中共深圳市委网络安全和信息化委员会办公室

中共深圳市委网信办关于印发《深圳市网络安全事件应急预案》的通知

各有关单位：

《深圳市网络安全事件应急预案》已经市委网络安全和信息化委员会同意，现印发你们，请认真组织实施。

中共深圳市委网信办

2020年5月25日

深圳市网络安全事件应急预案

目　　录

1　总则
1.1　编制目的
1.2　编制依据
1.3　事件定义和分类
1.4　事件分级
1.5　适用范围
1.6　工作原则
1.7 名称术语
2　组织机构与职责
2.1　领导机构与职责
2.2　成员单位职责
2.3　办事机构与职责
2.4　各部门职责
2.5　各区职责
3　监测与预警
3.1　预警分级
3.2　预警监测
3.3　网络安全事件信息接收方式

3.4　预警研判与发布
3.5　预警响应
3.6　预警解除
4　应急处置
4.1　事件报告
4.2　先期处置
4.3　应急响应
4.4　响应升级
4.5　应急结束
4.6　善后与恢复
5　调查评估和事件总结
5.1　调查评估
5.2　事件总结
6　预防工作
6.1　日常管理
6.2　演练
6.3　宣传
6.4　培训
6.5　重要敏感时期的预防措施
7　保障措施
7.1　机构和人员
7.2　技术支撑队伍
7.3　专家队伍

7.4　社会资源
7.5　技术支撑体系
7.6　情报力量
7.7　技术研发和产业促进
7.8　合作机制建设
7.9　物资保障
7.10　经费保障
7.11　其他保障措施
7.12　责任与奖惩
8　附则
8.1　预案管理
8.2　预案发布及解释
8.3　预案修订
8.4　预案实施时间
附件
1.深圳市网络安全事件信息报告表
2.深圳市网络安全技术支撑队伍的名单

1.总则

1.1 编制目的

建立健全全市网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

《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》《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《国家网络安全事件应急预案》《广东省突发事件总体应急预案》《深圳市突发事件总体应急预案》《深圳市突发事件应急预案管理办法（修订版）》《深圳市重大突发事件紧急信息报送和处置工作制度》《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）和《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）等。

1.3 事件定义和分类

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、灾害性事件和其他事件等。

（1）有害程序事件分为计算机病毒事件、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。

（2）网络攻击事件分为拒绝服务攻击事件、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、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、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。

（4）信息内容安全事件包括：通过网络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。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

1.4 事件分级

网络安全事件分为四级：由高到低划分为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。

（1）符合下列情形之一的，为特别重大网络安全事件：

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、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。

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。

（2）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、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。

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）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。

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。

（4）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，为一般网络安全事件。

1.5 适用范围

本预案适用于深圳市各区（行政区、新区、深汕合作区）内网络安全事件的应对工作。信息内容安全事件的应对，另行制定专项预案。

中央驻深单位参照本预案执行，在网络安全事件应急处置中加强与地方网信部门的沟通配合。

1.6 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，平战结合、军地结合，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

1.7 名称术语

网络：指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

网络安全:是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

电子政务外网：是指党政机关非涉密工作业务专网，与互联网逻辑隔离。

电子政务内网：是指满足我市各级政务部门内部办公、管理、协调、监督、决策等需要，支持政务部门之间安全互联、资源共享、业务协同的涉密政务网络。

各区：是指深圳市辖各行政区、新区、深汕合作区。

各部门：是指深圳市各级党政机关。

2.组织机构与职责

2.1 领导机构与职责

市委网络安全和信息化委员会（以下简你“市委网信委”）为全市网络安全事件应急处置最高领导机构。市委网络安全和信息化委员会办公室（以下简称“市委网信办”）在市委网信委的领导下，统筹协调组织全市网络安全事件应对工作，建立健全跨部门联动处置机制。市工业和信息化管理局、市公安局、市政务服务数据管理局、市国家保密局、市国家安全局、市通信管理局等相关部门按照职责分工负责相关网络安全事件应对工作。

结合深圳实际，设立全市网络安全事件应急指挥部（以下简称“市指挥部”），组织领导、指挥协调全市网络安全突发事件的防范和应对工作，负责特别重大、重大、较大网络安全事件的组织领导和指挥协调。市指挥部由总指挥、执行总指挥兼现场指挥官、副总指挥和各成员组成。

