恶意代码防范管理制度

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

恶意代码防范管理制度

第一条 为加强国家高能物理科学数据中心大湾区分中心网络及信息系统服务器对恶意代码的预防，避免信息系统及操作系统遭受恶意代码攻击和感染，特制定本细则。

第二条 本规定所称的恶意代码包含病毒、木马、蠕虫等，是指编制者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

第三条 计算机网络系统负责对所管理的服务器统一安装防病毒软件，更新病毒库，定期进行全网扫描；开展防病毒监控，及时发现防病毒预警，并对防火墙和路由器等设备进行配置。负责研究所病毒事件的协调处理和及时解决。

第四条 各信息系统应统一规划、统一部署具有国家许可的正版计算机防病毒系统软件，信息系统中所有服务器和终端必须安装配发的计算机防病毒软件，否则不允许连入网络和处理工作。

第五条 各信息系统内的所有服务器和计算机终端应使用正版软件，禁止随意安装软件，防止其中可能存在恶意软件。

第六条 服务器、终端计算机一旦发现被计算机病毒感染，应先将计算机与网络隔离，确保病毒库已更新至最新版本,并及时进行病毒查杀处理；当情况严重且无法在规定时限内紧急恢复或有效控制时，应按照《国家高能物理科学数据中心大湾区分中心网络信息安全应急预案》及时启动急响应预案，应注意保留防病毒系统记录。

第七条 系统管理员应定期执行计算机恶意代码检测、清除工作，检测并扫描所有的计算机硬盘分区，发现硬盘中可能存在恶意代码或异常情况应及时处理，同时将检测与处理结果记录备案。

第八条 对新购置的计算机软件或系统上线前应进行恶意代码检测。

第九条 本细则由计算机网络系统负责解释和修订，自发布之日起执行。