

郑州海关网络安全事件应急预案

1 总则

1.1 编制目的

建立健全郑州海关网络安全应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件对海关业务工作造成的损失和危害，保障关区正常的执法和办公秩序。

1.2 编制依据

根据《中华人民共和国网络安全法》《中华人民共和国海关法》《中华人民共和国突发事件应对法》《海关网络安全事件应急预案》等，制定本预案。

1.3 适用范围

本预案所指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（详见附件1）。

本预案适用于关区非涉密网络安全事件的应对工作。其中，有关信息内容安全事件，另行制定预案。涉及国家秘密的网络安全事件的应对工作，由主管部门根据国家有关要求组织开展。

1.4 事件分级

海关网络安全事件根据危害程度和影响范围分为四级：I 级（特别重大网络安全事件）、II 级（重大网络安全事件）、III 级（较大网络安全事件）和 IV 级（一般网络安全事件）。其中，I 级（特别重大网络安全事件）、II 级（重大网络安全事件）划分标准及处置流程参照《海关网络安全事件应急预案》执行。

结合关区实际，郑州海关关区网络安全事件分为 III 级（较大网络安全事件）和 IV 级（一般网络安全事件）。

1.4.1 III 级网络安全事件

符合下列条件之一的，为 III 级网络安全事件：

（1）发生海关业务数据被窃取、篡改的。

（2）海关业务网终端同时感染同一种恶意程序的终端总数达到全关区业务网终端总数 50% 以上，或同时感染同一种破坏性极强恶意程序的终端总数达到关区业务网终端总数 20% 以上的。

（3）海关业务网信息系统被外部入侵并控制 2 小时以上的。

（4）其他对国家安全、社会秩序、经济建设和公众利益构成较大威胁、造成较大影响的网络安全事件。

1.4.2 IV 级网络安全事件

（1）全关区的核心业务在业务高峰期中断（或运行效率明显下降）2 小时以上。

(2) 其他对国家安全、社会秩序、经济建设和公众利益构成一定威胁和影响,但未达到 III 级事件标准的网络安全事件为一般网络安全事件(IV 级)。

1.5 工作原则

网络安全事件应急工作,应当遵循预防为主、常备不懈的方针,贯彻统一领导、快速反应、属地负责、分级处置、协同配合的原则。

1.5.1 统一领导

网络安全事件应急工作启动、处置对策、对外联络、队伍调动、物资调配等均由网络安全事件应急指挥部做出决策,各单位必须坚决服从应急指挥部的指令。

1.5.2 快速反应

建立预警、应急响应和处置快速反应机制,确保各环节的衔接,做好人力、物力、财力储备,增强应急处理能力,保证一旦出现网络安全事件,能够迅速启动应急处置。

1.5.3 属地负责

网络安全事件应急处置实行条块结合、以块为主、属地管理。各级海关单位对本单位的网络安全事件应急处置具体负责。

1.5.4 分级处置

根据海关行政管理层级和网络安全事件发生的影响范围、性质和危害程度，分等级进行防控、处置。发生不同等级网络安全事件时，启动相应级别的应急响应。

1.5.5 协同配合

根据网络安全事件的性质和影响范围，应加强与相关海关单位、地方政府、有关部门等相关主管单位的密切协作，形成资源共享、优势互补的联动配合机制。

2 组织指挥机制

2.1 领导机构

在郑州海关网络安全和信息化领导小组领导下，按照行政管理层级，建立郑州海关、隶属海关两级网络安全事件应急指挥体系，负责指挥和协调网络安全事件应对工作。

2.2 郑州海关网络安全事件应急指挥部（以下简称“关应急指挥部”）构成

总指挥：由主管科技部门的关领导担任。

副总指挥：由科技处主要负责人担任。

成员单位：科技处、办公室、法规处、综合业务处、关税处、卫生检疫处、动植物检疫处、进出口食品安全处、商品检验处、口岸监管处、统计分析处、企业管理和稽查处、财务处、人事教育处、后勤管理中心、风险防控分局、数据分中心、技

