# 网络安全检查总结报告

来源：网络 作者：逝水流年 更新时间：2024-01-05

*网络安全（CyberSecurity）是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。今天为大家精心准备了网络安全检查总结报告，希望对大家有所帮助!...*

网络安全（CyberSecurity）是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。今天为大家精心准备了网络安全检查总结报告，希望对大家有所帮助![\_TAG\_h2]　　网络安全检查总结报告

　　网监处：

　　高度重视，立刻组织我院相关部门对我院网络中的安全隐患进行了逐一排查，现将自查情况总结如下：

　　>一、网络信息安全管理机制和制度建设落实情况

　　一是为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，\_X成\_以由\_导担任第一责任人、\_相关部门参与、\_息中心负责具体工作的计算机信息系统安全保护工作领导小组，统一协调全院各部门开展校园网络安全管理工作。

　　二是为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：一是系统管理员于每周五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7\_24小时联系渠道，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。

　　一是网络安全方面。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，规范全院的上网行为。

　　二是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。

　　三是\_X网\_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

　　今年以来，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，网络中心采取了：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\_X网\_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，进一步加强与德阳市公安局网监处沟通和协调。

　　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，让全院师生充分认识到做好“开展十八大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，确实做好我院网络与信息安全维护工作。

**网络安全检查总结报告**

　　按照《关于开展网络安全检查工作的通知》要求，我局自3月起开展了网络安全自查工作，现总结如下：

　　 >一、网络安全检查工作组织开展情况

　　 为落实有关网络安全检查的要求，我局按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，结合我局实际的网络信息系统现状，有步骤有次序地开展了网络安全自查活动。自查以副局长为领导，成立了由局办公室、网络安全中心等部门组成的自查小组，对我局的网络安全进行了全面梳理及综合分析。自查活动未发现重大安全问题，各网络系统运行稳定。

　　 >二、201x年网络安全主要工作情况

　　 一是领导重视。我局高度重视信息安全工作，成立了以局领导为组长的信息安全领导小组，统一领导我局的信息安全工作。202\_年，我局成立了保密和信息安全专家组，负责审定信息安全工作。202\_年根据局领导工作分工的调整情况，及时调整了我局信息安全工作领导小组。

　　 二是落实责任。我局信息安全工作由局办公室牵头，网络安全中心共同负责，工作人员相对稳定。目前，我局的网络与信息系统分别由办公室、网络安全中心负责运维和管理。我局认真落网络安全工作的有关要求和各项重大部署，对我局内部网络和信息安全工作进行监督、检查和常规管理。及时掌握和解决影响网络安全运行方面出现或存在的有关问题，组织力量对突发事件进行应急处置，最大限度的防止或降低网络安全事件的发生。

　　 三是加强技术防护。201x年我局对网络核心设备安全策略进行了梳理，并进行了网络安全方面的全面检查，根据系统服务需求开放端口，把不必要的端口进行了关闭，防火墙的安全策略做了相应的调整；重新完善了应急预案；WindowsXP操作系统停止安全服务后，对一些终端系统进行了升级，安装windows7操作系统。针对一些有特殊需求不能升级操作系统的终端.

　　 1.落实组织管理构成小组

　　 我委高度重视网络安全工作，成立了由主要领导任组长，分管领导任副组长，办公室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，办公室设在团区委办公室。为确保网络安全工作顺利开展，我委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。

　　 2.基本情况及网络安全管理现状

　　 我委目前共有电子内网1条，连接政府内网计算机1台；电子政务系统一条，门户网站及统一平台

　　 4个信息运营使用。其中，非涉密网络1个，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4台。我委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。

　　 3.展开督查整改

　　 为了确保计算机及其网络安全管理工作各项规定制度的落实，及时发现计算机及其网络的安全工作的督促检查，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，我委对所有计算机及其网络的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。

　　 4.严格规范管理

　　 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，我委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”。

　　 5.网络安全检查自查结果

　　 通过此次自查，我委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、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；

　　 2、做到禁止将涉密计算机、涉密存储设备接入非涉密网络及其他公共信息网络；

　　 3、做到严禁使用非涉密计算机、非涉密存储设备存储、处理涉密信息；

　　 4、做到严禁通过非涉密网络电子邮箱办理公务，存储、处理、传输涉密文件资料和敏感信息；

　　 5、做到信息公开坚持“先审查、后公开”和“一事一审”原则。

　　 6、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。

　　 7、做到全部计算机上的炒股、游戏、聊天、下载、在线视频等与工作无关的软件程序的全面卸载清理，杜绝利用计算机从事与工作无关行为的发生。

　　 通过此次自查也发现存在一定的问题，主要是计算机防范技术有待学习提高，今后我们将继续加强学习，提高技术水平，严防计算机网络安全事件的发生。

**网络安全检查总结报告**

　　接到《河南省卫生计生委关于开展河南省卫生系统网络与信息督导检查工作的通知》后，我院领导高度重视，立即召开相关科室负责人会议，深入学习和认真贯彻落实文件精神，充分认识到开展网络与信息安全自查工作的重要性和必要性，对自查工作做了详细部署，由主管院长负责安排、协调相关检查部门、监督检查项目，由信息科负责具体检查和自查工作，并就自查中发现的问题认真做好相关记录，及时整改，完善。

