# 2024年网络安全防护方案编制(七篇)

来源：网络 作者：星海浩瀚 更新时间：2024-10-17

*为了确保事情或工作有序有效开展，通常需要提前准备好一份方案，方案属于计划类文书的一种。优秀的方案都具备一些什么特点呢？又该怎么写呢？以下是我给大家收集整理的方案策划范文，供大家参考借鉴，希望可以帮助到有需要的朋友。网络安全防护方案编制篇一近...*

为了确保事情或工作有序有效开展，通常需要提前准备好一份方案，方案属于计划类文书的一种。优秀的方案都具备一些什么特点呢？又该怎么写呢？以下是我给大家收集整理的方案策划范文，供大家参考借鉴，希望可以帮助到有需要的朋友。

**网络安全防护方案编制篇一**

近年来，高新区网络与信息安全工作通过不断完善，日益健全，管委会领导十分重视计算机管理组织的建设，本着“控制源头、加强检查、明确责任、落实制度”的指导思想，成立了由管委会副主任为主管，办公室主任为负责人的网络安全工作小组，并设有专门的信息管理人员，所有上传信息都由办公室主任负责审查其合法性、准确性和保密性。高新区会在有关部门的监督和指导下，根据《中华人民共和国计算机信息系统安全保护条例》和《计算机病毒防治管理办法》等法规、规定，建立和健全了《安全管理责任制度》、《计算机及网络保密管理规定》和《文书保密工作制度》等防范制度，将计算机信息系统保密工作切实做到防微杜渐，把不安全苗头消除在萌芽状态。

按照文件要求，高新区及时制定了高新区门户网站安全突发事件应急预案，并根据应急预案组织应急演练。

高新区在开展网络与信息工作的每一步，都把强化信息安全教育放到首位，使管委会全体工作人员都意识到计算机安全保护是高新区中心工作的有机组成部分，而且在新形势下，网络和信息安全还将成为创建“平安高新、和谐高新”的重要内容。为进一步提高人员网络安全意识，我们还经常组织人员对相关部局进行计算机安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数计算机操作员对制度贯彻不够。对此，我们根据检查方案中的检查内容对不合格的部局提出批评，限期整改。各部局在安装杀毒软件时全部采用国家主管部门批准的查毒杀毒软件适时查毒和杀毒，不使用来历不明、未经杀毒的软件、u盘等载体，不访问非法网站，自觉严格控制和阻断病毒来源。单位电脑设备外送修理时，有指定人员跟随联系。电脑报废处理时，及时将硬盘等存储载体拆除或销毁。

在网络与信息安全管理工作中，我们就树立了以制度管理人员的思想，制定了网络信息安全相关制度，要求高新区管委会各部局提供的上传内容，由各部局负责人审查签字后报送至信息管理员，经办公室主任审核同意后上传;重大内容发布报管委会领导签发后再上传，以此作为高新区计算机网络内控制度，确保网站信息的保密性。

对照《通知》要求，高新区网站在以往的工作中，主要作了以上几方面的工作，但还有些方面要急待改进。

一是要今后还要进一步加强与市政府信息中心联系，

以此来查找差距，弥补工作中的不足。

二是要进一步加强对高新区管委会工作人员的计算机安全意识教育和防范技能训练，提高防范意识，充分认识到计算机网络与信息安全案件的严重性，把计算机安全保护知识真正融于工作人员业务素质的提高当中。

三是要进一步健全网络与信息安全管理制度，提高管理人员工作技能，经常聘请专业人员对管理人员进行培训，把学到的知识真正融于网络与信息安全保护工作中，而不是轻轻带过;做到人防与技防结合，真正设置起一道网络与信息安全工作的一道看不见的屏障。

**网络安全防护方案编制篇二**

根据《国科院办公厅关于印发政府网站发展指引的通知》、《互联网安全保护基础措施规定》等相关政策法规的要求，我单位接到\*\*市公安局《关于开展2024年\*\*市公安机关网络安全执法检查工作的通知》后，我单位领导高度重视，及时安排部署组织开展本年度网络安全检查，认真查找我单位网络与信息安全工作中存在的隐患及漏洞，完善安全管理措施，减少安全风险，提高应急处置能力，确保网络和信息安全，现将本单位自查工作情况汇报如下：

