# 最新网安工作总结简短(三篇)

来源：网络 作者：流年似水 更新时间：2025-08-01

*最新网安工作总结简短一根据《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）、《计算机网络国际互联网安全保护管理办法》和《信息安全等级保护管理办法》（公通字[20\_]43号）等文件要求，结合签定的《政府网站安全责任书》，我局...*

**最新网安工作总结简短一**

根据《中华人民共和国计算机信息系统安全保护条例》（国务院令第147号）、《计算机网络国际互联网安全保护管理办法》和《信息安全等级保护管理办法》（公通字[20\_]43号）等文件要求，结合签定的《政府网站安全责任书》，我局认真开展了网络安全防护自查工作，进一步完善制度，加强管理，细化技术措施，提高防护能力，确保网站顺利运行。成立了由分管副局长为组长，相关股室负责人和信息网络管理员为成员的网络信息安全领导小组，负责我局网站信息安全防护管理工作。及时建立了信息系统安全责任制、计算机及网络信息系统安全管理制度、应急预案、值班制度、信息发布审核制度、政府信息公开工作制度、责任追究制度等，进一步细化工作任务，做到执行严格，落实到位。同时，我局不断加大对信息公开业务知识的培训力度，采取以会代训的方式组织系统各单位和机关各股室相关人员系统的学习了《政府信息公开条例》等政策性文件，使全体干部职工明确实施政府信息公开的意义、基本内容以及相关配套措施和工作规范，提高了信息工作人员对网站安全防护的能力和水平。

我局严格按照“上网信息不涉密、涉密信息不上网”的原则，坚决杜绝在上传和发布政务信息过程中出现失密、泄密事件。一是定期对接入互联网计算机逐台进行检查，主要针对计算机密码管理、安全漏洞、防火墙、杀毒软件等涉及到我局办公电脑网络信息安全各个方面，加强了在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的严控性和有效性；二是实行安全网络定期查毒和杀毒，不使用来历不明、未经杀毒的软件、软盘、光盘、u盘等载体，不访问非法网站，严格控制和阻断病毒来源。在单位外的u盘，不得携带到单位内使用，局域网中的计算机在使用多功能一体机进行打印，专网计算机使用独立的打印机，专机专用；三是涉密计算机均设有开机密码，处于物理隔离未接入互联网，除专人使用和管理之外任何人不得接触或查看涉密计算机信息系统。禁止在非涉密计算机及信息系统内保存或流转任何涉密文件和内部敏感信息，所有涉密文件和内部敏感信息一律保存在涉密计算机信息系统中。涉密计算机信息系统配备单独的移动存储介质，不使用本局内其他科室的移动存储介质，禁止使用来历不明或未经杀毒的一切移动存储介质；同时，接入电子政务专网相关电脑与互联网物理隔离，均设有开机密码，并安装防火墙，同时配备专业杀毒软件，并由专人负责管理，有效地维护了我局网络信息安全。

为进一步加强信息系统安全，我局围绕信息系统安全综合治理的工作目标，重点在完善规章制度、丰富技术手段上下功夫，认真开展信息安全防护工作。一是根据省、市关于加强财政网站安全防护工作相关要求，结合我局信息系统安全工作实际，修订完善信息安全各项规章制度，建立健全了日常安全检查和信息通报制度，及时修订完善了《两当县财政局网络与信息安全应急预案》，使之能不断适应信息技术发展的各项要求；二是组织信息管理员等核心技术人员开展多种形式的信息系统安全知识学习、培训，进一步强化相关工作人员安全意识教育工作，加强设备安全巡检，做到防患于未然；三是针对现有网络防护设备陈旧不能满足工作要求的情况，积极筹措资金，采购较为先进、功能比较完善的网络安全防火墙一台，提高了财政广域网的安全防护能力；四是严格执行省、市、县政府信息公开工作要求，除涉及国家机密和个人隐私、可能影响国家利益和执法活动等以外的政府信息，积极主动进行了公开。同时，进一步规范对外政务公开的内容，及时更新各项行政法规依据，办事程序和服务承诺，行政许可事项和监督机制，并增设了工作动态、各类-3-

