网络时代的信息安全心得体会 移动网络的信息安全管理论文(通用7篇)

我们得到了一些心得体会以后，应该马上记录下来，写一篇心得体会，这样能够给人努力向前的动力。通过记录心得体会，我们可以更好地认识自己，借鉴他人的经验，规划自己的未来，为社会的进步做出贡献。以下我给大家整理了一些优质的心得体会范文，希望对大家能够有所帮助。

网络时代的信息安全心得体会篇一

随着我国的移动网络的迅速发展，在广泛的应用同时，移动网络信息安全问题也比较突出。加强对移动网络信息安全的管理就显得比较重要，本文主要就移动网络信息安全管理的特征体现以及主要内容加以分析，然后结合实际对移动网络信息安全管理问题和应对策略详细探究希望能通过此次理论研究，对移动网络信息安全的进一步发展起到促进作用。

移动网络信息的安全管理涉及到的内容比较多，在移动网络对人们的工作生活带来方便的同时，一些网络信息安全问题也逐渐的突出。构建完善化的移动网络信息的安全体系，保障移动网络信息的安全性，是当前移动网络企业发展的重要目标。通过从理论层面加强移动网络信息安全的管理研究，就能有助于从理论层面提供移动网络信息安全的支持。

网络时代的信息安全心得体会篇二

近年来网络个人信息泄露事件频发，给个人和社会都造成了不良影响。计算机网路信息安全保密不到位是产生这一问题的主要原因。要想保障网络信息的安全，就必须认真分析产问题的原因，并据此采取针对性的解决措施。

1影响网络信息安全保密的主要因素

信息网络自身的脆弱性和信息安全技术发展的滞后性是产生网络信息安全问题的根本原因。现阶段，主要由以下几种因素能够对网络信息安全保密造成影响。

1）骇客攻击：

计算机网络的最大威胁来自于骇客攻击。骇客攻击有两种形式，包括非破坏性攻击和破坏性攻击。信息的完整性和有效性被某种方式选择性的破坏是破坏性攻击的特点，这种攻击的目的完全在于破坏信息。在对网络正常工作造成影响的情况下，通过破译、窃取、截获而获得重要机密信息是非破坏性攻击的特点。计算机网络在受到这两种攻击时会产生极大的危害，进而造成机密信息被泄露。

2）人为因素：

网络安全的威胁还来自于内部人员破坏网络系统、更改网络配置和记录信息、内部非授权人员有意无意偷窃机密信息、用户与别人共享网络资源或将自己的账号转借他人、用户选择口令不慎、资源访问控制设置不合理、操作员安全配置不当等人员因素。

3）计算机病毒：

具有自我复制能力，通过在计算机程序中扰乱功能或者毁坏数据影响计算机使用的计算机指令或程序代码是计算机病毒。可执行性、破坏性、隐蔽性、潜伏性、传染性是计算机病毒的重要特点，能够随着软硬件的发展而不断升级和变化。计算机病毒的变化能力、适应能力、破坏能力、传播能力因信息网络规模的日益扩大和计算机技术不断发展而不断得到强化，人们越来越难以防范计算机病毒，国家信息网络安全因此而受到严重威胁。

4）预置陷阱：

预置一些可对系统运行造成干扰、破坏的程序或者窃取系统信息的“后门”于计算机系统的软硬件中行为就是预置陷阱，硬件制造商或软件公司编程人员为了自便而设置了这些“后门”，人们通常不会发觉。在需要的时候，硬件制造商或者软件编程人员会通过“后门”进入系统而无需进行安全检查，在没有获得授权的情况下对系统进行访问或者实施对事先预置好的程序的激活操作，最终造成对系统运行的破坏。

5）电磁泄漏：

计算机技术的广泛应用促进了信息的计算机系统存储和信息的计算机网络传输的实现。同其他电子系统一样，计算机系统也会发生电磁泄漏问题。电磁辐射不同程度地存在于网络端口、传输线路、打印机、键盘、显示器、计算机主机等，原来的信息能够被这些泄露的电测信息还原。实践证明，如果计算机在没有采取防范措施的.情况下工作，其内容可以在一千米之内被普通计算机和截收装置抄收，当前已经有很成熟的技术能够窃取显示其内容。

