晋城市能源行业
网络与信息安全事件应急预案

1 总则

1.1 编制目的

为预防和及时、有序、高效地处置能源行业网络与信息安全事件，最大程度地避免、减少能源行业网络与信息安全事件可能造成的危害与损失，维护国家安全和社会稳定，结合本单位、本行业实际情况，特制定本预案。

1.2 编制依据

依据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》《中华人民共和国安全生产法》《中华人民共和国计算机信息系统安全保护条例》《网络安全等级保护条例》《信息安全技术信息安全事件分类分级指南》《山西省突发事件应对条例》《晋城市突发公共事件总体应急预案》《晋城市网络与信息安全突发事件应急预案》等法律法规和规定，结合行业实际编制本预案。

1.3 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。

1.4 适用范围

本预案适用于晋城市行政区域范围内能源行业发生或可能发生的网络与信息安全事件的预防和应对工作。另有规定的，依照其规定执行。

1.5 事件分类分级

依据《信息安全技术信息安全事件分类分级指南》，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。（事件分类详见附录8.3）

网络与信息安全事件按照性质类型、严重程度、可控性和影响范围等因素，分为四级：特别重大、重大、较大和一般。（事件分级详见附录8.4）

2 组织机构和职责

2.1 应急指挥部组成及职责

晋城市能源局成立能源行业网络与信息安全事件应急指挥部（以下简称“市局指挥部”），各县（市、区）能源局成立相应的应急指挥机构。

指 挥 长：市能源局局长

副指挥长：市能源发展中心主任

成员单位（科室）：市能源发展中心、市局综合办公室、煤炭科、油气科、电力与新能源科等科室。

市局指挥部主要职责：

贯彻落实市委、市政府和上级有关部门决策部署；统一领导、指挥、协调全市能源行业网络与信息安全事件的应急处置工作；决定启动或结束晋城市能源行业网络与信息安全事件的应急响应；研究确定能源行业网络与信息安全事件应急工作重大决策和工作意见；保障本单位网络与信息安全工作经费及人员、车辆等；向市委、市政府、省能源局等上级有关部门报告能源行业网络与信息安全事件应急处置工作进展情况；完成市委、市政府和上级有关部门交办的其他任务。

2.2 市局指挥部办公室组成及职责

市局指挥部下设办公室（以下称“市局指挥部办公室”），办公室设在市能源发展中心，办公室主任由市能源发展中心分管网络安全负责人担任。

市局指挥部办公室职责：

落实市局指挥部指示和部署，承担市局指挥部日常工作；负责应急值守，监测汇总上报本市能源行业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，视情向市局指挥部提出启动或结束应急响应的建议；根据市局指挥部指示，协调市局指挥部成员单位（科室）、专业应急技术支撑队伍开展应急处置工作；配合有关部门做好舆情引导和管理工作；提出具体应急处置方案和措施建议；

负责能源行业网络与信息安全工作的宣传教育、培训和应急演练；协调处理相关善后工作；完成市局指挥部交办的其他任务。

2.3 市局指挥部成员单位（科室）职责

市能源发展中心：负责应急值守、信息汇总；组织、协调成员科室、相关技术支持人员及时到场，分析判断事件发展趋势，开展应急处置工作；配合上级能源主管部门、网络与信息安全部门、公安部门等单位进行调查取证；负责配合有关部门做好舆论引导和管理工作；协调配合处理相关善后工作；组织能源行业网络与信息安全的宣传教育、培训和应急演练；接收和办理向市委、市政府报送的紧急重要事项等工作。

