。

市财政局：负责市级网络与信息安全突发事件应急处置经费的保障工作。

市交通局：负责网络与信息安全应急处置人员、物资车辆公路运输保障。

市文旅局：负责组织监测、发现影响或可能影响全市广播电视传输网络正常运行的事件，并负责开展处置恢复工作；配合无线电管理部门监测、发现无线电干扰广播电视信号事件，配合有关部门开展处置恢复；组织监测、发现卫星干扰广播电视信号事件，并进行处置；组织监测、发现网上有害和敏感视听节目，并会同有关部门进行处置和管控。

市外事办：负责网络与信息安全突发事件中涉外、涉台港澳的指导、协调。

市市场监管局、市应急局：负责做好网络与信息安全应急市级地方标准制（修）订的指导工作。

市委机要保密局（市国家密码管理局、市国家保密局）：组织查处网络与信息安全突发事件中泄露国家秘密行为，对泄露国家秘密有关材料提请省国家保密局进行鉴定；负责网上失泄密事件的应急处置工作；负责党委重要信息系统密码保障和安全认证监督管理；协调发生突发事件时非机要部门使用的普通密码和商用密码、密码设备的配置及密码设备安全处置工作。

市政府新闻办：负责指导和协调突发事件信息发布工作；负责媒体记者的组织、管理和引导。

市国家安全局：搜集相关情报信息，为网络与信息安全应急工作提供情报支持；负责对互联网上危害国家安全和社会政治稳定的有害敏感信息进行监控，并会同有关部门进行处置；依法打击利用互联网进行渗透、颠覆、策反、窃密等严重危害国家安全的违法犯罪活动。

晋城军分区：重点承担对国家安全造成特别严重损害的网络与信息安全突发事件应急协调工作。

国网晋城供电公司：负责电力行业网络与信息安全突发事件的预防、监测、报告和应急处置工作；负责为网络与信息安全应急提供电力保障。

中国铁塔晋城分公司、中国联通晋城分公司、中国移动晋城分公司、中国电信晋城分公司：负责组织通信、信息网络安全等

事故的应急救援工作，做好应急救援通信保障工作。

本预案未列出的部门和单位，根据市指挥部指令，按照本部门、本单位职责，依法做好网络与信息安全应急相关工作。

2.4 各县（市、区）指挥部

各县（市、区）人民政府、开发区管委会设立相应的网络与信息安全突发事件应急指挥部，在市指挥部和县（市、区）人民政府的领导下，组织和指挥本地区网络与信息安全突发事件的预防、监测、报告和应急处置工作。

3 预防和预警

3.1 预防

市直各部门、各县（市、区）人民政府、开发区管委会应按照“谁主管谁负责，谁运行谁负责”的要求，做好网络与信息安全事件的风险评估和隐患排查工作，加强信息安全风险评估和等级保护工作，提高信息系统自身防护能力。落实涉密防范措施，提高涉密信息和系统的监管水平。加强网络监管，提高舆情驾驭能力。制订完善相关应急管理制度，及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害。

3.2 预警

3.2.1 预警分级

网络与信息安全事件预警等级分为四级：Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级，分别对应发生或可能发生特别重大、重大、较大和一般的网络与信息安全事件。

3.2.2 监测与发布

市委网信办、市大数据局、市公安局、市国家安全局、市委机要保密局、晋城军分区以及各重要信息系统主管部门，各县（市、区）人民政府、开发区管委会共同承担全市网络与信息安全预警监测工作。信息系统运营单位及其主管部门要建立健全网络与信息安全突发事件监测、预测、预警制度，及时对网络与信息安全突发事件和可能引发网络与信息安全突发事件有关信息进行收集、分析和持续监测。

根据各级各部门监测或预测报告，市指挥部办公室及时组织成员单位、技术支撑队伍及有关单位进行研判，提出预警等级建议，按照规定权限和程序，经批准后发布预警信息，同时报市人民政府。

3.2.3 预警行动

根据预警信息，相关单位要对本部门网络与信息系统安全状况的监测，做好应急队伍、装备等应急处置准备工作，随时向市指挥部报告事态进展情况，市指挥部办公室及有关部门要及时跟踪了解情况。