2网络信息安全保护防范对策

高技术的网络攻击手段需要高技术的防范措施来制衡，网络信息安全才能够得到保障。根据现阶段影响计算机网络信息安全保密的内容，要使网络信息的安全保密得到保证，就应当鸡西几个方面管理使用网络。

1）严格行政管理、加强法律监督

第一，加强人员管理。人的管理和技术时计算机网络信息安全保护的核心问题。因此，要实现计算机网络信息安全的有效治理，就应当先对人的因素进行考虑。内部人员存在问题是国内外大量危害计算机网络信息安全事件的根本原因，所以有必要对相关人员进行定期培训和教育，提升他们的职业道德水平和思想品质。此外还应当对相关规章制度进行建立

健全，提升对内部人员性的监督管理水平，从根本上对非法入侵和非法访问进行预防。最后，还应提升计算机网络信息技术人员的守法意识和职业能力，使他们在工作中能够自觉规范自身的行为并且有效保证计算机网络信息安全。第二，对安全管理体制进行健全。制度是机制的载体，机制的完善有赖于规章制度的高效运作。密钥管理、访问控制管理、运行管理、鉴别管理、资源管理是网络信息安全管理机制的主要内容。进行每一项管理的过程中都应当实现制度的严格遵守。实践中应当通过对在职人员安全意识的强化，使管理责任和目标得到明确。在工作中执行职责分工原则，使得各项有关安全制度得到有效贯彻。为有效实施计算机网络信息安全管理，应当使各个层次的安全工作机制得到有效建立，进而为工作活动提供依据。第三，强化信息安全法规建设。为了和信息化发展相适应，责任部门应当从实际应用基础和安全技术标准出发，对相关计算机网络信息安全保密的法规、制度进行不断完善，为计算机网络信息安全管理提供依据。相关计算机网络信息安全保密法规、制度应当具有稳定、严密、科学、宏观的特点，对相关实体、用户、信息主体的职责和权力以及安全保密检查管理部门的职责和权力进行明确。应当设置科学制度对信息的使用、保管、形成过程进行规范，并确保其得到有效落实。对于危害计算机网络信息技术保密安全的违规违法行为，相关法规和制度应当强化行为人的责任，加大处罚力度，提高责任人的违法违规成本。技术性强是计算机信息网络安全保密的重要特点，因此需要制定和完善相关的技术法规。要保证计算机网络信息的保密、及时、准确、完整，就必须对相关法律法规进行望山，严厉追究违法者的责任。

2）加强技术防范

第一，采用访问控制策略。防止网络资源被非法访问和非法使用是访问控制的主要任务。作为保证网络安全重要的核心策略，它包括多项内容，具体有网络终端及阶段安全控制、网络监测和锁定控制策略、网络服务器安全控制策略、属性

安全控制策略、目录安全控制策略、操作权限控制策略、入网访问控制策略。它的实现技术包括网络签证、基于目的的地址过滤管理、基于资源的集中式控制等。

第二，采用身份鉴别技术。验明信息或用户的身份是鉴别的目的，该技术是在识别实体身份的基础上，对实体的访问请求进行验证或为信息达到和来自指定目的和源提供保证。信息的完整性能够通过鉴别技术得到验证，重演、非法访问、冒充也可因此而得到避免。通信以鉴别对象双方相互鉴别和消息源鉴别是为依据对鉴别技术做的分类；消息内容鉴别和用户身份鉴别是以鉴别对象为依据对鉴别技术做的分类。实践中有很多鉴别方法：通过鉴别码对消息的完整性进行验证；通过访问控制机制、密钥机制、通行字机制对用户身份进行鉴别；通过单方数字签名鉴别消息源、鉴别访问身份、鉴别消息完整性；通过收发双方数字签名同时鉴别收发双方身份和消息完整性。

第三，传输与存储加密技术。线路加密和脱线加密是传输加密技术的两种形式。从起点到终点数据始终以加密形式存在是脱线加密的特点，在该种形式下数据只有在到达终端后才会被解密，使加密系统的同步问题得到了有效避免。容易维护、容易实现、容易控制成本是脱线加密的特点。不考虑端口的信息安全，只对网络线路进行加密是线路加密的特点。密文存储和存取控制是存储机密技术的两种分类，防止信息在存储过程中泄密是它的主要目的。为防止客户非法窃取数据信息或越权使用数据信息，而对用户的资质和使用权限进行严格审查是存取控制的主要内容。而加密模块、多层加密、算法转换则是密文存储的主要内容。

