2023年事业单位非涉密计算机自查报告(优秀5篇)

在经济发展迅速的今天，报告不再是罕见的东西，报告中提到的所有信息应该是准确无误的。那么我们该如何写一篇较为完美的报告呢？这里我整理了一些优秀的报告范文，希望对大家有所帮助，下面我们就来了解一下吧。

事业单位非涉密计算机自查报告篇一

第一条

为加强涉密计算机保密管理，依据《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理的规定》、《中华人民共和国计算机信息系统安全保护条例》及《公安机关计算机信息系统保密安全规定》，结合公安工作实际，特制定此制度。

第二条

严禁在涉密计算机硬盘内存储绝密级文件和信息；对涉密计算机存储的涉密文件，要进行不间断的检查和清理，严格落实保管责任人。

第三条

涉密计算机必须设定不少于8位数的开机密码，有专人使用和管理，密码报本单位保密领导小组成员备案。

第四条

涉密计算机出现故障需要送修的，须经保密部门和信息通信部门的检查和技术处理。涉密计算机硬盘损坏后，需将硬盘

拆下，交有关人员妥善存放，经分局保密领导小组组长批准后，交分局定点单位销毁。

第五条

要对涉密计算机硬件资源加贴标签及定密标识，设备的随机资料（含磁介质、光盘等）及保修（单）卡由各涉密单位保管。

第六条

严禁“一机两用”行为。涉密计算机要有完善的安防措施，严禁接入公安信息网、互联网或其他网络，在系统进入、资源共享、屏幕保护等方面必须采取必要的安全保密措施。

第七条

公安机关涉密计算机输出涉密信息，须经本单位主管领导审批，由专人进行操作并登记、备案，按相应密级进行管理。未经批准，不准私自下载涉密信息、拷贝涉密信息和将涉密信息制作成光盘。

第八条

公安机关涉密计算机系统的软件配置，不得进行公开交流和擅自对外公开发表。

第九条

外来人员和非本单位雇用人员不准单独接触非涉 密计算机，严禁接触涉密计算机。公安机关涉密计算机应严格控制参观，必要的参观须经主要领导批准。

第十条

公安机关涉密计算机中的涉密信息要严格备份，采取有效的防盗、防火措施，确保备份信息安全。

第十一条

非涉密计算机禁止存储、处理涉密文件及信息。

第十二条

非涉密计算机禁止使用涉密移动存储介质，涉密计算机严禁使用非涉密移动存储介质。

第十三条

涉密计算机及联入公安网络的计算机严禁安装有无线上网设备

事业单位非涉密计算机自查报告篇二

附件2：

吴忠市粮食局非涉密计算机保密管理制度

一、计算机操作人员必须遵守国家有关法律，任何人不得利用计算机从事违法活动。

二、计算机操作人员未经上级领导批准，不得对外提供内部信息和资料以及用户名、口令等内容。

三、网络设备必须安装防病毒工具，并具有漏洞扫描和入侵防护功能，以进行实时监控，定期检测。

四、计算机操作人员对计算机系统要经常检查，防止漏洞。禁止通过网络传递涉密文件，软盘、光盘等存贮介质要由相

关责任人编号建档，严格保管。除需存档和必须保留的副本外，计算机系统内产生的文档一律删除，在处理过程中产生的样品等必须立即销毁。

五、具有互联网访问权限的计算机访问互联网及其它网络时，严禁浏览、下载、传播、发布违法信息；严禁接收来历不明的电子邮件。

六、对重要数据要定期备份，定期复制副本以防止因存储工具损坏造成数据丢失。备份工具可采用光盘、硬盘、软盘等方式，并妥善保管。

员应对系统重新进行调整，重新设置用户名、密码。

八、对于违反本规定，发生泄密事件的，将视情节轻重追究责任。

九、本制度自印发之日起执行。

2011年2月25日

事业单位非涉密计算机自查报告篇三

为进一步加强涉密计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合实际，制定本制度。

第一条专人负责本计算机的管理，维护计算机正常运转，不得擅自接入网络或安装其他网络设备。

第二条秘密信息不得在与国际互联网联网(外网)的计算机中存储、处理、传递。涉密的材料必须与国际互联网（外网）物理隔离。

第六条各室发现计算机系统泄密后，应及时采取补救措施，并按规定在24小时内向县国家保密单位报告。

第七条涉密的计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

第八条不按规定管理和使用涉密计算机造成泄密事件的，将依法依规追究责任，构成犯罪的将移送司法机关处理。

第九条本制度由单位保密工作领导小组办公室负责解释。

第十条本制度从印发之日起执行。

**********2015年2月1日

事业单位非涉密计算机自查报告篇四

涉密和非涉密计算机保密管理制度

第一条为进一步加强我局计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《保守国家秘密法》相关规定，结合我局实际，特制定本制度。

