

广东省教育厅

广东省教育厅办公室关于做好学生 资助信息网络安全隐患排查工作的通知

各地级以上市教育局，各普通高校、省属中职学校、广东实验中学、华南师范大学附属中学、华南师范大学附属小学：

为防范和化解学生资助系统运行和数据管理风险，强化网络安全管理，现就做好学生资助信息网络安全隐患排查工作有关事项通知如下：

一、排查范围

各地各学校要对学生资助信息网络开展安全隐患排查，包括全国学生资助管理信息系统，国家开发银行助学贷款业务管理系统，与学生资助信息有关的各级各类网站、应用系统、新媒体平台、移动 APP、公共场所电子显示屏等。开放访问的网站、含有资助数据和学生个人信息的系统应重点排查。

二、自查自纠

（一）压实责任，强化属地管理。各地各学校使用资助信息系统、网站和各类平台等要严格遵守《中华人民共和国网络安全法》，落实网络安全保护等级制度。抓实防攻击、防病毒、防篡改、防瘫痪、防数据泄密等工作。委托第三方设计开发运营的涉及学生资助数据和个人信息的网站、系统、各类云平台、微信公

众号等，各地各学校承担安全防护职责，托管在外网的网站和信息系统发生的安全责任由业主单位承担。

（二）加强网站和信息系统账号管理，杜绝弱口令。全面排查操作系统、数据库、中间件、信息系统存在的弱口令，屏蔽或删除系统的默认账号，禁用僵尸账号。全国学生资助管理信息系统及各子系统的所有账户、传输数据的电子邮箱，必须定期修改口令，口令长度和复杂性应符合安全要求（口令应含字母、数字、特殊字符，长度 8 至 20 位），不同用途的账号不能设置相同口令。资助系统用户要进行全面清理，限制系统管理员账号数量，合理设置权限，不得使用公共管理账号，妥善保管助学贷款业务管理系统电子密钥，防范业务风险，堵塞安全漏洞。

（三）加强资助数据和学生个人信息保护，排查信息泄露隐患。各级学生资助管理部门应按《全国学生资助管理中心关于切实加强学生资助信息安全等有关事项的紧急通知》（教助中心〔2016〕122 号）要求，规范好学生资助数据用途，对资助数据和学生个人信息的采集、存储、传输、使用、提供、销毁等环节进行严格要求。不得通过 QQ、微信等传输含有学生身份证号、银行账户等个人隐私的信息；系统下载、传输学生数据应通过内网进行，如无法通过内网传输的，应对数据文件进行加密（密码及文件应分开提供）或通过刻录方式交换数据；学生资助数据和个人信息不得存储到公共云盘；加强数据访问权限管理，严防数据泄漏。

(四)加强安全管理,防范安全风险。严格落实网络信息发布审核制度,全面清查所属网站、邮箱、各类新媒体平台,重点检查附件文档,及时删除存在安全隐患或过期信息。须进行公示的资助信息,应严格审查公示内容,学生个人隐私信息或其他不必要信息不得公示。加强对网络运维服务厂商及人员的安全监管,必要时进行背景审查和安全检查,签订保密协议。确需外部人员协助处理的批量拷贝、导入导出资助数据和学生个人信息的,各地各学校安全人员须全程监控,不得使用开放的无人值守的远程控制方式。

三、督促整改

各地各学校务必在4月30日前完成所属网络安全隐患自查整改工作,按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的要求,压实责任,对自查发现的问题和漏洞要及时妥善处理,排除隐患。对因网络安全管理不善造成资助数据或学生信息泄露的,须追究相关人员责任,构成犯罪的,移送司法机关追究刑事责任。

广东省教育厅办公室

2020年4月15日

公开方式：依申请公开

校对人：廖希凯