第四，密钥管理技术。密钥管理是计算机网络数据信息加密的主要表现方式，骇客窃取信息的主要对象就是密钥，磁盘、磁卡、存储器是密钥的媒介，对蜜月的更换、保存是管理密钥的主要内容。非对称密钥和对称密钥是密钥技术的两种分类。数据解密和加密是一致的，在不泄露双方密钥的情况下，

数据安全就不会受到威胁是对称密钥的特点，邮件加密现阶段就是使用的这个技术□aes□des是应用最多的对称密钥。数据的解密密钥和加密密钥不通用是非对称性密钥的特点，保密密钥和公开密钥是其两种分类，在非对称性密钥中数据的稳定性和可靠性得到了有效提升。

第五，采用数字签名技术。篡改、冒充、伪造等安全问题能够通过数字签名机制提供的鉴别方法得到解决。一种数据交换协议被应用于数字签名中，它要求两个条件能够被收发数据双方满足。两个条件是：发送方所宣称的身份能够被接受方鉴别；自身发送过数据这一事实无法被发送方否认。对称加密技术很少应用于数据签名中，将整个明文被发送方加密变换得到的值作为签名。接收者解密运算发送者的签名时需借助公开密钥，若结果为明文，则签名有效，进而证明对方身份真实。

第六，采用反病毒技术。消除病毒、检测病毒、预防病毒是反病毒技术的三种分类，内存中常驻反病毒程序能够实现对系统的优先监控，进而对系统中是否存在病毒进行判断和监视，实现对计算机系统中进入病毒的有效预防，使计算机系统免遭破坏。我们应当对病毒的严重性形成充分的重视，首先保证严格审查所有软件，使用前必须经过相应的控制程序，其次加强对病毒软件的应用，及时检测系统中的应用软件和工具软件，避免各种病毒入侵到系统中。

第七，采用防火墙技术。将一组或一个系统用于两个网络之间的控制策略的强制实施就形成了防火墙。防火墙对网络安全有效管理的实现有赖于网络之间的信息交换、访问的检测和控制，防火墙的基本功能有：对非法用户和不安全的服务进行过滤，对未授权的用户访问受保护网络的行为进行控制；对特殊站点的访问进行控制，保护受保护网的一部分主机的同时，允许外部网络访问另一部分的主机；对所有通过的访问进行记录，进而提供统计数据和预警审计功能。

3结束语

通过以上论述可知，计算机网络信息安全保密是一项复杂而系统的工程，要是保障计算机网络信息的安全，相关人员必须针对影响信息安全的各项因素进行分析并采取科学有效的预防措施。实践中，相关人员应当充分认识计算机网络信息安全保密的重要性，为保障信息安全而共同努力。

网络时代的信息安全心得体会篇三

当前计算机技术与网络技术的逐渐普及与应用，网络已经成为构建现代社会文明的重要组成部分。并且，网络信息凭借其自身的高速传输以及便捷性等特点，人们对于信息的依赖程度正在逐渐增加。虽然网络信息促进了社会经济的全面发展，但其中涉及到的网络安全同样值得关注。

信息技术手段的飞速发展，使得各项网络威胁因素层出不穷，严重的影响网络信息运用与网络安全，造成不良的社会影响，威胁社会稳定健康发展。文章对网络信息安全威胁因素进行分析，并将其详细的划分为内部因素与外部因素两个层面的内容，具体如下：

1.1内部因素。

（1）系统自身脆弱性。网络技术的发展，最大的优点为开放性，这使得网络信息能够实时共享，提升了信息的普及率。但这种开放性的特点，在一定程度上也是造成影响安全性的重要项目，成为容易受到攻击的网络弱项。同时，网络技术依赖于tcp/ip协议，安全性基础薄弱，在运行与信息传递过程中容易受到攻击。

（2）用户操作不当。计算机作为人工智能系统，需要人作为主体进行操作，实现计算机的实施操作。但由于用户对安全意识重视程度不足，用户口令以及信息设置相对简单，为网

络信息埋下潜在的安全隐患。

1.2外部因素。

（1）攻击。攻击是近年来威胁网络信息安全的重要因素，对信息安全威胁程度较大。的攻击手段可以主要划分为两种类型，一是破坏性攻击，二是非破坏性攻击。其中破坏性攻击内容，主要是指通过非法手段，入侵他人电脑，调取系统中的保密文件，旨在破坏系统中存在的大量数据，以破坏为主；非破坏性手段主要是攻击模式并不是盗窃系统中存储的资料，而是扰乱系统的运行，一般通过采取拒绝服务攻击信息等手段[1]。