第二条局保密工作领导小组及办公室负责本局计算机网络的统一建设和管理，维护网络正常运转，各股（室）所、局属事业单位、不得擅自在局系统网络上安装其他设备。

第三条涉密计算机严禁直接或间接接入电子政务外网以及国际互联网等公共信息网络。非涉密计算机严禁直接或间接接入政务内网。

第四条涉密计算机主要用于处理涉密业务和内部办公业务，不得处理绝密级国家秘密信息。非涉密计算机严禁存储、处

理、传递和转载国家秘密信息和内部工作信息。

第五条未经单位领导批准和授权，个人使用的计算机不得交由非本岗位工作人员操作。

第六条不得使用移动存储设备在涉密和非涉密计算机间复制数据。确需复制的，应当利用中间计算机进行转存处理，并采取严格的保密措施，防止泄密。

第七条国家秘密信息输出实行严格的登记、审批手续，特别是对国家秘密信息输出的范围、数量和介质要有明确的记载，确保国家秘密信息可控。

第八条不得安装、运行、使用与工作无关的软件。

第九条涉密计算机应由局保密工作领导小组办公室（以下简称“局保密办”）统一检修和保养。维修前，应进行登记，并将涉密信息和软件备份，彻底清除涉密信息或卸除所有涉密存储介质。不能彻底清除或卸除的应采取可靠的保密措施，保证所存储的国家秘密信息不被泄露。

第十条涉密计算机不再继续使用时，须经单位领导批准，并在履行清点、登记手续，进行技术处理后将硬盘及时销毁，一律不得进行捐赠或当作废品出售。

第十一条各股（室）所、事业单位单位发现计算机系统泄密后，应及时采取补救措施，并按规定及时向局保密办、县保密局报告。

第十二条涉密的计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

第十三条计算机使用人即为管理责任人。对不按规定管理和

使用涉密与非涉密计算机造成泄密事件的，将依法依规追究责任，构成犯罪的将移送司法机关处理。

事业单位非涉密计算机自查报告篇五

一、涉密和非涉密计算机保密管理制度

为进一步加强涉密计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合实际，制定本制度。

第一条办公室负责本单位计算机网络的统一建设和管理，维护网络正常运转，各室各派出纪工委不得擅自在网络上安装其他设备。

第二条国家秘密信息不得在与国际互联网联网(外网)的计算机中存储、处理、传递。涉密的材料必须与国际互联网（外网）物理隔离。各室各派出纪工委的计算机不得上国际互联网。第三条凡是上国际互联网的信息要经单位保密工作领导小组审查，做到涉密的信息不上网，上网的信息不涉密。坚持“谁上网谁负责”的原则，加强上网人员的保密教育和管理，提高上网人员的保密观念，增强防范意识，自觉执行有关规定。第四条使用电子邮件进行网上信息交流，应当遵守国家有关保密规定，不得利用电子邮件传递、转发或抄送国家秘密信息。第五条凡涉及国家秘密信息的计算机设备的维修，应保证储存的国家秘密信息不被泄露。到保密工作部门指定的维修点进行维修，并派技术人员在现场负责监督。

第六条各室发现计算机系统泄密后，应及时采取补救措施，并按规定在24小时内向县国家保密单位报告。

第七条涉密的计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

第八条不按规定管理和使用涉密计算机造成泄密事件的，将依法依规追究责任，构成犯罪的将移送司法机关处理。第九条本制度由单位保密工作领导小组办公室负责解释。第十条本制度从2009年6月1日起执行。

二、涉密移动存储介质保密管理制度

为加强我单位涉密笔记本电脑、移动存储介质管理，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合我单位实际，制定本制度。

