Q/NESC

中国电力工程顾问集团新能源有限公司企业标准

Q/NESC KX02002—2025

网络与信息安全应急管理办法

2025-11-21发布　　2025-11-21实施

中国电力工程顾问集团新能源有限公司　　发布

目　　次

编制说明			
版本	发布日期	主要规范事项	批准权属
V1	2025.11.21	本办法详细界定了公司网络与信息安全应急管理工作的各项职责、管理活动的具体内容与方法，以及所需的报告与记录要求。	公司办公会
主办部门		主要起草人	解释权属
科技信息部		柴雨、陈妙军、潘晶雯	科技信息部
修订记录			
版本	发布日期	修订内容	主要修订人

前 言

为规范公司突发网络与信息安全事件应急管理工作，提升公司应对突发网络与信息安全事件的应对能力，营造有利于企业发展的良好舆论环境，避免或减少不良社会影响，推进应急管理体系建设工作，特制定本管理办法。

本标准编写格式和表述规则符合公司Q/NESC 21602-2025《企业标准编写规则》的要求。本标准的附录A是规范性附录。

本标准由科技信息部归口管理。

本标准起草部门：科技信息部

本标准主要起草人：陈妙军

本标准校核人：柴雨 潘晶雯

本标准审核人：王永吉 李绍敬

本标准批准人：陈稼苗

本标准为第一次发布。

网络与信息安全应急管理办法

1. 总则

1.1 编制目的及依据

（一）编制目的

为规范和加强中国电力工程顾问集团新能源有限公司（以下统称公司）网络与信息安全的应急管理和应急响应程序，全面提高公司防范和应对各类突发网络与信息安全事件的能力，正确、有效、快速处置各类突发网络与信息安全事件，最大程度地预防和减少突发网络与信息安全事件及其造成的损害和影响，确保公司生产经营秩序的稳定可控，特制订本管理办法。

（二） 编制依据

《中华人民共和国网络安全法》（中华人民共和国主席令第53 号）

《中华人民共和国突发事件应对法》（中华人民共和国主席令第 69 号）

《中华人民共和国计算机信息系统安全保护条例（2011 修订）》（国务院令第 588 号）

《生产经营单位安全生产事故应急预案编制导则》 GB/T 29639-2020

《中国能源建设股份有限公司应急管理办法》中能建股发QHSE〔2022〕138号

《中国能源建设股份有限公司突发事件总体应急预案》中能建股发 QHSE(2022〕275号

《中国能源建设股份有限公司网络与信息安全突发事件应急预案》中能建股发科信〔2022〕298 号

《中国电力工程顾问集团有限公司突发网络与信息安全事件应急预案》电顾发科信〔2023〕36 号

1.2 适用范围

本预案适用于指导公司范围内的突发网络与信息安全事件应对工作，指导分公司及项目部突发网络与信息安全事件应急管理办法的编制和实施。

1.3 事件分类

突发网络与信息安全事件分为广域网链路故障事件、广域网或局域网网络设备故障事件、信息系统软硬件故障事件、信息系统信息破坏事件等。

（1）广域网链路故障事件主要为运营商链路故障事件。

（2）广域网或局域网网络设备故障事件主要为广域网、承载信息系统局域网的网络设备硬件或设备运行故障事件。

（3）信息系统软硬件故障事件分为信息系统服务器或存储设备的硬件故障事件、信息系统服务器的操作系统运行异常、系统的中间件运行异常、信息系统程序运行异常、数据库运行异常等故障事件。

（4）信息系统信息破坏事件分为信息泄露或丢失事件、信息窃取事件、信息篡改或假冒事件、非法或敏感言论信息事件和其他信息破坏事件。

1.4 响应分级

公司突发网络与信息安全事件按中断时间、对生产经营的影响程度、造成的经济损失等方面进行分

级，分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）和Ⅳ级（一般）。对照突发事件分级，公司应急响应分为二级，具体分级标准见附件1。