（2）计算机病毒。说道计算机病毒，其蔓延速度不仅迅速，并且波及范围较广，所造成的损失难以估计。计算机病毒作为一种威胁计算机网络安全的存在，具有一定的传染性与潜伏性，可隐藏在执行文件当中，一旦触发之后获取计算机系统中的大量信息。计算机病毒的传播渠道主要是通过复制文件、传送文件以及运行程序等操作传播。

（3）逻辑炸弹。逻辑炸弹引发的时候，计算机所呈现出的状况与电脑病毒入侵相似，但相对于计算机病毒而言，逻辑炸弹主要是破坏，实施系统的破坏程序。逻辑炸弹在计算机的系统当中，通常处于沉睡的状态，除非是某一个具体程序的逻辑顺序启动，才会将其激活并影响计算机运行。

（4）间谍软件。现代基于pc端的计算机各类软件逐渐增多，增强了网络信息的传播性。计算机软件的大量出现，使得间谍软件成为不法分子影响网络安全的主要手段，间谍软件并不是对系统进行破坏，而是旨在窃取系统中的用户信息，威胁用户隐私以及计算机的安全，对系统的稳定性影响较小。

基于上述计算机网络信息安全中的内外部影响因素进行分析，其中存在大量人为与非人为影响计算机安全的因素。这造成

计算机网络安全受到影响，为维护网络信息安全，对策如下：

2.1账号安全管理。用户账号在整个网络系统的运用过程中，涉及到的范围相对广泛。在现代网络信息支持下，账号内容包括系统的登陆账号、网络银行账号、电子邮件账号□qq号等多种应用账号类型。而基于账号与登录密码的获取，是当前非法攻击的主要对象[2]。对于该方面的影响，应该做到两个方面：一方面，提升账号安全管理意识，在进行账号设置的过程中，重视设置复杂的密码，并保障密码不对外泄露；另一方面，可采取特殊的符号进行密码设置，避免由于设置内容过于简单以及密码雷同的状况出现，还应该注意定期更换密码。

2.2防火墙技术。防火墙技术是一种用来加强网络之间访问控制，并防止外部网络用户运用非法手段进入到网络系统内部的’一种防护措施，为网络运行的环境提供基础保障，保护内部网络操作环境的特殊网络互联设备。防火墙技术是安全网络之间的交互性，实现对传输数据包的检查，按照一定的安全措施执行操作，确定网络数据包传输是否被允许，有效监控网络运行的状态。基于防火墙采用技术层面的差异，可将其主要划分为包过滤型、地址转换型、代理型以及检测型。不同技术形势下的防火墙技术，通过不同的表现形式，能够全面提升网络信息的安全性，将威胁性的因素进行及时排除，为系统安全运行提供良好的运行环境。

2.3软件杀毒。在防火墙为系统信息运行提供保障的同时，软件杀毒可进一步配合防火墙对不良信息的检测。在杀毒软件方面，是当前运用较为广泛的安全防护软件类型之一，此种安全技术能够有效地针对病毒进行查杀。并且现代市面上的杀毒软件，能够对木马以及一些程序进行检测。但应用杀毒软件的同时，需要重视对软件的升级，保持最新版本，实现对网络信息安全的全面保障。

2.4漏洞补丁安装。现如今，病毒与对网络的入侵手段逐渐增

多，例如攻击波病毒就是利用微软的rpc漏洞进行传播，震荡波病毒就是利用windows的lsass中存在的一个缓冲区溢出漏洞进行攻击。一旦计算机系统中涉及到的程序泄露，将造成严重的影响。为纠正与处理安全隐患，需要进行漏洞补丁的安装，解决由于漏洞程序带来的安全隐患。可充分运用现有的软件对漏洞补丁进行安装，其中包括最常用的360安全卫士、瑞星卡卡等防护软件扫描并下载漏洞补丁。