总指挥由市委常委、宣传部长担任，负责市指挥部的领导工作，对深圳市网络安全事件应急处置工作实施统一指挥。

执行总指挥兼现场指挥官由市委网信办主任担任，履行现场决策、指挥、调度职责，协助总指挥、副总指挥在网络安全事件现场指挥市网安应急办、专家组、各应急专业技术队伍和各区、各部门、各单位应急处置工作组处置网络安全事件。

副总指挥由协助市委常委、宣传部长分管市委网信办工作的市委副秘书长、协助分管应急工作的市政府副秘书长、市应急局局长、市通信管理局局长、市公安局分管副局长、市政务服务数据管理局局长、市国家安全局分管副局长、市委网信办分管副主任担任，负责协助总指挥做好市指挥部各项工作，协调各区、各部

门、各单位实施应急工作。

执行总指挥兼现场指挥官根据工作需要指定现场副指挥官，协助总指挥或现场指挥官开展各项应急处置工作，或受现场指挥官委托，临时负责现场指挥工作。

2.2 成员单位职责

市指挥部成员由市委办公厅、市委宣传部、市委网信办、市工业和信息化局、市公安局、市文化广电旅游体育局、市应急管理局、市政务服务数据管理局、市国家保密局、市密码管理局、市国家安全局、市通信管理局等有关部门负责同志担任，可视情对成员进行调整。市指挥部成员单位职责如下：

（1）市委办公厅：根据中央、省信息报送标准及有关要求，向上级部门报送事件信息。负责深圳市电子政务内网相关应急管理工作。

（2）市委宣传部：负责较大及以上网络安全事件新闻发布工作。指导各区、各部门和相关单位做好网络安全事件新闻发布工作。

（3）市委网信办：统筹协调组织全市网络安全应急处置工作，负责市网安应急办的日常工作，建立健全与省委网信办、中央网信办的网络安全事件应急处置工作机制。网络安全事件发生后，根据网络安全事件分级及响应需求，统筹协调有关单位配置网络安全应急资源。

（4）市通信管理局：负责指导、监督、检查基础电信运营企业做好基础信息网络的安全防范工作；组织协调电信行业开展处置恢

复工作；配合有关单位监测、管控网络与信息安全事件；协调基础电信运营企业为信息系统的正常运行提供基础网络保障。

（5）市工业和信息化局：指导协调工业领域的工控系统网络安全事件应急处置工作。

（6）市公安局：依职责建立健全网络安全预警通报机制，协调、监督和指导开展网络安全事件的预防、监测、报告和应急处置工作，依法打击网络安全事件中的违法犯罪行为。

（7）市文化广电旅游体育局：负责广播电视网络安全事件的预防、监测、报告和应急处置工作；负责监督、检查、指导广播电视传输网络运营企业开展网络安全事件的预防和应急处置工作；配合有关部门处置网络安全事件。

（8）市应急管理局：及时掌握突发事件事态进展情况，传达并督促有关部门（单位）落实市委、市政府、市应急委有关决定事项。

（9）市政务服务数据管理局：负责全市电子政务外网网络安全事件的预防、监测、报告和应急处置工作。统筹协调市政府门户网站、各区政府（新区管委会）门户网站、市直各政府部门网站管理工作。统筹指导政务服务、电子政务、政务数据管理、政务信息安全、数字政府、智慧城市等网络安全应急处置工作。

（10）市国家保密局：负责涉及国家秘密的网络安全事件的预防、应对、查处和监管工作；依法组织查处互联网、无线通信网等公共信息网络以及党政机关、企事业单位和高等院校网络的泄密事件。

（11）市密码管理局：负责网络安全事件中涉及密码技术、密码产品事件的预防、应对、查处和监管工作。

（12）市国家安全局：负责深圳市网络安全事件中涉及国家安全事项的应急处置工作，包括：对网络、通信设备的检查、检验和窃密、泄密事件的查证、查处和防范工作；依法对破坏基础信息网络和利用网络传播有害信息、危害公众利益和国家安全等各种违法犯罪活动进行查处等。

