中国地质大学（北京）

信息网络中心文件

信息网络中心　　2020.9.21

中国地质大学（北京）信息系统应急预案

目　录

1. 总则

1.1. 编制目的

为了规范中国地质大学（北京）应急响应工作内容和工作流程，提高中国地质大学（北京）自身的应急响应能力，完善应急响应机制，确保网络信息系统的安全、稳定运行和业务的连续性，特制定本总体应急预案。

1.2. 编制依据

以国家有关法律、法规、规章、相关政策为依据，以国家突发公共事件总体应急预案为准则编制中国地质大学（北京）网络安全总体应急预案。适用性法规标准主要有：《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》、《国家网络安全事件应急预案》、《突发事件应急预案管理办法》和《信息安全技术信息安全事件分类分级指南》。

1.3. 适用范围

本预案适用于中国地质大学（北京）所有信息系统突发网络安全事件的应急处置。

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。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

2. 事件分类分级

2.1. 事件分类

根据网络安全事件的发生原因、性质和机理，网络安全事件主要分为以下两类：

(1) 可控网络安全事件：指相关网络信息系统内部可以解决或有能力解决的网络安全事件，如网络信息系统因计算机病毒感染、计算机软硬件故障、人为误操作、非法入侵等导致业务中断、系统宕机、网络因人为原因造成瘫痪、内部电力中断等情况。

(2) 不可控网络安全事件：指相关网络信息系统内部无法解决的网络安全事件，如由于网络供应商原因导致的网络瘫痪，以及因爆炸、火灾、雷击、地震、台风等外力因素导致网络与网络信息系统损毁、外部电力中断，造成业务中断、系统宕机、网络瘫痪等情况。

注：本预案只针对可控网络安全事件的处理，不包括不可控网络安全应急事件。

2.2. 事件分级

网络安全事件分级的参考要素包括信息密级、公众影响和资产损失等四项。各参考要素分别说明如下：

1. 信息密级是衡量因信息失窃或泄密所造成的网络安全事件中所涉及信息的重要程度的要素；

2. 公众影响是衡量网络安全事件所造成的负面影响范围和程度的要素；

3. 业务影响是衡量网络安全事件对事发单位正常业务开展所造成的负面影响程度的要素；

4. 资产损失是衡量恢复系统正常运行和消除网络安全事件负面影响所需付出资金代价的要素。

根据突发网络安全事件所造成后果的严重程度，突发网络安全事件可划分为四个等级。各级别的突发网络安全事件具体描述如下：

一级故障(特别重大)事件：现有的系统宕机，或遭到严重攻击、入侵等行为，使业务系统无法正常提供服务、网络信息系统的正常业务运作产生重大影响，或严重影响到业务提供服务的服务质量的，造成大范围不良影响的重大事件，包括重大网络事件、网站事件、应用事件和严重的基础设施故障等安全事件。

二级故障(重大)事件：现有系统的操作性能严重降低，或由于网络性能失常或安全事件严重影响数据中心业务运作，持续时间小于 4 小时，造成一定范围的不良影响的事件。持续时间超过 4 小时则升级到一级事件，包括一般网站事件、严重网络事件、严重应用事件和基础设施故障等安全事件。

三级故障(较大)事件：系统的操作性能受损，例如病毒在小范围内发作，或部分系统业务受到影响，但大部分业务运作仍可正常工作，持续时间小于 4 小时，造成较小范围不良影响的事件。持续时间超过 4 小时则升级到二级事件。

四级故障(一般)事件：在服务器、存储设备、安全设备等的功能、安装、配置或日志分析方面需要信息咨询或技术支持。本级故障事件对数据中心的业务运作几乎无影响，或根本没有影响。

一般定义，四级故障事件属于日常运维服务范畴，三级故障事件仍由日常运维服务人员处理，但需要向应急响应小组人员告知；二级故障事件和一级故障事件属于应急服务项目，故障事件从四级升级到三级时，由运维服务人员及时通知应急响应小组启动应急响应服务。

2.3. 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，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。

3. 组织机构

本单位的应急响应工作机构负责本单位的网络安全应急响应工作，并接受国家网络安全应急协调小组的统一指挥，必要时可以向安全主管部门或安全服务外包单位请求提供应急支援服务。

