盘龙区网络安全事件应急预案

目 录

1 总则

1.1 编制目的

根据《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），依照《国家网络安全事件应急预案》（中网办发文〔2017〕4号），《昆明市自然灾害应急管理委员会关于印发市级专项应急预案修编工作方案的通知》（昆应急委〔2019〕2号）等有关文件，建立科学、有效、反应迅速的盘龙区网络安全事件应急工作机制，提高处置网络安全事件的能力，保障盘龙区网络与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安全事件的危害，结合盘龙区网络安全管理工作实际，编制本预案。

1.2 指导思想

以习近平新时代中国特色社会主义思想为指导，依法管网、依法办网、依法上网，始终坚持依法治网，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与的网络安全治理格局。

1.3 编制依据

《信息技术 安全技术 信息安全事件管理指南》(GB/Z0985－2007)

《信息安全技术 信息安全事件分类分级指南》(GB/Z0986－

2007)

《信息安全技术 信息系统灾难恢复规范》(GBT 36957-2018)

《政务部门信息安全应急预案编制指南》（DB11T-1599-2018）

1.4 工作原则

1.4.1统一领导，密切协同。网络安全事件应急处置工作在盘龙区网络安全事件应急领导小组的统一领导下，充分调动和发挥各单位、各部门的积极作用，进行统一指挥、密切协同。

1.4.2条块结合、分级负责。按照属地管理，分级负责的原则，坚持“谁主管谁负责、谁运营谁负责、谁使用谁负责”，各区县、各部门负责本地、本部门网络安全事件应急工作。

1.4.3预防为主、重点防范。坚持“积极防御，综合防范”，以预防为主，采取多种有效措施，重点保护关系国家安全、社会稳定和公共利益的重要信息系统安全。

1.4.4快速反应、科学处置。网络安全事件发生时，必须以最快的速度进行事件响应，及时获取充分而准确的信息，正确研判，果断决策，科学处置，在最短的时间内控制事态发展并阻止影响进一步扩大，尽力挽救事件所造成的损失。

1.4.5 周密准备、平战结合。进一步完善应急响应救援体系建设，加强技术储备和日常监测，规范应急处置措施与操作流程，

实现网络安全事件应急处置工作的科学化、程序化与规范化；树立常备不懈的观念，定期进行预案演练，并根据实际情况变化对预案不断进行补充、完善。

1.5 适用范围

本预案主要适用于盘龙区网络安全事件的预防和处置工作。

2 组织体系与职责

2.1 领导机构与职责

在区委网信办的领导下，在区委网信办统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，区科信局、区公安分局、区委机要和保密局（区国家密码管理局、区国家保密局）等有关部门按照职责分工负责有关网络安全事件应对工作。必要时成立区网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。

2.2 办事机构与职责

成立盘龙区网络安全事件应急领导小组负责统筹协调组织全区网络安全事件应对工作，建立健全跨部门联动机制。成员单位为：区委网信办、区科信局、盘龙公安分局、区委机要和保密局（区国家密码管理局、区国家保密局）、区国安部门，成员单位相关处室负责同志为联络员。办公室设在区委网信办网络安全和信息化协调科，负责盘龙区网络安全事件应急领导小组事务性

工作。

2.3 成员单位职责

（1）区委网信办

负责具体组织全区网络安全事件应对工作，建立健全跨部门联动机制。

（2）区公安分局

承担接收、汇总和研判各单位、部门、街道报送的网络安全情况信息，定期编发网络与信息安全情况通报，监测网络安全情况，发现或接报网络安全重大事件、重要紧急的网络安全情况后，及时向本地党委政府和上级信息通报中心报告，并向有关部门通报等工作。