我单位高度重视网络安全工作，成立了由主要领导任组长，技术分管领导任副组长，全体干部为组员的网络安全领导小组，领导小组下设办公室，办公室设在技术部办公室。同时针对网络安全人员的配备及责任落实情况做了明确要求(附件一：《\*\*日报网络传媒中心网络安全人员及相关责任登记表》)，为确保网络安全工作顺利开展，我单位要求全体干部充分认识网络安全工作的重要性，认真学习网络安全知识，都能按照网络安全的各种规定，正确使用计算机网络和各类信息系统，并制定了《\*\*日报网络传媒中心网络安全规划方案》(附件五)。

我单位目前共有内网线路1条，即中国电信宽带网，由光纤接入办公室，共连接非涉密计算机244台;政务内网1条、档案专线1条，涉密计算机2台。上述所有电脑都配备了杀毒软件，能定期杀毒与升级。对涉密计算机的管理，明确了一名分管领导具体负责，并制定专人从事计算机保密管理工作。对非涉密计算机的管理，明确非涉密计算机不得处理涉密信息。对于计算机磁介质(软盘、u盘、移动硬盘等)的管理，采取专人保管、涉密文件单独存放，严禁携带存有涉密内容的磁介质到上网的计算机上加工、储存、传递处理文件。

另外，我单位在电信托管有7台服务器，维护\*\*市市委、市政府、市直部门及党群单位网站共计30余个(附件六：《\*\*市市委、市政府、市直部门及党群单位登记表》)，在日常进行安防、备份等方面的维护工作方面，能做到对网站和应用系统的程序升级、账户、口令、软件补丁、查杀病毒、外部接口以及网站维护等方面的问题逐一进行清理、排查，能及时更新升级的更新升级，进一步强化安全防范措施，及时堵塞漏洞、消除隐患、化解风险。

为确保计算机网络及服务器安全，实行了\*\*日报网络传媒中心技术部工作职责(附件二)、idc机房管理制度(附件三)及突发事件应急处理预案(附件四)等以有效提高管理员的工作效率。同时我室结合自身情况制定安全自查工作制度，做到四个确保：一是系统管理员于每周五定期检查计算机系统，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;三是实行领导定期询问制度，由系统管理员汇报使用情况，确保情况随时掌握;四是定期组织相关人员学习有关网络知识，提高计算机使用水平，确保预防。

为了构筑科学严密的制度防范体系，不断完善各项规章制度，规范计算机及其网络的安全保密管理，确保计算机及其网络安全管理工作各项规定制度的落实，我单位采取自查与抽查相结合，常规检查与重点检查相结合，定期检查与突击检查相结合等方式，对计算机及其网络管理制度的落实情况、涉密网络的管理和使用情况、防范措施的落实情况进行检查。今年以来，我单位对所有计算机及其网络的安全情况进行了一次全面的检查，通过检查，查找到计算机及其网络安全工作中存在的管理漏洞，并整改到位。我单位主要采取了以下几项措施：一是认真贯彻执行上级保密部门文件的有关规定和要求，不断增强依法做好计算机保密管理的能力;二是对处理信息类别进行了明确规定;三是定期对非涉密网络开展保密检查，严格涉密信息流转的规范性，弥补管理上存在的空档;四是针对信息发布存在的不规范等问题，及时对照《政府信息公开保密审查制度》进行整改，要求对上网信息严格审查、严格控制、严格把关，从制度上杜绝泄密隐患，做到上网信息不涉密、涉密信息不上网。

通过此次自查，我单位网络安全工作能做到制度到位、管理到位、检查到位，并做到以下几点：

1、安装了专业杀毒软件，加强了在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的有效性。

2、网络安全领导小组工作人员负责保密管理，相关的用户名和开机密码为其专有，且规定严禁外泄。做到禁止在未采取防护措施的情况下，涉密信息系统与非涉密网络及其他公共信息网络之间进行信息交换。