　　长期以来，我院在信息化建设过程中，一直非常重视网络与信息安全工作，并采取目一套有效的安全管理规范、有效的安全管理措施。自1月9日起，全院开展网络与信息安全工作自查，根据互联网安全和院内局域网安全的相应特点，逐项排查，消除安全隐患，现将我院信息安全工作情况汇报如下。

　　信息安全工作情况

　>　一、网络安全管理：我院的网络分为互联网和院内局域网，两网络实现物理隔离，以确保两网能够互不影响，独立、安全、高效运行。

　　1.硬件安全，包括防雷、防火、防盗和UPS电源连接等。医院服务器机房严格按照机房标准建设，工作人员坚持每天巡查，排除安全隐患。HIS、LIS、EMR、PACS等服务器、交换机、存储等都有UPS电源保护，可以保证短时间断电情况下，设备运行正常，不至于因突然断电致设备损坏。此外，局域网内所有计算机USB接口施行完全封闭，

　　这样就有效地避免了因外接介质（如U盘、移动硬盘）而引起中毒或泄密的发生。

　　2.网络安全:包括网络结构、密码管理、IP管理等；网络结构包括网络结构合理，网络连接的稳定性，网络设备（交换机、路由器、光纤收发器等）的稳定性，我院会定期检查网络设备的运转情况并在信息科有网络设备备件，发生故障可以第一时间更换以确保医院业务的正常进行。各个医院系统的操作人员，都有自己的登录名和密码，并分配相应的权限，账户施行“谁使用、谁管理、谁负责”的管理制度。互联网和院内局域网根据区域不同划分为5个IP段，均施行固定IP地址，由医院统一分配、管理，不允许私自添加新IP。

　　二、数据库安全管理：我院目前运行的数据库主要是ORACLE数据库，是保证医院诊疗、划价、收费、查询、统计等各项业务能够正常进行的基础，为确保医院各项业务正常、高效运行，数据库安全管理是极为有必要的。数据库系统的安全特性主要是针对数据的技术防护而言的，包括数据安全性、并发控制、故障恢复、数据库容灾备份等几个方面。我院对数据安全性采取以下措施：（1）将数据库中需要保护的部分与其他部分相隔。（2）采用授权规则，如账户、口令和权限控制等访问控制方法，并对数据库进行了优化，大大提高服务器数据库并发连接数的承载能力。（3）数据库容灾备份是数据库安全管理中极为重要的一部分，是数据库有效、安全运行的最后保障，也是保障数据库信息能够长期保存的有效措施。我院采用的备份类型为完全备份，每天凌晨备份整个数据库，包含用户表、系统表、索引、视图

　　和存储过程等所有数据库对象。在备份数据的过程中，主、从服务器正常运行，各客户端的业务能正常进行，也即是热备份。

　　三、软件管理：目前我院在运行的软件主要分为三类：医院系统、常用办公软件和杀毒软件。医院系统软件包括HIS、LIS、EMR、PACS等系统，其中HIS系统是我院日常业务中最主要的软件，是保障医院诊疗活动正常进行的`基础，自202\_年新系统上线以来，运行很稳定，未出现过重大安全问题，并根据业务需要，不断更新充实。常用办公软件均由医院信息科统一安装，维护。杀毒软件是保障电脑系统防病毒、防木马、防篡改、防瘫痪、防攻击、防泄密的有效工具。所有电脑，均安装了正版杀毒软件（360企业版杀毒软件和安全卫士），并定期更新病毒库，以保证杀毒软件的防御能力始终保持在很高的水平。

　　四、网站安全管理：在信息化高度发达的今天，网络宣传的作用日益突出，网站安全管理工作也不容忽视。我院的网站后台服务器施行托管管理，确保了网站后台服务的稳定性和安全性。我院设专门网站管-理-员，负责日常更新、维护，严格执行《网站管理规定》，网站自开放以来，从未发生过重大安全问题，并一直运行良好。

　　五、应急处置：我院HIS系统服务器运行安全、稳定，并配备了大型UPS电源，可以保证大面积断电情况下，服务器坚持运行数小时。虽然医院的信息系统长期以来运行良好，但医院仍然制定了应急处置预案，并对收费操作员和医护人员进行过培训，如果医院出现大面积、长时间停电情况，HIS系统无法正常运行，将临时开始手工收费、记账、发药，以确保诊疗活动能够正常、有序地进行，待到HIS系统恢复正常工作时，再补打发票、补记收费项目。

　　总体来说，我院对网络与信息安全工作非常重视，未发生过重大的安全事故，各系统运转稳定，各项业务能够正常运行。但自查中也发现了不足之处，如目前医院信息技术人员少，信息安全力量有限；信息安全意识还够，个别科室缺乏维护信息安全的主动性和自觉性；个别科室的计算机设备配置偏低，服务期限偏长。今后要加强信息技术人员的培养，更进一步提高信息安全技术水平；加强全院职工的信息安全教育，提高维护信息安全的主动性和自觉性；加大对医院信息化建设投入，提升计算机设备配置，进一步提高工作效率和系统运行的安全性。

　　经过了为期一周的自查工作，我院充分意识到安全工作是一个需要常抓不懈的工程，同时要不断创新，改变旧有的管理方法和理念，以适应新形势下的安全管理需要。

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！