教育技术中心文件

教育技术中心发〔2022〕1号

教育技术中心
关于印发《冬奥会和东残奥会网络安全保障方案》的通知

各单位、各部门：

《冬奥会和东残奥会网络安全保障方案》已经研究通过，现印发给你们，请认真贯彻执行。

特此通知。

教育技术中心

2022年1月5日

冬奥会和东残奥会网络安全保障方案

冬奥会和东残奥会的顺利召开，是国家乃至全世界的大事，保障冬奥会和东残奥会网络安全是教育系统的重要政治任务，为贯彻落实习近平总书记关于网络安全的重要指示精神，根据教育部办公厅、省教育厅的要求，结合我校的实际情况，制定此方案。

一、开展网络安全风险隐患自查，将发现的安全问题和风险隐患进行整改

1. 对学校的网络和信息系统进行排查和清理，重点是长期闲置的僵尸域名和系统。

2. 加强对于庆祝冬奥会、东残奥会直接相关、包含大量敏感信息和公民隐私信息，直接影响教学和管理的关键业务系统进行风险评估，并整改。

3. 梳理网络资产，做好门户网站、电子邮件系统以及其他核心业务系统问题隐患的排查。

二、加强网络安全管理，提高技术防护措施

1. 加强校园基础网络防护，保障校园网络的稳定运行。加强电子政务内网防护，强化敏感设备设施管控。

2. 加强对学校官网、教学资源平台等监测，定时扫描文件、链接、页面，及时发现和处置页面篡改、域名劫持、被插入暗链和跳转代码等安全事件。

3. 加强教育数据保护，重点加强重要数据和个人信息保护，

采用加强数据存储加密，限制数据访问权限，杜绝数据库违规外联，开展重要数据备份措施防止数据数据的外泄和破坏。

4.加强邮件安全，及时删除离职人员账户，优化邮件防护策略，提高对钓鱼邮件，仿冒、垃圾邮件的筛查能力，并加强师生邮件安全意识教育，提高对钓鱼邮件，仿冒邮件的辨识能力。

5.终端安全保障。做好系统的补丁升级和漏洞修复措施，关闭主机和终端不必要的端口、共享访问以及桌面的远程连接，安装并及时升级杀毒软件。定期对重要数据进行备份，防止勒索病毒破坏。

三、开展重点领域网络安全防护专项检查

加强网站的技术防护体系建设和应用管理，提高安全防护水平。重点对网站防篡改、防病毒、防攻击、防瘫痪、防泄密能力进行全面风险评估，找出薄弱环节，及时予以整改。

委托第三方网络安全机构（如千城、绿盟等），对学校网站进行漏洞扫描，对出现的问题进行及时处理并加以整改，保证学校网络的安全稳定。

四、完善网络安全应急机制，加强重要时期值班值守

1.重要时期必须对外开放的信息系统为学校官网和电子邮件系统，重要时间节点进行访问时间控制，值班人员熟知一键断网手段。组织开展一次以网站被篡改事件处置为核心的应急演练检查网络安全应急处置水平。

2.落实应急值守和零报告制度。在网络安全重要保障时期。

要加强应急值守，保持联络通畅，关键岗位、关键时间节点严格执行 7*24 小时值守和领导带班制度，重要保障期间每天 15 时上报 24 小时内的网络安全工作情况。

3. 发生网络安全事件，及时按照《河北省教育系统网络安全事件应急响应预案》以及《承德医学院网络与信息安全事件专项应急预案》的要求，第一时间采取有力措施将拂面影响降到最低，并及时报省教育厅 24 小时值守电话。重大事件并及时报承德市网信办，并加强舆情应对。

承德医学院教育技术中心　　2022 年 1 月 5 日印发