应急响应工作组织机构应包括应急领导小组和应急响应小组。

3.1. 应急领导小组

成立应急领导小组，负责本单位应急响应工作的整体规划以及各项应急准备工作。工作内容主要包括：

3.1.1. 应急响应规划

确定应急响应工作的基本内容和重点，成立应急响应小组，分配应急响应工作的角色和职责，并制定应急预案。

督促检查网络安全专项应急预案的制订、修订和执行情况，并给予指导；督促检查网络安全突发事件监测、预警工作情况，并给予指导；监督检查、协调指导各部门及各相关单位的有关部门的网络安全突发事件预防、应急准备、应急处置、事后恢复与重建工作；汇总有关网络安全突发事件的各种重要信息，进行综合分析，提出建议。

3.1.2. 应急资源准备

准备网络安全应急响应时所需的各项资源，保证在发生应急安全事件时这些资源能够及时投入使用。

3.1.3. 应急响应培训及演练

组织本单位人员的应急响应培训和应急响应演练工作。应急响应培训的对象范围很广，尤其是针对物理安全事件的应急响应培训，甚至包括一个单位内的所有人员。应急响应培训可以与常规的网络安全培训结合进行。但每当应急预案更新时，均必须及时开展新的应急响应培训。

应急响应演练能够模拟各种可能发生的网络安全事件，用于检验实际的应急响应能力，同时也可达到锻炼队伍、提高人员安全意识的目的。应急响应演练工作应以应急预案为基础，定期进行。应急响应小组应分析应急响应演练的结果，对应急预案做出必要修改。

3.1.4. 关系协调

协调与本单位网络安全应急响应相关的各方面关系，包括相关的业务主管部门、安全主管部门、专家组以及社会网络服务机构。

3.1.5. 其它

根据需要，应急领导小组还可参与本单位内的其它网络安全工作。

3.2. 应急响应小组

由应急领导小组负责组建成立应急响应小组。应急响应小组负责发生网络安全事件的应急响应工作。应急响应小组一般为虚拟形式，在发生网络安全事件时立即转换为实体形式并投入应急响应工作。应急响应小组，在出现安全事件后，对计算机系统和网络安全事件的处理提供技术支持和指导，遵循正确的流程，采取正确快速的行动做出响应，提出事件统计分析报告。应急响应小组的工作包括：

3.2.1. 事件报告

应急响应小组根据《信息安全技术信息安全事件分类分级指南》和《国家网络安全事件应急预案》，及时向相关部门报告本单位发生的网络安全事件。事件响应过程结束后，整理网络安全事件和应急响应工作的详细信息，形成事件处理报告，提交给相关主管部

门。

3.2.2. 事件应急响应

应急响应小组负责在本单位出现网络安全事件时启动应急预案，及时采取本地响应措施，阻止或限制网络安全事件的进一步发展，必要时向社会网络安全机构请求支援。

可视具体情况，自行确定应急响应服务机构。发生网络安全事件时，首先利用本单位和本地的应急响应资源，以保证应急响应工作的及时性。

3.2.3. 其它

根据需要，应急响应小组还可参与其它与网络安全应急响应相关的工作。

3.3. 应急保障小组

3.3.1. 机构和人员

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。

3.3.2. 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。

3.3.3. 专家队伍

建立网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。

3.3.4. 物资保障

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

3.3.5. 经费保障

资金主管部门为网络安全事件应急处置提供必要的资金保障，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、物资保障等各项工作开展。

4. 预测预警

预防预警是应急响应迅速启动的关键。利用自身的安全监控设备和工具，并结合社

会其它信息源(如安全厂商的公告、各类应急响应机构的公告等)，及时发现网络安全威胁或事件发生的迹象和趋势，分析导致网络安全事件的根源，为网络安全应急响应工作提供支持。

4.1. 信息监测与报告

为进一步完善网络安全突发公共事件监测、预测、预警制度，落实责任制，制定信息通报制度。按照“早发现、早报告、早处理、早恢复”的原则，加强对各类网络安全突发公共事件和可能引发突发公共事件的有关信息的收集、分析判断和持续监测。当发生网络安全突发事件时，由应急响应小组向有关部门报告，按安全事件报送的规定及时报告。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。

1．应急响应小组要加强网络安全监测、分析和预警工作，进一步提高网络安全监察能力。

2．建立网络安全事故报告制度。发现网络安全突发事件时应当在事件发生后，应急响应小组立即对发生的事件进行调查核实、保存相关证据，并在事件被发现或应当被发现时起 5 小时内将有关材料报至应急领导小组。

