# 2024信息安全自查及整改情况报告范文

来源：网络 作者：枫叶飘零 更新时间：2024-10-12

*生活之中的危险是无处不在的，我们要保护好自己，而网络之中的危险甚至要比现实生活中的更加的危险，那么下边就是小编收集的一些相关内容，一起来看看吧!根据路局《关于在全局范围内开展网络与信息安全检查行动的通知》(XXXXXXXX)文件精神。我站对...*

生活之中的危险是无处不在的，我们要保护好自己，而网络之中的危险甚至要比现实生活中的更加的危险，那么下边就是小编收集的一些相关内容，一起来看看吧!

根据路局《关于在全局范围内开展网络与信息安全检查行动的通知》(XXXXXXXX)文件精神。我站对本站网络与信息安全情况进行了自查，现汇报如下：

一、信息安全自查工作组织开展情况

1、成立了信息安全检查行动小组。由站长、书记任组长，相关科室(车间)负责人、信息技术科全体人员为组员负责对全站的重要信息系统全面排查并填记有关报表、建档留存。

2、信息安全检查小组对照网络与信息系统的实际情况进行了逐项排查、确认，并对自查结果进行了全面的核对、梳理、分析。整改，提高了对全站网络与信息安全状况的掌控。

二、网络与信息安全工作情况

1、8月2日前开展网络语信息系统的自查工作部署。

1)组织成立了网络与信息安全检查工作小组，由站长、书记任组长，相关科室(车间)负责人、信息技术科全体人员为组员。

2)研究制定自查实施方案，根据系统所承担的业务的独立性、责任主体的独立性、网络边界的独立性、安全防护设备设施的独立性四个因素，对客票发售与预订系统、旅客服务系统、办公信息系统进行全面的梳理并综合分析。

2、8月6日前对客票发售与预订系统、旅客服务系统、办公信息系统的基本情况进行逐项排查。

1)系统安全基本情况自查

客票发售与预订系统为实时性系统，对车站主要业务影响较高。目前拥有IBM服务器2台、cisco路由器2台、cisco交换机13台，系统均采用windows操作系统，灾备情况为系统级灾备，该系统不与互联网连接，防火墙采用永达公司永达安全管控防火墙。

旅客服务系统为实时性系统，对车站主要业务影响较高。目前拥有HP服务器13台、H3C路由5台、H3C交换机15台，系统采用linix操作系统，数据库采用SQLServer，灾备情况为数据灾备，该系统不与互联网连接，安全防护策略采用按照使用需求开放端口，重要数据均采用加密防护。

办公信息系统为实时性系统，对车站主要业务影响一般。目前拥有IBM服务器1台、cisco路由器1台、cisco交换机2台，系统采用windows操作系统，数据库采用SQLServer，灾备情况为数据灾备，该系统不与互联网连接，安全防护策略采用按照使用需求开放端口，重要数据均采用加密防护。

2)安全管理自查情况

人员管理方面，指定专职信息安全员，成立信息安全管理机构和信息安全专职工作机构。重要岗位人员全部签订安全保密协议，制定了《人员离职离岗安全规定》、《外部人员访问审批表》。

资产管理方面，指定了专人进行资产管理，完善了《资产管理制度》、《设备维修维护和报废管理制度》，建立了《设备维修维护记录表》。

存储介质管理方面，完善了《存储介质管理制度》，建立了《存储介质管理记录表》。

运行维护管理方面，建立了《客服系统维护标准》、《运行维护操作记录表》，完善了《日常运行维护制度》。

3)网络与信息安全培训情况

制定了《太原站网络与信息安全培训计划》，20xx年上半年组织信息安全教育培训2次，接受信息安全培训人数20人，站单位中人数的5%。组织信息安全管理和技术人员参加专业培训10人次。

三、自查发现的主要问题和面临的威胁分析

四、改进措施

五、整改效果

根据《广电总局办公厅贯彻落实国务院办公厅关于开展重点领域网络与信息安全检查行动的通知》文件精神，我台在青岛市文广新局的统一部署下，对本台网络与信息安全情景进行了自查，现汇报如下：

