

最新计算机安全自查报告(通用5篇)

随着社会不断地进步，报告使用的频率越来越高，报告具有语言陈述性的特点。通过报告，人们可以获取最新的信息，深入分析问题，并采取相应的行动。下面是小编帮大家整理的最新报告范文，仅供参考，希望能够帮助到大家。

计算机安全自查报告篇一

我县联社10月5日接到转发《金融机构计算机安全检查工作实施方案的通知》的通知后，联社领导班子十分重视，及时召集科技开发部、安全保卫部等部门负责人，按照文件要求，根据实施方案的指导思想和工作目标，逐条落实，周密安排，对全县个配备计算机的信用社和中心机房进行了排查，现将自查情况报告如下：

我县联社自设设立信息管理科以来，本着“谁主管理，谁负责”的指导思想，十分重视计算机管理组织的建设，成立了计算机安全保护领导小组，始终有一名联社副主任担任安全管理领导小组组长，并以信息管理、安全保卫、内部审计等部门负责人为成员。

联社科技开发部（原电脑信息科）为专职负责计算机信息系统安全保护工作的部门，对全县信用社主要计算机系统的资源配置、操作及业务系统、系统维护人员、操作人员进行登记。联社设立专职安全管理员，专职安全员由经过公安部门培训、获得《计算机安全员上岗证》的人员担任。基层信用社设立兼职安全管理员，负责对上属电子网点进行管理、监督，对本单位计算机出现的软、硬件问题及时上报联社科技部门。要求各信用社选用有责任心、有一定计算机知识、熟悉业务操作的人员担任。

我们在当地公安机关计算机安全保护部门的监督、检查、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》、《计算机病毒防治管理办法》、《金融机构计算机信息系统安全保护暂行规定》等法规、规定，建立、健全了各项防范制度，并编制成册，下发到全县xx年初，由主管计算机安全的副主任与保卫部门签订了目标责任书，并指定业务骨干担任计算机安全员，切实做到防危杜渐，把不安全苗头消除在萌芽状态。

在我县农信社实施电子化建设的每一步，我们都把强化信息安全教育和提高员工的计算机技能放到同等地位。在实施储蓄网络化过程中，联社专门举办了计算机培训班。培训内容不但包括计算机基础知识、储蓄业务操作流程，还重点讲解了计算机犯罪的特点、防范措施。使全体信用社员工意识到了，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。

随着计算机技术在信用社各项业务中的应用，为进一步提高职工安全意识和规范操作流程，我们还经常组织人员对基层信用社进行计算机业务系统运行及安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数微机操作员对制度贯彻行不够。对此，我们根据检查方案中的检查内容、评分标准对电子化网点进行打分，得分不合格者，除限期整改外，还根据《驻马店市农村信用社稽核处罚规定实施细则》、《平舆县农村信用社计算机信息系统安全保护实施细则》的有关规定，对有关责任人员如社主任、储蓄所负责人，操作员等，给予经济处罚、全县通报批评等处理。

从我县信息管理部门成立之日起，我们就树立了以制度管理人员的思想。为此，根据市办下发的信息科有关文件精神，对照人行中心支行的《科技工作管理制度》，先后制定了《中心机房管理制度》，《中心机房应急措施》，《计算机系统维修操作规程》，《电脑安全保密制度》，《计算机安全检查操作规程》，《计算机软件开发操作规程》等一系列内部

管理制度，让这些制度不但写在纸上，挂在墙上，还要牢记在心上。继而我们又印发了农信联《农村信用社计算机信息系统安全保护实施细则》、《农村信用社计算机综合业务系统管理办法》、《关于转发《市农村信用社计算机信息系统安全管理办法》的通知》，初步形成了较为完善的计算机内控制度。在以上文件中，要求明确规定了各级微机管理人员、操作员的权限和操作范围，对操作人员的上岗、调离等做出严格规定，详细制定了计算机综合业务系统的管理办法，要求各电子网点记录微机运行日志，对数据每日进行备份，对废弃的磁盘、磁带、报表不得随意丢弃，交由信息部门统一处理。

随着联社办公自动化的深入，各部门在处理业务报表、数据和日常办公中越来越多的用到了计算机。为保证各部门的计算机不受病毒危害，联社每台微机上都安装了实时的查、杀病毒软件，并及时进行软件升级和定期进行查杀病毒。同时还把计算机病毒预防措施下发至各部门的微机操作员手中，从专机专用、数据备份、软盘管理、实时杀毒、禁用盗版、禁玩游戏等几方面入手，使计算机病毒防治形成制度化。