市局综合办公室：做好文件处理、应急行文等；保障网络与信息安全工作经费及人员、车辆等；配合做好能源行业网络与信息安全相关工作。

煤炭科：协调参与煤炭行业网络与信息安全事件的预防、监测、报告和应急处置工作。

油气科：协调参与油气行业网络与信息安全事件的预防、监测、报告和应急处置工作。

电力和新能源科：协调参与电力、新能源行业网络与信息安全事件的预防、监测、报告和应急处置工作。

其他科室：按照本科室职责，配合参与网络与信息安全

事件的应急处置工作。

2.4 应急工作组组成及其职责

根据能源行业网络与信息事件应急救援工作需要，市局指挥部下设3个应急工作组，分别为综合协调组、现场抢修组、后勤保障组。

（1）综合协调组

牵头单位（科室）：市能源发展中心

组成单位（科室）：市局综合办公室、煤炭科、油气科、电力与新能源科。

职责：在市局指挥部的领导下，负责收集汇总相关数据、进行初步分析及技术研判，评估事件影响，提出突发事件应对意见；开展现场调查、应急监测、舆情引导等应急工作；及时向市局指挥部报告突发事件发生和发展情况，并按照市局指挥部的决定落实工作措施；负责市局指挥部的内外协调及各项组织计划工作；协调处理相关善后工作。

（2）现场抢修组

牵头单位（科室）：市能源发展中心

组成单位（科室）：市局煤炭科、油气科、电力与新能源科。

组成人员：委托第三方专业技术支撑团队，必要时聘请网络与信息等方面专家。

职责：根据现场情况，组织协调第三方专业技术支撑团队伍，开展网络与信息事件抢修恢复的各项具体工作，保障网络与信息系统畅通。

（3）后勤保障组

牵头单位（科室）：市局综合办公室

组成单位（科室）：市能源发展中心

职责：负责网络与信息安全应急工作经费及人员、车辆等后勤保障工作。

2.5 各县（市、区）能源局指挥部

各县（市、区）能源局设立相应的能源行业网络与信息安全事件应急指挥部，制定本区域能源行业网络与信息安全事件应急预案，在市局指挥部领导下，组织本地区能源行业网络与信息安全事件的预防、监测、报告和应急处置工作。

3 预警预防机制

3.1 预防机制

按照“谁主管谁负责，谁运行谁负责”的要求，各级各单位做好能源行业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，避免和减少能源行业网络与信息安全事件的发生及其危害。

3.2 会商机制

建立会商研判机制，对可能导致能源行业网络与信息事件风险的信息进行收集、分析和研判。建立健全会商研判制度，明确牵头科室，定期组织分析预判。重点时段加强对能源行业网络与信息事件的预判预测，指导做好预先防范。

3.3 预警机制

3.3.1 预警信息来源

（1）预测、预警系统监测到可能发生的能源行业网络与信息安全事件信息；

（2）上级机构或其他职能部门通报可能发生的能源行业网络与信息安全事件信息；

（3）基础电信运营企业经风险评估得出的网络与信息重大隐患和网络与信息安全事件发展趋势报告；

（4）能源企业上报的可能发生的网络与信息安全事件信息；

（5）其他能源行业网络与信息安全事件信息。

3.3.2 预警情形

（一）较大以上风险预警

预警情形：经研判，存在较大以上风险隐患，有可能发生较大以上或超出市局指挥部处置能力的能源行业网络与信息安全事件。

预警措施：及时召开有关会议，安排成员单位（科室）、

技术支撑队伍和基层人员做好预防工作，尽量避免或减少损失；组织技术支撑队伍和有关专家分析研判，及时采取有效措施控制事态发展，防止事件进一步蔓延；及时报请上级指挥部请求支援。

（二）一般风险预警

预警情形：经研判，存在一般风险隐患，有可能发生一般或超出基层处置能力需要市局指挥部协调处置才能应对的能源行业网络与信息安全事件。

预警措施：及时召开有关会议，安排成员单位（科室）、技术支撑队伍和基层人员做好预防工作，尽量减少损失；组织技术支撑队伍和有关专家分析研判，及时采取有效措施排除隐患。