4.2. 预警处理与发布

应急响应小组接到网络安全突发事件报告后，在经初步核实后，将有关情况及时向应急领导小组报告。在进一步综合情况，研究分析可能造成损害程度的基础上，提出初步行动对策，视情况召集协调会，并根据网络安全协调小组的决策实施行动方案，发布指示和命令。

1．对于可能发生或已经发生的网络与网络安全突发公共事件，应急响应小组应立即采取措施控制事态，并在最短的时间内进行风险评估，判定事件等级并在本系统内发布预警。必要时应启动相应的专项预案，同时向应急领导小组通报情况。

2．应急领导小组接到报告后，应及时对信息做出判断，提出处理意见。对发生和可能发生的网络安全突发事件时，应迅速召开应急工作小组会议，研究确定网络安全突发事件的等级，决定启动应急预案，同时确定应急指挥人员，并向上级相关部门进行通报。

3．对需要向社会发布预警的网络安全突发公共事件，由应急领导小组根据其可能造成的危害程度、紧急程度和发展态势，及时向上级主管部分通报预警信息。由上级主管

部门根据网络安全事件的管理权限、危害性和紧急程度，统一发布、调整和解除预警信息，对严重、特别严重或可能衍生其他安全事件的预警信息，应按照中央网信办的决定由授权部门发布。

4.3. 预警支持系统

应急领导小组应建立和逐步完善信息监测、传递网络和指挥决策支持系统，要保证资源共享、运转正常、指挥有力。

4.4. 预防机制

积极推行网络安全等级保护，逐步实行网络安全风险评估。各基础信息网络和重要网络信息系统建设要充分考虑抗毁性与灾难恢复，制定完善网络安全应急处理预案。针对基础信息网络的突发性、大规模安全事件，各相关部门建立制度化、程序化的处理流程。

5. 应急响应

应急响应主要是应对系统出现的突发事件，可以快速、可靠的采取应对措施，解决突然出现的事件。从而保证整个系统的持续、正常的运行。

5.1. 应急事件的发现

应急事件的发现通过以下方式：

- 监控设备报警
- 监控过程日志分析
- 接听监控人员或部门反馈
- 第三方机构反馈

5.2. 确认应急事件及等级

确认事件及等级主要是为了准确无误的启动相关专项预案，并同时根据事件类型及事件等级逐级向相关管理人员进行汇报。

5.3. 不同等级应急事件处理方式

不同等级事件的应急处理方式及要求需要细化，处理事件的相关人员应严格遵守。

5.3.1. 一级应急事件响应要求

- 响应时间要求

严重应急事件需要立即响应，应急响应处理部门应立即组织技术人员 1 个小时内到机房，除特殊原因外，原则上 2 小时内解决问题。

- 汇报层次

严重应急事件应逐级汇报到应急领导小组，所有事件处理过程和事件处理状态都需要在第一时间汇报给应急领导小组领导和应急响应小组成员，整个事件响应由应急响应小组专人统一协调。

- 调用资源

严重应急事件响应需要在领导小组办公室以及故障系统所属部门调动资源，涉及到的所有技术和非技术部门都无条件参与。

以首先解决安全问题为原则，保障事件得到快速解决，严重应急事件响应需要及时调用备份设备资源时，可以简化审批手续，事件负责人授权签字即可。

5.3.2. 二级应急事件响应要求

- 响应时间要求

中等应急事件需要立即响应，应急响应处理部门应立即组织技术人员 2 小时内到现场，除特殊原因外，原则上 4 小时内解决问题。

- 汇报层次

中等应急事件应逐级汇报到应急响应小组，所有事件处理过程和事件处理状态都需要在第一时间汇报给应急响应小组成员，整个事件由应急响应小组专人统一协调。

- 调用资源

中等应急事件响应需要在系统所属单位整个单位调动资源，涉及到的所有技术和非技术部门都无条件参与。

以首先解决安全问题为原则，保障事件得到快速解决，事件响应需要及时调用备份设备资源时，可以简化审批手续，事件负责人授权签字即可。

5.3.3. 三级应急事件响应要求

- 响应时间要求

轻度应急事件需要立即响应，事件响应处理部门应立即组织技术人员 8 小时内到现场，除特殊原因外，原则上 48 小时内解决问题。

- 汇报层次

轻度应急事件响应需要直接汇报给应急响应小组，所有事件处理过程和事件处理状态都需要在第一时间汇报给应急响应小组和事件处理小组成员。整个事件响应由应急响应小组指派专人统一协调。

