2023 网络安全工作自查报告

2023 网络安全工作自查报告 1

为了加强我校教育信息网络安全管理，保护信息系统的安全，促进我校信息技术的应用和发展，保障教育教学和管理工作的顺利进行，并配合省公安厅、省教育厅（豫公通[]220 号文件精神，对我校计算机信息系统开展以“反、反破坏、扫黄打非、清理垃圾邮件”为主要内容的安全大检查，净化校园网络环境，不断提高学校计算机信息系统安全防范能力，从而为学生提供健康，安全的上网环境。

一、领导重视，责任分明，加强领导

为了认真做好迎检准备工作，进一步提高教育网络信息安全工作水平，促进教育信息化健康发展，我校建立了专门的网络信息安全管理组织，成立了由分管领导、网络管理员组成的计算机网络信息安全管理领导小组。负责制定学校计算机信息系统安全管理的办法和规定，协调处理全校有关计算机信息系统安全的重大问题；负责学校计算机信息系统的建设、管理、应用等工作；负责信息系统安全的监督、事故的调查和处罚。学校网络管理人员要在学校计算机安全管理领导小组的领导下，负责校园网的安全保护工作和设备的维护工作，必须模范遵守安全管理制度，积极采取必要的防范技术措施，预防网络安全事故的发生。

二、完善制度，加强管理

为了更好的安全管理网络，我校建立了健全的.安全管理制度：

（一）计算机机房安全管理制度

1、重视安全工作的思想教育，防患于未然。

2、遵守“教学仪器设备和实验室管理办法”，做好安全保卫工作。

3、凡进入机房的人员除须遵守校规校纪外，还必须遵守机房的各项管理规定，爱护机房内的所有财产，爱护仪器设备，未经管理人员许可不得随意使用，更不得损坏，如发现人为损坏将视情节按有关规定严肃处理。

4、机房内禁止吸烟，严禁明火。

5、工作人员必须熟悉实验室用电线路、仪器设备性能及安全工作的有关规定。

6、实验室使用的用电线路必须符合安全要求，定期检查、检修。

7、杜绝黄色、迷信、反动软件，严禁登录黄色、迷信、反动，做好计算机病毒的防范工作。

8、工作人员须随时监测机器和网络状况，确保计算机和网络安全运转。

9、机房开放结束时，工作人员必须要关妥门窗，认真检查并切断每一台微机的电源和所有电器的电源，然后切断电源总开关。

（二）操作人员权限等级分配制度

1、校领导统一确定操作人员职能权限。

2、电教组成员负责管理、维修学校所有计算机，出现重大事故应及时报上级领导。

3、教师用户帐号、密码由网络管理员发放，并统一管理。

4、学校计算机管理人员需定期维护计算机软件和数据，重要信息定期进行检查和备份。

5、网络管理员负责校园用户计算机系统能够正常上网，为用户提供日常网络维护服务和日常数据备份。

（三）账号安全保密制度

1、网络用户的账号、密码不得外传、外借。

2、非法用户使用合法用户的账号进入校园网的，追究该帐号拥有者的安全责任。

（四）计算机病毒防治制度

1、学校购买使用公安部颁布批准的电脑杀毒产品。

2、未经许可证，任何人不得携入软件使用，防止病毒传染。

3、凡需引入使用的软件，均须首先防止病毒传染。

4、电脑出现病毒，操作人员不能杀除的，须及时报电脑主管处理。

5、在各种杀毒办法无效后，须重新对电脑格式化，装入正规渠道获得的无毒系统软件。

6、建立双备份制度，对重要资料除在电脑贮存外，还应拷贝到软盘上，以防遭病毒破坏而遗失。

7、及时关注电脑界病毒防治情况和提示，根据要求调节电脑参数，避免电脑病毒侵袭。

（五）安全教育培训制度

1、学校组织教师认真学习《计算机信息网络国际互联网安全保护管理办法》，提高教师的维护网络安全的警惕性和自觉性。

2、学校负责对本校教师进行安全教育和培训，使教师自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

3、校管理中心对信息源接入的骨干人员进行安全教育和培训，使之自觉遵守和维护《计算机信息网络国际互联安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。