一、信息安全自查工作组织开展情景

1、成立了信息安全检查行动小组。由台长任组长，分管领导为副组长，相关科室负责人为组员的行动小组，负责对全台的重要信息系统的全面指挥、排查并填记有关报表、建档留存等。

2、信息安全检查小组对照网络与信息系统的实际情景进行了逐项排查、确认，并对自查结果进行了全面的核对、分析，提高了对全台网络与信息安全状况的掌控。

二、信息安全工作情景

1、8月6日完成信息系统的自查工作部署，并研究制定自查实施方案，根据所承担的业务要求和网络边界安全性对硬盘播出系统、非线性修改系统、XX有线电视传输系统进行全面的梳理并综合分析。

2、8月7日对硬盘播出系统、非线性修改系统、XX有线电视传输系统进行了细致的自查工作。

(1)系统安全自查基本情景

硬盘播出系统为实时性系统，对主要业务影响较高。目前拥有DELL服务器5台、惠普服务器2台、cisco交换机2台，操作系统均采用windows系统，数据库采用SQLServer，灾备情景为数据级灾备，该系统不与互联网连接。

非线性修改系统为非实时性系统，对主要业务影响较高。目前拥有DELL服务器6台、华为交换机1台，网关采用UNIX操作系统，数据库采用SQLServer，灾备情景为数据灾备，该系统不与互联网连接，安全防护策略采用默认规则。

XX有线电视传输系统为实时性系统，对主要业务影响高，灾备情景为数据灾备，该系统不与互联网连接。

(2)、安全管理自查情景

人员管理方面，指定专职信息安全员，成立信息安全管理机构和信息安全专职工作机构。重要岗位人员全部签订安全保密协议，制定了《人员离职离岗安全规定》、《外部人员访问审批表》。

资产管理方面，指定了专人进行资产管理，完善了《资产管理制度》、《设备维修维护和报废管理制度》，建立了《设备维修维护记录表》。

存储介质管理方面，完善了《存储介质管理制度》，建立了《存储介质管理记录表》。

(3)、网络与信息安全培训情景

制定了《XX市广播电视台信息安全培训计划》，2024年上半年组织信息安全教育培训2次，理解信息安全培训人数40人，站单位中人数的20%。组织信息安全管理和技术人员参加专业培训4次。

为落实“教育部办公厅关于开展网络安全检查的通知”、“教育部关于加强教育行业网络与信息安全工作的指导意见”、陕西省教育厅“关于开展全省教育系统网络与信息安全专项检查工作的通知”，全面加强我校网络与信息安全工作，校信息化建设领导小组办公室于9月16日—25日对全校网络、信息系统和网站的安全问题组织了自查，现将自查情况汇报如下：

一、学校网络与信息安全状况

本次检查采用本单位自查、远程检查与现场抽查相结合的方式，检查内容主要包含网络与信息系统安全的组织管理、日常维护、技术防护、应急管理、技术培训等5各方面，共涉及信息系统28个、各类网站89个。

从检查情况看，我校网络与信息安全总体情况良好。学校一贯重视信息安全工作，始终把信息安全作为信息化工作的重点内容。网络信息安全工作机构健全、责任明确，日常管理维护工作比较规范;管理制度完善，技术防护措施得当，信息安全风险得到有效降低;比较重视信息系统(网站)系统管理员和网络安全技术人员培训，应急预案与应急处置技术队伍有落实，工作经费有一定保障，基本保证了校园网信息系统(网站)持续安全稳定运行。但在网络安全管理、技术防护设施、网站建设与维护、信息系统等级保护工作等方面，还需要进一步加强和完善。

二、网络信息安全工作情况

1、网络信息安全组织管理

按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学校网络信息安全工作实行“三级”管理。学校设有信息化工作领导小组，校主要领导担任组长，信息化工作办公室设在网教中心，中心主任兼办公室主任。领导小组全面负责学校网络信息安全工作，授权信息办对全校网络信息安全工作进行安全管理和监督责任。网教中心作为校园网运维部门承担信息系统安全技术防护与技术保障工作。各处室、学院承担本单位信息系统和网站信息内容的直接安全责任。