术中心、保健中心等。视突发事件的类型、严重程度和影响范围等情况，成员单位可适当调整或增减。

关应急指挥部下设办公室（以下简称“关应急指挥办”），具体工作由科技处承担。关应急指挥办依托海关内、外部网络安全专家组建专家队伍，为网络安全事件的预防和处置提供技术咨询和决策建议，并充分发挥专家在应急处置工作中的作用。

关应急指挥部下设应急工作组，由科技处、数据分中心相关技术人员组成，视情况增加外部机构专家。

隶属海关的应急指挥部及其成员构成可参照关应急指挥部的形式组建。

2.3 工作职责

2.3.1 关应急指挥部职责

负责统一领导郑州海关网络安全事件的应对工作。包括：

（1）负责建立郑州海关关区监测预警、应急处置和应急响应机制，发布网络安全事件预防警报，组织实施网络安全事件应急处置。

（2）决定启动和终止应急预案。

（3）负责海关内外部跨部门的组织协调工作。

（4）统一指挥调配关区内的应急资源。

（5）组织应急工作组的应急处置行动。

（6）向总署应急指挥部办公室报告有关情况。

（7）研究新闻发布方案。

（8）组织网络安全事件的调查与总结工作。

2.3.2 关应急指挥部各成员单位主要职责

（1）科技处：承担总关应急指挥部办公室工作。

（2）办公室：负责对外信息发布和舆情监测等工作。

（3）法规处：负责网络安全事件应急工作的法律支持等工作。

（4）财务处：负责应急资金及装备设备的保障和调配。

（5）人教处：负责网络安全事件应急工作人员的奖惩和培训支持等工作。

（6）后勤管理中心：负责应急处置中的后勤保障等工作。

（7）数据分中心：负责协助总关应急指挥部办公室承担网络安全事件应急管理事务性工作。

(8)各业务处室：负责协调网络安全事件引发的业务应急处置工作。

2.3.3 关应急指挥办职责

负责关区网络安全事件应急管理日常工作，负责网络安全事件应急管理中跨部门、跨单位的综合协调工作，负责网络安全事件应急预案的制定、完善、宣传培训及检查评估等工作，对口海关总署和地方网络安全应急办公室。

2.3.4 关应急工作组职责

负责预警监测、预警研判、预警信息初拟及上报、预警响应、网络安全事件的初步研判及报告，提出处置措施，做好应急响应，承担应急指挥部下达的各项现场应急处置任务，及时通报事件处置情况。

各隶属海关单位、数据分中心的应急指挥部成员单位、办公室及应急工作组职责参照关应急指挥部相关单位职责确定。

3 监测与预警

3.1 预警分级

依据关区内网络安全事件可能造成的危害程度、发展情况和紧迫性等因素，预警级别由高到低依次用黄色和蓝色表示，分别对应发生或可能发生较大(Ⅲ级)和一般网络安全事件(Ⅳ级)。

3.2 预警监测

科技处负责组织指导关区网络安全预警监测工作，各信息

系统运行单位负责对本单位运行的网络和信息开展网络安全监测工作，重要信息及时报告科技处。

监测信息范围主要包括：

- （1）国家有关部门发布或向海关通报的信息。
- （2）国家及地方网络安全信息共享机制共享的信息。
- （3）海关总署发布的信息。
- （4）系统监控、巡检发现的信息。
- （5）海关工作人员或企业等外部人员发现并报告的信息。
- （6）网络安全事件处置过程中发现的信息。
- （7）网络安全风险评估活动中发现的信息。
- （8）其他信息。

3.3 预警研判和发布

III 级（黄色）、IV 级（蓝色）突发事件预警发布、变更或取消由关应急指挥部负责。关应急指挥办组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时向关应急指挥部报告，并根据监测研判情况发布预警信息。

III 级（黄色）、涉及 2 个以上隶属单位的 IV 级（蓝色）突发事件预警范围为全关区。

仅涉及个别隶属单位的 IV 级（蓝色）预警，由关应急指挥办指导相关单位自行发布或取消。如需提高预警级别，应及时提出预警升级建议，报关应急指挥部决定。

关应急指挥办及相关单位要密切关注事件进展情况，根据

事态变化情况，适时调整预警级别，并将调整结果及时宣布、通报相关单位。

预警信息发布应包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

3.4 预警响应

对于红色、橙色预警，根据总署统筹安排做好响应工作。对于国家网络安全应急办公室、海关总署发布的黄色、蓝色预警，河南省网络安全应急办公室发布的预警，由关应急指挥办统一组织开展响应工作。