2.5入侵检测技术。入侵检测是近年来发展起来的一种防范技术，综合采用了统计技术、规范方法、网络通信技术、人工职能、推理等技术与方法，该项检测技术的内容主要是为监控计算机系统中存在的威胁因素。涉及到的具体分析方法包括签名分析法与统计分析法两种。签名分析法：该方法主要是针对系统当中的已知弱项攻击行为的检测。在具体的攻击方式与攻击行为方面分析，归纳总结出其中涉及到的签名因素，编写到ds系统的代码当中，进行模板匹配操作[3]。统计分析法：将统计学的内容作为理论基础，将系统正常的使用情况进行分析，观察其中涉及到的各项信息内容是否偏离正常运行轨迹。

2.6数字签名法。数字签名能够有效的解决网络通信当中涉及到的安全问题，是一种行之有效的检测方法，能够实现电子文档的有效辨认与验证，为数据的完整性与私密性提供保障，对信息方面具有积极作用。数据签名的算法当中包含多种内容，其中在具体应用方面较为广泛的包括□hash签名□dss签名以及rsa签名。

网络信息技术不断变化与更新，使得网络信息环境呈现出不同的发展趋势。这就意味着计算机网络信息防护手段也将不断更新，安全防护措施的应用可根据不同的攻击方式应用不同的防护手段，旨在构建健全的网络信息安全防护体系。在未来发展中，最大限度上的维护计算机网络信息安全。

文档为doc格式

网络时代的信息安全心得体会篇四

网络的管理中，信息安全管理是重要的组成部分。在一定程度上涉及到家庭以及金融和文化传承等各个方面。进一步信息安全还涉及到国家的隐私以及国家的利益等各个方面。在技术方面进行分析，信息技术涉及到计算机技术以及网络技术和密码技术等多个技术。在信息管理工作中，需要结合多元化才能对其进行有效的控制。在网络信息安全中，网络信息不仅是单纯的自我循环与合作，再加上具有很强的.社会作用。在信息制作中以及传输的过程中，都有着十分重要的意义。信息管理在一定程度上也需要社会的管理以及运行。从而对信息安全进行更加严密的处理。更好地为用户服务。信息的安全管理中，涉及到方方面面。在管理的过程中，主要使得信息中的计算机数据得到保护。

从而保护信息安全隐私不被泄露以及篡改。信息技术不被恶意篡改以及使用，就要加大对计算机系统安全的保护措施以及力度。在传输过程中要对传输文件进行保护以及加强。从而使得计算机硬件具有可靠的性能以及安全正常的运行。技术上要对计算机网络运行软件以及硬件和运行等三个方面进行处理。在相应的问题上，也要对计算机的密码技术以及信息控制等进行有效的处理。从而使得信息安全管理技术得到全面的管理。在计算机的目标要求上讲，计算机的首要目标是保证信息的准确性。在信息的生成以及信息的传输使用中要不被恶意篡改。即使被恶意进行篡改后，也能根据相关的数据和软件进行恢复。信息的准确性关键是信息发布者能够在一定程度上进行了解以及确保信息表达的准确性以及安全概念。信息安全管理中实现的目标是使得信息不易被泄露，保护信息的隐私和安全性能。在信息管理中，保证用户的重要数据不会丢失，在信息丢失后能够通过安全可靠的软件进行恢复，在信息数据传输的过程中，能够保证信息有效的进行输送，保证信息在安全的系统下进行，人为破坏时，能够

进行及时的拦截以及技术处理。

2技术管理与社会管理存在的技术分歧

信息网络安全中，并非拥有技术控制以及在技术控制前提上的综合性技术装置就能解决其问题。在解决问题的同时，还要进行进一步的社会管理。社会管理系统对计算机网络安全有着相对重要的意义。网络信息过程就是信息技术以及计算机技术综合一体实现的功能。在技术方面，同科学技术相仿，是综合性的社会功能实现以及运用的过程。在技术研发以及技术提供中，都需要一个与其相对应的社会管理体系来进行实现以及保障。在技术的实现以及技术综合来讲，信息技术具有相对的开放性和动态性以及传输和使用的海量性，在网络的开放性能以及互动性能中，对社会的管理以及稳定性的维护具有重要的意义。对信息技术进行安全管理在一定程度上能促进社会经济的发展。在信息安全管理中，很可能会出现与社会管理相冲突以及一致的方面。在一定程度上会存在求同存异的关系，也在相应的程度上产生冲突和相互的不一致。原因是由于两者的不同环境以及不同的形式所造成。技术管理与社会管理中，社会管理的要求目标更为明确。在相应程度上，社会管理相对于技术管理显得更加有力度。使得技术控制在一定程度上要依附于社会管理的相关要求。