第一条办公室负有建立健全使用复制、转送、携带、移交、保管、销毁等制度以及对各室各派出纪工委执行本制度的监督、检查职责。单位保密工作领导小组界定涉密与非涉密移动存储介质（包括硬盘、移动硬盘、软盘□u盘、光盘及各种存储卡）及笔记本电脑，并由办公室登记造册。第二条各室各派出纪工委必须指定专人负责本部门笔记本电脑和涉密移动存储介质的日常管理工作。涉密移动存储介质、笔记本电脑必须妥善保存。日常使用由使用人员保管，暂停使用的交由指定的专人保管。

第三条涉密笔记本电脑、涉密移动存储介质只能在本单位内使用，严禁在互联网外网上使用。确因工作需要携带涉密笔记本电脑、涉密移动存储介质外出，须报经单位领导批准，履行相关手续和采取严格的保密措施。严禁将涉密笔记本电脑、涉密移动存储介质借给外单位使用。

第四条非涉密笔记本电脑、移动存储介质不能与涉密相混用，严禁将私人笔记本电脑、移动存储介质带入本单位内使用。第五条涉密笔记本电脑、移动存储介质需要送外部维修时，必须到国家保密工作部门指定的具有保密资质的单位进行维修，并将废旧的存储介质收回。涉密移动存储介质在报废前，应进行信息清除处理。

第六条涉密笔记本电脑硬盘、移动存储介质的销毁，经单位主要领导批准后，到县国家保密单位指定的销毁点销毁或送交县国家保密单位统一销毁，各室各派出纪工委不得擅自销毁。禁止将涉密移动存储介质作为废品出售。

第七条不按规定管理和使用涉密笔记本电脑和涉密移动存储介质造成泄密事件的，将依法依规追究责任，构成犯罪的将移送司法机关处理。

第八条本制度由单位保密工作领导小组办公室负责解释。第九条本制度从2009年6月1日起执行。

三、计算机及网络保密管理制度

一、计算机操作人员必须遵守国家有关法律，任何人不得利用计算机从事违法活动。

二、计算机操作人员未经领导批准，不得对外提供内部信息和资料以及用户名、口令等内容。

三、网络设备必须安装防病毒工具，并具有漏洞扫描和入侵防护功能，以进行实时监控，定期检测。

四、计算机操作人员对计算机系统要经常检查，防止漏洞。禁止通过网络传递涉密文件，软盘、光盘等存贮介质要由相关责任人编号建档，严格保管。除需存档和必须保留的副本外，计算机系统内产生的文档一律删除，在处理过程中产生的样品等必须立即销毁。

五、具有互联网访问权限的计算机访问互联网及其它网络时，严禁浏览、下载、传播、发布违法信息。严禁接收来历不明的电子邮件。

六、对重要数据要定期备份，定期复制副本以防止因存储工

具损坏造成数据丢失。备份工具可采用光盘、硬盘、软盘等方式，并妥善保管。

七、计算机操作人员调离时应将有关材料、档案、软件移交给其它工作人员，调离后对需要保密的内容要严格保密。接替人员应对系统重新进行调整，重新设置用户名、密码。

八、对于违反本规定，发生泄密事件的，将视情节轻重追究责任。

九、本制度自印发之日起执行。

四、涉密计算机维修、更换、报废保密管理规定

一、涉密计算机系统进行维护检修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒体等安全保密措施。无法采取上述措施时，安全保密人员和该涉密单位计算机系统维护人员必须在维修现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。

二、各涉密室（各派出纪工委）应将本室（委）设备的故障现象、故障原因、扩充情况记录在设备的维修档案记录本上。

三、凡需外送修理的涉密设备，必须经保密工作领导小组和分管单位领导批准，并将涉密信息进行不可恢复性删除处理后方可实施。

四、办公室负责对办公计算机软件的安装和设备的维护维修工作，严禁使用者私自安装计算机软件和擅自拆卸计算机设备。

五、涉密计算机的报废由保密领导小组专人负责定点销毁。

六、本制度自印发之日起执行。

五、计算机网络信息保密管理制度

我单位为保密要害部门。涉密信息包括各室各派出纪工委在工作中产生的信访处置、案件检查、案件审理、案件申诉和重大违纪违法案件的查处。在案件调查工作中虽不属于国家秘密，但又属不宜公开的工作秘密，涉及被检查单位的密级文件资料、技术信息和经营信息等商业秘密。我单位全体人员应严格遵守国家对计算机信息系统安全保密管理的有关规定。