3、领导小组要求对网站所要发布内容一律要通过分管领导审核同意后才能够发表、删除、修改。做到信息公开坚持先审查、后公开和一事一审原则。

(1)在发布信息的权威、一致性方面规定了网站发布、转载有关信息须依据国家有关规定执行，内容加入或更新不得出现有关法律、行政法规禁止的内容，不得有不宜公开的内容;(2)在网站信息处理和人员落实方面规定了栏目的内容及相应的信息提供实行各科室分工负责制，网站领导小组负责网站信息的分类、整理、更新、发布。(3)在网站涉密信息方面明确了要严格遵守上网不涉密，涉密不上网的规定，确保党和国家秘密的绝对安全。

通过此次自查也发现存在一定的问题和不足，主要是计算机防范技术有待学习提高，二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;三是应急机制初步建立，但还不完善;四是网站发布信息的时效性不强。

**网络安全防护方案编制篇三**

为了贯彻落实《关于开展网络与信息安全检查工作的通知》的精神，切实加强我局政务信息系统运行管理和对外网站安全防范工作，严防攻击、网络中断、病毒传播、信息失窃密，为国庆60周年庆祝活动的顺利举行创造良好的\"网络信息环境，现就我局网络信息安全自查自纠情况汇报如下：

        我局接到区信息办下发的《关于开展网络与信息安全检查工作的通知》后，局领导班子高度重视，立即进行安排部署，落实责任，强化防护措施，加强对本单位网络和信息系统的安全保护,做好我局内部网络和信息系统的安全防范和安全检查工作。

1.责任制度。对网络信息安全各项制度进行了全面梳理，重点抓好安全责任制、应急预案、值班值守、信息发布审核等制度的落实。严格落实领导责任制，一把手亲自过问，分管负责人直接抓,一级抓一级,层层抓落实。

2.原则要求。坚决执行“谁主管谁负责、谁运行谁负责、谁使用谁负责、谁发布谁负责”的原则，认真履行网络信息安全保障职责。

3.“五到位”。坚决做到领导、机构、人员、责任、措施“五到位”。健全安全工作机制，对发生重大安全责任事故的，要严肃追究相关人员的责任。

1.清查网站隐患。针对和应用系统的程序升级、账户、密码、杀病毒、网站维护、政务网接入和运行等方面存在的突出问题，我们逐一进行清理、排查，能及时更新升级的更新升级，进一步强化安全防范措施，及时堵塞漏洞、消除隐患、化解风险。

2.严格执行网络信息安全“五禁止”规定。能够按要求禁止将涉密信息系统接入国际互联网及其他公共信息网络，能够禁止在没有防护措施的情况下将国际互联网等公共信息网络上的数据拷贝到涉密信息系统，能够禁止将涉密与非涉密网络混用，能够禁止将涉密与非涉密计算机、移动存储设备混用，能够禁止使用具有无线互联功能的设备处理涉密信息。

通过自查，我们发现我局网络与信息系统安全隐患还是存在一些问题，我们将切实对涉及到的有关问题逐步解决，进一步加强网络信息安全管理。

**网络安全防护方案编制篇四**

根据衡水市网络与信息安全协调小组印发《衡水市20xx年网络与信息安全检查方案》要求，结合实际，认真对我市信息系统安全进行了检查，现将检查情况报告如下：

今年来，市、局高度重视信息安全工作，把信息安全工作列入重要议事日程，为规范信息公开工作，落实好信息安全的相关规定，成立了信息安全工作领导小组，落实了管理机构，由专门的信息化公室负责信息安全的日常管理工作，明确了信息安全的主管领导、分管领导和具体管理人员。

相继建立健全了日常信息管理、信息安全防护管理等相关工作制度，加强了信息安全教育工作，信息安全工作领导小组定期或不定期地对我市信息安全工作进行检查，对查找出的问题及时进行整改，进一步规范了信息安全工作，确保了信息安全工作的有效开展，全市信息安全工作取得了新进展。