关区内其他地级市（或区县）网络安全应急办公室发布的预警，由所在地隶属海关应急指挥部办公室报告关应急指挥办，并在关应急指挥办指导下组织开展响应工作。

预警通报发布后，相关单位应依据发布的预警级别，加强网络与信息系统安全状况的监测，做好应急处理准备工作。

3.4.1 蓝色预警响应：

相关单位应加强监控，密切关注事态发展，重要信息及时报告关应急指挥办。

3.4.2 黄色预警响应：

（1）关应急指挥办保持通信联系畅通，密切关注事态发展，收集、汇总监测信息，重要信息及时向单位领导、上一级应急指挥部办公室报告。

(2)关应急指挥办加强网络安全事件监测和事态发展信息搜集工作，重要信息及时报告科技司。

(3)应急工作组应立即根据预警信息明确影响范围、开展网络安全风险评估、根据预警事件类别实施控制措施、控制事态发展。

3.5 预警变更与解除

关应急指挥办及相关单位要密切关注事件进展情况，根据事态变化情况，适时调整预警级别，及时通报调整结果。

构成预警事件的要素消失或得到控制后，预警发布单位应及时解除预警状态。

4 应急处置

4.1 事件级别初步判断与核定

网络安全事件发生后，海关网络安全事件级别由事发地海关单位进行初步判断。I、II级网络安全事件由总署应急指挥部办公室核定，III、IV级事件网络安全事件由事发地海关单位应急指挥部办公室核定。

4.2 情况报告

4.2.1 报告原则

(1)“即现即报”原则：一旦发现有网络安全事件发生，须注意保存证据，按照报告程序要求立即向上级应急指挥部办公室报告。

(2)“核实准确”原则：报告内容要客观真实，重点要素

要准确，不得主观臆断。

（3）“双线同步”原则：事发地海关在按规定向上一级应急指挥部办公室报告网络安全事件的同时，可视事件的性质、特点和影响范围，通报当地有关部门。

（4）“追踪反馈”原则：事发地海关应将网络安全事件的原因、变化动态、应急措施、处置结果等情况及时向上级应急指挥部办公室报告。

4.2.2 报告程序

（1）发生网络安全各类突发事件，事发地海关应于 15 分钟内通过电话或报障平台报告关应急指挥办，2 小时内以书面形式报告。正常情况下，突发事件报告须经事发地单位领导审批，单位领导来不及书面审批的情况，应由单位领导口头批准，由值班人员或指定人员直接上报。

（2）关应急指挥办在初步判断发生Ⅲ级事件后 30 分钟内，将有关情况向本关领导和总署应急指挥部办公室（科技司）及应急指挥部相关成员单位报告，24 小时内以书面形式报告科技司。