- 调用资源

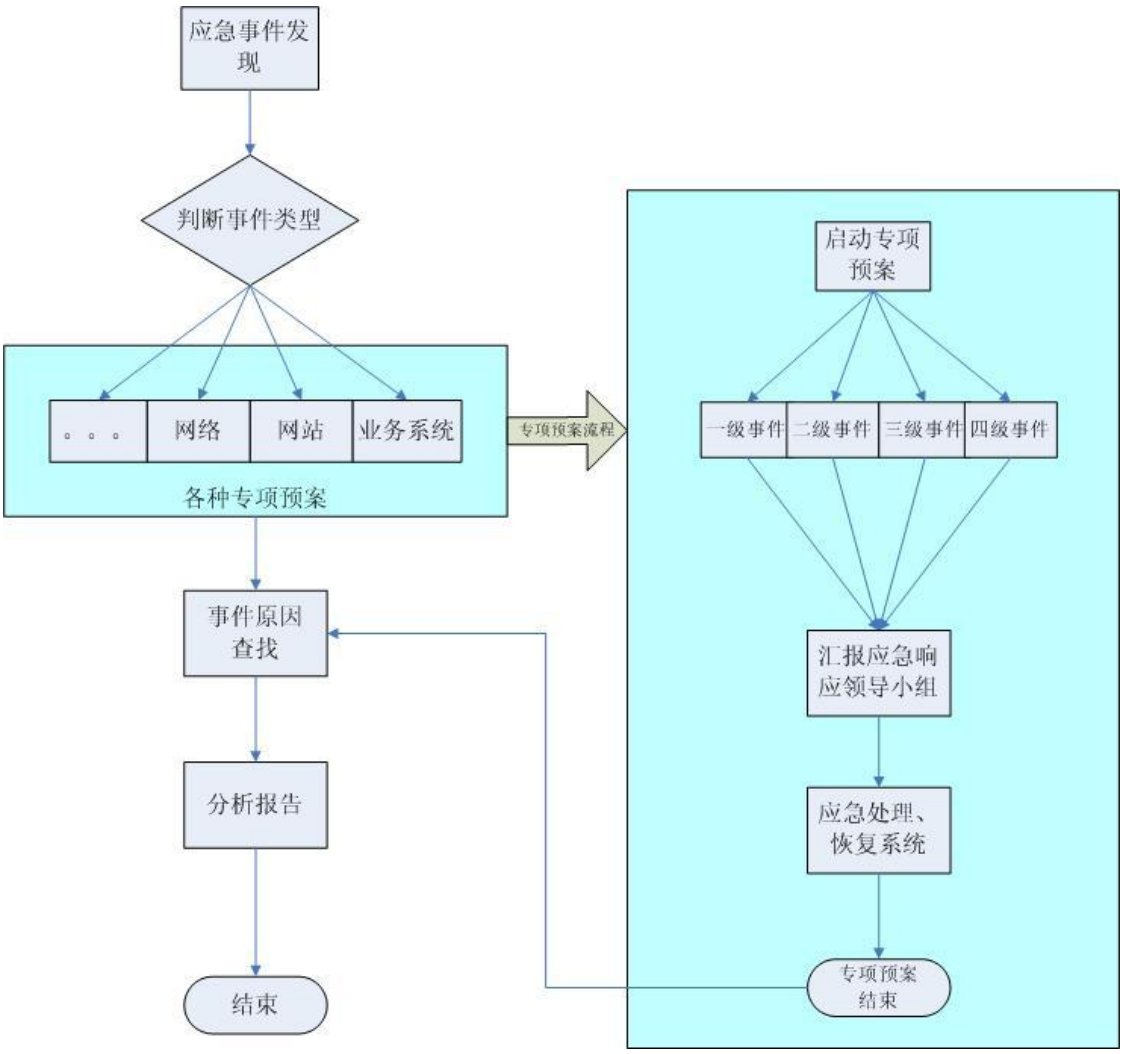
轻度应急事件响应需要在故障系统所涉及的所有技术部门间调动资源，应急事件响应需要及时调用备份设备资源时，可以简化审批手续，事件负责人授权签字即可。