（六）、事故和案件及时报告制度

1、任何单位和个人不得利用互联网制作、复制、查阅和传播下列信息：

煽动抗拒、破坏宪法和法律、行政法规实施。

煽动颠覆国家政权，推翻社会主义制度。

煽动分裂国家、破坏国家统一。

煽动民族仇恨、民族歧视、破坏民族团结。

捏造或者歪曲事实、散布谣言，扰乱社会秩序。

宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪。

公然侮辱他人或者捏造事实他人。

损害国家机关信誉。

其他违反宪法

和法律、行政法规。

如发现有上述行为，保留有关原始记录，并填写好《安全日志》，在12小时内向上级报告。

2、接受并配合区电教中心和公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

3、发现有关计算机病毒、危害国家安全、违反国家有关法律、法规等计算机安全案情的，应在12小时以内向上级报告。

4、计算机机房设管理员一名，其职责是每天不定期浏览主页或自己页面，负责领导还应经常巡视操作者，如发现有违反上述规定者应立即制止并报告校园网安全领导小组。

（七）、面对大面积病毒应急处理方案

1、制定计算机病毒防治管理制度和技术规程，并检查执行情况；

2、培训计算机病毒防治管理人员；

3、采取计算机病毒安全技术防治措施；

4、对计算机信息系统应用和使用人员进行计算机病毒防治教育和培训；

5、及时检测、清除计算机系统中的计算机病毒，并做好检测、清除的记录；

6、购置和使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品；

7、向公安机关报告发现的计算机病毒，并协助公安机关追查计算机病毒的_____；

8、对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

除以上健全的安全管理制度外，我校也认真落实相关安全技术措施，安全基础措施良好拥有完善的安全保护措施，设有学校重要部位值班制度，做到昼夜值班，任何人不得擅自进入微机房。

__x 小学

、02

__x 小学网络信息安全管理领导小组

组长：__x

副组长：__x

成员：_____

2023 网络安全工作自查报告 2

根据 x 高法〔〕75 号《关于加强全省法院信息网络安全保密管理和开展建设整改的通知》文件的要求，我院网络安全保密工作领导小组高度重视，对全院网络安全保密工作进行了一次全面的自评自查。现将本次自评自查情况汇报如下：

一、加强学习，提高保密工作认识

迅速贯彻落实文件精神，组织全院干警认真学习《中华人民共和国保密法》、《国家工作人员保密守则》、《党政机关和涉密单位网络保密管理规定》等，强调保密工作的极端重要性，提高干警对国家秘密和审判秘密的认识，牢固树立“涉密无小事，失密是大事”的保密意识。对公文收发人员、档案管理员、书记员等加强保密教育，加强做好保密工作的检查督促，促进全体干警提高思想认识，增强做好保密工作的责任感。同时，进一步明确涉密人员对文件收发、登记、传递、归档、销毁等环节的职能，使保密工作真正做到行有规章、做有依据、查有准则，真正实现制度化、规范化、科学化。

二、自纠自查，排除泄密安全隐患

按照本院制定的《网络信息安全及保密工作制度》，明确自查的内容和标准，并对自查工作进行了统一部署和安排。各部门根据所负保密工作职责，对信息系统保密管理工作进行了全面、认真地自查，对可能存在的泄密隐患进行了重点排查，认真整改。

一是严格要害部门的管理与防护。档案室、办公室等部门是保密重点部门，涉密文件的收发，卷宗的存档与查阅应重点防护。通过自查，这些部门的规章制度健全，能从每个环节做起，保密观念强，措施得力，落实较好，能严格控制机要文件、加密传真和归档案卷的阅读范围，严格阅读纪律，严格机要文件存放点和保密防范，对传真文件坚决做到明来明往，密来密复。

二是加强涉密计算机的管理。涉密计算机主要用于处理电子政务、涉密文件和公文的收发，经定期检查，未感染“木马”等危害性病毒，做到了专机专用，未与非涉密介质互用，严格执行了公文处理的有关保密规定，未发现违规行为。

三是严格存储介质的使用管理。涉密U盘主要是将秘密文件直接在专用计算机上处理。经检查，未用存储介质来回移动及在介质上存储涉密信息，对交叉使用移动存储介质的问题及时进行了纠正和整改。

四是强化办公网络使用的管理。根据工作需要，经区法院计算机所连网络分为法院系统内部网络与互联网，做到了专网专用，定位准确，非涉密计算所连互联网未存储、处理涉密信息。

五是狠抓涉密载体的清理。及时对涉密载体进行严密保管和认真清理，对发现存在的问题及时进行了纠正。

三、强化监督，落实保密工作责任

一是保密监督检查工作长效制，定期对各个庭室的保密情况进行督察，发现保密工作未到位的，及时督促整改。每庭室确定一名内勤人员负责文件收发与保管，堵塞漏洞，确保秘密安全。

二是坚持日常规范与重点督察相结合。切实做到法院工作做到哪里，保密工作就跟进到哪里。在落实保密工作的过程中，抽调专人对保密工作进行经常检查，尤其对于涉密的要害部门、重点部门进行定期检查，一旦发现不严格执行保密规定的责令整改。

