网络信息安全事件应急预案

国家高能物理科学数据中心大湾区分中心

二〇二〇年十二月一日

网络信息安全事件应急预案

第一章　总则

第一条 为健全国家高能物理科学数据中心大湾区分中心网络信息安全事件应急工作机制，提高应对网络信息安全事件能力，预防和减少网络信息安全事件造成的损失和危害，保护国家高能物理科学数据中心大湾区分中心正常科研秩序，根据《国家高能物理科学数据中心大湾区分中心网络信息安全管理办法》，制定本应急预案。

第二条 网络信息安全事件应急工作坚持统一领导、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信息安全事件的预防和处置工作。

第三条 计算机网络系统统筹协调组织国家高能物理科学数据中心大湾区分中心网络信息安全事件应对工作，工作开展过程中涉及的其他部门或人员应积极配合。必要时成立国家高能物理科学数据中心大湾区分中心网络信息安全事件应急指挥部，负责特别重大网络信息安全事件处置的指挥和协调。

第四条 各系统、部门负责人负责本部门管理的信息系统的网络信息安全事件应急响应相关的协调工作。

第二章　网络信息安全事件分类和分级

第五条 根据《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007），结合国家高能物理科学数据中心大湾区分中心网络信息安全工作实际，对网络信息安全事件进行分类和分级。

第六条 网络信息安全事件根据其起因和表现，分为以下九类：

1.有害程序事件。包括计算机病毒、蠕虫、木马、僵尸网络、网页内嵌恶意代码等；

2.网络攻击事件。包括拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、干扰、APT 攻击等；

3.信息破坏事件。包括信息篡改、信息假冒、敏感信息泄露、重要信息窃取、重要数据丢失等；

4.信息内容安全事件。包括利用网络发布违法违规信息、非法篡改网站等；

5.设备设施故障。包括软硬件自身故障、外围设施故障、人为破坏事故等导致的网络信息安全事件；

6.灾害性事件。指由于自然灾害等其他突发事件导致的信息安全事件；

7.漏洞或隐患事件。指由本所执行安全检测、检查发现的信息系统存在漏洞或安全隐患需要立即整改的情形；

8.安全通报事件。指收到中科院、公安部、国家互联网应急响应中心等上级主管部门通知或通报我所存在安全漏洞或隐患需要立即整改的情形；

9.其他安全事件。指不能归为以上分类的网络信息安全事件。

第七条 根据涉事信息系统的重要程度、事件造成的损失和社会影响，将网络信息安全事件进行分为以下四级：

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信息安全事件。

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信息安全事件；

（4）中科院、公安部、国家互联网应急响应中心等上级主管部门通报的网络信息安全事件。

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信息安全事件；

（4）由本所执行安全检测、检查发现的信息系统存在需立即整改的漏洞或安全隐患事件。

4.符合以下情形之一的，为一般网络信息安全事件：

（1）重要网络信息系统遭受一般的系统损失，造成系统短时间中断，业务处理能力受到一般影响；

（2）由本所执行安全检测、检查发现的信息系统存在的低风险漏洞或安全隐患事件；

（3）其他一般网络信息安全事件。

第三章　监测与预警

第八条 网络信息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、较大和一般网络信息安全事件。

第九条 各信息系统安全责任人对其负责的信息系统需开展日常安全监测工作。计算网络系统对全所网络安全整体运行情况开展日常监测工作。

第十条 网络安全技术人员根据安全运行监测信息及其他信息综合评估，启动相应安全预警级别。启动黄色预警应向安全应急小组汇报，启动橙色和红色预警应向高能所计算中心网络工作领导小组汇报。

第十一条 预警响应

1.蓝色预警响应：网络技术人员与网络安全人员加强安全防护和监控，对已发生的安全事件进行调查处置。

2.黄色预警响应：网络技术人员与网络安全技术人员全面加强安全防护，对重要系统进行密切监控，对发生的安全事件及时迅速处理。对安全态势和情况进行上报。

3.橙色、红色预警响应：必要时成立应急指挥部，对事态发展情况进行跟踪评估，研究制定防范措施和应急工作方案，协调组织资源和技术力量应对安全事件，应急指挥部实行 24 小时值班。必要时向上级主管部门汇报。

第十二条 预警解除。当不具备蓝色预警启动条件时，网络安全人员应宣布安全预警解除。

第四章　安全事件应急处置

第十三条 安全事件发现与确认

1.网络信息系统的管理员在日常运维和安全监测中发现系统可能发生安全事件的，应及时联系网络安全技术人员。网络安全技术人员对安全事件进行确认和分级。

2.计算机网络系统在日常安全运行监控、检查或评估中发现各类安全事件的，应及时联系系统管理员和网络安全技术人员对安全事件进行确认和分级。

3.收到上级主管部门或其他来源的安全通报或通知信息，应由计算机网络系统的网络安全相关人员讨论并对事件进行确认和分级。

第十四条 事件报告。在确认安全事件后，根据事件级别立即启动应急预案，网络安全人员向上汇报事件及其处理进展，启动相应预警级别，开展应急处置工作。

第十五条 网络信息安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络信息安全事件。I 级为最高响应级别。