第一条为保证我单位计算机网络信息安全，防止计算机网络信息失密泄密事件发生，特制定本制度。

第二条各室各派出纪工委计算机内不得保存涉及国家、部门秘密事项的信息（标有密级的文件）。若必须保存则需报经有关部门和领导同意，并遵守有关保密安全规定。

第三条本单位计算机限于使用与纪检监察工作相关的软件，不得在工作时间将计算机用于非工作内容。严禁各室各派出纪工委计算机使用人员私装、私卸计算机软件。第四条使用外来数据盘，必须在检测、清除病毒后方可使用。如遇杀毒仍旧无法清除的，应及时与办公室联系，以免病毒侵扰计算机及网络系统，造成严重后果。

第五条外单位人员以及本单位人员家属，不得使用本单位计算机及附属设备。跨室（委）使用计算机设备的，需征得该室（委）负责人的同意。

第六条计算机及系统设置参数(如用户帐号、登录口令□ip地址、系统路径等)为单位内部工作秘密,任何人不得以任何借口向外泄露。

第七条严禁窃用他人口令登陆oa系统，不得在他人已登陆的情况下使用系统，若需使用必须首先退出他人帐号后，并以自己的用户名登陆，工作完毕后应立即退出，以维护信息系统的安全、保密、有序。

第八条要与互联网实行物理隔离，严禁同一机器内外网混用。第九条单位内网只限本单位人员使用，未经部门负责人同意，严禁外单位的人员使用单位内网。

第十条网络操作时不得随意运行、修改有关调整系统设置的软件。开设共享目录时，应注意设置访问控制口令（如共享文件夹），并在完成工作后立即关闭共享，以保证本地文件的安全与保密。第十一条上网信息的保密管理坚持“谁发布谁负责”的原则。不得在聊天室、电子公告系统、网络新闻上发布、谈论和传播国家秘密信息或工作秘密信息。

第十二条使用电子函件进行网上信息交流，应当遵守国家保密规定，不得利用电子函件传递、转发或抄送国家秘密信息。第十三条各室各派出纪工委及个人未经单位主要领导同意，不得私自连接集线器（hub）、调制解调器（modem）等网络设备。第十四条严禁下载或购买、安装黑客软件，要定期用杀毒软件检测机器上有无木马、病毒程序。

第十五条涉及我单位内部工作信息的计算机，不得直接或间接地与互联网或其他公共信息网络相联接。

第十六条携带电脑或移动存储介质到被检查单位工作，携带人为该电脑或移动存储介质的第一责任人，不得将我单位工作内部信息给被检查单位或其他人员查阅、转存等。

第十七条携带有工作涉密信息的电脑、存储介质外出，须经分管领导批准，并采取必要的保密措施。将单位电脑或存储介质带回家，不得用该电脑上互联网，且需采取必要的保密措施。第十八条涉密计算机系统进行维护检修时，须保证所

存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒体等安全保密措施。无法采取上述措施时，涉密室领导必须在维修现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。

第十九条凡需外送修理的涉密计算机或存储介质，必须经主管领导批准，并将涉密信息进行不可恢复性删除处理后方可实施。第二十条凡私自改变计算机网络（如内网改外网、私接线路等），一经发现取消该室（委）主任（书记）和私接人年终评优资格。第二十一条凡不遵循以上条款，造成涉密信息或我单位内部工作信息泄密的，一经发现取消其评优资格，并按有关规定严肃处理。故意或过失泄露国家、部门秘密者，由保密部门依照《中华人民共和国保守国家秘密法实施办法》的规定进行处理。本制度自印发之日起执行。