（含突发）事件处理情况等，使我局对外信息公开得到进一步完善，真正体现了“以民为本、为民解困、为民服务”的财政宗旨，维护了党和政府执政为民的良好形象。

通过全局干部职工的大力支持和相关工作人员的努力，我局及时建立完善了财政网站信息安全工作制度，全体工作人员普及了基本的信息安全知识，修补了单位网络系统的安全漏洞，制定并演练了信息安全应急预案，提高了信息安全的防护质量。同时，也暴露出了信息安全专业人员，现有人员掌握信息安全防范知识不全面、不系统等一些薄弱环节，我们将在以后的工作中及时加以解决完善，并严格按照省市财政网站安全防护工作相关要求，加大对财政网站安全监督和检查力度，进一步巩固已有成果，着力健全政府信息网站安全防护工作长效机制，为全面推进财政事业又好又快发展做出积极贡献。

**最新网安工作总结简短二**

1、适应形式需求，增强全局观念，加强调度纪律，确保电网安全稳定运行。调度运行系统成员要清醒的认识所担负的电网安全责任，以高度的责任感和使命感突出抓电网的安全管理，全力以赴保证电网的安全稳定运行，结合电网运行情况，制定并贯彻实施切实可行的电网稳定措施和反事故措施，严格执行电网管理中的各项规章制度，切实履行好职责。调度人员、变电运行人员、各设备线路维护部门要以高、精、细、严的标准严格要求自己，坚持事故预想天天做，每季度坚持开展反事故演习，根据不同季节，不同情况，积极合理有效地开展工作，保证电网安全稳定运行。

2、强调经济调度，高度重视运行分析，努力提高电网经济运行水平。对于经济调度重点落实电网监控和经济运行理论计算分析，加强对电网的实时监控，坚持开展负荷预测，总结负荷变化规律特点，结合潮流分布，以及经济运行理论计算数值，及时调整运行方式;并且要建立相应的运行管理现场规程、制度，强调目标责任的落实，努力提高电网经济运行水平。

3、加强对继电保护定值的校验工作，要根据规程规定结合电网结构及电网运行方式的改变，及时对系统进行短路电流计算，保护定值校核;突出抓好继电保护和安全自动装置的基础管理，进一步完善电网安全自动装置，杜绝继电保护“三误”现象的发生，切实落实继电保护“反措”，以满足电网运行的安全性需求。

4、以年度运行方式为指导，认真分析研究电网存在的薄弱环节，加强设备预防性试验和设备缺陷管理，推行以状态检修为基础的动态检修，提高设备健康水平。要认真准备，做好“春、秋季检修”及“迎峰度夏”准备工作，及时消除电网、设备隐患。

5、加强检修的组织管理。定检必须依据修必修好的原则按计划严格落实，严格控制临检，推行以停电工作的必要性和紧迫性为客观依据对停电计划进行测算考核，实行“先测算后停电”，合理制定检修停电计划，严格控制停电范围。在开展“零点工程”的同时，加强各检修单位的配合和联系，统一管理，统一安排，严格控制停电时间;检修单位要有工作计划，优化施工方案，落实工作措施，减少工作时间;停送电管理实行预报告制度，积极推行对检修、调度、运行操作部门停送电时间分级考核制度，减少设备在非检修状态的停电时间，杜绝设备停电等人现象，努力提高电网健康水平和供电可靠性。

6、加快农网建设改造及各变电站设备的技改步伐，积极推行技术进步。完善和优化电网结构，按照电网规划，优先安排增加电网传输容量提高电网安全和供电质量的项目，改善电网供电设备状况，增强供电设备供电能力。

7、高度重视无功管理，按照无功平衡的原则和有关导则规定，作好无功补偿的规划工作，同时加强无功管理措施的落实。按照总体平衡与局部平衡相结合，以局部为主;电力部门补偿与用户补偿相结合;分散补偿与集中补偿相结合，以分散为主;降损与调压相结合，以降损为主等几项原则，加大管理和宣传力度，提高各级管理人员和用户对无功的重视程度，使无功管理工作纳入规范化轨道。

8、加快通信及调度自动化系统建设改造步伐。按照二期农网结余资金和三期农网通信及调度自动化建设规划，争取早日完成东部光纤通信环网工程，加快调度主站系统改造，以开发高级应用为主导，不断完善调度主站系统功能及指标，争取早日实现调度自动化实用化达标。

**最新网安工作总结简短三**

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。

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20xx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。

本文档由范文网【dddot.com】收集整理，更多优质范文文档请移步dddot.com站内查找