2. 组织机构与职责

2.1 突发网络与信息安全事件应急指挥小组及工作机构

公司应急管理领导小组下设突发网络与信息安全事件应急指挥小组，具体负责指挥协调突发网络与信息安全事件的管理与应对工作。

组长：分管科技信息部领导

成员：办公室(党委办公室、董事会办公室)、法务与合规部、企业发展部、人力资源部(组织人事部)、财务与产权管理部、规划与设计中心、安质环部、科技信息部等部门负责人。公司突发网络与信息安全事件应急指挥小组成员部门应急职责及联系方式见附件 2。

突发网络与信息安全事件应急指挥小组下设办公室，办公室设在公司科技信息部，办公室主任由公司科技信息部主任担任。办公室的主要职责：落实突发网络与信息安全事件应急指挥小组部署的各项任务；收集、汇总网络与信息安全事件相关信息，向突发网络与信息安全事件应急指挥小组汇报，与中电工程和政府有关监管机构沟通、汇报相关信息；按照突发网络与信息安全事件应急指挥小组决策，具体组织实施应急处置工作。

2.2 现场应急指挥部

网络与信息安全突发事件发生后，根据突发事件响应级别，公司、分公司或工程项目部在现场组建应急指挥部，具体负责现场应急指挥、协调、处置等职责。

现场应急指挥部设总指挥、副总指挥及综合协调组、故障处置组、技术支持组、舆情处置组等相关工作组。现场应急指挥部工作组及职责见附件3。

3. 应急响应

3.1 突发网络与信息安全事件应急响应流程

公司按照“分级负责、分类应对、快速反映、协调联动”原则，开展突发网络与信息安全事件应急响应。

3.2 信息接报与处置

（一）信息接报

1.突发事件信息

突发网络与信息安全事件发生后，涉及的分公司、工程项目部，要及时汇总、核实相关信息，并迅速报告。

发生一般事故（事件），分公司、工程项目部负责人应50分钟内电话报告至公司分管领导、专项应急指挥小组办公室和公司应急管理办公室，3小时30分钟时内书面报告；发生较大事故（事件），分公司、工程项目部负责人应40分钟内电话报告至公司分管领导、专项应急指挥小组办公室和公司应急管理

办公室，2小时20分钟内书面报告；发生重大及以上事故（事件），分公司、工程项目部负责人应15分钟内电话报告至公司分管领导、专项应急指挥小组办公室和公司应急管理办公室，50分钟内书面报告。

公司负责人接到突发事故（事件）信息后，应立即向中电工程分管领导、中电工程专项应急指挥小组办公室和中电工程应急管理办公室报告。

报告内容至少应包括：突发网络与信息安全事件发生的单位、时间、地点和事故性质、种类；

突发网络与信息安全事件涉及范围及经济损失情况；突发网络与信息安全事件发生的简要经过、事件初步原因以及采取的措施及效果；对突发网络与信息安全事件发展已经或可能造成的影响和风险；

信息报告的签发人及报告人的单位、姓名、职务和联系电话等。

2.预警信息

突发网络与信息安全事件应急指挥办公室应通过以下途径，获取预警信息：

经风险评估确定的可能发生的重特大突发网络与信息安全事件；

分公司、工程项目部上报的预警信息；

网络信息安全相关服务商和机构告知的预警信息；

其他来源的预警信息。

（二）信息处置与研判

网络与信息安全突发事件应急指挥办公室接到预警信息或事发分公司、工程项目部突发事件信息后，及时组织分析评估，研判发生的可能性、程度和影响范围，提出处置建议，及时向网络与信息安全突发事件应急指挥小组报告。

达到响应启动条件时，公司应急管理领导小组作出启动相应等级的应急响应决策后，突发网络与信息安全事件应急指挥小组启动应急响应。若未达到响应启动的条件，突发网络与信息安全事件应急指挥小组突发网络与信息安全事件作出预警启动决策，并做好响应准备，实时跟踪事态发展。根据事态发展，及时调整预警级别或响应启动。

3.3 预警

（一）预警启动

按照突发事故性质、严重程度、可控性和影响范围，预警分为四级，由高到低分别为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级。依次用红色、橙色、黄色、蓝色标示，红色为最高级别。

预警信息通过工作群、邮件、电话及内部网站等有效渠道及时发布，并根据情况变化适时调整预警级别。

预警信息的内容包括突发事件名称、预警级别、预警区域或场所、预警期起始时间、影响估计及应对措施、发布单位和时间等。

（二）响应准备

发布网络与信息安全突发事件预警信息后，公司、分公司、工程项目部应采取以下部分或全部措施:

