伊宁海关信息系统突发事件应急预案

1　总则

1.1 目的及依据

为提高我关处置网络与信息安全突发公共事件的能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络与信息安全突发公共事件造成的危害，维护正常的通关贸易秩序，根据《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《海关总署突发事件应急预案》和《乌鲁木齐海关突发事件应急处理预案》的相关规定，制订本预案。

1.2 事件分类及级别

本预案所称网络与信息安全突发事件，是指重要信息系统突然遭受不可预知外力的破坏、毁损、故障，发生对国家、社会、公众造成或者可能造成重大危害，危及公共安全的紧急事件。

1.2.1　事件分类

根据网络与信息安全突发事件的发生过程、性质和机理，网络与信息突发公共事件主要分为以下三类：

（1）自然灾害。指地震、台风、雷电、火灾、洪水等引起的网络与信息系统的损坏。

（2）事故灾害。指电力中断、网络损坏或由于软件、硬

件设备故障等引起的网络与信息系统的损坏。

（3）人为破坏。指人为破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等引起的网络与信息系统的损坏。

1.2.2　事件分级

根据网络与信息安全突发事件的可控性、严重程度和影响范围，一般分为四级：I 级（特别重大）、II 级（重大）、III 级（较大）和 IV 级（一般）。国家有关法律法规有明确规定的，按国家有关规定执行。

（1）I 级（特别重大）。重要网络与信息系统发生全局性大规模瘫痪，事态发展超出我关和主管部门的控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发事件。

（2）II 级（重大）。重要网络与信息系统发生全局性瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害，需要跨部门、跨地区协同处置的突发事件。

（3）III 级（较大）。某一重要网络与信息系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但不需要跨部门、跨地区协同处置的突发事件。

（4）IV 级（一般）。重要网络与信息系统受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的突发事件。

1.3 适用范围

本预案适用于涉及市的 I 级、II 级、III 级网络与信息突发事件

和可能导致I级、II级、III级网络与信息安全突发事件的应对工作。

本预案适用于伊宁海关各监管现场以及办公场所。

2 组织管理机构及职责

2.1 组织体系

统一领导，分级负责。在关领导的统一领导下，建立健全分级负责、条块结合、属地管理为主的应急管理体制，按照“谁主管谁负责、谁运营谁负责”的原则，建立和完善日常安全管理责任制。相关部门根据工作职能和本预案规定，各司其职，做好日常管理和应急处置工作。伊宁海关成立信息系统突发事件应急指挥小组（以下简称：指挥小组），负责统一指挥、协调处理各种突发事件。

组　长：关长

副组长：副关长

成　员：各部门负责人

应急指挥小组下设应急办公室、业务应急小组、技术应急小组、对外协调小组。

2.2 工作职责

2.2.1 应急办公室

指挥小组下设应急办公室（设在伊宁海关办公室，电话0999—8073004），负责具体协调处理突发事件，收集突发事件信息，提出参考处置意见报指挥小组审批实施。

2.2.2 业务应急小组

业务应急小组由各业务科组成：负责处置突发事件中的业

务问题，按照既定应急处理模式和流程处置突发事件，追踪督促、检查突发事件过后的业务善后处理工作。

2.2.3 技术应急小组

技术应急小组由综合业务科组成：负责处置突发事件中的技术问题，组织人员排除故障，确保信息系统安全运行。

2.2.4 对外协调小组

对外协调小组由关办公室组成：负责处理突发事件中的对外协调、对外宣传、对外告示以及必要时召开新闻发布会等事项。

3 监测、报告、预警和先期处置

3.1 信息监测与报告

（1）重要信息系统主管部门要制定和完善网络与信息安全突发事件监测、预测、预警、通报制度。按照“早发现、早报告、早处置”的原则，加强对各类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的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发事件时，在按规定报告的同时，按紧急信息报送的规定及时向总关通报。初次报告最迟不得超过 2 小时，重大和特别重大的网络与信息安全突发事件实行即时报告、态势变化进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