2、信息系统(网站)日常安全管理

学校建有“校园网管理条例”、“中心机房安全管理制度“、“数据安全管理办法”、“网站管理办法”、“服务器托管管理办法”、“网络故障处理规范”等系列规章制度。各系统(网站)使用单位基本能按要求，落实责任人，较好地履行网站信息上传审签制度、信息系统数据保密与防篡改制度。日常维护操作较规范，多数单位做到了杜绝弱口令并定期更改，严密防护个人电脑，定期备份数据，定期查看安全日志等，随时掌握系统(网站)状态，保证正常运行。

3、信息系统(网站)技术防护

校园网数据中心建有一定规模的综合安全防护措施。

一是建有专业中心机房，配备视频监控、备用电力供应设备，有防水、防潮、防静、温湿度控制、电磁防护等措施，进出机房实行门禁和登记制度;

二是网络出口部署有安全系统，站群系统部署有应用防火墙，并定期更新检测规则库，重要信息系统建立专网以便与校园网物理隔离;

三是对服务器、网络设备、安全设备等定期进行安全漏洞检查，及时更新操作系统和补丁，配置口令策略保证更新频度;

四是全面实行实名认证制度，具备上网行为回溯追踪能力;

五是对重要系统和数据进行定期备份，并建有灾备中心。

4、信息安全应急管理

制定了《西北农林科技大学网络与信息安全突发事件应急预案》。网教中心为应急技术支持单位，确保网络安全事件的快速有效处置。

5、信息安全教育培训

派员参加了陕西省信息安全保密培训。暑期处级干部培训安排有信息安全与保密专题，每年组织全校网管员技术培训，增强管理干部和技术人员的安全防范意识，提高技术防护能力。

三、检查发现的主要问题

对照《通知》中的具体检查项目，我校在信息安全工作上还存在一定的\'问题：

1、安全管理方面：网管员为兼职，投入精力难以保证，部分网管员长时间未登录过自己管理的系统(网站)，无法及时知晓已发生的安全事件。部分系统(网站)日常管理维护不够规范，仍存在管理员弱口令、数据备份重视不够、信息保密意识差等问题(2024年发生2起个人隐私信息上传网站的事件)。

2、技术防护方面：校园网安全技术防护设施仍不足，如缺少数据中心安全防御系统和审计系统，欠缺安全检测设施，无法对服务器、信息系统(网站)进行安全漏洞扫描与隐患检查。

3、应用系统(网站)方面：个别应用系统(网站)存在设计缺陷和安全漏洞，容易发生安全事故。(经统计2024年以来14个网站发生安全事故17起，其中11起是因为网站存在技术问题，如安全漏洞或设计缺陷)。

4、信息系统等级保护工作尚未全面开展。

5、部分院(系)管辖的机房或学习室尚未实行认证和审计。

四、整改措施

针对存在的问题，学校信息化领导小组专门进行了研究部署。

1、进一步完善网络信息安全管理制度，规范信息系统和网站日常管理维护工作程序。加强网管员技术培训，提高安全意识和技术能力。

2、继续完善网络信息安全技术防护设施，配备必要的安全防御和检测设备，实行信息系统(网站)安全检测准入制度，从根本上降低安全风险。定期对服务器、操作系统进行漏洞扫描和隐患排查，建立针对性的主动防护体系。

3、针对各级网站建设水平参差不齐问题，学校2024年引入了站群系统管理平台，目前已将多个部门共计12个网站迁移到站群系统管理平台。今后将加大推进力度，逐步将全部各级网站迁入站群系统管理平台，提高网站技术安全性能。

4、全面开展信息系统等级保护工作，按照新颁布的《教育行政部门及高等院校信息系统安全等级保护定级指南》，完成所有在线系统的定级、备案工作。积极创造条件开展后续定级测评、整改等工作。