3.2.4 预警解除

市指挥部办公室根据事件发展情况，组织有关部门、技术支撑队伍进行研判，提出预警解除建议，按照规定的权限和程序，经批准同意后，发布预警解除信息，并报市人民政府和上级有关部门。

4 应急响应

4.1 信息安全报告

网络与信息安全突发事件发生后，事发单位和监测单位立即向上级单位和事发地人民政府报告，并报送市指挥部。对较大和暂时无法判明等级的突发事件，事发后 1 小时内报告市人民政府。对特别重大、重大突发事件，事发地人民政府或有关部门在获知事件发生后立即报告市人民政府和上级有关部门。

突发事件报告内容应包括时间、地点、单位名称、信息来源、事件类别、伤亡或者经济损失的初步评估、影响范围、事件发展态势及处置情况等。

4.2 分级响应

根据突发事件危害程度、影响范围等实际情况，应急响应分为三级，一级为最高级别。

4.2.1 I 级响应

4.2.1.1 I 级应急响应启动条件

当符合以下情形之一时，市指挥部拟启动 I 级应急响应：

（1）发生或暂时情况不明有可能发生重大以上网络与信息安全突发事件时。

（2）发生或有可能发生重大以上网络与信息安全突发事件，市指挥部无法应付的。

（3）市指挥部根据事发当时情形，经过分析研判，认为需要启动 I 级应急响应的。

4.2.1.2 I级应急响应启动程序

事件发生后，市指挥部办公室经评估，向市指挥部提出建议，由市指挥部指挥长决定启动I级响应。

4.2.1.3 I级应急响应措施

市指挥部组织有关力量对突发事件进行先期处置，控制事态发展。同时上报上级指挥部请求支援，在省级应急领导机构统一指挥下，开展应急处置工作。主要处置措施如下：

（1）启动指挥体系

市指挥部进入应急状态，履行全市应急处置工作的统一领导、指挥、协调职责。市指挥部成员单位24小时值班，保持联络畅通；组织专家、技术人才研究对策，提出处置方案建议，为领导决策提供支撑。

（2）掌握事件动态

事件影响单位将事态发展变化情况和处置进展情况及时上报，市指挥部组织全面了解本市行政区域内的基础网络和信息系统受到事件波及或影响情况，及时汇总并上报省、市人民政府和上级指挥部，并通报市指挥部各成员单位。

（3）决策部署

待上级指挥部到达时，立即移交指挥权，在上级网络与信息安全应急机构的统一指挥下，市指挥部组织成员单位、技术支撑队伍，积极配合开展应急救援。

（4）处置实施

控制事态，防止蔓延。现场指挥部根据上级指挥部的部署或指导意见，组织事发单位及应急队伍，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；市指挥部全面启动预警机制，及时督促、指挥本市网络与信息系统运营使用管理单位有针对性地加强防范，防止事件进一步蔓延。

迅速处置，消除隐患。现场指挥部组织专家、应急技术力量、事发单位尽快分析事件发生原因、特点、发展趋势，快速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。

及时开展调查取证。事发单位在应急恢复过程中应尽量保留相关证据，对于人为破坏活动，公安、国家安全等部门按职责分工负责组织侦查和调查工作，并及时向上级指挥部报告有关情况。

4.2.2 II级响应

4.2.2.1 II级应急响应启动条件

当符合以下情形之一时，市指挥部拟启动II级应急响应：

（1）发生或暂时情况不明有可能发生较大网络与信息安全突发事件时。

（2）发生或有可能发生较大网络与信息安全突发事件，且事发单位无法应对需市指挥部来指挥协调的。

（3）市指挥部根据事发当时情形，经分析研判，认为应当启动II级应急响应的。

4.2.2.2 II级应急响应启动程序

市指挥部办公室会同成员单位、技术支撑队伍对事件信息进行研判，及时向市指挥部提出启动II级响应建议，市指挥部指挥长或副指挥长批准后，决定启动II级响应状态。

4.2.2.3 II级应急响应措施

（1）启动指挥体系

市指挥部进入应急状态，履行全市应急处置工作的统一领导、指挥、协调职责。市指挥部成员单位保持24小时联络畅通。市指挥部办公室24小时值班。

各县指挥部和市指挥部成员单位进入应急状态，在市指挥部统一指挥、协调下，负责本地区、本部门应急处置工作或支援保障工作，24小时值班，并派出联络员参加市指挥部办公室工作。