（三）一般以下风险预警

预警情形：经研判，存在一定风险隐患，影响较小，有可能发生一般以下或依靠基层力量能够处置的能源行业网络与信息安全事件。

预警措施：关注事态发展，加强与有关单位的沟通联系；督导基层做好事件的预防工作，及时排除隐患；视情派技术团队到现场进行协调指导。

3.3.3 预警结束

市局指挥部办公室根据事件发展情况，组织成员单位（科室）、技术支撑团队进行研判，认为网络与信息安全隐

患已消除，且网络与信息系统已恢复正常运行后，预警结束，适时终止相关措施。

4 应急响应

4.1 信息报告

能源行业网络与信息安全事件发生后，单位负责人应当按照属地管理原则立即向事件发生地能源主管部门报告，并视情逐级上报。（晋城市能源行业网络与信息安全事件上报表详见附录 8.5）

市局指挥部办公室收到报告后，立即组织相关人员和专家，对事件发展情况进行分析研判。对特别重大、重大事件，立即报告市人民政府；对一般、较大和暂时无法判明等级的事件，事发后 1 小时内报告市人民政府。

事件报告内容应包括时间、地点、单位名称、对网络与信息设施造成影响的灾害性质，引发造成网络与信息中断的原因、影响的范围、拟采取的措施、社会影响等情况。

4.2 先期处置

能源行业网络与信息安全事件发生后，事发单位必须在第一时间实施处置，并按职责和规定权限启动相关应急预案处置规程，控制事态发展并及时按照属地原则进行上报。

市局指挥部办公室在接报事件信息后，及时掌握事件的发展情况，评估事件的影响和可能波及的范围，研判事件的发展态势，根据需要组织成员单位（科室）、专家、技术支

撑团队，在各自职责范围内参与先期应急处置工作。

4.3 分级响应

根据网络与信息安全事件的严重程度、发展态势和应对能力，将应急响应设定为Ⅰ级、Ⅱ级、Ⅲ级三个等级，Ⅰ级为最高级别。

4.3.1 Ⅰ级响应

启动条件：

（1）发生或暂时情况不明有可能发生较大以上能源行业网络与信息安全事件的；

（2）超出市局指挥部处置能力的；

（3）市局指挥部经分析研判认为应当启动Ⅰ级响应的。

启动程序：

市局指挥部办公室接到网络与信息安全事件报告后，立即组织相关人员进行调查、核实、分析，并做出评估和判断，向市局指挥部提出启动Ⅰ级响应的建议，由市局指挥部指挥长宣布启动Ⅰ级响应。

响应措施：

（1）市局指挥部组织各成员单位（科室）、技术支撑队伍赶赴事发现场，做好先期处置工作，采取有效措施控制事态发展，防止事件进一步蔓延；

（2）市局指挥部根据事态发展情况及时报请上级指挥部请求支援；

（3）上级指挥部到达现场后，立即向上级移交指挥权，并根据上级指挥部的指令，开展各项应急处置工作；

（4）按照有关规定做好事件信息的报送工作。

4.3.2 II级响应

启动条件：

（1）发生或暂时情况不明有可能发生一般能源行业网络与信息安全事件的；

（2）超出基层处置能力需要市局指挥部协调处置才能能够应对的；

（3）市局指挥部经分析研判认为应当启动II级响应的。

启动程序：

市局指挥部办公室接到网络与信息安全事件报告后，立即组织相关人员进行调查、核实、分析，并做出评估和判断，向市局指挥部提出启动II级响应的建议，由市局指挥部副指挥长宣布启动II级响应。

响应措施：

（1）迅速通知相关市局指挥部成员单位（科室）、技术支撑团队，赶赴事件现场；

（2）市局指挥部副指挥长亲临现场，成立现场指挥部，组织召开网络与信息安全事件处置协商会议，分析研判事件发展情况，立即全面了解主管范围内的网络与信息系统受到的波及或影响；