5、加强应急管理，修订应急预案，组建以网教中心技术人员为骨干、重要系统管理员参加的应急支援技术队伍，加强部门间协作，做好应急演练，将安全事件的影响降到最低。

6、对院(系)管机房或学习室强制认证和审计。

五、几点建议

1、建议按年度列支相关经费，用于培训、应急演练、网站改造等工作开展。(“网络安全经费预算投入情况”也是教技厅函[2024]51号文件9个检查项目之一);

2、建议在数字校园建设经费里列支专项经费用于等保定级、测评、整改等工作;

3、建议各类网站在适当的时候(最好是改版时)加入学校站群系统管理平台，一旦加入该站群系统管理平台，管理者将无需考虑网站的技术安全及风险，只需考虑网站的信息与内容安全。

按照《关于组织开展20xx年全市政府信息系统安全检查工作的通知》(镇信安联办【20xx】5号)要求，我局高度重视，立即组织开展全局范围的信息系统安全检查工作。现将自查情景汇报如下。

我局信息系统运转以来，能严格按照上级部门要求，进取完善各项安全制度、充分加强信息化安全工作人员教育培训、全面落实安全防范措施、全力保障信息安全工作经费，信息安全风险得到有效降低，应急处置本事得到切实提高，保证了政府信息系统持续安全稳定运行。

一、信息安全组织管理工作情景

我局高度重视信息系统安全工作，成立有由主要领导任组长、分管领导任副组长、各处室负责人为组员组成的局信息安全工作领导小组，明确了局办公室为主要职能部门，确定了一名兼职信息安全员，召开了由分管领导、信息安全工作职能部门和重点部门负责人参加的会议，对上级有关文件进行了认真学习，对自查工作进行了周密的部署，确定了自查任务和人员分工，真正做到领导到位、机构到位、人员到位、职责到位、措施到位。为确保我局网络信息安全工作有效顺利开展，我局要求以各处室、下属单位为单位认真组织学习相关法律、法规和网络信息安全的相关知识，使全体人员都能正确领会信息安全工作的重要性，都能掌握计算机安全使用的规定要求，都能正确的。使用计算机网络和各类信息系统。

二、日常信息安全管理工作情景

我局在以前建立一系列信息安全制度的基础上，针对信息安全工作的特点，结合我局实际，重新修订了一系列信息安全制度和程序，做到按制度办事，提高执行力。按照市政府和市经信委要求，我局与计算机维保单位重新签订了服务协议，增加了信息安全与保密协议资料。同时我局还与全局所有工作人员签订了安全保密协议。我局对涉密计算机和涉密移动存储介质高度关注，对所有涉密计算机和涉密移动存储介质全部进行编号在册统一管理，明确职责人和保管人，对涉密信息系统的使用进行多次重点检查，强化涉密人员管理，严格执行涉密计算机和涉密移动存储介质的相关管理制度，专门为涉密人员配发了带有硬件锁的U盘，严禁在涉密和非涉密信息系统间混用移动存储介质等等。对非涉密计算机的保密系统和防火墙、杀毒软件等皆为国产产品，公文处理软件使用微软公司的正版office系统，信息系统的第三方服务外包均为国内公司。

三、信息安全防护管理工作情景

我局网络系统的组成结构及其配置合理，并贴合有关的安全规定;网络使用的各种硬件设备、软件和网络接口是也过安全检验、鉴定合格后才投入使用的，自安装以来运转基本正常。我局经常开展信息安全检查工作，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、网页篡改情景等进行监管，认真做好系统安全日记。今年，我局在市政府办的指导下试运行协同办公系统，投入10多万元为所有局领导、各处室配置了内网计算机，为涉密处室另配备了涉密计算机，从硬件上加强了涉密信息系统管理。

四、信息安全应急管理工作情景

我局认真做好各项准备工作，对可能发生的各类信息安全事件做到心中有数，进一步完善了信息安全应急预案，明确应急处置流程，落实了应急技术支撑队伍，把工作做深做细做在前面。