2.3 办事机构与职责

全市网络安全应急指挥部办公室（以下简称“市网安应急办”）设在市委网信办。市网安应急办负责网络安全应急跨部门、跨区协调工作和指挥部的事务性工作，组织指导市级网络安全应急技术支撑队伍做好应急处置的技术支撑工作。市委办公厅、市委宣传部、市工业和信息化局、市公安局、市文化广电旅游体育局、市应急管理局、市政务服务数据管理局、市国家保密局、市密码管理局、市国家安全局、市通信管理局、市信息安全测评中心（市网络与信息安全应急处置协调中心）、市大数据资源管理中心等部门负责相关工作的处级同志为联络员，联系市网安应急办工作。

2.4 各部门职责

市委和市政府各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

2.5 各区职责

各区网信部门在区委网络安全和信息化委员会统一领导下，统筹协调组织本区网络安全事件的预防、监测、报告和应急处置工作。

3. 监测与预警

3.1 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、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“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。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各区网信部门结合本区实际，统筹组织开展对本区网络安全监测工作。各区、各部门、各单位将重要监测信息报市网安应急办，市网安应急办组织开展跨区、跨部门的网络安全信息共享。

市通信管理局、市公安局、市政务服务数据管理局、市国家保密局等单位根据职责，监督、指导网络与信息系统的运营使用单位开展风险评估，对重要基础网络与信息系统及其等级保护落实工作进行定期检查，及时掌握分管领域内重要基础网络与信息系统的风险现状，加强风险管理。

3.3 网络安全事件信息接收方式

市网安应急办通过媒体、网络等途径，面向公众公布网络安全事件接收电话、传真、电子邮箱等信息。

3.4 预警研判与发布

各区、各部门、各单位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。各区各部

门各单位可根据监测研判情况，发布本辖区本行业的蓝色预警。对可能发生较大及以上网络安全事件的信息，1小时内向市网安应急办报告。

市网安应急办组织专家组进行研判，对可能达到红色、橙色、黄色预警等级的，要及时上报省网安应急办，同时报告市委值班室、市政府总值班室。确定为红色预警的，由国家网安应急办发布；确定为橙色预警的，由省网安应急办发布；确定为黄色预警和涉及多个区、多部门、多行业的预警，由市网安应急办发布。

预警信息包括事件类别、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。

3.5 预警响应

3.5.1 红色、橙色预警响应

市网安应急办根据国家、省网安应急办的决策部署和统一指挥，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，重要情况报省网安应急办。

3.5.2 黄色预警响应

（1）市网安应急办、有关部门网络安全事件应急指挥机构启动相应应急预案，组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施，协调组织资源调度和部门联动的各项准备工作，做好风险评估、应急准备和风险控制工作，重要情况报省网安应急办。

（2）有关区、部门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，重要情况及时报市网安应急办，市网安应急办密切关注事态发展，有关重大事项及时通报相关区和部门。

（3）市级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。

3.5.3 蓝色预警响应

有关区、部门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。

3.6 预警解除

按照“谁发布谁解除”的原则，市网安应急办根据实际情况，按程序确定解除对本市发布的黄色预警信息；配合省、国家网安应急办做好红色、橙色预警信息解除的相关工作。各区网信部门或各部门根据实际情况，确定是否解除预警，按程序及时对所发布蓝色预警的解除信息。

4 应急处置

4.1 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。事件报告要按照首报、续报、终报全过程报送要求，做到有头有尾。对于初判为特别重大、重大、较大网

络安全事件的，事发单位应立即将简要情况及联系人通过电话、传真等方式上报市网安应急办，事件详细情况应在1小时内上报。市网安应急办接到事件报告后，及时报市委值班室、市政府总值班室，并上报省网安应急办。

事件报告内容包括：事件发生时间和地点、发生事件的基础网络与信息系统名称、事件原因、信息来源、事件类型及性质、危害和损失程度、影响单位及业务、事件发展趋势、采取的处置措施等。对涉密的信息，参与涉密网络安全事件应急处置人员应按有关规定签署保密协议；知情人员应遵守相关的管理规定，做好保密工作。

事件报告要符合以下要求：对重要基础网络与信息系统及在敏感期可能演化为重大和特别重大网络安全事件的信息系统的事件，事发单位应立即上报。对涉密的信息，参与涉密网络安全事件应急处置人员应按有关规定签署保密协议；知情人员应遵守相关的管理规定，做好保密工作。