（3）市局指挥部统一指导，安排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，及时采取必要的管控措施，防止事件传播扩散蔓延至其他网络与信息系统；根据事件发生原因，有针对性地采取措施，尽快恢复受破坏网络与信息系统正常运行；

（4）市局指挥部办公室负责汇总上述有关情况，重大事项及时报市人民政府及上级有关部门。当超出市局指挥部处置能力时，立即请求上级指挥机构进行增援；

（5）配合有关部门做好新闻发布和舆情引导工作；

（6）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，积极配合公安部门进行侦查和取证工作。

4.3.3 III级响应

启动条件：

（1）发生或暂时情况不明有可能发生一般以下能源行业网络与信息安全事件的；

（2）依靠基层力量能够处置的；

（3）市局指挥部经分析研判认为应当启动III级响应的。

启动程序：

市局指挥部办公室接到网络与信息安全事件报告后，立即组织相关人员进行调查、核实、分析，并做出评估和判断，向市局指挥部提出启动III级响应的建议，由市局指挥部副指挥长宣布启动III级响应。

响应措施：

（1）市局指挥部办公室应当立即进入应急状态，关注事态发展，加强与相关单位的沟通联系，督导做好事件的应急处置工作，视情派技术人员到现场进行协调指导；

（2）将事件处理进展情况及时报告市政府及上级有关部门。

4.4 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处置工作。

4.5 信息发布

按照实事求是、及时准确的原则，市局指挥部办公室负责能源行业网络与信息安全事件应急信息资料的核实，配合相关部门引导舆论宣传，做好新闻报道工作。

市局指挥部配合相关部门按照《政府信息公开条例》及《晋城市突发公共事件新闻发布应急预案》等规定，配合新闻媒体向社会发布能源行业网络与信息安全事件信息。

未经批准，其他部门和单位一律不得发布相关信息。

4.6 响应结束

受破坏的网络与信息系统已恢复正常运行，危害网络与信息系统安全运行的因素得到消除，导致次生、衍生事故的风险消除，无继发可能，符合有关标准，遵循“谁启动，谁

结束”的原则，市局指挥部办公室向市局指挥部提出应急响应结束的建议，由市局指挥部宣布应急响应结束。

5 后期处置

5.1 善后处置

市、县（市、区）两级局指挥部、主管部门、事件责任单位要积极稳妥、深入细致地搞好善后处置，尽快恢复企业正常运营。

5.2 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。

5.3 事件总结

一般能源行业网络与信息安全事件由市局指挥部办公室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。

较大、重大、特别重大能源行业网络与信息安全事件市局指挥部办公室配合上级应急指挥机构进行调查处理和总结评估。

6 应急保障

6.1 技术支撑队伍

鉴于行业的特殊性、专业性和本局实际情况，能源行业网络与信息安全事件的应急处置委托第三方专业技术支撑团队，市局指挥部办公室要加强与第三方的联系与沟通，及时了解应急技术支撑队伍建设情况，并督导技术支撑队伍完善检查监测装备、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。同时密切与省、市的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，提高应对网络与信息安全事件的能力。

6.2 通信信息

市、县（市、区）两级局指挥部按照职责分工，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。

6.3 基础平台

相关部门和企业要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，确保在网络与信息系统遭到破坏或毁损后，及时有效处置事件，恢复系统基本功能，提高应急处置能力。

6.4 情报力量

加强与市大数据局、市委网信办、市公安局、市国家安全局等部门的联系与沟通,为网络与信息安全应急工作提供情

报支持。

6.5 经费保障

积极协调同级财政部门，落实网络与信息安全应急保障所需的各项经费；同时，积极争取同级政府设立应急保障专项基金，并确保专款专用。

企业常备物资经费由企业自筹资金解决。同时鼓励自然人、法人或者其他组织按照有关法律法规的规定进行捐赠和援助。

6.6 宣传、演练和培训

市局指挥部办公室、能源企业应加强安全知识宣传工作，及时向从业人员宣传网络与信息安全事件预防和处置的有关法律法规和政策、基本知识和技能。

市局指挥部办公室要制定落实事件应急救援和管理人员的培训计划，提高其专业技能及应急处置能力。

市局指挥部每年至少组织一次应急演练。加强各单位（科室）之间的协同能力，提高防范和处置事件的技能，增强实战能力。

能源企业按有关规定定期组织应急救援演练。

7 附则

7.1 名词解释

网络与信息安全事件：由于人为原因、软硬件缺陷或故障、自然灾害等，对网络与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。