五、信息安全教育培训工作情景

我局针对信息管理人员实际情景，每年开展信息化教育培训，以掌握信息化管理技能为目的进行实践操作本事培训。还组织有关工作人员参加了相关信息安全培训，职工信息安全意识得到有效提高。

六、信息安全专项检查工作情景

目前我局在市行政中心大楼内办公，网络和信息系统便于统一管理，内外网完全物理隔离，内网计算机均在有效管理范围内。局信息安全工作领导小组针对我局的信息安全形势，定期组织由专业技术人员组成的检查小组到各个办公室专项检查网络和信息安全情景，仔细排查信息系统的漏洞和安全隐患，用专用工具查杀木马、病毒，及时加强防范措施，为所有计算机安装了正版杀毒软件和防火墙，有效提高了计算机和网络防范、抵御风险的本事。此外，检查小组针对个别在市行政中心大楼外办公的处室进行了上门检查，不放过任何信息安全死角。在检查的同时，检查小组还就信息安全知识进行了上门培训。经多次检查，我局信息系统总体情景良好，运行正常，未发现重大隐患。

七、信息安全检查工作发现的主要问题及整改情景

(一)存在的主要问题

一是专业技术人员较少，信息系统安全方面可投入的力量有限。

二是规章制度体系初步建立，但还不完善，未能覆盖到信息系统安全的所有方面。

三是遇到计算机病毒侵袭等突发事件处理不够及时。

(二)下一步工作打算

根据自查过程中发现的不足，同时结合我局实际，将着重以下几个方面进行整改：

一是进一步扩大对计算机安全知识的培训面，组织信息员和干部职工进行培训。

二是要切实增强信息安全制度的落实工作，不定期的对安全制度执行情景进行检查，从而提高人员安全防护意识。

三是要以制度为根本，在进一步完善信息安全制度的同时，安排专人，完善设施，密切监测，随时随地解决可能发生的信息安全事故。

历城六中学校网站于20\_\_年9月重新改版上线，自新网站运行以来，我校对网络信息安全系统工作一直十分重视，成立了专门的领导组，建立健全了网络安全保密责任制和有关规章制度，由学校谢主任统一管理，各科室负责各自的网络信息安全工作。严格落实有关网络信息安全保密方面的各项规定，采取了多种措施防范安全保密有关事件的发生，总体上看，我校网络信息安全工作做得扎实有效。

一、计算机和网络安全情况

一是网络安全方面。我校配备了防病毒软件、，采用了强口令密码、数据库存储备份、移动存储设备管理、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。

二是信息系统安全方面实行领导审查签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传;二是开展经常性安全检查，聘请网站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，认真做好系统安全日记。

三是日常管理方面切实抓好外网、网站和应用软件“五层管理”，确保“涉密计算机不上网，上网计算机不涉密”，严格按照保密要求处理光盘、硬盘、U盘、移动硬盘等管理、维修和销毁工作。重点抓好“三大安全”排查:一是硬件安全，包括防雷、防火、防盗和电源连接等;二是网络安全，包括网络结构、安全日志管理、密码管理、IP管理、互联网行为管理等;三是应用安全，包括网站、邮件系统、资源库管理、软件管理等。

二、学校硬件设备运转正常。

我校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，单位硬件的运行环境符合要求，打印机配件、色带架等基本使用设备原装产品;防雷地线正常，对于有问题的防雷插座已进行更换，防雷设备运行基本稳定，没有出现雷击事故;UPS运转正常。网站系统安全有效，暂未出现任何安全隐患。

三、严格管理、规范设备维护

我校对电脑及其设备实行“谁使用、谁管理、谁负责”的管理制度。在管理方面我们一是坚持“制度管人”。二是强化信息安全教育、提高员工计算机技能。同时在学校开展网络安全知识宣传，使全体人员意识到了，计算机安全保护是“三防一保”工作的有机组成部分。而且在新形势下，计算机犯罪还将成为安全保卫工作的重要内容。在设备维护方面，专门设置了网络设备故障登记簿、计算机维护及维修表对于设备故障和维护情况属实登记，并及时处理。对外来维护人员，要求有相关人员陪同，并对其身份和处理情况进行登记，规范设备的维护和管理。