4.2 先期处置

发生网络安全事件后，事发单位应立即采取以下先期处置措施。

（1）紧急控制事态发展。根据本单位相关应急预案采取紧急措施，及时、最大限度控制事态发展。

（2）快速判断事件危害。根据基础网络与信息系统的运行、使用、承载业务的情况，初步判断发生事件的原因、影响力、破坏程度、波及的范围等，提出初步应对措施建议。

（3）及时上报信息。先期处置的同时，及时向单位责任人、

市网安应急办和相关应急主管部门报告。保持通信畅通联系，实时报告事件进展情况。

（4）保留相关证据。在事件处置过程中，可采取记录、截屏、备份、录像等手段，对事件的发生、发展、处置过程、步骤、结果进行详细记录；涉及网络犯罪行为的，按照相关法律法规要求，向市公安局网警支队报案，协助进行电子数据取证，为事件调查、处理提供证据。

如先期处置措施不能有效控制事件，应进行分级响应。

4.3 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。

4.3.1 Ⅰ级、Ⅱ级响应

启动Ⅰ级响应。市网安应急办组织对事件信息进行研判，认为属特别重大网络安全事件的，及时向省网安应急办报告，提出启动Ⅰ级响应的建议。省网安应急办对事件信息进行研判，按流程上报国家网安应急办。经国家网安应急办确认启动Ⅰ级响应后，市网安应急办迅速向市委网信委报告，启动市指挥部工作。

启动Ⅱ级响应。市网安应急办组织对事件信息进行研判，认为属重大网络安全事件的，及时向省网安应急办报告，提出启动Ⅱ级响应的建议，经省网安应急办确认后，迅速向市委网信委报告，启动市指挥部工作。

（1）启动指挥体系

市指挥部进入应急状态，在国家、省指挥部统一领导、指挥、

协调下，负责统筹指挥全市应急处置工作或资源保障工作。指挥部成员保持24小时联络通畅，市网安应急办24小时值班，并派员参加国家、省网安应急办工作。

（2）掌握事件动态

①跟踪事态发展。市网安应急办及时将事态发展变化情况和处置进展报省网安应急办。

②检查影响范围。市网安应急办立即全面了解全市范围内的网络和信息系统是否受到事件的波及或影响，有关情况及时报省网安应急办。

③及时通报情况。市网安应急办负责汇总上述有关情况，重大事项及时报省网安应急办，并通报有关区和部门。

（3）决策部署

市网安应急办根据省网安应急办的统一部署和我市实际做好统筹应对工作。

（4）处置实施

①控制事态防止蔓延。市网安应急办组织实施，尽快控制事态；组织、督促相关运行单位有针对性的加强防范，防止事态蔓延。

②消除隐患恢复系统。市网安应急办根据事件发生原因，有针对性地采取措施，备份数据、保护设备、排查隐患，恢复受破坏网络和信息系统正常运行。必要时可以依法征用单位和个人的设备和资源，并按规定给予补偿。

③调查举证。事发单位在应急恢复过程中应保留相关证据。对于人为破坏活动，市公安局、市国家安全局、市保密局按职责

分工负责组织开展调查取证工作。

④信息发布。在中央宣传部（国务院政府新闻办公室）的指导下，省委宣传部指导协调、市委宣传部协助开展网络安全突发事件的应急新闻发布和舆论引导工作。未经批准，其他部门和单位不得擅自发布相关信息。

⑤区域协调。有关部门根据统一要求，建立健全市际间网络安全事件应急处置联动机制，按照各自渠道，开展与有关市之间的协调。

⑥协调配合引发的其他突发事件的应急处置。对于引发或可能引发其他特别重大安全事件的，市网安应急办应及时按程序上报。在相关区、部门应急处置中，市网安应急办做好协调配合工作。

4.3.2 III级响应

市网安应急办组织对事件进行研判，认为属较大网络安全事件的，及时向市委网信委提出启动III级响应的建议，经市委网信委批准后，及时发布预警信息。

（1）市指挥部进入应急状态，履行应急处置工作的统一领导、指挥、协调职责，按照相关应急预案做好应急处置工作。市网安应急办24小时值班，指挥部成员单位保持24小时联络畅通。有关区、部门应急指挥机构进入应急状态，24小时值班，负责做好本区、本部门应急处置工作或支援保障工作，派员参加市网安应急办工作。