六、纸质文件管理制度

为进一步规范对各类文件的管理，根据中央和县委有关文件精神，结合本单位具体情况，特作如下规定：

一、关于文件的阅读范围

（一）中央文件（包括中央纪委监察部文件）：发至县团级的中央文件，供书记阅读。

（二）省委文件（包括省纪委监察厅文件）：

1、发至州单位以上单位的省委文件，供书记阅读。

2、发至县团级的省委文件，可供科级以上职务的党员干部阅读。文件注明传达范围的，按规定办理。

（三）市委文件（包括市纪委监察局文件）：由单位领导决定阅读范围。文件注明传达范围的，按规定办理。

（四）离、退休干部阅读文件的规定：

离、退休干部，可按原来的职级或规定享受的政治待遇阅读相应级别的中央文件和省委文件及州委文件，由原所在单位党组织根据实际情况组织阅读或传达。

（五）文件有领导批示的，按批示范围传阅。

二、关于文件的处理程序

1、签收和启封：文件的收发由专人履行签收手续，其他人员不得随意签收和启封。如果标有具体人员亲收、亲拆的公文、信函，除本人委托外，任何人不得启封，应原封不动交给亲收人或指定人员。办公室收到的各类公文及重要资料、刊物须及时交送有关领导和相关室（委），按有关程序和规定及时处理，防止耽搁、延误。

2、登记：登记文件必须将收发文时间、来文单位（发往单位）、文件字号、密级、标题、缓急程序、份数及处理时间、处理情况逐项登记清楚。

3、办理：经办人员必须根据文件的内容和阅知的范围，及时、迅速传阅、办理，不得拖延，事后必须在办文单上签字或写明办理经过及结果，需向领导反馈情况的必须及时反馈。领导批示后的文件，应按领导批示意见进行办理。凡经注办的文件，办公室要及时对承办情况进行督促检查，做好催办工作，以避免漏办和延误。

4、传阅：传阅文件应突出一个“快”，随时掌握文件的去向，避免文件漏传、误传和延误、遗失。

(1)严格登记手续。文件传阅时应做好登记手续或请传阅者做好传阅签收。

(2)文件传阅时，应设立必要的文件传阅夹和办文单，以便县别于其他材料和领导阅后签字、批示。要提醒传阅者不要随意抽取文件夹里的文件，以避免文件漏传。

(3)文件传阅应在办公室进行，不得将文件带到住所或公共场所阅处。

(4)文件传阅必须根据规定的文件阅读范围进行传阅，由专人按单位领导的排序或主次先后递送。对传阅的文件应及时收回，重要文件应当天送达，当天收回。要避免文件在传阅对象之间发生相互传递的“横传”现象，以免传阅的文件失去控制，造成文件积压、丢失和下落不明等情况。要加快文件传阅的速度，送文人员应尽可能了解有关领导人和有关部门的工作规律与时间安排，有时间阅读的要及时送阅，如领导外出，可适当调整传阅秩序，要尽量减少文件传阅时的停留时间，缩短文件传阅周期。

三、关于文件的保管

文件的保管、存放必须明确专人负责，并建立健全管理制度。

1、对传阅好的文件、办理好的文件，应及时核对清点，并分门别类保管存放。

2、文件借阅时，必须符合规定的文件阅知范围，办理借阅文件的登记手续，在规定的场所阅读。如遇特殊情况需要携带文件外出时，必须经本单位主管领导批准，并采取必要的保密措施。涉及密级的公文和内部重要资料，要注意保密。凡是有密级的文件，不得随意复印，确因工作需要必须经办公室负责人同意才可复印，其复印件按正式文件管理。

3、文件的存放场所应安全、保密，不得将文件随意放在办公桌面上或存放在玻璃橱和敞开式的橱柜中。

四、关于文件的清退、销毁

要建立定期的文件清理制度，定期做好文件的清退和销毁工作。清退和销毁文件，必须严格履行登记手续。文件销毁时需经主管领导人批准同意。个人不得擅自销毁文件。

(1)中央文件、省委文件、州委文件和县委文件的清退工作，按县委办公室下发的文件清退，认真核对应清退的文件，按时、如数将清退的文件送县委机要室并办理清退、注销手续。
(2)所有上级文件需要归档的，根据有关归档要求，要定期清理归档，并做好归档手续。

(3)对不需要归档的其他文件、资料及内部刊物，应按县委保密办的规定进行清退、销毁。

(4)文件管理人员在工作调动、离职时，应先办理文件的移交手续，清退所持的全部文件，方可办理调动、离职手续。任何个人不得私自带走文件或私自销毁文件。

五、关于文件管理职责

1、办公室是文件管理的职能部门，应加强对文件，特别是中央文件、县委文件的管理，严格执行有关规定和保密纪律，做到既充分发挥每份文件的作用，又严防失密、泄密现象的发生。