（一）加强领导，明确职责，抓好网络与信息安全组织管理工作。为规范、加强信息安全工作，市领导高度重视，把该项工作列为重点工作任务，成立了由主管市长为组长，分管信息工作的局级领导为副组长，各相关市直单位为成员的信息安全工作领导小组。做到了分工明确，责任到人，形成了主管领导负总责，具体管理人负主责，分级管理，一级抓一级，层层抓落实的领导体制和工作机制，切实把信息安全工作落到实处。

（二）做好网络与信息安全日常管理工作。根据工作实际，我局建立健全了信息系统安全状况自查制度、信息系统安全责任制、计算机及网络保密管理等相关制度，使信息安全工作进一步规范化和制度化。

（三）落实好网络与信息安全防护管理。健全完善了非涉密计算机保密管理制度、非涉密移动储存介质保密等管理制度。在计算机上安装了防火墙，同时配置安装了专业杀毒软件，加强了在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的有效性。网络终端没有违规上国际互联网及其他的信息网的现象，单位未安装无线网络等无线设备，并安装了针对移动存储设备的专业杀毒软件。

（四）制定信息安全应急管理机制。结合实际，我市初步建立应急预案，建立了电子公文和信息报送办理制度（试行）和电子公文和信息报送岗位责任制，严格文件的收发，完善了清点、修理、编号、签收制度；信息管理员及时对系统和软件进行更新，对重要文件、信息资源做到及时备份，数据恢复。

（五）安全教育培训情况正在逐步开展。今年下半年，我市计划对全体计算机使用人员开展了网络与信息安全等方面的操作培训，并讲解网络安全的一些知识。

（六）认真开展信息安全检查工作。市信息安全工作领导小组会定期或不定期地对我市网络与信息安全工作进行检查，对查找出的问题及时进行整改，确保了信息安全工作的有效展。

根据《衡水市20xx年网络与信息安全检查方案》中的具体要求，在工作自查过程中我们也发现了一些不足及待以整改的情况。

1、存在问题。在自查过程中主要存在以下情况：一是投入不足。由于我市缺少专业技术人员，且市财政在信息系统安全方面可投入的资金有限，因此在网络与信息安全建设过程中投入的力量有限；二是规章制度体系初步建立，但还不完善，未能覆盖相关信息系统安全的所有方面；三是在遇到计算机病毒侵袭等突发事件上，处理不够及时。

2、整改情况。针对以上存在的问题，我们将做好四个“继续”。一是继续完善并执行信息安全工作制度，应经常不定期的对信息安全工作制度执行情况进行检查，对于导致不良后果的责任人，要严肃追究责任，从而提高信息人员安全防护意识；二是继续抓好制度落实，在进一步完善网络与信息安全制度的同时，安排专人密切监测，随时随地解决可能发生的信息系统安全事故；三是继续加强对全市领导干部、网络信息人员的安全意识教育，提高做好信息安全工作的主动性和自觉性；四是继续加强加大对全市信息线路、信息系统等方面的及时维护、保养、更新力度。

建议省、市加大对县市区信息安全工作的指导，经常性开展信息安全教育培训，不断提高信息安全工作的现代化水平，便于工作人员进一步加强对网络与信息安全方面的防范和保密工作；建议省、市加大与对信息安全工作的资金和技术投入力度，确保工作顺利开展，保证信息安全。

**网络安全防护方案编制篇五**

为了认真贯彻落实公安部《关于开展重要信息系统和重点网站网络安全保护状况自检自查工作的通知》文件精神，为进一步做好我院网络与信息系统安全自查工作，提高安全防护能力和水平，预防和减少重大信息安全事件的发生，切实加强网络与信息系统安全防范工作，创造良好的网络信息环境。近期，我院进行了信息系统和网站网络安全自查，现就我院网络与信息系统安全自查工作情况汇报如下：

（一）自查的总体评价

我院严格按照公安部对网络与信息系统安全检查工作的要求，积极加强组织领导，落实工作责任，完善各项信息系统安全制度，强化日常监督检查，全面落实信息系统安全防范工作。今年着重抓了以下排查工作：一是硬件安全，包括防雷、防火和电源连接等；二是网络安全，包括网络结构、互联网行为管理等；三是应用安全，公文传输系统、软件管理等，形成了良好稳定的安全保密网络环境。