（2）事件发生地辖区或部门及时将事态发展变化情况和处置进展情况，以及本区、本部门主管范围内的网络和信息系统是

否受到事件的波及或影响情况报市网安应急办。市网安应急办负责汇总上述有关情况，重大事项及时报省网安应急办，并通报有关区和部门。

（3）市网安应急办会同公安、通管等有关部门，组织有关区、单位、专家组和应急技术支撑队伍等及时研究对策意见，对应对工作进行决策部署。

（4）有关区和部门根据市网安应急办的部署组织、督促相关运行单位组织实施，尽快控制事态，防止事态蔓延。处置中需要省或其他有关区、部门网络安全应急支撑队伍配合和支持的，商市网安应急办予以协调，相关网络安全应急支撑队伍根据各自职责，积极配合、提供支持。

（5）有关区和部门根据事件发生原因，有针对性地采取措施，备份数据、保护设备、排查隐患，恢复受破坏网络和信息系统正常运行。事发单位在应急恢复过程中应保留相关证据。对于人为破坏活动，公安、安全、保密等部门按职责分工负责组织开展调查取证工作。必要时可依法征用单位和个人的设备和资源，并按规定给予补偿。

（6）市委宣传部组织网络安全突发事件的应急新闻工作，指导协调有关区和部门开展应急新闻发布和舆论引导工作。未经批准，其他部门和单位不得擅自发布相关信息。

（7）对于引发或者可能引发其他重大安全事件的，市网安应急办应及时按程序上报，统筹协调做好处置工作。有关区和部门根据市网安应急办的通报，结合实际有针对性地加强防范，防

止造成更大范围影响和损失。

4.3.4 Ⅳ级响应

一般网络安全事件由事发辖区、部门按相关预案进行应急响应。

（1）事发单位按照本单位相关的应急预案进行先期处置。将突发事件信息、处置进展情况填写《深圳市网络安全事件信息报告表》（见附件），及时报市网安应急办。

（2）事发单位负责人及时赶赴现场，组织协调、指挥本单位专业技术队伍进行处置工作，必要时请求市网安应急办安排专家组、专业技术队伍支援处置。

（3）根据事发单位需要，市网安应急办组织专家组、专业技术队伍及时赶赴现场，指导开展应急处置工作。

（4）需要向社会发布信息的，由事发单位负责人审批后，报相关业务领域市级主管部门或区网信部门审核后，在市委宣传部的指导下发布。未经批准，其他部门和单位不得发布相关信息。

4.4 响应升级

4.4.1 响应级别变更

应急响应过程中，市网安应急办、各相关部门应密切关注事件事态发展和响应工作进展情况，根据事态变化、响应效果及专家组建议，适时调整响应级别。超出自身应急处置能力的，应及时报告上一级部门，建议变更响应级别，开展相关处置工作。

4.4.2 响应级别升级

（1）事件发展蔓延，事态发展得不到控制，超出了市网安

应急办处置能力，需要其它部门、单位参与处置时，市网安应急办应及时报告市委网信委，由市委网信委组织、协调市其它专项应急指挥部和各部门参与处置工作。

（2）事件造成的危害程度特别严重，超出了本市处置能力，需要国家有关部门（单位）、其他省市等提供援助和支持时，依照《深圳市突发事件总体应急预案》，市指挥部通过市委网信委及时向国家、省网安应急办及应急相关部门报告事件情况。应急处置工作在国家、省网安应急办及应急相关部门或指定部门的领导下开展。

4.5 应急结束

Ⅰ级响应结束，由国家网安应急办及时通报省（区、市）和部门。

Ⅱ级响应结束，由省网安应急办按程序上报国家网安应急办，由国家网安应急办通报省网安应急办，省网安应急办及时通报相关地区和部门。

Ⅲ级响应结束，由市网安应急办提出建议，报市委网信委批准后，上报省网安应急办，省网安应急办通报市网安应急办。

Ⅳ级响应结束，由事发区或部门决定，按程序报市网安应急办，市网安应急办通报相关区和部门。

4.6 善后与恢复

应急处置工作结束后，事发单位和其他有关应急管理工作机构要积极稳妥、深入细致地做好善后处置工作，及时处理征用的物资和设备。对参与处置的工作人员以及紧急调集、征用的物资，