（2）掌握事件动态

跟踪事态发展。事件发生地人民政府及有关部门及时将事件发展变化情况和处置进展情况报市指挥部办公室。

检查影响范围。网络与信息系统主管部门立即全面了解本部门主管范围内的网络与信息系统是否受到事件的波及或影响，并将有关情况及时报市指挥部办公室。

及时通报情况。市指挥部办公室负责汇总上述有关情况，重大事项及时报省、市人民政府及上级有关部门，并通报市指挥部成员单位。

（3）决策部署

市指挥部统一指导，组织成员单位、技术支撑队伍，及时开

展应急救援工作。

（4）处置实施

控制事态、防止蔓延。有关部门和单位要负责组织实施，安排网络与信息安全应急技术支撑队伍采取技术措施，尽快控制事态；组织、督促相关运行单位有针对性地加强防范，防止事件蔓延至其他网络与信息系统。对于信息内容安全事件要及时采取必要的管控措施，防止有害信息传播扩散。

迅速处置、消除隐患。有关部门和单位要根据事件发生原因，有针对性地采取措施，恢复受破坏网络与信息系统正常运行。

及时开展调查取证。事发单位在应急恢复过程中应尽量保留相关证据，对于人为破坏活动，公安、国家安全等部门按职责分工负责组织侦查和调查工作，并及时上报上级指挥部。

根据实际需要，市指挥部及有关成员单位、技术支撑单位与市对口部门联系，开展协助，向上级有关部门或技术支撑队伍申请援助。

4.2.3 Ⅲ级响应

4.2.3.1 Ⅲ级应急响应启动条件

当符合以下情形之一时，市指挥部拟启动Ⅲ级应急响应：

（1）发生或暂时情况不明有可能发生一般网络与信息安全突发事件时。

（2）发生或有可能发生一般网络与信息安全突发事件，且事发单位可以应对的。

（3）市指挥部根据事发当时情形，经分析研判，认为需要启动III级应急响应的。

4.2.3.2 III级应急响应启动程序

市指挥部办公室对事件信息进行分析研判，及时向市指挥部提出启动III级响应建议，由市指挥部办公室主任决定并宣布启动III级响应

4.2.3.3 III级应急响应措施

（1）市指挥部办公室密切关注事态发展，视情派出应急工作组到事发地进行协调指导。

（2）各网络与信息安全应急技术支撑队伍根据各自职责，积极提供配合和支持。

（3）将事件处理进展情况及时报告市政府及相关部门。

4.3 社会力量动员与参与

依托社会优秀互联网网络安全企业，充分发挥社会力量和人才在网络与信息安全中的积极作用，合理动员、组织其参与网络与信息安全事件应急响应工作。

4.4 信息发布

新闻主管部门按照指挥部意见，组织做好对外信息发布工作，对受影响的公众进行解释、疏导。未经批准，其他部门和单位一律不得发布相关信息。

4.5 应急结束

应急响应结束应遵循“谁启动，谁结束”的原则。市级响应

结束经市指挥部批准后，由市指挥部办公室宣布应急响应结束，必要时向社会公布。

5 后期处置

5.1 事件总结

特别重大、重大网络与信息安全事件由市指挥部办公室组织有关部门和地区配合上级应急指挥机构进行调查处理和总结评估。

较大、一般网络与信息安全事件由事件发生地区或部门组织调查处理和总结评估，对事件的起因、性质、影响、责任等进行调查，提出处理意见和改进措施。相关总结调查报告上报市指挥部办公室，同时市指挥部办公室总结调查报告上报省指挥部办公室。

5.2 善后处置

市指挥部、事发地区县（市、区）政府、事件责任单位要积极稳妥、深入细致地搞好善后处置。对参与处置的工作人员，以及紧急调集、征用有关单位、个人的物资，要按照规定给予补助或补偿。

5.3 恢复重建

恢复重建工作按照“谁主管谁负责，谁运营谁负责”的原则，由事发单位负责。事发单位和相关职能部门在对可利用的资源进行评估后，制订重建和恢复计划，迅速采取各种有效措施，恢复网络与信息系统的正常运行。