计算机安全自查报告篇二

为更好地做好保密工作，杜绝非涉密办公电脑处理密件的行为，根据xxxxx要求，我局围绕非涉密计算机、移动存储介质、办公网络使用情况等进行了自查。现将有关情况汇报如下：

一、对局内所有办公电脑、移动存储介质和网络进行全面检查。局内x台办公电脑，均未发现非涉密计算机在连接互联网的计算机中制作、存储、传递和处理涉密文件、信息以及机关内部资料的行为；未感染木马病毒；未安装无线网卡等设备；未使用非涉密移动存储介质；无违规上国际互联网及其他公共信息网的记录。安全情况良好。

二、加强保密工作培训，提高保密工作意识。为提高全局领

导干部的保密工作意识，提高保密工作能力，组织大家认真学习了《国家保密法》、《中华人民共和国保守国家秘密法实施办法》等法律法规。组织全局领导干部认真观看警示教育影片，使大家进一步认识到了泄密事件造成的严重后果，从而自觉维护国家安全和利益。

计算机安全自查报告篇三

20xx年以来，在市委、市政府的正确领导下，我局严格按照《保密法》的规定，认真贯彻落实保密工作的要求，积极深入抓好保密工作，从而使我局的保密工作取得明显的成效。我局结合实际工作情况，对照检查目录表，逐条自查，现将自查情况报告如下：

一、高度重视，强化组织领导。

二、落实各项措施，确保机密安全。

为切实落实保密制度，做好保密机要工作，我局采取了以下几个方面的措施。

（一）严格计算机管理。目前我局所有股室和局领导办公室都配备了计算机，党政网电脑与政府网络信息中心联网，杜绝同一台计算机同时连接内外网。每台电脑上都安装了网络防火墙，对每台电脑的软件进行清理，删除一切与工作无关的信息和软件，尤其是网络游戏等联网软件，防止信息流失或遭受外界恶意攻击。

（二）严格文件资料管理。办公室是文件资料的加工、储存场所，为确保文件不随意外流，我局设立了1名专职人员，负责纸品文书的管理和电子文档的管理。具体做好文件资料的收发、分放、整理、归档、销毁等，对涉密的文件资料，只准在机关办公室阅，未经批准，不得带出机关；做好电子文档的输入、存档、发送、印制、备份等，确保电子文档安全。

同时加大对档案室的日常管理，非工作人员一般不准进入档案室，防止机密外泄。

记录。会议讨论的内容，未作出决定待定的、需要保密或一段时间内保密的，不得随意扩散传播。

（四）严格公章管理。局指定办公室负责对局行政、党组公章的保管，办公室主任为局公章的保管责任人。所有需加盖局行政公章的文书材料，一律需经得主要领导同意方可加盖；所有需加盖局党组公章的文书材料，一律需经得局长同意方可加盖。任何人不得随意加盖公章。并对加盖公章的材料作详细登记。

（五）严格工作程序。工作人员不在日常工作手册上记录秘密，不随意摘录、引用秘密文件、或擅自将秘密文件给他人传看，凡是自己在工作中掌握的秘密事项，没有传达义务的绝不告诉知密范围以外的人。不在无人看管的情况下将秘密文件和手册置于办公桌上，甚至带回家，非本机关人员不能单独留于办公室内，室内无人要锁门。

三、加强保密教育，提高思想认识

为认真做好保密机要工作，我局结合工作实际，切实把保密教育工作贯穿于日常工作中，在平时的学习例会上，多次强调做好保密工作的极端重要性，组织全体干部职工认真学习了《中华人民共和国保密法》、《国家工作人员保密守则》等保密工作规章制度以及州、县保密工作有关文件精神等。对办公室档案管理员、文书收发等加强保密教育，加强做好保密工作的检查督促，促进全体工作人员提高思想认识，增强做好保密工作的责任感。

计算机安全自查报告篇四

我校信息中心自成立以来，本着“责任到人，一丝不苟”的

指导思想，十分重视计算机管理组织的建设，成立了计算机安全保护领导小组，始终有一名信息中心主任担任安全管理领导小组组长，并以信息管理、安全保卫、各教研组等部门负责人为成员。

信息中心为专职负责计算机信息系统安全保护工作的部门，对全校教研室主要计算机系统的资源配置、操作及业务系统、系统维护人员、操作人员进行登记。信息中心设立专职安全管理员，专职安全员由经过公安部门培训、获得《计算机安全员上岗证》的人员担任。基层教研室设立兼职安全管理员，负责对电子网点进行管理、监督，对本单位计算机出现的软、硬件问题及时上报信息中心。要求各教研室选用有责任心、有一定计算机知识、熟悉业务操作的人员担任。