要按照规定给予补助或补偿。事发单位迅速组织人员制订基础网络、信息系统的重建和恢复计划，尽快恢复受损基础网络和信息系统，降低对正常工作业务的影响。

5 调查评估和事件总结

5.1 调查评估

特别重大网络安全事件，由国家网安应急办组织有关部门和省（区、市）进行调查和总结评估，并按程序上报。重大网络安全事件，由省网安应急办组织有关部门和地区进行调查处理和总结评估，将总结调查报告报国家网安应急办。较大网络安全事件，由市网安应急办组织有关部门和区进行调查处理和总结评估，将总结调查报告报省网安应急办。一般网络安全事件，由事件发生区或部门自行组织调查处理和总结评估。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。

事件调查处理和总结评估工作原则上应在应急响应结束后30天内完成。

5.2 事件总结

网络安全事件应急任务结束后，事发单位应牵头组织专家，与市网安应急办组成事件调查组，对事件发生原因及处置过程进行全面调查，查清事件发生的原因及事件中基础网络与信息系统、网络设施损失情况，总结经验教训，不断改进网络安全事件应急管理工作。事发单位应在30个工作日内将相关报告报送给市网安应急办。

6. 预防工作

6.1 日常管理

各区、各部门、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。

6.2 演练

市委网信办牵头，协调市政务服务数据管理局等有关部门，每年至少组织一次全市网络安全应急演练，模拟处置影响较大的网络安全事件。通过演练，检验应急体系和工作机制运行情况、应急物资配备情况，及时发现问题，完善应急预案，提高应急处置能力。演练情况报市委网信委和省委网信办。

应急演练主要开展以下工作：

（1）市委网信办确定应急响应演练的目标和范围。主要开展重要信息系统的应急演练。

（2）按照全市网络安全应急演练工作要求，各区、各部门、各单位成立应急演练小组，制订应急演练方案。

（3）市委网信办统筹调配应急演练所需的各项资源，组织有关部门和单位进行应急演练。评估演练情况，总结经验，通报应急演练结果。针对演练中暴露的问题，分析应急预案的科学性和合理性并加以修订完善。

各区、各部门、各单位每年至少组织一次网络安全应急演练，

演练情况报市委网信办。

6.3 宣传

各区、各部门、各单位要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。

6.4 培训

各区、各部门、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应急预案的培训，提高防范意识和技能。

市政务服务数据管理局组织全市党政机关开展网络安全应急管理、应急处置等培训，提高各区各单位信息化管理人员、应急处置人员防范意识及技能。

6.5 重要敏感时期的预防措施

在国家、省、市重要活动和会议等重要敏感时期，各区、各部门、各单位要加强网络安全事件的防范和应急响应，确保网络安全。市网安应急办统筹协调网络安全保障工作，根据需要启动预警响应。各区、部门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。

7 保障措施

7.1 机构和人员

各区、各部门、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。

7.2 技术支撑队伍

深圳市网络安全应急处置专业技术队伍由常设专业技术队伍和非常设专业技术队伍共同组成。

深圳市网络安全事件应急处置常设专业技术队伍由市委网信办、市公安局、市通信管理局的网络安全工作专班，深圳市信息安全测评中心（市网络与信息安全应急处置协调中心）、深圳市大数据资源管理中心，广东移动通信集团深圳分公司、广东电信集团深圳分公司、广东联合网络通信集团有限公司深圳分公司组成。

市网安应急办根据相关单位的网络安全事件应急处置工作能力和相关国家资质条件等，授权相关单位成立专业技术队伍，作为深圳市非常设专业技术队伍。市网安应急办根据非常设专业技术队伍应急工作的开展情况，每年进行一次评估，适时调整。各区、各部门、各单位应配备必要网络安全专业技术人才，根据实际情况加强与网络安全相关技术单位沟通、合作，建立必要的网络安全信息共享机制。

专业技术队伍主要职责：发生突发事件时，按照市网安应急办的指令，开展应急救援；根据事发单位应急支援要求，提供应急救援服务；负责应急物资的储备、相关软件的日常管理和维护等工作。

7.3 专家队伍

成立市网络安全应急专家组，建立网络安全事件应急处置咨询机制。专家组成员从中共深圳市委网络安全和信息化委员会专

家咨询委员会中选取。

专家组主要职责：对预防发生网络安全事件和相关应急处置工作提供咨询与研判建议；对与预案相关的规章制度的制定和项目建设提供参考意见；对应急工作中存在的问题和不足提出改进建议；参与相关应急培训和教材编审工作。

