湖南省教育厅

湘教通〔2019〕157号

关于加强教育系统重要数据安全管理防范泄露工作的通知

各市州教育（体）局、高等学校，厅委直属各单位:

近期，我国发生多起敏感和重要数据信息泄露事件。为认真贯彻落实中央领导关于敏感、重要数据库信息泄露事件指示精神，按照湖南省公安厅《关于开展防范重要数据和公民个人信息泄露工作的函》要求，现就加强教育系统重要数据和公民个人信息安全防护工作，严防发生重要数据和公民个人信息泄露事件有关事项通知如下:

一、加强组织领导，规范数据安全管理

1.进一步明确和落实数据安全管理责任。重要数据和公民个人信息等敏感数据安全事关国家安全和社会稳定，各单位网络安全和信息化领导小组应加强对数据安全工作的全面领导，制订数据管理办法，规范数据采集、存储、使用、开发和交换共享流程；应指定机构和人员负责数据安全管理，建立数据安全审核和保密

审查制度，明确审核审查程序，确保数据全生命周期的安全。

2.加强网站重要和敏感数据发布管理。各单位应建立和完善数据发布管理制度，指定专人负责数据网上发布的审核，凡涉及到单位重要数据和公民个人隐私数据上网发布的，必须进行脱敏处理。各单位应全面清查网站数据发布情况，对发布的数据中存在法律和行政法规禁止发布或传输的重要数据、涉及到公民个人隐私的敏感数据的，必须采取措施立即整改。

3.加强信息系统的网络安全管理。各单位应全面加强对涉及到重要和敏感数据信息系统的安全管理，要全面清理信息系统用户管理权限，特别是加强对超级管理员账号的管理，原则上系统超级管理员不能由运维服务企业人员管理；要加强对信息系统用户密码管理，对使用简单密码必须采取措施更换，并建立定期更新密码的制度。

二、加强安全基础防护能力建设，有效预防数据丢失和泄露事件

1.加快推进网络安全基础设施建设。各单位在推进教育信息化 2.0 建设中，应将网络安全技术防范措施和信息化建设同步实施，及时配置和更新网络防火墙、数据库防火墙、入侵检测、漏洞扫描、数据库审计、数据脱敏、防病毒软件等网络安全产品，有效预防数据采集、存储、使用、开发和交换共享过程中的安全，防止重要数据和个人隐私等敏感数据失、泄露事件发生。

2.全面落实网络安全等级保护制度。各单位应按照《网络安

全法》的要求，参照教育部《教育行业信息系统安全等级保护定级工作指南》，明确信息系统网络安全保护主体责任，落实系统定级备案和测评整改，特别是做好数据的安全检测，加强数据安全管理和技术防范，切实维护重要数据和公民个人信息安全。

3.开展安全监测，及时应对处置网络安全突发事件。各单位应组织技术力量，对本单位关键信息基础设施和重要信息系统开展实时安全监测，发现网络渗透、数据窃取等攻击行为时，及时采取针对性防护措施；应健全网络安全应急处置预案，组织开展应急演练，提高网络安全事件应急处置能力；必须加强日常值班值守，对于发生攻击入侵、数据泄露等网络安全事件时，要第一时间启动预案并妥善处置，固定相关日志，第一时间向受理备案的公安机关和省教育厅报告，配合公安等有关部门开展事件调查和案件侦查。

三、开展专项治理行动，全面清除信息系统数据安全隐患

1.立即开展数据资产清查和网络安全隐患排查工作。各单位应迅速部署排查本单位以及主管或下属的信息系统（网站），以收集、存储、处理重要业务数据和公民个人信息的互联网相关信息系统为重点，全面排查相关信息系统重要数据和公民个人信息在采集存储（含缓存）、传输、使用、提供、销毁等环节的具体情况，摸清本单位重要数据和公民个人信息等敏感数据底数，形成本单位数据资产清单（见附件），于5月15日前报辖区公安机关的同时，通过“湖南省教育网络安全信息上报系统”