（3）关应急指挥办在初步判断发生Ⅳ级事件后，事发地海关需在 30 分钟内，将有关情况向本单位领导和关应急指挥办报告，24 小时内以书面形式报告关应急指挥办。

4.2.3 报告形式

4.2.3.1 电话报告

(1)电话报告的“六个要素”：网络安全事件发生的时间、位置、事由、现状、影响、已采取的措施。其中，时间报告要精确到分，位置要明确具体口岸、现场及信息系统。

(2)具备条件的情况下,接报人员必须填写电话报告记录。

4.2.3.2 文字报告

文字报告应采用固定报送载体，应当由单位领导签发，注明承办人姓名和联系电话，标明缓急程度、发送时间和报告编号。内容要条理清楚，语句简洁，重点突出。

(1)网络安全事件详细情况,包括事件发生的时间、位置、过程、状况、原因、影响等。

(2)事发地海关已经采取的措施及效果。

(3)事态发展预测和下一步行动计划，如需上级单位提供支持，还需提出相应处置建议。

4.3 应急响应

4.3.1 响应分级

对应郑州海关网络安全事件的两个等级将应急响应分为两个级别：III级和IV级应急响应。根据不同事件核定级别，启动相应级别的应急响应。

4.3.2 启动程序

4.3.2.1 III级应急响应启动程序如下：

(1) 关应急指挥办结合应急指挥部组成单位建议提出 III 级应急响应启动建议，报请总指挥（或授权副总指挥）批准。

(2) 总指挥（或授权副总指挥）批准后，启动 III 级应急响应；

(3) III 级应急响应宣布后，关应急指挥办成员首先到位，并通知成员单位负责人就位进入应急指挥状态；

(4) III 级应急响应启动后，郑州海关应急指挥部及其办公室和相关成员单位应保持 24 小时联系畅通，根据职责分工开展应急工作；

(5) 关应急指挥办通报相关单位做好协同应急处置准备。

4.3.2.2 IV 级应急响应启动程序如下：

(1) 关应急指挥办结合应急指挥部组成单位建议提出 IV 级应急响应启动建议，报请副总指挥批准。

(2) 副总指挥批准后，启动 IV 级应急响应；

(3) IV 级应急响应宣布后，关应急指挥办成员首先到位，并通知成员单位负责人就位进入应急指挥状态；

(4) IV 级应急响应启动后，关应急指挥办和涉及单位应急指挥部及其办公室和相关成员单位应保持 24 小时联系畅通，根据职责分工开展应急工作。

4.3.3 处置阶段

(1) 控制事态。应急工作组应针对事件进行紧急处置，控制事态，以防止事件进一步扩大；及时寻求电力、通信等服务

和设备供应商紧急支援；必要时报告应急指挥部申请启动相应的业务应急预案。

（2）升级处置。根据事态发展，若事件超出本级应急指挥部的处置能力，需要更多的部门和单位参与处置时，应及时报告上一级应急指挥部组织、协调其他有关部门及单位参与处置工作。

（3）做好处置消除隐患。应急工作组根据事件发生原因，有针对性的采取措施，恢复受破坏信息系统正常运行，并做好异常数据处理等善后工作。

（4）加强沟通。应急工作组应在事件处置过程中及时与事发地海关沟通确认事件影响，通报处置情况。

（5）做好处置记录。应急工作组在应急恢复过程中应保留有关证据，做好处置记录。处置记录应条理清楚，内容详实。

4.3.4 分类处置

应急工作组应当根据事件的分类，采取有针对性的处置措施，可协调外部组织进行技术协助，并在处置过程中保持与应急指挥办及有关部门的联系。

（1）有害程序事件

对于病毒及破坏性程序蔓延事件，应急工作组应分析有害程序，保护现场，阻断有害程序蔓延途径，必要时切断相关网络连接。应急工作组在有害程序大面积清除前，应制定有害程序清除方案，对方案进行验证，减少对业务的影响，尽快清除

有害程序并恢复受影响网络和信息系统的正常运行。

（2）网络攻击事件

应急工作组通过入侵检测和安全审计等手段确定攻击方法，采取措施保护现场，阻止攻击行为进一步造成危害，尽快恢复受影响网络和信息系统的正常运行，并对现场进行全面勘查取证，查明网络攻击来源。

（3）信息破坏事件

应急工作组应采取有效措施，阻断数据外泄渠道，保护现场，分析判断，查明数据泄露、窃取和丢失的途径及窃取对象。

（4）设备设施故障事件

应急工作组按照《海关信息系统故障管理规程》对设备设施故障进行处理。

（5）灾害性事件

应急指挥办及工作组应对事件进行内部和外部紧急通报，采取措施尽快恢复网络和信息系统的正常运行，并协调外部组织协助对网络和信息系统的受损情况进行调查，并对灾害性事件进行评估，充分评估涉及部门、业务范围和社会影响。