三是坚持接受监督与责任追究相结合。严格内部保密管理的同时，主动接受上级部门的监督、检查、指导。规定对于缺乏保密观念和保密意识、思想严重麻痹、保密管理责任不落实、保密人员疏于管理，由此造成失泄密事件的人和事

都要做到发生一起查处一起，绝不姑息迁就，保密管理水平明显提高，自建院以来无失、泄密事件发生。

四、物力保障，夯实保密工作物质基础

保密工作除了人员到位、定密到位，还要经费到位，才能较好地防止失泄密事件的发生。近年来，我院加大保密工作物质保障，对保密工作的资金投入近五万元，配置购买了保密柜、文件粉碎机，安装防火墙、隔离卡，使用专网U盘等，为做好保密工作提供有力的物质保障。

五、加大教育宣传，务求保密工作落实到位

结合当前信息网络安全保密工作的形势和任务，定期开展保密宣传教育活动，提高全院干警的保密意识、保密责任和保密技能。并将保密工作完成情况纳入年终绩效考核，确保信息网络安全保密工作落实到位。

通过这次的自评自查活动，提高了我院保密工作水平，也提升了我院全体干警的保密工作意识，但按照上级的要求还存在一定的的差距和不足，做好保密工作仍然任重道远。在今后的工作中，我院将进一步加强对保密工作的重视，强化对涉密内容的管理，力争保密工作取得新的成绩，确保审判执行工作顺利开展。

2023 网络安全工作自查报告 3

为进一步加强广播电视行业网络信息安全保障工作，维护公众利益和国家安全，根据有关文件的通知精神。我台高度重视，立即召开专题会议，周密部署我台广播电视行业网络安全自查行动，并对我台广播电视节目制作、播出、传输、

等业务相关的网络以及__视听进行了全面、认真、仔细的检查。现将自查的情况报告如下：

一、加强领导，成立了网络安全工作领导小组

为进一步加强全信息网络系统安全管理工作，我台成立了以副台长为组长、分管主任为副组长、技术保障中心人员为成员网络安全工作领导小组，做到分工明确，责任具体到人。分工与各自的职责如下:副台长为计算机网络安全工作第一责任人，全面负责计算机网络与信息安全管理工作。副组长分管计算机网络与信息安全管理工作。负责计算机网络安全管理工作的日常协调、督促工作。技术保障人员负责计算机网络安全管理工作的日常事务。

二、信息安全管理情况

1、信息安全制度健全，责任落实。成立了网络安全工作领导小组，落实了安全管理责任人和安全管理员。建立了《机房进出安全管理制度》、《安全管理员岗位职责》、等一系列信息系统安全管理制度，各系统运行管理人员在日常操作中严格按制度执行，台定期和不定期对操作人员执行各项安全制度情况进行检查和抽查，发现问题及时整改，切实避免了因操作人员操作不当引起的安全事故。各项信息系统安全稳定运行，确保了系统安全无事故发生。

2、配备了防病毒软件以及专业硬件防火墙、切实抓好外网、防控，确保“涉密计算机不上网，上网计算机不涉密”，加强密码管理，采用了强口令密码，明确了网络安全责任，保障了网络安全工作。

3、凡上传的信息，须经有关领导审查后方可上传。开展经常性安全检查，聘请制作公司的技术人员，主要对 sql 注入攻击、跨站脚本攻击、弱口令、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。

三、技术防护情况

不同区域采用了正确的隔离措施，外部网络接入内部网络采用了安全的防火墙传输方式。安全功能配置合理有效。制定了重要数据传输、存储安全防护措施。重要数据按要求多重存储并有备份。

四、安全保卫情况

对外来人员进行登记制度，要找谁由值班人员通知本人到登记处接待。禁止了无关人员和外来人员的进入，为营造安全播出环境提供了基本保障。

五、整改措施及工作建议

1、进一步建立健全网络信息安全相关制度，并严格执行出现问题不隐瞒、不推诿，及时解决。

2、加大对广播电视网络与信息安全的资金投入，添置播出服务器及配套设备，确保网络安全。

3、严明纪律加强内部管理与协调，杜绝违规使用移动存储设备，以防止病毒带入网络，影响信息安全。

4、加强对信息安全管理与操作人员的培训，增强保密意识、安全意识，提高网络信息安全工作人员的业务技能。

网络安全工作自查报告 4

为进一步加强政府信息保密工作，根据政府办[]10 号文件精神，我会严格按照文件要求，结合妇联实际，及时查找问题，采取有效措施，政府信息安全保密工作取得实效。

一、 领导重视、责任落实