（2）依托信息网络突发事件应急信息通报与预警监测平台，整合现有的报警接警资源，全天候 24 小时运作，实行网

络与信息安全突发事件的统一接警,保证信息通报和联系渠道畅通。

（3）重要信息系统主管部门及相关负责人员应确定 2 个以上的即时联系方式，关员可通过固定电话、移动电话、互联网等多种联系方式进行报警。

3.2 预警处理与预警发布

（1）对于可能发生或已经发生的网络与信息安全突发事件，事发单位应立即采取措施控制事态，进行风险评估，判定事件等级并在本系统发布预警。必要的应启动相应的预案，同时向总关通报。

（2)各小组在接到报警信息后应及时组织有关人员对信息进行技术分析、研判，根据问题的性质、危害程度，提出安全警报级别，并及时向指挥小组报告，其中 I 级、II 级、III 级网络与信息安全突发事件还须在事发后 4 小时内向总关报告。

（3）指挥小组接到报告后，应及时对信息作出判断，提出处理意见。发生和可能发生 I 级、II 级 和 III 级的网络与信息安全突发事件时，应迅速召开协调小组会议，研究确定网络与信息安全突发事件的等级，决定启动本预案，并确定指挥人员。

（4）需要向社会发布预警的网络与信息安全突发事件，由指挥小组通过广播、电视、信息网络等方式及时发布预警信息。根据其可能造成的危害程度、紧急程度和发展态势，预警级别分别用蓝色（一般）、黄色（较重）、橙色（严重）和红色

（特别严重）来表示。预警信息应包括事件的类别、可能波及的范围、可能危害的程度、可能延续的时间、提醒事宜和应采取的措施等。

（5）各相关应急联动机构应根据发布的预警信息，做好相应的网络与信息安全应急保障准备工作。

3.3 先期处置

（1）当发生网络与信息安全突发事件时，事发地应做好先期应急处置工作，立即采取措施控制事态，同时向相关主管小组通报。

（2）相关主管小组在接到本系统网络与信息安全突发事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展态势。对 IV 级网络与信息安全突发事件，由主管部门自行负责应急处置，并将有关情况向指挥小组通报。对有可能演变为 III 级、II 级或 I 级的网络与信息安全突发事件，要为指挥小组处置工作提出建议方案，并做好启动本预案的各项准备工作。指挥小组要根据网络与信息安全突发事件发展态势，视情况决定赶赴现场指导、组织派遣应急支援力量，支持事发地做好应急处置工作。

4 应急处置

4.1 应急指挥

（1）本预案启动后，根据指挥小组会议的部署，担任总指挥的领导和参与指挥的有关科室负责人迅速赶赴相应的指挥平台，启动指挥系统。相关联动部门按照本预案规定的有关

职责立即开展工作。

要迅速建立与现场指挥的通讯联系，要及时掌握现场处置工作状态，分析事件发展趋势，研究提出处置方案，调集和配置应急处置所需要的人、财、物等资源，统一指挥网络与信息安全应急处置工作。

（2）需要成立现场指挥部的，事发地立即在现场开设指挥部，并提供现场指挥的相关保障。现场指挥部要根据事件性质迅速组建各类应急工作组，根据指挥小组的要求全权负责现场的应急援救工作。

4.2 应急支援

本预案启动后，指挥小组立即组织应急响应工作小组赶赴事发地点，督促、指导和协调处置工作。指挥小组办公室根据事态的发展和处置工作的需要，及时增派专家小组和应急支援人员，调动必需的物资、设备，支援应急工作。

参加现场处置工作的各小组要在现场指挥部统一指挥下，协助开展处置行动。

4.3 信息处理

（1）现场信息收集、分析和上报。相应主管部门应对突发事件进行动态监测、评估，并按指挥小组紧急信息报送的有关规定，及时将事件的性质、危害程度、造成的损失及处置工作等情况报送给指挥小组办公室，不得瞒报、缓报、谎报。