本预案有关数量的表述中，“以上”包括本数，“以下”不包括本数。

7.2 预案修订

本预案原则上每3年修订一次。预案实施过程中发现有问题，要及时修订和完善。

当出现下列情形之一时，应当组织修改完善本预案：

（1）预案依据的有关法律、行政法规、规章、标准、上位预案中的有关规定发生变化的；

（2）能源行业网络与信息安全事件应急机构及其职责发生重大变化或调整的；

（3）预案中的其他重要信息发生变化的；

（4）在事件实际应对和应急演练中发现问题需要进行重大调整的；

（5）预案制定单位认为应当修订的其他情况。

7.3 预案管理

本预案由晋城市能源行业网络与信息安全事件应急指挥部办公室统一管理，县（市、区）能源部门应急指挥机构要根据本预案和所承担的应急处置任务，制定相应的应急预案。

7.4 责任追究

在能源行业网络与信息安全事件应急救援工作中玩忽

职守、失职渎职或拒不执行应急规定，扰乱能源行业网络与信息安全事件应急工作的有关单位和人员，要按照有关规定依法、依纪、依规追究责任。

7.5 预案制定与解释

本预案由晋城市能源局负责制定、组织实施和解释。

7.6 预案实施时间

本预案自印发之日起实施。

8 附录

8.1 晋城市能源行业网络与信息安全事件应急指挥部组织机构图

8.2 晋城市能源行业网络与信息安全事件处置流程图

8.3 网络与信息安全事件分类

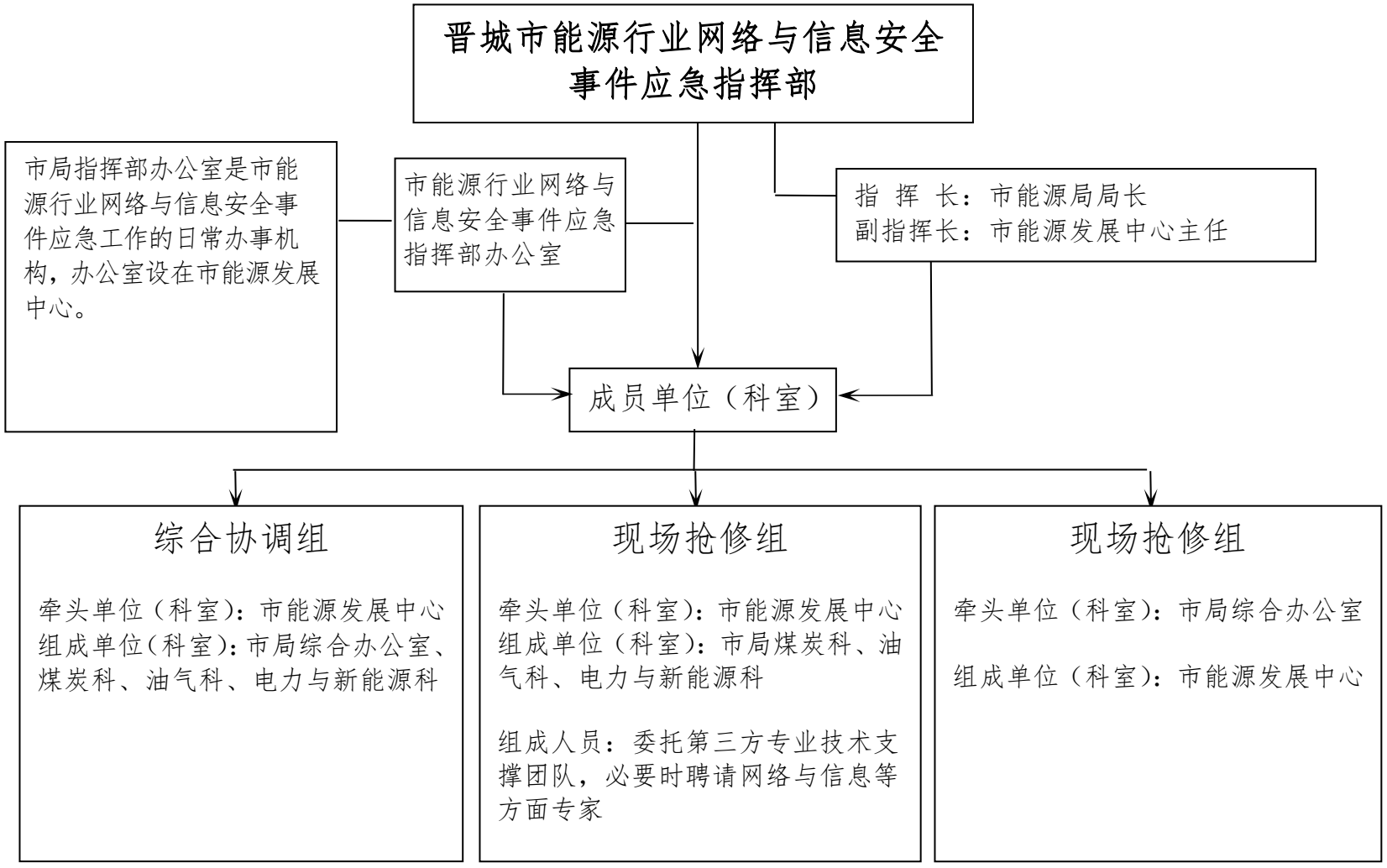
8.4 网络与信息安全事件分级

8.5 晋城市网络与信息安全事件上报表

8.6 晋城市能源行业网络与信息安全事件应急通讯录

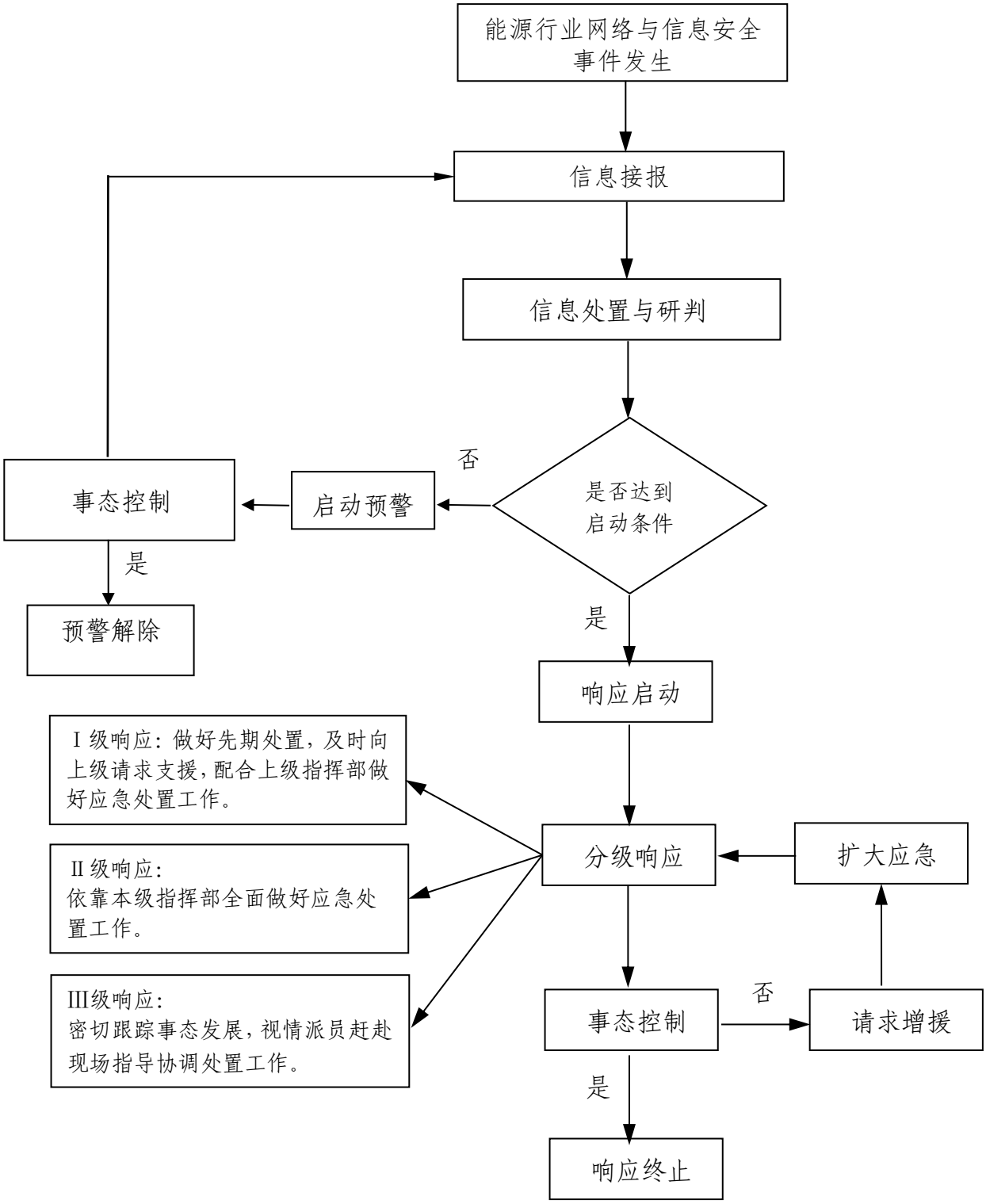