各区、各部门、各单位应加强各自的专家队伍建设，建立网络安全事件应急处置咨询机制，为网络安全事件的预防和处置提供技术咨询和决策建议。

7.4 社会资源

从教育科研机构、企事业单位、协会中选拔网络安全人才，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、较大网络安全事件的能力。

7.5 技术支撑体系

（1）建设态势感知和应急指挥平台。市网安应急办整合全市网络安全监测预警资源，统筹建设市级网络安全态势感知和应急管理平台以及相应的运营机制。建立覆盖全市的网络安全事件应急响应闭环体系，实现监测预警信息的接收、研判、推送和应急联动响应，实现网络安全事件处理过程的信息快速获取传递、会商研判、科学决策、统一指挥、联动响应、统计分析，做到早发现、早预警、早响应、早处置，提高深圳市网络安全事件应急处置能力。市政务服务数据管理局、市公安局等单位以及各行业主管部门分别负责主管监管领域内网络安全监测预警系统建设与管理工作，对各区各有关单位进行监督、检查、指导。各区、

各部门、各单位按照市级技术规范要求自行建设监测预警系统，接入市级网络安全态势感知和应急管理平台，按照“谁主管谁负责、谁运行谁负责”的要求开展网络安全监测工作。

（2）充分发挥容灾备份中心作用。充分发挥统一建设的市级容灾备份中心作用，为全市党政机关和各区重要政务信息系统提供不同等级的容灾备份服务，提升深圳市重要政务信息系统数据安全和抵抗灾难打击的能力。

（3）开展基础网络与信息系统普查。根据应急工作需要，定期开展全市党政机关、重要领域、重点行业基础网络与信息系统普查工作，根据等级保护和关键信息基础设施保护要求，确定重点保障对象和关键信息基础设施，建立全市基础网络与信息系统资源目录、关键信息基础设施目录和数据库。各基础网络与信息系统、关键信息基础设施的运营、使用单位应根据本预案，结合网络安全等级保护和关键信息基础设施保护要求，制定、完善本单位应急处置预案。

（4）开展网络安全技术研究。深圳市信息化、科技、等级保护、保密、密码管理等有关部门应组织开展网络安全防护相关关键技术的研究工作，研究、制定相关基础网络与信息系统的应急处置事件库、应急处置方案库；加强政策引导，支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力，为全市网络安全应急管理提供技术保障。

7.6 情报力量

市公安局、市国家安全局、市政务服务数据管理局、市通信管理局等部门加强网络安全有关情报搜集能力建设，完善情报共享机制，为网络安全应急工作提供情报支撑。

7.7 技术研发和产业促进

有关部门加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.8 合作机制建设

市网安应急办加强深圳市网络安全应急合作机制建设，建立与国家计算机网络应急技术处理协调中心及其广东分中心和深圳应急保障中心、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机病毒应急处理中心、省应急相关单位以及专业机构的合作渠道，实现信息共享和应急联动。

7.9 物资保障

各区、各部门、各单位在建设信息系统时应适当配备网络安全应急装备、工具，及时调整、升级软件硬件工具，不断增强应急技术支撑能力，必要时由市指挥部统一调用。

专业技术队伍须储备相应的应急基础设备、软件。

7.10 经费保障

财政部门为网络安全应急工作提供必要的经费保障。各区、各部门、各单位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、情报力量建设、技术研发、预案演练、物资保障等工作开展。

按照现行市区体制事权、财权划分原则，处置电子政务网络安全事件所需要的经费实行市区财政分级负担。各单位网络安全事件应急管理工作经费应纳入年度部门预算。各应急保障资金使用单位要按照国家相关规定，严格规范应急保障资金的使用，并接受有关部门的监督。

7.11 其他保障措施

（1）通信与信息保障。市通信管理局负责建立健全应急通信保障工作体系，完善备份系统和紧急保障措施。及时根据通信网络破坏状况，采取启用应急通信保障系统等应急保障措施，确保通信畅通。

（2）交通运输保障。各区、各部门、各单位应配备网络安全事件应急交通工具，满足应急期间人员、物资、信息传输的需要，必要时由市网安应急办统一调配。

（3）技术资料保障。各区、各部门、各单位应将应急技术资料纳入应急工作范围。应急技术资料包括网络拓扑结构、重要系统或设备的型号及配置（操作系统及版本号、应用软件及版本号等）、主要设备厂商信息、设备使用人员的详细信息等，建立技术档案并及时更新，以保证与实际系统的一致性。应根据需要对信息系统进行风险评估，开展等级保护和关键信息基础设施保护工作，随时掌握信息系统安全状况和存在的风险。