5.3.4. 四级应急事件响应要求

四级定义为一般事件对系统毫无影响，属于日常运维范畴，对应急响应要求没有太高要求，由运维商代为处理。

5.4. 应急事件处理流程

5.4.1. 应急事件处理流程图



5.4.2. 判断事件类型

通过上报事件排除误报行为，确定事件类型，启动相关专项应急预案，并通知相关负责人。

5.4.3. 启动专项预案

确定事件类型和级别后，由负责人启动该专项预案，确定事件级别，是否向应急领导小组汇报情况，由专项负责人协调有关人员，调用相关资源，快速高效的解决应急事件。

5.4.4. 事件处理

根据专项预案内容，第一时间恢复系统，确保系统能够稳定运行，业务恢复运转，具体操作流程详见各专项预案。

5.5. 应急响应总结

事件处理完毕，网络信息系统恢复正常运行后，由应急事件处理人员对整个事件进行分析，总结经验教训，并形成一个应急事件响应总结报告。

报告中应详细记录应急响应事件的起因、处理过程、建议改进的应急方案，估计造成的损失等，备案作为内部参考，并逐步形成知识库，指导以后类似应急事件的响应。

5.6. 后续补救措施

尽快采集相关日志进行时间分析查找出原因，随后采取相应措施避免同样事件再次发生，彻底根除事件影响。

6. 后期处置

6.1. 调查评估

应急响应小组对网络安全事件的起因、性质、影响、责任、经验教训和恢复重建等问题进行调查和评估。

(1)、责任确定。应急处置工作结束后，应当分析产生该次事件的原因，对事件进行调查，确定责任人。如果涉及违法犯罪行为，由司法机关及时追究当事人的刑事责任。

(2)、事件备案与归档。应急处置工作结束后，实施事件处置的过程和结果须备案。

(3)、预案维护。应急处置工作结束后，需根据应急过程中暴露的问题和调查评估的结果，对预案进行相应的修改和维护。

6.2. 恢复重建

在对可利用的资源进行评估后，制订重建和恢复生产的计划，迅速采取各种有效措施，恢复网络与网络信息系统的正常运行。

6.3. 信息发布

信息发布由中国地质大学（北京）统一管理。

6.4. 文档管理

对于整个应急事件响应处理的所有过程，都需要有详细的文档记录，部分文档需要经过应急领导小组或应急响应小组组长的签字和审批。

涉及到的应急事件应急记录文档包括以下内容，可根据应急事件类型选择生成部分文档：

- 《应急事件通报》
- 《故障分析报告》
- 《故障解决报告》
- 《应急响应分析报告》

所有文档记录标明具体的日期和人员，并有明确的文档编号。所有文档按照事件和日期统一归档保存。

事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

7. 预防工作

7.1. 日常管理

要求各部门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

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，提高应急处置能力。应急响应演练是模拟突发网络安全事件，中国地质大学（北京）相关人员组织开发商、运维商按照应急预案所进行的一系列活动和措施。每隔一定时间(一年)，或更新应急预案后，或遇有可预见的安全事件时，要开展应急响应演练，以检验应急预案的正确性，不断加强人员的应急安全意识和应急响应的熟练程度。

应急响应演练以应急预案为基础，在每次演练前应首先确定演练的目标和范围，制定详细、严谨的应急响应演练方案，避免对正常业务造成不必要影响。应急响应演练的范围可视具体情况而定。应急响应演练过程中如需涉及上级主管部门或其他相关部门，应事先做好协调沟通工作，避免由于协调工作不到位而导致对这些部门的正常工作的干扰。如果应急响应演练过程涉及到社会网络服务机构，需要事先与其进行协商，并明确服务范围、服务级别及相关费用等事项。

在每次应急响应过程结束之后，应针对应急响应工作过程中遇到的问题，分析应急响应预案的科学性和合理性，针对预案中的问题进行修改。修改后的预案应经评估通过后，发布实施。

7.3. 宣传

充分利用各种传播媒介及有效的形式，加强网络安全突发公共事件应急和处置的有关法律、法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高防范意识和应急处置能力。中国地质大学（北京）要制定相应的教育材料，普遍开展网络安全教育，及时向社会和公众公布有关信息网络突发公共事件应急预案、报警电话等。

加强对网络安全等方面的知识培训，提高防范意识及技能，指定专人负责安全技术工作。并将网络安全突发公共事件的应急管理、工作流程等列为行政管理干部的培训内容，增强应急处置工作的组织能力。

7.4. 培训

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。

应急响应培训用于确保整个应急响应体系或单位内的所有人员具备了对网络安全事件的意识和知识，确保所有人员了解了本单位应急响应的策略和应急预案，并能够熟练执行应急预案。