附录 8.1

晋城市能源行业网络与信息安全事件应急指挥部组织机构



附录 8.2

晋城市能源行业网络与信息安全事件应急处置流程图



附录 8.3

网络与信息安全事件分类

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。

附录 8.4

网络与信息安全事件分级

事件级别	可能的事件描述
特别重大网络与信息安全事件	重要网络与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。
	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。
	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。
重大网络与信息安全事件	重要网络与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。
	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。
	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。
较大网络与信息安全事件	重要网络与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。
	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。
	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。
一般网络与信息安全事件	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。

附录 8.5

晋城市能源行业网络与信息安全事件上报表

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（包括事件发生的原因、性质，初步原因和危害程度判断）:			
处置措施（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 8.6

晋城市能源行业网络与信息安全事件应急工作联络表

单位	值班电话	单位	值班电话
山西省能源局	0351-4041904	城区能源局	2286311
市委办公室	2062298	泽州县能源局	2028156
市政府办公室	2198345	高平市能源局	2355950
市委网信办	2566200	阳城县能源局	4232261
市大数据局	2218958	陵川县能源局	6202429
市科技局	2888666	沁水县能源局	7022019
市工信局	2218748	市局综合办公室	2061323
市公安局	3010100	煤炭科	2027123
市交通局	2023595	油气科	2061150
市应急局	2027255	电力与新能源科	2068037
市市场监管局	2022239	市能源发展中心	2032979
市委机要保密局	2198056	铁塔晋城分公司	6996000
市政府新闻办	2198741	联通晋城分公司	2034777
市国家安全局	2034918	移动晋城分公司	3035518
晋城军分区	2043211	电信晋城分公司	6997099