我们在当地公安机关计算机安全保护部门的监督、检查、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》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》、《河南省学校计算机信息系统安全管理暂行规定》、《计算机病毒防治管理办法》、以及公安部、教育部、信息产业部、国务院新闻办《关于开展垃圾邮件专项治理工作的通知》及教育部《关于开展高校上网场所清理整理工作，进一步加强校园网管理的紧急通知》等法规、规定，建立、健全了各项防范制度，并编制成册，下发到全校各个教研室。在年初，由主管计算机安全的主任与保卫部门签订了目标责任书，并指定业务骨干担任计算机安全员，切实做到防微杜渐，把不安全苗头消除在萌芽状态。

二、强化安全教育定期检查督促

在我校实施计算机信息化建设的每一步，我们都把强化信息安全教育和提高员工的计算机技能放到同等地位。在实施信息网络化过程中，信息中心专门举办了计算机培训班。培训内容不但包括计算机基础知识、课件制作，还重点讲解了计算机犯罪的特点、防范措施。使全体教职员工都意识到了，

计算机安全保护是学校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。

随着计算机技术在教研室各项业务中的应用，为进一步提高职工安全意识和规范操作流程，我们还经常组织人员对基层教研室进行计算机业务系统运行及安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数微机操作员对制度贯彻行不够。对此，我们根据检查方案中的检查内容、评分标准对各科室进行打分，得分不合格者，除限期整改外，还根据学校的有关规定，对有关责任人员，给予相应处罚、全校通报批评等处理。

三、信息安全制度日趋完善

从我校信息中心成立之日起，我们就树立了以制度管理人员的思想。为此，根据市办下发的有关文件精神，先后制定了《中心机房管理制度》，《中心机房应急措施》，《计算机系统维修操作规程》，《电脑安全保密制度》，《计算机安全检查操作规程》，《潢川一中电教管理员职责》、《潢川一中电子备课室管理制度》等一系列内部管理制度，让这些制度不但写在纸上，挂在墙上，还要牢记在心上。继而我们又印发了《潢川一中教研室计算机信息系统安全保护实施细则》、《潢川一中教研室计算机综合业务系统管理办法》、《潢川一中机房上机操作守则》、《潢川一中信息中心管理条例》等，初步形成了较为完善的计算机内控制度。在以上文件中，要求明确规定了微机管理人员、操作员的权限和操作范围，对操作人员的上岗、调离等做出严格规定，详细制定了计算机综合业务系统的管理办法，要求各电子网点记录微机运行日志，对数据每日进行备份，对废弃的磁盘、磁带、报表不得随意丢弃，交由信息中心统一处理。

四、防治计算机病毒

随着信息办公自动化的深入，各教研室在处理业务报表、数

据和日常办公中越来越多的用到了计算机。为保证各教研室的计算机不受病毒危害，信息中心为每台微机上都安装了实时的查、杀、防病毒的软件，并及时进行软件升级和定期进行查杀病毒。同时还把计算机病毒预防措施下发至各教研室的微机操作员手中，从专机专用、数据备份、软盘管理、实时杀毒、禁用盗版、禁玩游戏等几方面入手，使计算机病毒防治形成制度化。

对照《学校计算机信息系统安全检查表》的要求，我校信息中心在以往的工作中，主要作了以上几方面的工作，但还有些方面要急待改进。

一是今后还要进一步加强与公安机关和教育主管部门的工作联系，以此来查找差距，弥补工作中的不足。

二是要加强计算机安全意识教育和防范技能训练，充分认识到计

算机案件的严重性。把计算机安全保护知识真正融于学校知识的学习中，而不是轻轻带过；人防与技防结合，把计算机安全保护的技术措施看作是保护信息安全的一道看不见的屏障。

计算机安全自查报告篇五

我县联社10月15日接到转发《金融机构计算机安全检查工作实施方案的通知》的通知后，联社领导班子十分重视，及时召集科技开发部、安全保卫部等部门负责人，按照文件要求，根据实施方案的指导思想和工作目标，逐条落实，周密安排，对全县个配备计算机的信用社和中心机房进行了排查，现将自查情况报告如下：