网络信息管理技术与社会管理在基本能源上都是相同的。在信息网络管理与社会管理中，其归根结底都是为人服务的。对管理的充分认识，在一定程度上有利于其对信息安全技术管理的认识。有助于人们能有效的避免网络技术给人带来的科技异化问题。即人制造的科学在使用中会对人进行控制。在控制中在一定程度上对人产生了影响。在信息管理以及社会管理中，要有一个相对清晰的区分，并在一定程度上消除其存在的内在纠纷。使得其能够更好地为人类服务。网络信息具有一定程度的开放性，还具有相应的动态性以及互动性，在使用中容易受到现实社会的阻力。究其根本来讲，网络信息的动态性以及互动性有助于更好的实现社会管理。在网络

技术管理与社会管理中，存在着一定程度的矛盾。在相互互动的过程中，使得网络信息技术在程度上对社会管理要处于弱势。在一方面使得网络信息管理在管理的权限中会相对增大，网络信息管理在相应程度上使得社会管理的服务所引导以及限制的可能。从而会使得网络信息管理中存在着弱化以及影响。

3网络信息管理的国际合作探讨

国际网络服务为用户服务已持续将近。在20年里，在用户数量以及信息的容量上都存在着飞速的跨越发展。在相应的程度上使得网络信息技术变得越来越重要。由于网络信息技术的快速发展，网络的信息和安全管理变得尤为重要。现阶段，网络的安全管理以及发展仍旧是一个新的事物。网络信息安全是国际性的问题，因此加强信息管理十分重要。

4结语

网络信息管理是当今的重要问题。在进行互联网以及计算机的管理过程中，要致力于消除网络管理主体之间的相对分歧。增加其相互的信任，主动承担应有的责任。网络安全管理要与社会管理相适应。在一定的程度上使得其能发挥良好的效益。进行网络的安全管理工作中，要充分的研究其数据以及安全信息保护功能，从而促进信息管理的加速发展。

参考文献

[1]何悦，郑文娟。我国网络信息安全立法研究[j]□科技与法律，（1）：747。

[2]王华楠。浅谈网络信息安全面临的问题及对策[j]□中国电子商务，2011（12）：132。

[3]孙波。基于现代网络信息安全的信息管理分析[j]□信息通

信，（2）：134—135。

网络时代的信息安全心得体会篇五

随着现代教育网络的发展，校园网的发展有了一定规模，它已成为学校教学、科研和管理等教育提供资源共享、信息交流和协同工作的重要平台。与此同时，校园网的安全性也成为校园网能否正常、有效运行的关键。本文从校园网现状以及面临的主要安全问题出发，提出保障正常运行的安全措施。

网络安全是指使用各种网络管理、控制和技术措施，使得网络系统的硬件、软件及其系统中的数据不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，保证网络系统可靠、连续不间断地运行。 而网络安全包含网络硬件安全、网络软件安全、网络信息安全。

从广义来说，就是我们的信息，从源头的网络设备开始，到网络的传输过程，最后到网络的设备终端，都是涉及到网络安全保护的范围，最后保证信息的完整性、保密性和可用性。

校园网面临的安全问题主要有以下几个方面：

(1)校园中的计算机设备千差万别。比如学生宿舍的计算机、老师的计算机、学校机房的计算机，这些计算机应用的安全策略都不尽相同，没有一个统一的计算机管理制度，就会造成校园网的安全责任难以区分。

(2)开放的校园环境。极大部分的高校处于一种开放式的校园，很难保证校园内的计算机和通信设备免收破坏。机房出入管理不严，使潜在的入侵者有机会接近重要的设备。所以硬件设备的物理安全是整个校园网正常运行的基本条件，高校必须重视设备的物理安全，完善学校的安保系统。

(3)“家贼难防”。校园网中的用户是一个多元化的群体，有

老师、学生和外来人员等，要使得校园网正常稳定运行，就要确保每个用户正确使用校园网。其中学生是一个活跃的群体，他们对新知识充满好奇，一些新的网络知识，比如入侵和攻击技术，会让他们铤而走险，不考虑后果，以校园网作为对象去实施这些攻击。例如ddo□对服务器会造成很大的负载，导致校园网瘫痪。

