园区网与控制网边界
安全管理细则

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

园区网与控制网边界安全管理细则

第一章　总 则

第一条 为加强国家高能物理科学数据中心大湾区分中心园区网络与控制网络边界的安全管理，确保控制网络安全、可靠、稳定地运行和业务的正常运行，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》和《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实施细则》，特制定本细则。

第二条 国家高能物理科学数据中心大湾区分中心园区网络与各控制网络边界的基本安全策略为：

（一） 默认及缺省情况下，禁止一切数据通信，阻断所有通信流量。

（二） 根据各控制网络特殊的与园区网络资源通信的使用需求，放开相应的访问权限，并密切关注开放权限的通信流量情况。对已开放的通信策略，无用即回收。

（三） 禁止各控制网络内部设备访问互联网资源及与互联网之间的通信。

第三条 本办法适用于国家高能物理科学数据中心大湾区分中心园区网络以及加速器控制网络、靶站普仪控制网络。

第二章　基本原则

第四条 计算机网络系统负责国家高能物理科学数据中心大湾区分中心园区网络的总体规划，负责国家高能物理科学数据中心大湾区分中心园区网络及园区网络与控制网络边界的网络安全规划与建设等。

第五条 加速器控制网络、靶站普仪控制网络需要指定专人负责本部门网络的运维管理。

第六条 控制网网络管理员负责控制网内部网络安全的规划与建设，网络安全的日常运维，应急响应等。

第七条 控制网网络管理员负责控制网络内 IP 地址的规划、登记、维护和分配，并及时更新 IP 地址的使用信息。

第八条 服务器等设备入网前需要进行安全检查，确保没有问题后再接入到控制网络内部。网络规划、建设时应采用区域划分、逻辑隔离的方法，限制病毒的传播范围，做到可防可控。同时，对重要通信线路、关键设备采用冗余的方法，保障整体系统稳定运行。

第九条 网络内所有的远程访问必须具备身份鉴别和访问授权控制，至少应采用用户名/口令方式，密码级别需达到“强”级别及以上。

第十条 在网络上传输机密数据信息时，必须启用可靠的加密算法保证数据传输安全。

第十一条 网络在规划、建设过程中应充分考虑边界防护功能，针对关键网络节点处的网络攻击行为的检测、防护和审计告

警，以保证跨域访问的数据流经过受控接口进行通信。

第三章　安全规则

第十二条 控制网络与园区网络之间，如因业务访问需要开通服务端口时，需填写《防火墙规则变更申请表》（附件 1），并将端口描述的详细信息予以说明，经过领导审批后，交由计算机网络系统开通相应端口。

第十三条 严格控制网络资源的通信授权，按照最小权限原则对设备资源进行授权。

第四章　附 则

第十四条 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。

第十五条 本办法自发布之日起生效。

附件 1：防火墙规则变更申请表

申请人姓名		联系电话	
申请人 Email		申请日期	
申请目的和需求			
需要设置以下规则的 IP 地址			
对所内网开放的 TCP 端口			
对所内网开放的 UDP 端口			
对所外网开放的 TCP 端口			
对所外开放的 UDP 端口			
对特定 IP 开放的 TCP 端口			
对特定 IP 开放的 UDP 端口			
申请人签字			
系统负责人签字			
主任签字			
备注			