6 应急保障

6.1 技术支撑队伍

相关部门应加强网络与信息安全应急技术支撑队伍建设，完善技术支撑队伍检查监测装备、培养和引进人才，开展网络与信息安全防范技术研究，做好网络与信息安全事件的应急技术支援工作。积极支持科研院所开展网络与信息安全研究与服务，充实壮大我市网络与信息安全应急技术支撑队伍。密切与省网络与信息安全应急技术支撑队伍的联系，及时取得技术外援支持，提高应对突发网络与信息安全事件的能力。

6.2 专家队伍

市指挥部办公室设立网络与信息安全咨询工作组，为网络与信息安全事件的预防和处置提供技术咨询，充分发挥专家在科学决策中的作用。

6.3 通信信息

市、县两级指挥部和成员单位按照职责分工，加强应急通信装备准备，确保应急响应启动后，指挥系统通信与信息传达联络畅通。

6.4 基础平台

预留重要信息系统应急硬件，备份重要系统软件和基础数据库，确保在网络与系统遭到破坏或毁损后，及时有效处置突发事件，恢复系统基本功能，提高应急处置能力。

6.5 情报力量

市公安局、市国家安全局等部门加强网络与信息安全有关情报搜集能力建设，为网络与信息安全应急工作提供情报支持。

6.6 经费保障

市县两级人民政府及其有关部门应根据网络与信息安全突发事件应急救援需要，统筹安排应急救援专项资金和应急培训、演练所需经费，市县两级财政部门要纳入财政预算。

6.7 宣传教育和培训演练

市、县两级指挥部和成员单位应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络与信息安全事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣传活动。

市、县两级指挥部和成员单位要将网络与信息安全事件的应急知识等列为行政管理干部和有关人员的培训内容，加强网络与信息安全特别是网络与信息安全应急预案的培训，提高防范意识及技能。

市指挥部办公室会同有关部门、技术支撑队伍每年至少组织一次应急演练，模拟处置重大网络与信息安全事件，提高实战能力，检验和完善预案。

7 附则

7.1 预案管理与更新

本预案根据网络和信息安全发展形势以及相关法律法规的变更，三年修订一次，修订工作由市大数据局负责。各县（市、区）要结合本预案制订或修订本地区网络与信息安全事件相关应急预案，做好预案之间的衔接。