（2）指挥小组办公室要明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告等工作。

信息编发和研判。要及时编发事件动态信息供领导参阅；组织有关人员研判各类信息，研究提出对策措施，完善应急处置计划方案。

信息报告。要根据有关规定做好向总关的信息上报工作。上报的信息必须经总指挥或其授权代表签发。

信息通报。指挥小组办公室应及时将网络与信息安全突发事件的有关情况向市有关部门进行通报。

（3）信息发布与咨询。在应急处置期间，指挥小组办公室要按国家的有关规定和程序及时进行信息发布与新闻报道。密切关注国内外关于网络与信息安全突发事件的新闻报道，对媒体关于事件以及处置工作的不正确信息，及时进行澄清。必要时开通咨询热线，接受群众咨询，释疑解惑，稳定人心。

4.4 应急结束

网络与信息突发事件经应急处置得到有效控制后，由指挥小组办公室提出应急结束的建议，经指挥小组批准后实施。

4.5 具体技术故障事件的处置

具体技术故障事件是指由于服务器硬件、服务器操作系统、数据库系统、应用软件、磁盘存贮设备、网络交换机（包括骨干交换和接入交换）、网络通信线路、供电系统、机房空调设备不能正常工作，以及黑客侵袭、病毒对网络、系统造成严重影响以致造成通关业务不能正常运转甚至瘫痪的事件。

1、当现场全部机器出现系统无法进行实时资料录入，现场值班科长或组长立即报告技术应急小组，初步判别问题的严

重程度，如综合业务科确定不能解决，联系总关科技处做进一步诊断。向值班关领导汇报从综合业务科反馈回的故障情况、请示并对事件进行定级。

2、经过确定为 III 级以上突发事件的，值班关领导报告应急指挥小组、各应急小组负责人。

3、技术应急小组立即组织人力按照总关科技处既定预案排除故障；对于存在备用系统的，应立即启用备用系统，并实时汇报，直至故障排除，恢复正常。

4、值班关领导合理调配人员维护现场正常秩序。现场关员手工填写业务单据，由值班科长签名确认，以备事后补录资料。

5、本关值班领导、各应急小组成员均到现场协调处理。

6、重要信息系统均应建立异地容灾备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。各容灾备份系统应具有一定兼容性，在特殊情况下各系统间可互为备份。

7、在日常工作中，要加强对 H2010 通关作业系统、计算机、网络、通信和各种检查设备的检查维护工作，指定专人负责维护管理；检查维护包括计算机、路由器、网络交换机等设备运行状况、有线线路、传真机设备、各类设备后备电源（UPS）等设备在内的所有设备的安全，必须保证各类设备运行正常。

5　人员培训与演习、现场硬件配置要求

5.1 人员培训与演习

1、建立应急预案定期演练制度。通过演练，发现应急工作体

系和工作机制存在的问题，不断完善应急预案，提高应急处理能力。

2、各科室负责组织现场关员理论和实际操作培训；定期检查有关应急印章、印油、作业单证和技术设备。

5.2 现场硬件配置要求

1、根据业务发展的实际需要，由各科室提出需求，办公室进行调研，适时更新硬件设施，拓展监管区，缓解通关压力，确保通关畅顺。

2、设立危险品专用存放区，安装防爆设施。

3、安装无线报警装置。

4、配备录音、照相、摄影等设备。

5、储备必要的备份容灾设备及相关仪器。

6 责任追究制度

6.1 突发事件发生后，各有关部门、人员应服从指挥，通力合作，采取有效措施排除故障。对在网络与信息安全突发公共事件应急处置中作出突出贡献的集体和个人，给予表彰奖励；对在网络与信息安全突发公共事件预防和应急处置中有玩忽职守、失职等行为者，依法追究责任。

6.2 如有违反本办法规定造成不良影响或过失的，将按乌鲁木齐海关有关惩戒制度的规定追究关人员的责任。