网络信息安全管理办法

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

网络信息安全管理办法

第一章　总则

第一条 为规范和加强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，保障国家高能物理科学数据中心大湾区分中心网络信息系统稳定运行，提高国家高能物理科学数据中心大湾区分中心网络信息安全防护能力，根据《中华人民共和国网络安全法》和《中国科学院网络安全工作管理办法（试行）》等有关指导文件，制定此办法。

第二条 国家高能物理科学数据中心大湾区分中心网络信息系统包括：直接或间接与国家高能物理科学数据中心大湾区分中心网络相连接的个人计算机、工作站、服务器以及所有外设；国家高能物理科学数据中心大湾区分中心统一购置和所内各单位、课题拥有的计算机、工作站、服务器及网络设备；合作单位及来访人员接入国家高能物理科学数据中心大湾区分中心网络的计算机及网络设备；国家高能物理科学数据中心大湾区分中心提供的所有计算服务、软件程序、文件数据、电子邮件等各种网络信息服务。

第三条 “用户”指所有长期或临时使用国家高能物理科学数据中心大湾区分中心网络信息系统的人员，包括但不限于员工、

学生、来访者。

第四条 网络信息安全工作遵循“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，实行统一领导、分级治理、定责到人。

第五条 坚持网络信息化发展与安全并重。网络信息系统与安全应同步规划、同步建设、同步运维。

第六条 违反本管理办法，特别是滥用或恶意使用国家高能物理科学数据中心大湾区分中心网络信息系统对我所网络信息安全工作造成重大影响者，国家高能物理科学数据中心大湾区分中心有权追究其法律责任。

第二章　　基本原则

第七条 计算机网络系统是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和运维的职能部门，负责网络信息安全工作的规划、建设和实施。

第八条 国家高能物理科学数据中心大湾区分中心网络信息系统的所有者或管理员为该设备或系统的安全责任人，负责其设备或系统的安全配置和管理。

第九条 用户使用国家高能物理科学数据中心大湾区分中心网络信息系统仅可以从事科研相关的活动。非公用途的条款参见第十章。

第十条 国家高能物理科学数据中心大湾区分中心将采取各

种措施尽力维护网络信息系统的正常运转，对因不可抗拒的因素造成的信息丢失或泄露，高能所不承担责任。

第三章　用户账号安全

第十一条 应保证个人账号安全，妥善管理和保存个人账号和口令相关信息。

第十二条 不得盗用他人账号，不得将个人账号转借给他人使用。

第十三条 一旦发现账号被盗用，必须及时向计算机网络系统报告。

第四章　用户个人终端安全

第十四条 必须遵守知识产权的相关法律，不得安装使用盗版软件，不得破坏国家高能物理科学数据中心大湾区分中心与第三方签订的硬件、软件、网络以及服务相关的知识产权条款。计算机网络系统不对使用盗版软件的计算机和软件提供技术支持。

第十五条 终端接入国家高能物理科学数据中心大湾区分中心网络前，应及时启动本机防火墙。

第十六条 应安装防病毒软件，保持病毒库更新，并定期进行病毒木马查杀。

第十七条 应及时更新操作系统和软件的安全补丁。

第十八条 拒绝采取安全措施的个人终端设备不得接入高能

所网络。

第十九条 一旦发现个人终端设备被攻击或者疑似攻击，应及时和计算机网络系统联系。

第五章　用户网络安全

第二十条 所有接入国家高能物理科学数据中心大湾区分中心网络计算机或网络设备必须完成硬件配置信息、主要使用人、系统管理人联系方式（包括电话、邮件地址）、IP 地址、使用地点等信息登记。

第二十一条 用户不得改动任何网络设施、结构和配置。

第二十二条 任何新增接入国家高能物理科学数据中心大湾区分中心网络计算机等终端设备或者变更现有设备信息，必须得到计算中心的同意，在获得新的 IP 地址和端口后方可接入网络。

第二十三条 用户不得占用出口带宽和所内网络带宽传输或下载与工作无关的数据、媒体资料、非法软件和有可能含有病毒的软件。

第二十四条 网络管理员将监测国家高能物理科学数据中心大湾区分中心网络运行使用情况，对非正常使用网络的用户将进行提醒、警告或终止网络通讯。用户必须配合网络管理员对问题进行调查，以便及时解决影响网络正常运行的问题。

第六章　电子邮件安全

第二十七条 使用国家高能物理科学数据中心大湾区分中心的邮件服务器不得发送邮件炸弹、发送或传播垃圾邮件、发送或传播带有攻击性、侮辱性内容或违反国家法律法规的邮件。

第二十八条 不打开来历不明的邮件。如接收到带有病毒或其他有害内容的邮件，应立刻向计算机网络系统邮件服务管理员报告。

第二十九条 使用加密协议进行个人终端和邮件服务器之间的网络通讯。

第七章　网络安全运行管理

第三十条 网络安全运行管理具体工作由计算中心承担。

第三十一条 应根据国家相关法律法规和标准规范，不断修订和完善高能所网络信息安全各项管理制度和流程。

第三十二条 应按照国家网络安全等级保护制度要求，开展等级保护相关工作。

第三十三条 应定期开展网络安全检查、信息资产梳理、安全评估、风险处置和隐患整改。对于维护不力、漏洞和隐患较多且无法完成整改的系统予以关停。

第三十四条 应严格管理对外发布的网站和信息系统，坚持非必要不得对外提供服务、未通过安全评估不得对外提供服务的原则。对外提供服务的信息系统，应进行备案。

第三十五条 应定期开展网络安全教育培训，提高网络安全

防范意识。

第三十六条 应落实网络安全技术保障措施，监测和记录网络安全运行状态，对可疑网络通信予以阻断，并保存不少于六个月网络安全运行日志。

第八章　事件应急处置

第三十七条 事件应急处置具体工作由计算机网络系统承担。

第三十八条 应制订网络信息安全事件应急预案，并定期组织演练。

第三十九条 应根据网络信息安全事件发生后的危害程度、影响范围等因素对事件进行分级，并规定相应的应急处理措施。

第四十条 发现网络信息安全事件时，应立即启动网络信息安全事件应急预案，对事件进行调查、评估和处理，并及时向上汇报事件处理进展。

第四十一条 国家高能物理科学数据中心大湾区分中心各部门和单位应对网络信息安全事件的处置给予必要的支持与协助。

第四十二条 网络信息安全事件涉及到的信息设备、系统的使用人和管理员应配合事件的调查和处理。

第九章　责任与处罚

第四十三条 用户应对违反本管理办法造成的后果负责。

第四十四条 用户违反本管理办法，根据事件的严重程度，

安全管理员、系统管理员或用户所在单位的负责人将向当事人进行提示或警告。情节严重的，国家高能物理科学数据中心大湾区分中心有权追究其法律责任。

第十章　关于非公用途

第四十五条 “非公用途”指所有与工作无关的活动。

第四十六条 国家高能物理科学数据中心大湾区分中心网络信息系统用于非公用途不得影响高能所网络的正常工作，并必须符合（但不仅限于）以下条件：

1.应在下班时间或休息时间进行；

2.不得影响本职工作，不得影响他人的工作；

3.不得从事商业或赢利性的活动；

4.不得从事攻击性、破坏性或侮辱性的活动；

5.不得从事任何违反国家法律法规的活动。

第十一章　附则

第四十七条 本规定由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负责解释。

第四十八条 涉及国家秘密的网络安全工作，按照保密相关规定执行。

第四十九条 本办法自发布之日起生效。