固原市实验小学网络安全排查报告

按照市教育体育局通知要求，我单位高度重视，根据《关于做好近期全市网络安全保障工作的通知》开展全校网络安全排查，现将排查情况汇报如下:

一、网络信息安全管理机制和制度建设落实情况

(一)维护和规范计算机硬件的使用管理及网络信息安全,提高计算机硬件的正常使用、网络系统安全性及日常办公效率，学校成立由安全副校长担任第一责任人、各相关部门参与、教务处负责具体工作的计算机信息系统安全保护工作领导小组，统一协调全校开展校园网络安全管理工作。

(二)确保计算机网络安全，实行了网络专管员制度、计算机安全保密制度、网站安全管理制度、网络信息安全突发事件应急预案等保障制度。同时结合自身情况制定计算机系统安全自查工作制度，做到三个确保:一是系统管理员定期检查中心计算机系统，确保无隐患问题;二是制作安全检查工作记录，确保工作落实;三是定期组织有关人员学习有关网络及信息安全的知识，提高计算机使用水平，及早防范风险。同时，信息安全工作领导小组具有畅通的联系渠道，可以确保能及时发现、处置、上报有害信息。

二、计算机日常网络及信息安全管理情况

加强组织领导，强化宣传教育，落实工作责任，加强日常监督检查。

(一)网络安全方面。配备了防病毒软件、对个人使用的计算机都实行密码登录、对重要计算机信息存储备份、对移动存储设备严格管理、对重要数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。对接入计算机的终端采取实名认证制，采取将计算机 MAC 地址绑定交换机端口的做法，规范全校的上网行为。

(二)信息系统安全方面实行严格签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传;开展经常性安全检查，主要对操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

(三)学校网络中心具有不低于 60 日的系统网络运行日志和用户使用日志。网络中心有防火墙、统一身份认证、网络安全审计、访问控制等相应的安全保护技术措施。

三、信息安全技术防护手段建设及硬件设备使用情况。

加强网络设备及网站安全防护管理。每台终端机都安装了防病毒软件，系统相关设备的应用一直采取规范化管理，硬件设备

的使用符合国家相关产品质量安全规定，硬件的运行环境符合要求，网站系统安全有效。

四、加强建设网络与信息安全通报机制，网站安全维护

近几年以来，学校切实加强网络信息安全防范工作，未发生较大的网络及信息突发事件，采取了网站后台密码经常性更换、传文件提前进行病毒检测、网站分模块分权限进行维护、定期进后台清理垃圾文件、网站更新由段计算机管理员专人负责等多种措施，确保学校网站的信息安全。

五、网络与信息安全教育

为保证网络及各种设备安全有效地运行，减少病毒侵入，就网络安全及信息系统安全的相关知识对有关人员进行了培训。期间，各计算机使用人员及管理人员对实际工作中遇到的计算机方面的有关问题进行了详细的咨询，并得到了满意的答复，学习到了实用的网络安全防范技巧，促进了计算机使用人员对网络信息安全的认识力度。

六、自查存在的问题及整改意见

在检查过程中发现了一些管理方面存在的薄弱环节，今后还要加强对网络安全的监管及网络安全设备的维护，进一步加强与上级部门的沟通和协调

在以后的工作中，我们将继续加强对计算机信息安全意识教育和防范技能训练，让全校师生充分认识到做好校园网络安全隐患排查工作的重要性和必要性。将人防与技防结合，确实做好我校网络与信息安全维护工作。

附：排查清单

1.网络安全组织管理

学校有主管网络安全领导，有网络管理员。

2.网络安全日常管理

学校建立了网络安全管理制度，外部人员访问机房等重要区域时采取人员陪同进出记录等安全措施，资产由后勤处建立台账，统一管理，资产台账与实际设备相一致。现场服务过程中有专人陪同，并记录服务过程。厂商负责运维服务，网络安全设施运维服务纳入年度预算中，网站信息发布由专人审核。

3.信息安全防护管理

学校中心机房配备门禁系统，设备配备软件防火墙防止入侵，服务器系统无弱口令并定期更新口令，LED 屏幕发布内容严格按照审核机制，服务器补丁由软件厂商定期更新，终端计算机网络配固定 IP，未与 MAC 地址绑定，新媒体包括微信公众号、微官网、智慧校园平台、企业微信账号由专人负责开通和管理，并定期更换口令。

4.网络安全应急管理

学校制定了网络安全事件应急预案，发生网络安全事件后，及时

向主管领导报告，按照预案开展处置工作；重大事件及时通报网络安全主管部门。

5.网络安全教育培训

利用信息技术课对三年级以上学生开展过网络安全教育活动。

6.网络安全检查

学校有专人负责网络设备的安全检查。