应急响应培训应建立在日常安全培训的基础上，或作为日常安全培训的一部分，主要培训有关应急准备和应急响应的各项知识、技术、技能和经验。

应急响应培训的重点是应急预案，使所有人员了解各自在应急响应工作中的职责，明确发生网络安全事件时应采取的行动步骤。可针对不同角色的人员设置不同的培训内

容，例如安全管理员应接受有关安全工具使用的培训，安全分析员应接受最新的入侵技术及攻击特征识别的培训。

应急响应培训应定期更新，并通过实际的应急响应演练过程，帮助所有人员不断更新应急响应相关的知识和技能，同时有助于促进人员的安全意识和应急响应的熟练程度，提高突发事件时应急响应的效率。应强调培训效果的反馈机制和培训计划的更新机制，通过应急响应演练方式等及时发现培训计划中存在的问题，依据这些反馈结果调整培训的课程设置、培训的时间计划以及培训的重点。由于关键岗位的人力资源同样需要备份，对于各关键岗位均必须培训多个能胜任该工作岗位应急工作的人员，保证人员的连续性。

7.5. 重要活动期间的预防措施

在国家重要活动、会议期间，要加强网络安全事件的防范和应急响应，确保网络安全。应急领导小组协调网络安全保障工作，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. 保障措施

8.1. 通信与信息保障

及时维护网络信息系统开放商、系统维护商、安全服务提供商、设备提供商以及本单位相关人员联系表，并确保联系方式有效。

8.2. 应急设备保障

各重要网络与网络信息系统的单位在建设系统时应事先预留一定的应急设备，建立软件、信息网络硬件等应急物资库。在网络安全事件发生时，由应急领导小组负责统一调用。

同时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。

8.3. 数据保障

重要网络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。各个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。

8.4. 基础平台

加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

8.5. 技术研发和产业促进

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。

8.6. 应急队伍保障

按照一专多能的要求建立网络安全应急保障队伍。由应急领导小组选择若干经国家有关部门资质认可的，管理规范、服务能力较强的企业作为单位网络与网络安全的社会应急支援单位，提供技术支持与服务；必要时能够有效调动机关团体、企事业单位等保障力量，进行技术支援。

8.7. 经费保障

领导小组办公室负责协调网络安全事件应急管理工作的日常运作、应急处置和基础设施运维等应急管理经费预算。

8.8. 责任与惩罚

重要网络与网络信息系统的主管人员要认真贯彻落实预案的各项要求与任务，建立监督检查和奖惩机制。应急领导小组将不定期进行检查，对各项制度、计划、方案、人员、物资等进行实地验证，并以演练的评定结果作为是否有效落实预案的依据。对未有效落实预案各项规定的单位和部门进行指导改正。

对下列情况可以经应急响应小组评估审核，报应急领导小组批准后予以奖励。

- 在应急行动中做出特殊贡献的先进单位和集体；
- 在应急行动中提出重要建议方案，节约大量应急资源或避免重大损失的人员；
- 在应急行动第一线做出重大成绩的现场作业人员。

在发生重大网络安全事件后，有关责任单位、责任人有瞒报、缓报、漏报和其它失职、渎职行为的，应急领导小组将予以通报批评；对造成严重不良后果的，将视情节由有关主管部门追究责任领导和责任人的行政责任；构成犯罪的，由有关部门依法追究其法律责任。

9. 附则

9.1. 预案的制定

本预案由应急领导小组负责制订、修订，报相关部门批准后实施。本单位应根据本预案，制定部门和本行政区域的网络安全应急预案。在上级预案或相关的法律标准修改后，本预案应进行调整与其保持一致。调整后，应急响应小组应组织专家组对其评审，评审通过后发布实施。

9.2. 解释部门

本预案由网络安全和信息化工作领导小组办公室负责解释。

9.3. 实施时间

本预案自发布之日起实施。

附件 1

名词术语

一、重要网络与网络信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和网络信息系统。

（参考依据：《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007））

二、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果：

a) 损害国防、国际关系；

b) 损害国家财产、公共利益以及个人财产或人身安全；

c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d) 影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；

e) 干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f) 危害国家关键基础设施、政府网络信息系统安全；

g) 影响市场秩序，造成不公平竞争，破坏市场规律；

h) 可推论出国家秘密事项；

i) 侵犯个人隐私、企业商业秘密和知识产权；

j) 损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术云计算服务安全指南》（GB/T31167-2014））

附件 2

网络和网络信息系统损失程度划分说明

网络和网络信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a) 特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b) 严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c) 较大的系统损失：造成系统中断，明显影响系统效率，使重要网络信息系统或一般网络信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d) 较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。