（3）区国家密码管理局

承担因违反《中华人民共和国密码法》有关条例造成的网络安全事件会同有关部门进行查处工作。

（4）区科信局

承担指导监督政府部门、重点行业重要信息系统与信息网络安全保障工作，协调处理网络与信息安全重大事件应急处置具体工作。

（5）区国家保密局

承担发生泄密案件时的文件资料密级确认相关工作，并牵头

组织协调泄密案件查处，指导部署补救措施，督促涉事单位和人员及时进行保密工作整改，并承担机要相关协调工作。

（6）区国安部门

承担依法履行国家安全审查和监管、技术处置等工作。

2.4 各地各部门职责

全区各单位、部门、街道参照盘龙区网络安全应急指挥机构模式，指定或成立本单位网络安全应急工作机构，编制应急预案，负责统筹协调组织本单位的网络安全事件的预防、监测、报告和应急响应处置工作。各单位、部门、街道要指定网络安全负责人和联络员，并及时向盘龙区网络安全事件应急领导小组报备。

3 响应机制

3.1 事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

3.1.1 特别重大事件（Ⅰ级）

符合下列情形之一的，为特别重大网络与信息安全事件(Ⅰ级)：

（1）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。

（2）国家秘密信息、工作秘密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。

（3）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。

3.1.2 重大事件（II级）

符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

（1）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。

（2）国家秘密信息、工作秘密或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。

（3）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。

3.1.3 较大事件（III级）

符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

（1）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。

（2）国家工作秘密、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。

（3）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。

3.1.4 一般事件（Ⅳ级）

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，为一般网络安全事件。

3.2 预防预警

3.2.1 预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色、蓝色表示，分别对应发生或可能发生特别重大、重大、较大、一般网络安全事件。

3.3 预警监测

预警信息来源是依据国家网络安全机构、各大安全厂商发布的网络安全预警信息。

各单位、部门、街道按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。将重要监测信息上报盘龙区网络安全事件应急领导小组。

3.3.1 预警研判和发布

各单位、部门、街道组织对监测信息进行研判，认为需要立即采取防范措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向盘龙区网络安全事件应急领导小组报告。

各单位、部门、街道可根据监测研判情况，发布本地区、本单位的橙色及以下预警。

区委网信办组织研判，确定和发布红色预警。

预警信息包括事件的类别、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。

3.3.2 预警响应

1.红色预警响应

（1）盘龙区网络安全事件应急领导小组组织预警响应工作，联系专家和区信息安全技术支撑机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

（2）各单位、部门、街道网络安全事件应急指挥机构实行24小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报区委网信办。

（3）网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

2.橙色预警响应

（1）各单位、部门、街道网络安全事件应急指挥机构启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2）各单位、部门、街道及时将事态发展情况上报区科信局、区委网信办。盘龙区网络安全事件应急领导小组密切关注事态发展，有关重大事项及时通报各部门。

（3）网络安全应急技术支撑队伍保持联络畅通，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.黄色、蓝色预警响应

各单位、部门、街道网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

4 应急响应

4.1 特别重大网络安全事件应急处置

4.1.1事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各单位立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大网络安全事件的、重大网络安全事件的，分别在1小时和2小时内报告盘龙区网络安全事件应急领导小组；其它网络安全事件在24小时内报告盘龙区网络安全事件应急领导小

组。

4.1.2 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I级为最高响应级别。

（1）属特别重大网络安全事件的，根据事件分级及时启动I级响应，盘龙区网络安全事件应急领导小组履行应急处置工作的统一领导、指挥、协调职责。

（2）各单位应急指挥机构进入应急状态，在盘龙区网络安全事件应急领导小组统一领导、指挥、协调下，负责本单位应急处置工作或支援保障工作，24小时值班，并派员参加应急办工作。

（3）各单位跟踪事态发展，检查影响范围，1小时内将事态发展变化情况、处置进展情况报区委网信办。

（4）各单位跟踪事态发展，检查影响范围，应当将事态发展变化情况、处置进展情况1小时内向盘龙区网络安全事件应急领导小组报告。

4.1.3 应急结束

盘龙区网络安全事件应急领导小组提出建议经批准后，及时通报有关省（区、市）和部门。

4.2 重大网络安全事件应急处置

4.2.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各单位立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大网络安全事件的、重大网络安全事件的，分别在1小时和2小时内报告盘龙区网络安全事件应急领导小组；其它网络安全事件在24小时内报告盘龙区网络安全事件应急领导小组。