（4）治安保障。本预案启动后，当网络安全事件造成或可

能造成严重社会治安问题时，公安机关应立即启动治安保障方案和有关预案。

7.12 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

市委网信办及有关区和部门按照国家、省、市相关规定，对网络安全事件应急管理工作中表现突出的单位和个人给予表扬。

市委网信办及有关区和部门对不按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在应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；涉嫌犯罪的，依法移送司法机关处理。

8. 附则

8.1 预案管理

本预案指导全市网络安全事件应急处置工作，原则上每年评估一次，根据实际情况适时修订，修订工作由市委网信办负责。

各区、各部门、各单位要根据本预案制定完善本区、本部门、本行业或重要领域的网络安全事件应急预案和专项应急预案，各预案要做好与本预案的衔接，并报市委网信办备案。

其中，市委军民融合办负责国防军工行业和装备制造行业；市发展改革委负责石油石化行业；市教育局负责教育行业；市工业和信息化局指导协调工业领域工控系统相关应急预案；市生态环境局负责民用核设施行业；市住房建设局负责燃气行业；市交通运输局负责交通领域内交通运输（公路、航运、轨道交通）行业；市水务局负责供、排水行业；市文化广电旅游体育局负责广

播电视行业；市卫生健康委负责医疗卫生行业；市通信管理局负责通讯行业；深圳银保监局负责银行、保险行业；深圳证监局负责证券行业。

8.2 预案发布及解释

本预案由市委网信办发布、解释。

8.3 预案修订

有下列情形之一的，应当及时修订应急预案：

（1）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）应急指挥机构及其职责发生重大调整的；

（3）面临的风险发生重大变化的；

（4）重要应急资源发生重大变化的；

（5）预案中的其他重要信息发生变化的；

（6）在突发事件实际应对和应急演练中发现问题需要作出重大调整的；

（7）相关单位名称或职能发生变化的；

（8）应急预案制定单位认为应当修订的其他情况。

8.4 预案实施时间

本预案自印发之日起实施。

附件 1

深圳市网络安全事件信息报告表

报告时间：

单位名称		报 告 人	
联系电话		通讯地址	
传　　真		电子邮件	
审批主管领导		联系方式	
网络安全事件的客体	名　　称		
	用途描述		
简要描述			
事件发生原因			
初步判定的事件类型	□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　□灾害性事件 □其他信息安全事件		
本次网络与信息安全突发事件的初步影响状况	事件后果	□业务中断 □系统破坏 □数据丢失 □其他	
	影响范围	□单台主机 □多台主机 □整个信息系统 □其他	
突发事件的发展趋势			
当前采取的应对措施			
附件			
报告人签字确认			
主管领导审批意见、签字			

附件 2

2020 年深圳市网络安全技术支撑队伍的名单

序号	单　位	姓　名	联系方式
1	国家计算机网络与信息安全管理中心广东省分中心深圳市应急保障中心	黄兴城	13823104145
2	市电子政务资源中心	姚元琪	13509658016
3	市信息安全测评中心	董安波	13590132701
4	市信息安全测评中心	余晓斌	15914026994
5	深圳市能信安科技股份有限公司	李德庆	18922849880
6	北京启明星辰信息安全技术有限公司	卢佳煜	13927442877
7	网神信息技术（北京）股份有限公司	周启明	15920001981
8	深信服科技股份有限公司	余文群	17722423639
9	亚信科技（成都）有限公司	方锦鹏	13824410935
10	北京知道创宇信息技术有限公司	袁亚琦	18617094443
11	深圳竹云科技有限公司	沈　默	15920001981
12	杭州安恒信息技术服份有限公司	罗剑东	13828765030
13	远江盛邦（深圳）信息技术有限公司	汤志强	18318876976
14	深圳市易聆科信息技术有限公司	朱建新	15012987815
15	北京天融信网络安全技术有限公司	黄文坚	13922289142
16	深圳市安络科技有限公司	欧伟权	13510631903
17	任子行网络技术股份有限公司	黄洪发	18002516073