1.开展应急值班，及时收集、报告广域网、信息系统、数据备份系统等运行有关信息，做好突发事件发生、发展情况的监测和事态跟踪工作；加强与政府相关部门的沟通，及时报告事件信息。

2.与本事件相关的应急技术支持力量(广域网服务商、电信运营商、网络设备服务商、信息系统开发商等)、内外部有关专家进入待命状态，动员 IT运维人员做好参加应急救援和处置工作的准备。

3.调集应急救援所需网络设备、服务器等，准备应急设施，确保其处于良好状态，随时可投入使用。

4.加强对重要系统、重要设备、重要数据备份情况、重要设施的巡视检查。

5.转移重要息系统数据、设备等。

6.做好其他启动应急响应准备工作。

（三）预警解除

根据事态变化和采取措施的效果，预警可以升级、降级或解除。根据已预警事件的发展，有关情况证明突发网络与信息安全事件不可能发生或危险已经解除，按照“谁启动，谁终止”的原则，由启动预警的应急管理机构解除预警。

3.4 响应启动

（一）一级响应(Ⅰ、Ⅱ级事故）

符合一级响应条件时，由公司应急管理领导小组启动一级响应。

公司网络与信息安全突发事件响应程序如下:

1.组织召开应急指挥小组会议，就有关重大应急处置问题作出决策和部署。

2.网络与信息安全突发事件应急救援指挥办公室立即进入24 小时应急值守状态，及时收集汇总事件信息，并按有关规定向上级主管部门汇报有关情况。

3.组织成立现场应急指挥部，迅速组织与突发事件相关的广域网服务商或电信运营商或网络设备服务商或信息系统开发商开展现场应急救援工作。

4.各成员部门按应急职责分工，落实应急指令，提供各项资源保障。

5.加强与政府有关部门联系沟通，必要时向政府部门提出援助请求。

6.协调解决应急处置中发生的其他问题。

现场应急指挥部响应程序如下：

1.根据公司网络与信息安全突发事件应急指挥小组指令进行现场应急指挥，针对事态发展制定和调整现场应急处置工作方案。

2.整合调配现场应急资源，组织与突发事件相关的广域网服务商或电信运营商或网络设备服务商或信息系统开发商开展应急救援、善后处置、调查、恢复网络或系统等应急处置工作。

3.按信息报送要求，及时向政府有关部门、公司等汇报应急处置情况。

4.分析舆情态势，制定网络与信息安全发布和宣传方案，做好媒体记者的组织和服务工作。

5.收集、整理应急处置过程有关资料，做好现场应急处置全过程记录。

6.核实应急状态解除条件，并向当地政府、公司网络与信息安全突发事件应急指挥小组请示应急状态解除。

事发单位（分公司、工程项目部）响应程序如下:

1.启动本单位网络与信息安全突发事件应急处置工作；

2.确定专人负责事件情况监测、信息收集和分析工作，按规定向公司报告事件最新进展。

3.整合调配现场应急资源，组织与突发事件相关的广域网服务商或电信运营商或网络设备服务商或信息系统开发商开展应急救援、善后处置、调查、恢复网络或系统等应急处置工作。

4.落实各项应急指令或协调解决应急处置中发生的其他问题。

（二）二级响应(Ⅲ、Ⅳ级事故）

符合二级响应条件时，由事发单位（分公司、工程项目部）应急管理领导小组启动级响应。

公司网络与信息安全突发事件应急指挥小组响应程序如下:

1.网络与信息安全突发事件应急指挥办公室及时收集汇总事件信息，并按有关规定向上级主管部门报送信息。

2.视情况组成工作组，指导应急处置工作。

3.应急指挥小组各成员部门按应急职责分工，落实应急指令，提供各项资源保障。

4.若突发事件超出事发单位（分公司、工程项目部）自身处置能力或事态有扩大发展趋势时，公司立即启动应急预案，提级响应。

3.5 处置措施

（一）广域网故障

1.广域网发生链路中断故障后，各单位应及时联系链路运营商，责成运营商尽快恢复或提出备份措施。

2.如广域网链路较长时间不能修复的，应组织进行广域网专线链路改为 VPN 的方式进行互联。

（二）广域网或局域网网络设备故障。

1.网络设备出现故障后，公司科信部技术负责人员应尽快定位具体的故障点。

2.如设备指示等明显异常，应进行重启网络设备等操作。如设备指示等正常，需要登录设备进行有关配置的排查。

3.如设备重启或者设备配置数据修复后仍不能恢复，需要对网络设备进行备件替换和调试工作。

（三）信息系统软硬件故障。

1.信息系统应做好系统应用程序、数据库的定期备份及恢复演练工作。

2.信息系统不能正常访问时，系统运维人员应尽快定位故障点，必要时应有系统开发商、系统基础软件或硬件集成商予以协助。

3.故障定位为信息系统的服务器、存储设备硬件原因时，需采用硬件重启、提供备用服务器等手段进行应急处置。

4.故障定位为信息系统的操作系统、应用程序、中间件、 数据库软件、数据库等原因时，需要采用热备切换、应急接管、重新部署有关软件环境、恢复数据库等手段进行应急处置。

（四）信息系统信息破坏事件

1.发生信息系统信息破坏事件后，应由技术人员研判取证后迅速将信息系统从网络中隔离。

2.隔离信息系统后，技术人员应结合系统日志、入侵检测设备等排查信息破坏缘由。

3.信息破坏来源排查清楚，且对信息系统漏洞、隐患等彻底修复后，才可通过恢复系统运行环境、恢复数据库等对信息系统有关信息进行修复。

4.信息破坏严重的，还需经研究后上报公安部门或中电工程。

3.6 应急支援

发生突发事件时，根据事件对社会和企业的影响程度，或在自身处置发生困难时，应报告上级主管部门，请求上级主管部门或政府启动社会应急机制，在地方政府统一领导下，组织开展应急救援与处置工作。

根据政府要求，积极参与社会应急救援，为突发事件应急救援工作提供人力、物资和技术装备支持。

3.7 响应终止

现场应急指挥部或事发单位在现场应急处置工作结束并确认危害因素消除后，向批准预案启动的应急管理组织机构提出结束现场应急处置工作的报告。按照“谁启动，谁终止”的原则，由相关应急管理组织机构决定并发布解除应急状态命令，转入常态管理。响应终止后，按照总体应急预案有关要求转入常态管理并开展善后处置、调查评估、恢复生产等后期处置工作。

4. 应急保障

4.1 应急队伍保障

公司、分公司及工程项目部应组建应急救援机构和完善应急救援处置队伍，加强应急队伍的业务培训和应急演练，强化员工应急能力建设，保证应急状态时能及时、有效地实施救援。

公司、分公司及工程项目部宜建立外部支援机制，与地方应急力量建立联动机制，确保应急期间的医疗救治、消防、治安保卫、交通维护和运输等应急力量到位。

4.2 应急物资保障

公司、分公司及工程项目部应组建应急救援机构和完善应急救援处置队伍，加强应急队伍的业务培训和应急演练，强化员工应急能力建设，保证应急状态时能及时、有效地实施救援。

依据突发网络与信息安全事件应急处置的需求，公司、分公司及工程项目部应建立健全突发网络与信息安全事件应急物资供应保障体系，备有有关网络硬件、服务器、软件及其他应急物资。一旦发生突发网络与信息安全事件，进行统一调配。重要信息系统应建立有数据备份、应急接管的有关备份及恢复措施，以备应急处置。