第十六条 安全事件分级处置

1.IV 级响应：安全应急小组安排安全技术人员，与涉事系统安全责任人一起调查和处理安全事件。

2.III 级响应：事件上报计算中心网络工作领导小组。安全应急小组与涉事系统安全责任人、系统管理员和系统开发人员一

起分析和处理安全事件。必要时协调厂商技术人员进行应急支持。

3. II 级响应：事件上报高能所信息化和网络领导小组。在领导小组指导下，安全应急小组协调各方面资源和人力调查处理安全事件。

4. I 级响应：事件上报高能所信息化和网络领导小组。成立应急指挥部，履行应急处置工作的统一领导、指挥、协调职责，指挥部 24 小时值班。必要时向上级主管部门汇报或请求协助。

第十七条 安全事件跟踪与记录。安全应急小组应对安全事件的处置过程做好记录。

第十八条 事后分析。安全事件处理完毕后，安全应急小组应对事件的全过程进行分析。研究事件发生的原因，评估事件造成的损失和影响。根据分析结果对现有安全防护机制进行修订和完善。

第五章　各类安全事件处理流程

第十九条 有害程序事件

1. 对于一般性病毒、木马，使用反病毒软件进行查杀，或者定位恶意进程、文件后进行删除；

2. 当发现计算机感染了传播性较强或者危害程度较大的病毒时，应立即将该计算机从网络上隔离出来；

3. 当发现计算机感染了勒索病毒，并且正在加密文件时，应立即关闭计算机电源。将磁盘挂载到另一台计算机进行数据紧急

备份和病毒查杀；

4.当发现无法清除的病毒木马时，应联络专业反病毒厂商处理；

5.当发现利用某些端口的软件漏洞进行扩散的病毒时，可应急采取在网络交换机上封锁特定端口的措施；

6.当发现严重的病毒大规模爆发事件时，应启动橙色预警；

7.病毒、木马处理完毕，并进行安全加固后，将计算机重新接入网络。

第二十条 网络攻击事件

1.发现计算机、服务器、网站或信息系统被黑客入侵时，应立即切断该计算机或服务器与互联网的连接，保护现场；

2.对重要配置文件、日志和重要数据进行紧急备份。防止损失进一步扩大；

3.网络安全技术人员对入侵事件进行分析、取证和溯源；

4.针对入侵的原因进行安全加固，恢复系统并重新上线；

5.当发现拒绝服务攻击时，安全应急小组应及时对攻击流量进行分析，对恶意攻击流量进行阻断。当出现分布式拒绝服务攻击时，紧急启动白名单模式，保障信息系统的基本可用性，同时联系科技网应急中心进行处理。

第二十一条 信息破坏事件

1.当发生信息篡改、信息假冒、信息泄露、数据丢失等事件

时，应立即断开涉事信息系统与互联网的连接；

2.安全应急小组组织技术人员与系统管理员一起调查信息破坏的原因；

3.对存在的安全漏洞和隐患进行整改，对系统的数据安全防护方案重新评估；

4.利用备份数据对被篡改或丢失的数据进行恢复；

5.发生敏感信息泄露的（如账号、口令等），应立即修改相关信息；

6.安全加固完成、数据恢复后，将信息系统重新上线。

第二十二条 信息内容安全事件

1.当发现信息内容安全事件时，应立即切断涉事信息系统的网络。同时采取措施消除事件造成的影响；

2.安全应急小组组织技术人员对事件原因进行调查取证；

3.对于内部人员发布违规信息的，按照相关规章制度处理；

4.对于由于安全漏洞原因，系统被黑客入侵并发布违规信息的，保留相关证据和记录；

5.在删除违规内容、修复安全漏洞和隐患之后，对系统重新上线。

第二十三条 设备设施故障

1.当确认安全事件成因是系统软硬件等设备设施故障时，相关系统管理员应尽快修复设备或设施故障，必要时联系厂商协助

处理；

2.在系统恢复正常后，安全应急小组与管理员一起确认系统功能和数据恢复正常，并进行安全评估通过后，重新上线提供服务。

第二十四条 灾害性事件

1.当确认安全事件成因是自然灾害等不可抗力时，应尽快确定损失范围，根据事件严重程度，应上报计算中心或所级事件应急机构统一指挥和协调处理；

2.在救灾工作完成后，开展信息系统软硬件和重要数据的重建和恢复工作；

3.在信息系统恢复测试正常，经过安全评估后，重新上线提供服务。

第二十五条 漏洞或隐患事件

1.发现计算机、服务器、网站或信息系统存在安全漏洞或隐患时，立即联系系统管理员进行核实；

2.评估漏洞或隐患的影响，以及安全加固工作对系统可能造成的影响和可行性；

3.制定并推动安全整改方案的实施；

4.核实、检查漏洞或隐患整改实施的效果；

5.形成信息系统安全检查处理档案。

第二十六条 安全通报事件

1.根据安全通报信息，立即联系系统管理员对通报内容进行核实；

2.评估漏洞或隐患的影响，以及安全加固工作对系统可能造成的影响和可行性；

3.制定并推动安全整改方案的实施；

4.核实、检查漏洞或隐患整改实施的效果；

5.形成信息系统安全检查处理档案；

6.根据安全通报要求，反馈安全整改报告。

第二十七条 其他事件。当发生其他安全事件时，由安全应急小组讨论，制定临时处置方案。

第六章 预案管理

第二十八条 计算机网络系统每年应组织一次网络信息安全事件应急预案演练，检验和完善预案。

第二十九条 计算机网络系统应对相关人员开展应急预案宣传和培训。

第三十条 在重要活动网络安全保障时期，安全预警级别比平时提高一级。

第七章 附则

第三十一条 本应急预案的解释权归国家高能物理科学数据中心大湾区分中心计算机网络系统。

第三十二条 本应急预案自发布之日起实施。