7.2 表彰和惩处

对在网络与信息安全应急工作中表现突出的单位和个人给予表彰；对保障不力、瞒报漏报网络与信息安全事件，给国家和社会造成严重损失的单位和个人按照相关规定进行惩处。

7.3 预案解释部门

本预案由市大数据局制定并负责解释。

7.4 预案实施时间

本预案自印发之日起实施。2017 年 12 月 29 日印发的《晋城市网络与信息安全突发事件应急预案》（晋市政办〔2017〕110 号）同时废止。

8 附录

8.1 晋城市网络与信息安全应急组织机构图

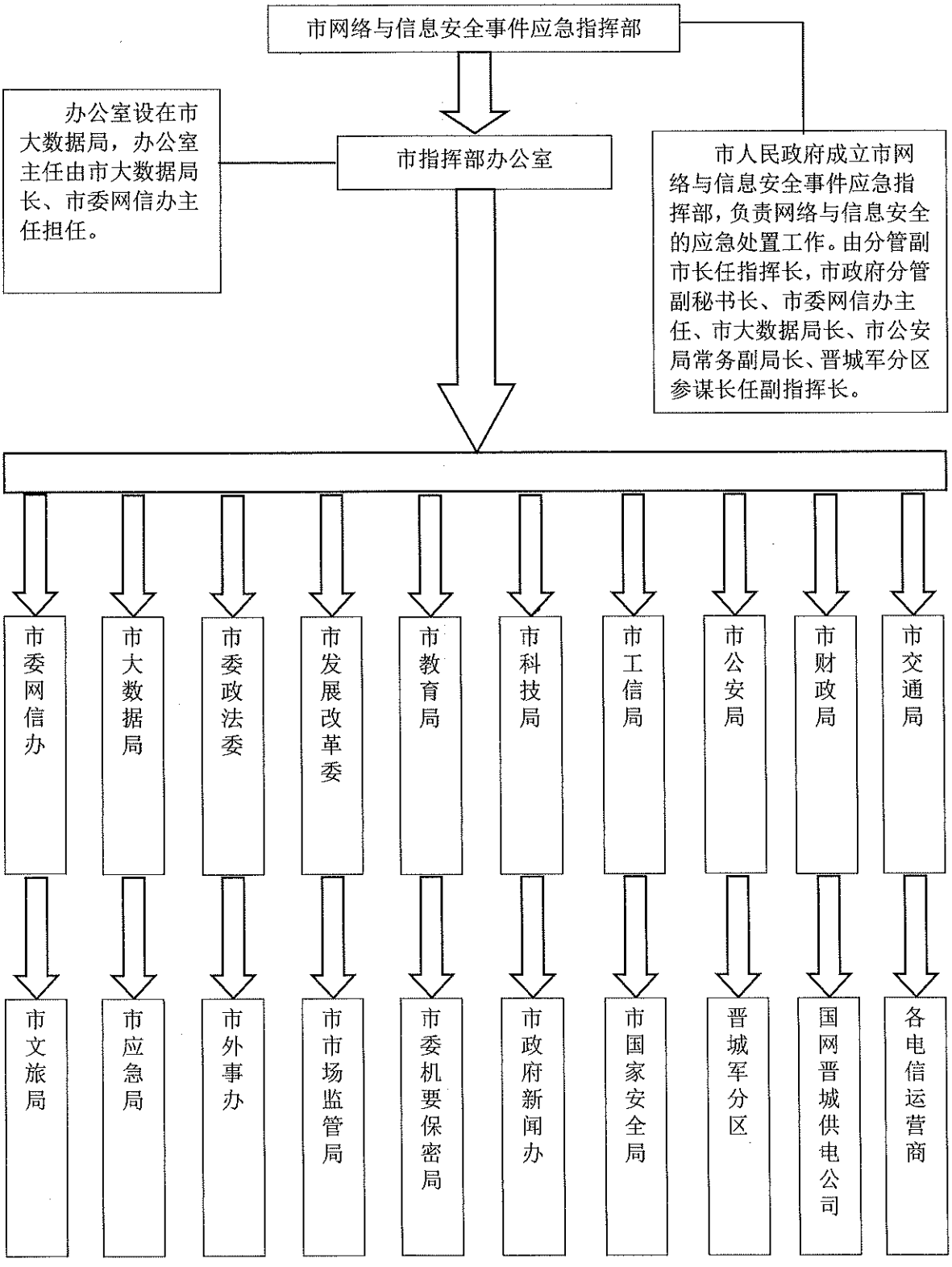
8.2 晋城市网络与信息安全应急工作流程图

8.3 晋城市网络与信息安全突发事件上报表

8.4 晋城市网络与信息安全应急联络表

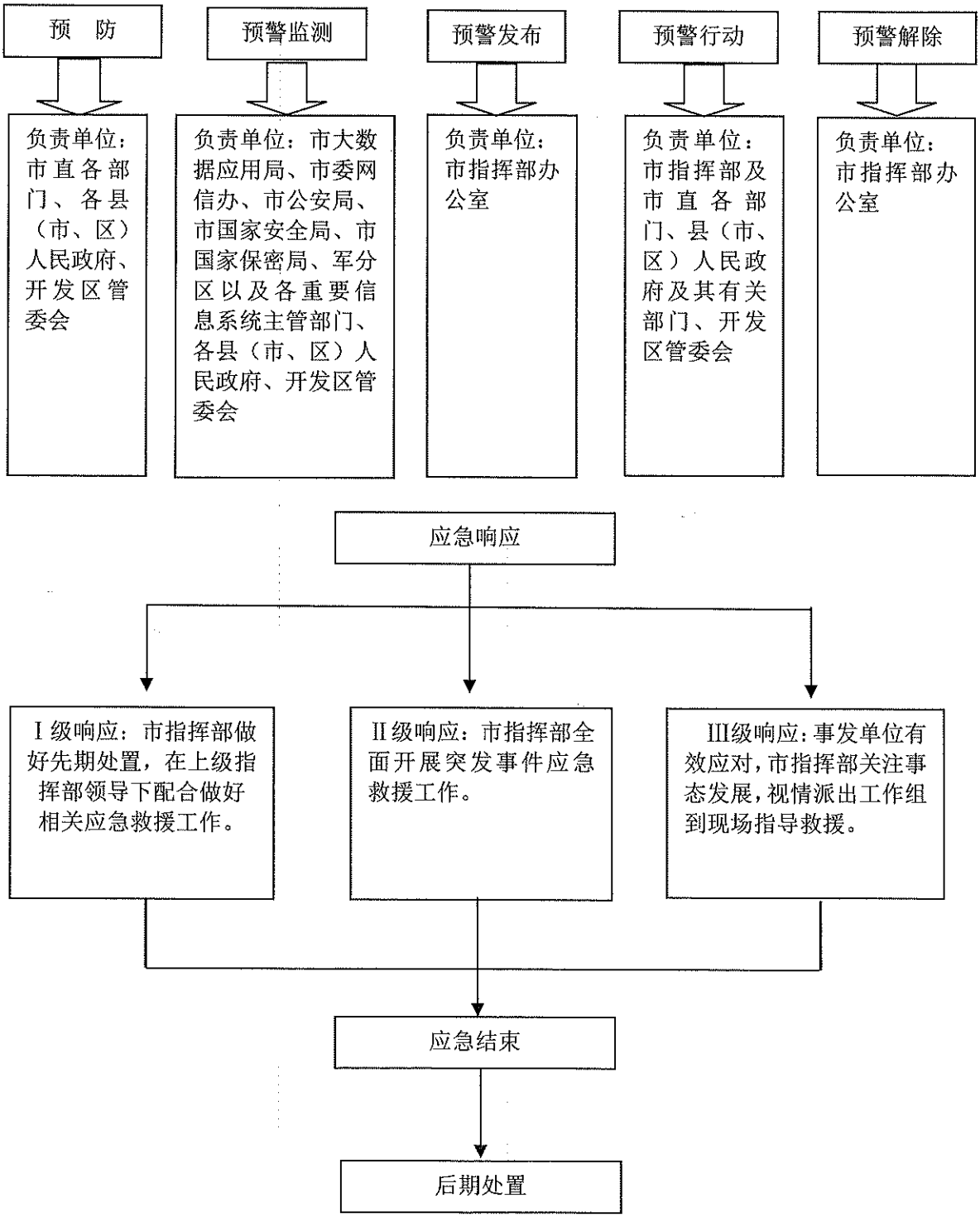
附录 8.1

晋城市网络与信息安全应急组织机构图



附录 8.2

晋城市网络与信息安全应急工作流程图



附录 8.3

晋城市网络与信息安全突发事件上报表

报告单位		报告时间	年 月 日 时
事发单位		事件起始时间	
填 报 人		审 核 人	
事件分类	□有害程序类事件 □网络攻击类事件 □信息破坏类事件 □信息内容安全类事件 □设备设施故障类事件 □灾害类事件 □其他类事件		
事件级别	□特别重大网络与信息安全事件 □重大网络与信息安全事件 □较大网络与信息安全事件 □一般网络与信息安全事件		
危害表象	□网络中断 □系统瘫痪 □数据毁坏 □数据泄密 □其他危害		