四、网站安全及维护

我校对网站安全方面有相关要求，一是使用专属权限密码锁登陆后台;二是上传文件提前进行病素检测;三是网站分模块分权限进行维护，定期进后台清理垃圾文件;四是网站更新专人负责。

五、安全教育

为保证我校网络安全有效地运行，减少病毒侵入，我校就网络安全及系统安全的有关知识进行了培训。期间，大家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。

六、自查存在的问题及整改意见

我们在管理过程中发现了一些管理方面存在的薄弱环节，今后我们还要在以下几个方面进行改进。

(一) 网站的安全防护设备还存在不足，只有路由器附带的防火墙，没有硬件版防火墙设备，存在安全隐患。

(二)加强设备维护，及时更换和维护好故障设备。

(三)自查中发现个别人员计算机安全意识不强。在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让员工充分认识到计算机案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

内蒙古自治区信息化领导小组办公室：

按照自治区信息化领导小组下发的《关于20xx年我区开展重点领域信息安全检查工作的通知》(内信领办字[20xx]15号)文件精神，内蒙古自治区民政厅结合自身情况，认真组织自查，取得预期效果，现将检查结果报告如下：

一、重点网络与信息系统基本情况

正式运行中的业务应用系统包括：自治区最低生活保障信息系统、自治区婚姻登记信息系统、自治区优待抚恤信息系统、自治区社会团体信息系统、自治区五保供养信息系统及自治区城乡医疗救助信息系统等6个主要业务信息系统，由信息中心负责日常保障和维护。

从应用系统的实时性、服务对象、连接互联网、数据集中、灾备情况来看，以上6个业务信息系统全部采用实时交互、逻辑强隔离措施连接互联网、省级数据集中、数据级灾备模式运行。

从网络硬件构成情况来看，中心机房配置有30台服务器、2台小型机、2部路由器、1台隔离网闸、3台负载均衡设备等。

二、整体安全状况的基本判断

从总体来看，各类业务信息系统上线运行以来，严格遵照有关规章制度的要求、完善各项安全防范措施、加强信息安全工作人员教育培训、信息安全风险得到有效降低，应急处置能力得到显著提高，切实保障了业务信息系统安全、稳定，高效运行。

三、发现的主要问题

(一)专业技术人员队伍薄弱，网络与信息系统安全保障工作可投入的人力物力有限。

(二)处于规章制度体系建立初期，尚未能覆盖网络与信息系统安全保障工作的各个方面。

(三)当遇到计算机病毒大规模集中爆发、恶意侵袭信息系统等突发事件时，应急处理能力未得到实践检验。

四、 薄弱环节及整改情况

(一)安全保障预算资金和技术人员缺乏的问题已提请厅领导审批。

(二)在实际工作中不断发现问题、解决问题，修订各类规章制度。

(三)不定期开展数据恢复演练，密切监测，检验各项应急预案的可操作性和实际有效性，随时预防发生的信息系统安全隐患。

五、意见和建议

随着现代信息技术日新月异的发展，新的、不可预测的信息安全漏洞和安全隐患将层出不穷。建议每年组织一些系统的信息安全技术培训，有针对性地提高安全防范水平和安全可控能力，预防和减少重大信息安全事件的发生。

以上就是小编整理的相关内容了，想要了解更多内容，请持续的关注网，谢谢!

【2024信息安全自查及整改情况报告范文】相关推荐文章：

黄河流域生态保护心得体会范文2024

卫生部个人工作计划范文最新2024 2024卫生部个人工作计划模板大全

2024健康管理工作计划报告范文大全 健康管理工作计划及目标怎么写范文

中班安全工作计划下学期2024秋季 中班安全工作计划2024秋季开学范文

社区居委会2024工作计划书范文2024 2024社区居委会工作计划及举措怎么写

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找