4.2.2 II 级响应

属重大网络安全事件的，根据事件分级及时启动 II 级响应，盘龙区网络安全事件应急领导小组履行应急处置工作的统一领导、指挥、协调职责。

（1）事件发生单位的应急指挥机构进入应急状态，按照相关流程应急预案做好应急处置工作。

（2）事件发生单位及时将事态发展变化情况2小时内报盘龙区网络安全事件应急领导小组。

（3）各单位跟踪事态发展，检查影响范围，应当将事态发展变化情况、处置进展情况2小时内向盘龙区网络安全事件应急领导小组报告。

（4）处置中需要其他有关单位和部门网络安全应急技术支撑队伍配合和支持的，盘龙区网络安全事件应急领导小组予以协

调。相关单位和网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

（5）有关单位根据盘龙区网络安全事件应急领导小组的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 应急结束

由事件发生单位或部门决定，报盘龙区网络安全事件应急领导小组。

4.3 较大和一般网络安全事件应急处置

4.3.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各单位立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作，在24小时内报告盘龙区网络安全事件应急领导小组。

4.3.2 应急响应

各单位按相关预案进行应急响应处置相关工作，同时将事态发展变化情况、处置进展情况24小时内向盘龙区网络安全事件应急领导小组报告。

4.3.3 应急结束

由事件发生单位提出建议经批准后，向盘龙区网络安全事件

应急领导小组进行报备。

5 调查与评估

特别重大网络安全事件由盘龙区网络安全事件应急领导小组组织有关单位进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生单位自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报盘龙区网络安全事件应急领导小组。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。事件的调查处理和总结评估工作属III级、IV级在应急响应结束后5个工作日内完成，属Ⅰ级、Ⅱ级在应急响应结束后15个工作日内完成。

6 保障措施

6.1 机构和人员

各单位要落实区党委（党组）网络安全工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全的应急工作机制。

6.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。各单位根据工作需要以签订合同等方式采购相应技术支撑服务。

相关职能单位和部门从教育科研机构、企事业单位、协会中选拔网络安全人才，建立网络安全应急专家组，汇集技术与数据

资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力，为网络安全事件的预防和处置提供技术咨询和决策建议。

6.3 社会资源

与相关大专院校、教育培训机构合作，采取多种方式培养网络安全人才，支持网络安全技术研发和产业发展。

6.4 基础平台

加快推进我区网络安全应急协调联动平台建设。建立完善网络安全信息收集、共享、通报机制，形成网络安全信息共享感知预警、应急处置体系，提升全区网络安全整体协调指挥应急处置能力。

6.5 物资保障

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

6.6 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。

6.7 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

各部门、各重要网络系统运营单位对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励。

各地、各部门、各重要网络系统运营单位对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职等违纪违法行为的，依照相关规定对有关责任人给予处分；涉嫌犯罪的，依法追究刑事责任。

7 预防工作

7.1 日常管理

各单位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、风险评估和容灾备份，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。

7.2 演练

由盘龙区网络安全事件应急领导小组统筹组织，每年至少组织一次预案演练，根据工作需要模拟不同等级的网络与信息安全事件进行演练，检验预案的可执行性，并对预案进行修订完善。

7.3 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，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

7.4 培训

区科信局，区公安分局网安支队等相关职能部门根据业务需要组织培训工作。各单位、部门、街道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应急预案的培训，提高防范意识及技能。

7.5 重要活动期间的预防措施

在国家重要活动、大型活动及会议期间，各单位、部门、街道要加强网络安全事件的防范和应急响应，确保网络安全。盘龙区网络安全事件应急领导小组统筹协调网络安全保障工作，各职能部门按照工作职责编制相关预案，根据需要要求有关单位启动红色预警响应。有关单位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、重点岗位保持24小时值班，及时发现和处置网络安全事件隐患。

8 附则

8.1 预案解释部门

本预案由盘龙区科信局负责解释。

8.2 实施时间

本预案自印发之日起实施。