（二）积极组织部署网络与信息安全自查工作

1、专门成立网络与信息安全自查协调领导机构

成立了由分管领导、分管部门、网络管理组成的信息安全协调领导小组，确保信息系统高效运行、理顺信息安全管理、规范信息化安全等级建设。

2、明确网络与信息安全自查责任部门和工作岗位

我院领导非常注重信息系统建设，多次开会明确信息化建设责任部门，做到分工明确，责任具体到人。

3、贯彻落实网络与信息安全自查各项工作文件或方案

信息系统责任部门和工作人员认真贯彻落实市工业和信息化委员会各项工作文件或方案，根据网络与信息安全检查工作的特点，制定出一系列规章制度，落实网络与信息安全工作。

4、召开工作动员会议，组织人员培训，专门部署网络与信息安全自查工作

我院每季度召开一次工作动员会议，定期、不定期对技术人员进行培训，并开展考核。技术人员认真学习贯彻有关文件精神，把信息安全工作提升到重要位置，常抓不懈。

（一）网络安全管理情况

1、认真落实信息安全责任制

我院制定出相应信息安全责任追究制度，定岗到人，明确责任分工，把信息安全责任事故降低到最低。

2、积极推进信息安全制度建设

（1）加强人员安全管理制度建设

我院建立了人员录用、离岗、考核、安全保密、教育培训、外来人员管理等安全管理制度，对新进人员进行培训，加强人员安全管理，不定期开展考核。

（2）严格执行机房安全管理制度

我院制定出《机房管理制度》，加强机房进出人员管理和日常监控制度，严格实施机房安全管理条例，做好防火防盗，保证机房安全。

（二）技术安全防范和措施落实情况

1、网络安全方面

我院配备了防病毒软件、网络隔离卡，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。计算机及网络配置安装了专业杀毒软件，加强了在防病毒、防攻击、防泄密等方面的有效性。并按照保密规定，在重要的涉密计算机上实行了开机密码管理，专人专用，杜绝涉密和非涉密计算机之间的混用。

2、信息系统安全方面

涉密计算机没有违规上国际互联网及其他的信息网的情况，未发生过失密、泄密现象。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，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）应急工作情况

1、开展日常信息安全监测和预警

我院建立日常信息安全监测和预警机制，提高处置网络与信息安全突发公共能力事件，加强网络信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网站网络与信息安全突发公共事件的危害。

2、建立安全事件报告和响应处理程序

我院建立健全分级负责的应急管理体制，完善日常安全管理责任制。相关部门各司其职，做好日常管理和应急处置工作。设立安全事件报告和相应处理程序，根据安全事件分类和分级，进行不同的上报程序，开展不同的响应处理。

3、制定应急处置预案，定期演练并不断完善

我院制定了安全应急预案，根据预警信息，启动相应应急程序，加强值班值守工作，做好应急处理各项准备工作。定期演练预警方案，不断完善预警方案可行性、可操作性。

（四）安全教育培训情况

为保证我院网络安全有效地运行，减少病毒侵入，我院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。

经过安全检查，我单位信息系统安全总体情况良好，但也存在了一些不足：

1、信息安全意识不够。员工的信息安全教育还不够，缺乏维护信息安全主动性和自觉性。

2、设备维护、更新还不够及时。

3、专业技术人员少，信息系统安全力量有限，信息系统安全技术水平还有待提高。

4、信息系统安全工作机制有待进一步完善。

根据自查过程中发现的不足，同时结合我院实际，将着重以下几个方面进行整改：

一是要继续加强对全员的信息安全教育，提高做好安全工作的主动性和自觉性。

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况进行检查，对于导致不良后果的责任人，要严肃追进责任，从而提高人员安全防范意识。