针对校园网所面对的安全问题，如何正确保护校园网的正常稳定运行，主要体现在管理安全、物理安全、数据安全、网络安全等方面。

3.1管理安全

校园网的管理安全就是对校园内的一切人、设备和环境等资源的状态管理与控制，有以下几个项目：

(1)对校园网进行定期维护和保养，主要的设备应当集中管理，对校园网中的路由器、交换机、服务器等网络资源进行监视、测试、配置、分析、评价和控制，对设备进行实时的监控，及时处理异常情况。

(2)建立完善的机房出入登记制度，任何人出入机房都必须登记姓名和部门等相关信息，而机房管理人员应当每天下班前检查机房是否完好，水电和门锁是否已关闭等。

(3)加强校园网安全基础设备的建设，如重要的校园网设备应当按照监控录像，如遇异常情况能提供录像证明。

3.2物理安全

硬件设备的物理安全是整个校园网正常运行的基本条件，其中包括物理位置选择、物理访问控制、防盗防破坏、防火防潮、防静电、防雷击、电力供应等方面。

(1)校园网主要设备的物理位置应该远离产生粉尘、油烟，以及生产或贮存具有腐蚀性、易燃、易爆物品的场所，避开强电磁场干扰(广播电视发射塔等)，与垃圾房、厨房、餐厅保持相当距离，防止鼠害。

(2)机房应该使用专门的防静电地板，重要的设备旁边应该有灭火器等灭火工具;建立有效的制冷系统，保证设备运行在正常的温度和湿度状态下。

(3)机房必须配备up□即不间断电源，保证机房24小时不间断运行。

3.3数据安全

在信息化时代里，信息数据是最宝贵的资源，很多违法者想方设法都要窃取这些重要的数据。对于高校校园网而言，最可能的数据安全包括：重要的科研数据被破坏或泄密;财务系统数据被破坏或泄密;教务系统被破坏，教师或学生的个人资料被破坏或泄密。为了保护这些重要的数据，可以从以下几方面着手：

(1)利用数据加密技术(如3des算法)对校园网中敏感数据进行加密，防止数据在通信过程当中被窃取。

(2)重要数据应当做好异地备份，防止数据被破坏。当出现数据丢失或损坏的时候能够迅速还原。

(3)利用身份认证和权限控制，把校园网内的用户分权限，不同用户依据自身获得的相关权限进行相关数据或信息的处理，从而实现数据和相关信息资源的安全。

3.4网络安全

网络安全主要是利用路由器、交换机、防火墙和入侵防御系

统等设备防止数据在通信过程当中遭到破坏。具体方案有如下几点：

(1)构建校园网入网设备的病毒防御体系。在校园网的出口处设置网关防病毒系统。对通过ftp下载文件、通过pop3接收下载外部邮件时可能携带的恶性的程序和病毒进行查杀扫描。在网络中心机房建立防病毒监测与控制中心，能够及时有效地发现、抵御病毒的攻击和彻底清除病毒。

(2)建立7*24小时监控的网络信息入侵检测体系。入侵检测系统(ids)是新一代动态安全防范技术，通过对计算机网络或主机中的若干关键信息的收集和分析，从中发现是否有违反安全策略的行为和被攻击的迹象。

(3)建立高效可靠的内网安全管理体系。对于移动设备(笔记本等)和新增设备未经过安全过滤和检查，监测内网计算机的一些违规接入网络的行为。对于一些端口(无线接入设备或固定端口)可以使用ip地址与mac地址进行绑定。

保证信息的安全是校园网能够得到广泛应用的重要前提条件，一个方面的安全解决方案很难充分保证校园网安全，因此建立一套多方位的安全管理方案是十分必要的。虽然信息没有百分之百的安全，但这样的全面保护方案也仍然是必要的，而且必须与时俱进，随时更新各种网络技术。本文提出的信息安全应用，能够有效保证校园网的信息安全。

网络时代的信息安全心得体会篇六

摘要：在如今这个信息高速发展的时代，信息安全问题变得越来越重要。在进行网络的管理中，一定的程度上，相关的技术点以及出发站存在着诸多争议。网络信息管理中，基于网络安全的管理，一定程度上有着重要的作用。信息管理中，技术选择以及社会选择也成为相对的一种动态秩序。就互联网的技术以及社会现状来讲，也要进行相应程度的国际合作。