（6）其他网络安全事件

对于其他网络安全事件，特别是业务、系统、设备具备特殊性的网络安全事件的处理，应急工作组应按照专门的应急措施处置。

4.4 应急结束

应急指挥部确认网络安全事件已得到控制或取得预期处置结果后，可宣布应急行动结束，及时通报有关单位和部门。

4.5 后续处理

关应急指挥办负责牵头组织有关部门对事件的起因、性质、影响、责任等进行分析，提出处理意见和改进措施，撰写总结报告。对于 III 级事件，事件涉及单位应于事件结束后 3 个工作日内向关应急指挥办报送书面总结报告；关应急指挥办于 10 个工作日内完成总结报告并上报总署相应应急指挥部办公室。对于 IV 级事件，事件涉及单位应于事件结束后 10 个工作日内完成总结报告并报关应急指挥办存档备案。

事发地海关单位应根据突发事件的经验教训，及时完善有关防范预警和应急处置的方案及措施。

4.6 信息发布

针对 III 级、IV 级事件，关应急指挥办会同关办公室研究制定新闻报道方案和对外答复口径，报关领导批准后统一进行发布。

仅个别隶属单位发生的 IV 级事件，对外发布和舆情监测应根据郑州海关新闻宣传有关规定，按程序上报关办公室，不得擅自对外发布。

5 应急预案管理

5.1 预案管理

根据国家相关法律、法规和海关系统应急管理工作的规定，

结合实际情况适时修订本预案。

各隶属海关可依照本预案制订本级预案。

5.1.1 监督检查

关应急指挥办会同有关部门不定期对关区应急预案的执行情况进行检查评估，查找问题和提出改进意见。各隶属海关应加强对本级预案的检查评估。

5.1.2 修订与更新

有下列情形之一的，应当及时对本预案进行修订：

（1）本预案所依据的相关法律、行政法规、规章制度及上位预案等有关规定发生变化的；

（2）应急指挥机构及其职责发生重大调整的；

（3）面临的风险、重要应急资源或预案中的其他重要信息发生变化的；

（4）在网络安全事件实际应对和日常应急演练中发现问题需要做出重大调整的；

（5）其他经核准需对本预案进行修订的情况。

5.2 日常管理

各单位应按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

5.3 演练

定期举行不同类型的应急演练，以检验、改善和强化应急准备和应急响应的能力。应急演练由关应急指挥办组织实施，一般每年举行一次，并将演练情况报郑州海关应急指挥部和总署应急指挥部办公室。

5.4 宣传

各单位应充分利用各种传播媒介及其他有效的宣传形式，加强网络安全事件预防和处置的有关法律、法规 and 政策的宣传，开展网络安全基本知识和技能的宣讲活动。

5.5 培训

各单位要将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全事件应急预案的培训，提高防范意识及技能。

5.6 重要活动期间的预防措施

在国家重要活动、会议期间，各单位要加强网络安全事件的防范和应急响应，同时加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位做好值班工作，及时发现和处置网络安全事件隐患。

5.7 责任与奖惩

郑州海关网络安全事件应急处置工作的责任与奖惩依照《海关系统突发事件应急预案》的相关规定办理。

6 保障措施

6.1 机构和人员

各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

关应急指挥办应建立本单位应急指挥部成员、部门负责人、应急工作组人员名册和联络方式。应建立与处置各类网络安全事件有关的政府部门、机构、专家、设备供应商等的联系渠道，建立社会化应急联络保障机制，并经常更新通讯录，确保联系畅通。

6.2 基础平台

海关信息系统运行管理平台和海关信息系统安全管理中心是海关网络安全事件应急管理工作的日常管理平台，海关监控指挥中心是海关网络安全事件应急管理工作的指挥平台，海关网络安全事件应急管理工作的沟通协调应当通过统一通信系统开展。各单位应当加强相关系统的日常运维管理，落实责任，做到早发现、早预警、早响应，提高应急处置能力。

6.3 经费保障

各单位应加强对网络安全应急装备、工具的储备，及时调整、升级软硬件工具，不断增强应急技术支撑能力。

网络安全应急工作所需资金在年度海关科技经费预算中统筹安排，支持网络安全应急工作组建设、预案演练、应急物资保障、网络安全事件培训、网络安全事件预防、重要活动期间安全保障等工作开展。

7 附则

7.1 解释

本预案由郑州海关负责解释。

7.2 实施

本预案自发布之日起实施。