三是要加强专业信息技术人员的培养，进一步提高信息安全工作技术水平，便于我们进一步加强计算机信息系统安全防范和保密工作。

四是要加大对线路、系统、网络设备的维护和保养，同时，针对信息技术发展迅速的特点，要加大系统设备更新力度。

五是要创新完善信息安全工作机制，进一步规范办公秩序，提高信息工作安全性。

五、关于加强信息安全工作的意见和建议

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：

一是对于线路不整齐、暴露的，立即对线路进行限期整改，并做好防鼠、防火安全工作。

二是加强设备维护，及时更换和维护好故障设备。

三是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。

**网络安全防护方案编制篇六**

我区接到市信息化领导小组办公室下发的《xx市信息化工作领导小组办公室关于开展重点领域网络与信息安全检查的通知》后，高新区管委会领导十分重视，及时召集相关人员按照文件要求，逐条落实，周密安排自查，对机关各部局配备的计算机网络与信息安全工作进行了排查，现将自查情况报告如下：

近年来，高新区网络与信息安全工作通过不断完善，日益健全，管委会领导十分重视计算机管理组织的建设，本着“控制源头、加强检查、明确责任、落实制度”的指导思想，成立了由管委会副主任为主管，办公室主任为负责人的网络安全工作小组，并设有专门的信息管理人员，所有上传信息都由办公室主任负责审查其合法性、准确性和保密性。高新区会在有关部门的监督和指导下，根据《中华人民共和国计算机信息系统安全保护条例》和《计算机病毒防治管理办法》等法规、规定，建立和健全了《安全管理责任制度》、《计算机及网络保密管理规定》和《文书保密工作制度》等防范制度，将计算机信息系统保密工作切实做到防微杜渐，把不安全苗头消除在萌芽状态。

按照文件要求，高新区及时制定了高新区门户网站安全突发事件应急预案，并根据应急预案组织应急演练。

高新区在开展网络与信息工作的每一步，都把强化信息安全教育放到首位，使管委会全体工作人员都意识到计算机安全保护是高新区中心工作的有机组成部分，而且在新形势下，网络和信息安全还将成为创建“平安高新、和谐高新”的重要内容。为进一步提高人员网络安全意识，我们还经常组织人员对相关部局进行计算机安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数计算机操作员对制度贯彻不够。对此，我们根据检查方案中的检查内容对不合格的部局提出批评，限期整改。各部局在安装杀毒软件时全部采用国家主管部门批准的查毒杀毒软件适时查毒和杀毒，不使用来历不明、未经杀毒的软件、u盘等载体，不访问非法网站，自觉严格控制和阻断病毒来源。单位电脑设备外送修理时，有指定人员跟随联系。电脑报废处理时，及时将硬盘等存储载体拆除或销毁。

在网络与信息安全管理工作中，我们就树立了以制度管理人员的思想，制定了网络信息安全相关制度，要求高新区管委会各部局提供的上传内容，由各部局负责人审查签字后报送至信息管理员，经办公室主任审核同意后上传；重大内容发布报管委会领导签发后再上传，以此作为高新区计算机网络内控制度，确保网站信息的保密性。

对照《通知》要求，高新区网站在以往的工作中，主要作了以上几方面的工作，但还有些方面要急待改进。

一是要今后还要进一步加强与市政府信息中心联系，以此来查找差距，弥补工作中的不足。

二是要进一步加强对高新区管委会工作人员的计算机安全意识教育和防范技能训练，提高防范意识，充分认识到计算机网络与信息安全案件的严重性，把计算机安全保护知识真正融于工作人员业务素质的提高当中。

三是要进一步健全网络与信息安全管理制度，提高管理人员工作技能，经常聘请专业人员对管理人员进行培训，把学到的知识真正融于网络与信息安全保护工作中，而不是轻轻带过；做到人防与技防结合，真正设置起一道网络与信息安全工作的一道看不见的屏障。

**网络安全防护方案编制篇七**

为落实“教育部办公厅关于开展网络安全检查的通知”(教技厅函[xxx6]5号)、“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”(教技[xxx6]4号)、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”(陕教保【xxx6】8号)，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：

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。

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

xxx9年制定了《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

xxx6年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。

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(xxx3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xxx3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。

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xxx3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。

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[xxx5]51号文件9个检查项目之一)

2.建议在xxx6年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(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。

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