我县联社自设设立信息管理科以来，本着“谁主管理，谁负责”的指导思想，十分重视计算机管理组织的建设，成立了计

计算机安全保护领导小组，始终有一名联社副主任担任安全管理领导小组组长，并以信息管理、安全保卫、内部审计等部门负责人为成员。

联社科技开发部（原电脑信息科）为专职负责计算机信息系统安全保护工作的部门，对全县信用社主要计算机系统的资源配置、操作及业务系统、系统维护人员、操作人员进行登记。联社设立专职安全管理员，专职安全员由经过公安部门培训、获得《计算机安全员上岗证》的人员担任。基层信用社设立兼职安全管理员，负责对上属电子网点进行管理、监督，对本单位计算机出现的软、硬件问题及时上报联社科技部门。要求各信用社选用有责任心、有一定计算机知识、熟悉业务操作的人员担任。

我们在当地公安机关计算机安全保护部门的监督、检查、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》、《计算机病毒防治管理办法》、《金融机构计算机信息系统安全保护暂行规定》等法规、规定，建立、健全了各项防范制度，并编制成册，下发到全县20个信用社。在年初，由主管计算机安全的副主任与保卫部门签订了目标责任书，并指定业务骨干担任计算机安全员，切实做到防危杜渐，把不安全苗头消除在萌芽状态。

在我县农信社实施电子化建设的每一步，我们都把强化信息安全教育和提高员工的计算机技能放到同等地位。在实施储蓄网络化过程中，联社专门举办了计算机培训班。培训内容不但包括计算机基础知识、储蓄业务操作流程，还重点讲解了计算机犯罪的特点、防范措施。使全体信用社员工意识到了，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。

随着计算机技术在信用社各项业务中的应用，为进一步提高职工安全意识和规范操作流程，我们还经常组织人员对基层

信用社进行计算机业务系统运行及安全保护的检查。通过检查，我们发现部分人员安全意识不强，少数微机操作员对制度贯彻行不够。对此，我们根据检查方案中的'检查内容、评分标准对电子化网点进行打分，得分不合格者，除限期整改外，还根据《驻马店市农村信用社稽核处罚规定实施细则》、《平舆县农村信用社计算机信息系统安全保护实施细则》的有关规定，对有关责任人员如社主任、储蓄所负责人，操作员等，给予经济处罚、全县通报批评等处理。

从我县信息管理部门成立之日起，我们就树立了以制度管理人员的思想。为此，根据市办下发的信息科有关文件精神，对照人行中心支行的《科技工作管理制度》，先后制定了《中心机房管理制度》，《中心机房应急措施》，《计算机系统维修操作规程》，《电脑安全保密制度》，《计算机安全检查操作规程》，《计算机软件开发操作规程》等一系列内部管理制度，让这些制度不但写在纸上，挂在墙上，还要牢记在心上。继而我们又印发了农信联（）2号《农村信用社计算机信息系统安全保护实施细则》、（）31号《农村信用社计算机综合业务系统管理办法》、（）84号《关于转发《市农村信用社计算机信息系统安全管理办法》的通知》，初步形成了较为完善的计算机内控制度。在以上文件中，要求明确规定了各级微机管理人员、操作员的'权限和操作范围，对操作人员的上岗、调离等做出严格规定，详细制定了计算机综合业务系统的管理办法，要求各电子网点记录微机运行日志，对数据每日进行备份，对废弃的磁盘、磁带、报表不得随意丢弃，交由信息部门统一处理。

随着联社办公自动化的深入，各部门在处理业务报表、数据和日常办公中越来越多的用到了计算机。为保证各部门的计算机不受病毒危害，联社每台微机上都安装了实时的查、杀病软件，并及时进行软件升级和定期进行查杀病毒。同时还把计算机病毒预防措施下发至各部门的微机操作员手中，从专机专用、数据备份、软盘管理、实时杀毒、禁用盗版、禁玩游戏等几方面入手，使计算机病毒防治形成制度化。

对照《金融机构计算机信息系统安全检查评分表》的要求，我县农村信用联社在以往的工作中，主要作了以上几方面的工作，但还有些方面要急待改进。

一是今后还要进一步加强与公安机关的工作联系，以此来查找差距，弥补工作中的不足。

二是要加强计算机安全意识教育和防范技能训练，充分认识到计算机案件的严重性。把计算机安全保护知识真正融于“三防一保”知识的学习中，而不是轻轻带过；人防与技防结合，把计算机安全保护的技术措施看作是保护资金安全的一道看不见的屏障。

三是由于工作场地所限，部分营业网点备份的数据不能做到异地保存。