（https://aq.hnedu.cn）报送省教育厅信息中心。各单位应全面排查整改信息系统网络安全风险隐患，根据数据资源梳理情况，聚焦数据安全突出风险，紧急排查信息系统数据库存在弱口令、未授权访问、数据明文传输、缺少安全审计、访问控制策略不严、未脱敏使用等突出安全隐患，针对发现的问题立即组织清查整改，完善数据生命周期安全保护，切实提高重要数据和公民个人信息安全保护能力。

2.全面排查物理隔离的业务专网、内部网络边界安全措施。各单位应排查有线无线违规接入互联网的问题，强化网络边界违规外联安全监测和防护，加强内部人员安全管理和责任追究，坚决防止违规外联。对于与互联网逻辑隔离的业务专网和内部网络，要全面排查互联网接入区边界安全防护措施，验证内外网数据交换的安全有效性。要全面排查安全隔离等安全保护措施，并及时升级病毒库，查杀病毒木马，实时监测内外网数据流量，及时阻断外部攻击探测，有效防范黑客通过互联网渗透攻击内网造成数据泄露和丢失。

3.重点排查数据库和基础应用软件运行环境的安全隐患。各单位应重点排查信息系统使用开源数据库（如：MongoDB）和应用软件情况，及时升级数据库和应用软件安全补丁，严格数据访问权限管理，对重要应用软件开展第三方安全检测，防范应用软件供应链安全；全面排查为本单位提供网络系统建设、运维服务厂商及其系统建设情况，防止企业违规私自在互联网上存储

或缓存数据；加强对运维企业的安全监管，与企业在本单位长期驻场运维的人员签订保密协议，进行背景审查和安全检查，防范人员安全风险。对于托管在电信运营商、云服务商、IDC 机房的系统，应主动督促托管部门落实安全管理和技术防范措施，坚决防止通过第三方企业泄露重要数据和公民个人信息。

四、联系方式

湖南省教育厅发展规划处　甘　敏　0731－89920620

湖南省教育厅信息中心　许鞍铭　0731－89728306

吴日云　0731－89728306

附件：1.重要行业部门和存在有大量公民个人信息单位数据资产清单

2.在互联网上存储（含缓存）的重要数据和公民个人信息统计表

湖南省教育厅

2019 年 5 月 8 日

附件 1

教育系统重要数据和公民个人信息资产清单

<table>
<tr><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>单位地址</td><td colspan="4"></td></tr>
<tr><td>网络安全责任部门</td><td colspan="4"></td></tr>
<tr><td rowspan="2">责任部门联系人</td><td>姓　　名</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td></td></tr>
<tr><td>数据保护责任部门</td><td colspan="4"></td></tr>
<tr><td rowspan="2">责任部门联系人</td><td>姓　　名</td><td></td><td>职务/职称</td><td></td></tr>
<tr><td>办公电话</td><td></td><td>移动电话</td><td></td></tr>
<tr><td>单位数据总量（TB/PB）</td><td colspan="4"></td></tr>
<tr><td>数据存储位置</td><td colspan="4">☐互联网　　☐业务专网　　☐互联网和业务专网
☐其他_____</td></tr>
<tr><td>数据内容描述</td><td colspan="4"></td></tr>
<tr><td>数据保护策略</td><td colspan="4"></td></tr>
</table>

附件 2

在互联网上存储（含缓存）的重要数据和公民个人信息统计表

单位信息	信息系统名称	等级保护定级备案编号\定级级别（如没备案填写无）	包含的数据类型	数据量(GB/TB/PB)	数据存储位置	数据库 IP 地址	数据库维护单位、联系人及联系方式
本级部门							
……							

注：包含的数据类型：业务数据/公民个人信息； 数据存储位置：互联网/互联网和业务专网/托管单位。