2、办公室应定期检查文件的收发、登记、传阅、保管和清退、销毁情况，加强文件管理和保密教育。

3、办公室负责文件处理、保管的人员要增强责任性和保密意识，忠于职守，严格遵守有关规章制度和保密纪律，勤恳工作，确保文件正常运转，防止遗失。本制度自印发之日起执行。

七、计算机及网络管理的规定

为保障我单位机关各室,各纪工委计算机正常运行，规范和管理、使用及维护，特制定本规定：

一、计算机管理规定

1、各室、各纪工委需在办公室办理计算机的登记手续，驱动盘、使用说明、保修卡及配置清单等原始资料由办公室负责保管，同时登记固定资产台帐。

2、将计算机管理纳入各室、各纪工委职责范围，指定日常使用人为专管人员，负责计算机的日常维护、清洁、查杀病毒、数据备份等工作。办公室负有监督检查的职责。

3、计算机发生故障时，专管人员应及时向办公室报告，需外联技术员检查、维修的，由办公室负责联系接洽。未经办公室许可任何人不得随意私请外部人员维修，不得随意增（删）系统软件或拆装硬件。

4、为保证计算机性能正常，各室、各纪工委应定期清洁计算机。办公室检查内容包括查杀病毒情况、外观清洁情况（屏幕、显示器、主机、键盘、鼠标等）。

二、计算机安全规定

1、任何人不得利用计算机进行侵害国家、单位和个人利益与合法权益的活动。

2、要设置开机密码和重要文件的读取密码。密码由专人负责保管，应视情况及时更改，并报办公室备案。

3、定期做好文件、数据的备份工作，防止文件丢失，确保数据安全。

4、根据各室、各纪工委文件、数据的性质及重要程度，按照一定周期（如每周或每月），及时备份文件和数据，对重要数据应做好随时备份、多个备份工作。备份资料需要存档的，及时交办公室存档。

5、各室、各纪工委或个人不得私自安装、使用未经许可的软件（包括游戏软件等一切与工作无关的软件）。凡需在可入网的计算机上安装任何软件，需经办公室审批同意后进行安装。

6、为防止计算机病毒传播，使用任何外来文件需首先进行病毒清查，安装有杀毒软件的计算机须定期查毒（每周一次）。

三、计算机使用规定

1、按照“谁使用、谁负责”的原则，各室、各纪工委对所属计算机的日常使用及清洁维护、查毒清毒、数据备。

2、专管人员应经常检查计算机及设备状况，如发现异常应立即报告，禁止因不规范操作等原因造成硬件损坏。

3、日常工作涉及计算机使用的人员应注意相关知识的学习与积累，不断提高自身应用水平。

4、使用中应注意随时存盘，为消除安全隐患，下班后应关闭计算机及附属设备并切断电源。

5、任何人不可利用计算机进行与工作无关的活动，不允许在计算机（或网络）上存储与工作无关的资料。

四、计算机网络管理

1、使用人应严格遵守我单位保密制度，不得随意通过网络获取或对外泄露文件、资料、数据等。

2、可以登陆互联网的计算机由专人负责管理，定期上网升级

杀毒软件。除工作需要外，禁止上网浏览、游戏或聊天。

3、电子邮箱以“保密性佳、满足需要、费用最低”为原则，做到“及时下载、定期清理”，谨慎对待不明邮件，避免病毒的传播。发出邮件需经办公室审核后，及时传送，及时清理，不留痕迹。

五、计算机保密规定

1、涉密计算机系统必须与互联网实行物理隔离，严禁用处理国家秘密信息的计算机上互联网。

2、采取切实措施，加强对计算机的使用管理，上互联网的计算机必须与处理涉密信息的计算机严格区分，做到专机专用，不得既用于上互联网又用于处理国家秘密信息。

3、涉及文件、档案、案件管理及案件查处情况的计算机不准上互联网。并且专机专用，专人管理。

4、涉密信息应标明密级和保密期限，存贮涉密信息的软盘、硬盘、光盘□u盘以及打印出来的文件等，应视为“三密”件，由专人管理。

5、涉及国家秘密信息的，不得在与国际互联网相连的计算机信息系统中存储、处理、传递。

6、计算机与其网络未经批准，不得直接或间接地与国际互连网相连接。

7、未经批准，严禁外单位人员使用相单位计算机及其网络。本规定自2009年6月1日起执行。