4.3 其他保障

公司、分公司及工程项目部应根据实际情况，做好通信与信息保障、经费保障等其他保障。

5. 附则

本预案由公司突发网络与信息安全事件应急救援指挥小组办公室负责解释，自发文之日起实施。

附 录 A
（规范性附录）表格样式
表 A.1 公司突发网络与信息安全事件应急响应分级标准

响应级别	事件级别	分级标准
一级响应	Ⅰ级（特别重大）	1.广域网或信息系统中断对公司生产经营活动造成特别重大的影响。 2.信息系统中的数据丢失或被窃取、篡改、假冒，对国家、公司安全和社会稳定构成特别严重威胁。 3.通过网络传播反动信息、煽动性信息、涉密信息、谣 言等，对国家、公司安全和社会稳定构成特别严重危害的事件。 4.其他对国家和公司安全、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突发网络与信息安全事件。
	Ⅱ级（重大）	1.广域网或信息系统中断对公司生产经营活动造成严重影响。 2.信息系统中的数据丢失或被窃取、篡改、假冒，对国家、公司安全和社会稳定构成严重威胁。 3.通过网络传播反动信息、煽动性信息、涉密信息、谣言等，对国家、公司安全和社会稳定构成严重危害的事件。 4.其他对国家和公司安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的突发网络与信息安全事件。
二级响应	Ⅲ级（较大）	1.广域网或信息系统中断对公司生产经营活动造成较为严重影响。 2.信息系统中的数据丢失或被窃取、篡改、假冒，对国家、公司安全和社会稳定构成较为严重威胁。 3.通过网络传播反动信息、煽动性信息、涉密信息、谣言等，对国家、公司安全和社会稳定构成较大危害的事件。 4.其他对国家和公司安全、社会秩序、经济建设和公众利益构成较大威胁、造成较为严重影响的突发网络与信息安全事件。
	Ⅳ级（一般）	1.广域网或信息系统中断对公司生产经营活动造成一定影响。 2.信息系统中的数据丢失或被窃取、篡改、假冒，对国家、公司安全和社会稳定构成一定威胁。 3.通过网络传播反动信息、煽动性信息、涉密信息、谣言等，对国家、公司安全和社会稳定构成一定危害的事件。 4.其他对国家和公司安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的突发网络与信息安全事件。

表A.2　公司突发网络与信息事件应急指挥小组成员部门职责及联系方式

职能部门	应急职责	联系方式
办公室(党委办公室、董事会办公室)	是突发网络与信息安全事件的应急管理协管部门。负责应急救援信息传递；上级及相关单位协助救援及调查人员的接待；为应急救援人员提供交通保障；参与突发网络与信息安全事故事件调查处理。	010-83017200
法务与合规部	指导公司、分公司、工程项目部做好突发事件处置法律保障等相关工作。	010-83017290
人力资源部(组织人事部)	配合突发网络与信息安全事件 的应急处置工作；指导事故事件单位做好善后处置及保险理赔等 相关工作；参与突发网络与信息安全事故事件调查处理。	010-83017211
财务与产权管理部	指导事故事件单位做好资产处置、商业保险 理赔及财力保障等相关工作；参与突发网络与信息安全事故事件调查处理。	010-83017222
企业发展部	协助做好突发网络与信息事件的应急处置工作。	010-83017300
安质环部	协助做好突发网络与信息事件的应急处置工作。	010-83017280
科技信息部	是公司网络与信息安全管理部门和突发网络与信息安全事件应急管理的分管部门，负责突发网络与信息安全事件应急管理的日常工作；负责组织应急专家组为应急救援工作提供技术支持；负责应急管理系统的正常运转并保持信息畅通；负责公司突发网络与信息安全事件应急预案的编制、评估、备案、培训和演练；负责突发网络与信息安全事件的应急 处置；组织或参与突发网络与信息安全事件的调查处理。	010-83017373
其他部门	根据突发事件应急处置工作需要，协调做好相关工作。	

表A.3 现场应急指挥部工作组及职责

工作组	应急职责
综合协调组	负责各应急工作组之间的协调组织和沟通，事故信息的汇总与上报；负责应急工作善后处置及后勤保障工作。
故障处置组	负责组织实施应急处置、抢险、通信及信息设备设施修复、通信安全保障等工作。
技术支持组	负责制定应急处置技术措施和方案，为应急救援提供技术支持。
舆情处置组	负责收集、跟踪舆论信息分析舆情态势，分析突发事件应急处置的相关法律责任，提供法律支持;落实应急救援指挥部决定的重大事项。

表A.4　政府部门、上级单位应急联系电话

单位名称	值班室电话
北京市西城区应急管理局	010-83975375
中国能源建设股份有限公司	010-59099999
中国电力工程顾问集团有限公司 应急管理办公室	010-83011133
中国电力工程顾问集团有限公司 突发网络与信息事件应急指挥办公室	010-83011176
公安部门	110
消防部门	119
医疗急救	120