事件描述（包括突发事件发生的原因、性质，初步原因和危害程度判断）：			
处置措施（突发事件发生单位已采取的控制措施及其他应对措施）：			
事件后果的初步估计：			
有关意见和建议：			

附录 8.4

晋城市网络与信息安全应急联络表

单位	值班电话	单位	值班电话
省委办公室	0351-4045001	市交通局	2023595
省政府办公室	0351-3046789	市文旅局	2057555
省经济信息中心	0351-3119999	市应急局	2027255
市委办公室	2062298	市外事办	2198848
市政府办公室	2198345	市市场监管局	2022239
市委网信办	2566200	市委机要保密局	2198056
市大数据局	2218958	市政府新闻办	2198741
市委政法委	2198013	市国家安全局	2034918
市发展改革委	2198993	晋城军分区	2043211
市教育局	2066102	国网晋城供电公司	2162216
市科技局	2888666	铁塔晋城分公司	6996000
市工信局	2218748	联通晋城分公司	2034777
市公安局	3010100	移动晋城分公司	3035518
市财政局	2065580	电信晋城分公司	6997099

抄送：市委各部门，市人大常委会办公室，市政协办公室，市法院，市检察院，各人民团体，各新闻单位。

市属各事业单位，驻市各单位，各大中型企业。

晋城市人民政府办公室　　2020年12月31日印发