关键词：现代网络；安全；信息管理

在当今，随着信息技术的快速发展，信息安全问题已成为不可忽视的内容。网络信息管理已成为一个凸显问题。在发展中，信息技术设计到多个行业。使得网络信息管理变得越来越不容易进行处理。从网络信息以及个人隐私保护的环节上，更需要对其加大力度。信息安全的处理还要与国际接轨，在一定程度上对信息的安全以及隐私做到相应程度的保护。

网络时代的信息安全心得体会篇七

对信息系统进行模糊评价的步骤是先建立评价因素集t/评价集、再用从u到f(f)的模糊映射7导出模糊矩阵再给出各因素的权重，并选择相应的函数进行综合，最后进行评判。数学模型为:召=4rs=b广，其中b为评价矩阵，4为权重集合，为从f/到f的一个模糊关系□s为系统得分，严为系统风险得分m□

下面以以某单位局域网信息系统为评估对象，运用模糊评价理论和ahp方法对其进行风险评估。

2.1风险评估准备

主要是确定风fe评估的目标和范围。目标是识别单位局域网信息系统及管理上的不足，以及可能造成的风险大小;范围是单位局域网信息系统及系统内存储的内部信息。

2.2资产识别

2.2.1资产分类机密性、完整性和可用性是评价资产的三个安全属性。这里的局域网信息系统的资产表现形式主要是单位内部文件、科研成果、人员档案等数据资料，系统安装的应用软件、源程序等软件和网络设备、计算机设备、存储设备等硬件。

2.2.2资产赋值这里仅给出机密性的赋值。不同等级对应资产在机密性上达成的程度或者机密性缺失时对整个单位的影响。

2.2.3资产重要度区分资产价值可依据资产在机密上、完整性和可用性上的赋值等级得出。这里以资产机密性的赋值结果作为资产的最终赋值结果。为与上述机密生赋值相对应，将资产划分为五级，级别越高表示资产越重要。

2.3威胁识别

这里采用德尔菲集体讨论法进行威胁识别，确定评估对象面临的主要威胁，生成威胁集r:kk=i2...□m□其中为第；种威胁，〃为评估对象面临的威胁种类数。单位内部网络信息系统有别于一般网络信息系统的是，其在运行时一般要求与外网相隔离，因此，其面临的安全威胁，特别是网络攻击和泄密主要来自内部人员。

2.4脆弱性识别

脆弱性识别是风险评估中最重要的一个环节。这里采用问卷调查的方法，从技术和管理两个方面进行识别。

2.5建立风险评估指标体系

建立潜在风睑指标体系时要尽量包括其所面临的各方面的风验，根据以上分析的单位局域网信息系统所面临的威胁，并结合系统的脆弱性识别结果，建立了该系统所面临的潜在风险的指标体系。

2.6建立关于风险严重程度的评价集

根据风s可能造成的影响的程度，建立评价集v=jvi□v2□v3v4mi□ninivi=丨灾难性的，严重的，轻微的，可忽略的！

2.7评价结果及建议

由系统风险得分对照表8风险级别对应的风险值，可以看出该评估对象的风险等级为“严重的”，说明该单位局域网存在较大风险。结合最大隶属度原则和评价权重可以看出该系统的信息安全风险隐患主要来自于制度落实不到位和有意泄密2个方面。一方面说明该系统安全管理制度制定较健全，但在管理制度的落实上存在问题，执行过程中未严格落实，因而存在发生安全风险的可能。另外，系统设计时防范措施不严密，存在内部人员利用系统安全漏洞进行攻击的风险。所以，该单位信息系统需加强信息安全管理制度的落实监督，及时检测系统漏洞，并制定方案修补漏洞，从而提高其安全性。

文中以信息安全问题为研究对象，用模糊评价模型对某单位的局域网信息系统进行风险评估，通过风险识别和威胁识别，将其面临的风险威胁进行分类，建立评估指标，对系统进行风险评估，确定了系统的风险得分，并指出了风险隐患和建议，可为该单位局域网信息系统的安全建设提供参考。可以看出，该方法可以计算各种威胁的相对风险程度和整个局域网信息系统的安全风险等级，为控制风险、减少风险和转移风险提供帮助，实例应用也证明了该方法的科学性和有效性，适用于信息安全风险评估。