网络安全保密知识与法律法规宣传

第一部份：网络安全保密常识

1、认清计算机网络安全面临的问题与挑战，提高网络安全保密防范意识

在信息化社会中，网络信息系统在政治、军事、金融、商业、交通、电信、文教等方面发挥着越来越大的作用。社会对网络信息系统的依赖也日益增强。

网络信息安全与保密是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。网络信息系统的安全和保密是保密工作的一个新领域。 当前，各种各样完备的网络信息系统，使得秘密信息和财富高度集中于计算机中。另一方面，这些网络信息系统都依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

随着网络的开放性、共享性、互联程度的扩大，特别是因特网的出现，网络的重要性和对社会的影响也越来越大。网络上各种新业务的兴起，以及各种专用网的建设，使得网络与信息系统的安全与保密问题显得越来越重要。特别是随着全球信息基础设施和各国信息基础设施的逐渐形成，国与国之间变得"近在咫尺"。网络化、信息化已成为现代社会的一个重要特征。网络信息本身就是时间、就是财富、就是生命、就是生产力。

事物总是辩证统一的。科技进步在造福人类的同时，也带来了新的危害。网络信息系统中的各种犯罪活动已经严重危害着社会的发展和国家的安全。据统计，商业信息被窃取的事件以每月 260%的速率在增加。目前在已发生的泄密案件中，计算机网络泄密是重要途径。现在，几乎每天都有各种各样的黑客故事：

1994 年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国城市银行发动了一连串攻击，通过电子转帐方式，从城市银行在纽约的计算机主机里窃取 1100 万美元。

1996 年 8 月 17 日，黑客入侵美国司法部的网络服务器，并将"美国司法部"的主页改为"美国不公正部"，将司法部部长的照片换成了阿道夫·希特勒，将司法部徽章换成了纳粹党徽，并加上一幅色情女郎的图片作为所谓司法部部长的助手。

1996 年 9 月 18 日，黑客又光顾美国中央情报局的网络服务器，将其主页由"中央情报局"改为'"中央愚蠢局"。1996 年 12 月 29 日，黑客侵入美国空军的全球网并将其主页肆意改动，迫使美国国防部一度关闭了其他 80 多个军方网址，美国空军的全球网页完全变了样，其中空军介绍、新闻发布等内容被替换成一段简短的黄色录像，且声称美国政府所说的一切都是谎言。1988 年 11 月，美国康乃尔大学的学生 Morris 编制的名为"蠕虫"的计算机病毒通过因特网传播，致使网络中约 7000 台计算机被传染，造成经济损失约 1 亿美元。

在我国计算机黑客事件也时有发生，1998 年 4 月 25 日下午 5 时 30 分左右，一神秘的电脑黑客非法侵入中国公众多媒体信息网（CHINANET）贵州站点的 WWW 主机，将"贵州省情"的 WEB 页面改换成一幅不堪人目的淫秽画面。1998 年 6 月 16 日，黑客入侵了上海某信息网的 8 台服务器，破译了网络大部分工作人员的口令和 500 多个合法用户的帐号和密码，其中包括两台服务器上超级用户的帐号和密码。1998 年 8 月 22 日，江西省中国公用多媒体信息网（169 台）被电脑黑客攻击，整个系统瘫痪。1998 年 10 月 27 日，刚刚开通的，由中国人权研究会与中国国际互联网新闻中心联合创办的"中国人权研究会"网页，被黑客严重篡改。

进入 2000 年，国内外网站被"黑客"入侵的事件仍频频发生。

事实上，我们听到的关于通过网络的入侵只是实际所发生的事例中非常微小的一部分。相当多的网络入侵或攻击并没有被发现。即使被发现了，由于这样或那样的原因，人们并不愿意公开它，以免公众作出强烈的惊慌失措的反应。绝大多数涉及数据安全的事件从来就没有被公开报道过。据专家估计，每公开报道一次网络入侵，就有近 500 例是不被公众所知晓的。

上述的数字和实例说明，计算机网络具有难以克服的自身脆弱性，因而其信息保密和网络安全总会受到威胁。目前，国内使用较多的 Ethernet 网络和最受欢迎的 Novell 网络，在通信网络上基本上以明文形式传输数据，非授权用户在通信网链路上搭线攻击、篡改、收集信息比较容易。虽然 Mail 电子邮件采用了简单的字母映射加密，攻击者仍很容易进入网络获得这一字母对照表。在 Novell Netware 的网络服务器上提供了四级安全保密措施：登记 / 口令保密、代理员保密、目录最大权限保密和文件属性 / 目录属性保密。open 提供了两种级别的网络保密：共享级和使用级。上述几种常用网络所采取的安全措施主要是为了防止非授权用户进入网络和越级操作、修改信息资源，但对一个熟悉网络软件和操作使用的攻击者来说，

上述措施是非常脆弱的。因此，认清计算机网络的脆弱性和潜在威胁，采用相应的安全措施，保护计算机网络中传输数据的完整性、秘密性和可用性就变得越来越重要。

随着计算机技术的飞速发展，计算机系统和计算机网络已经成为信息化社会发展的重要通信保证。在网络中存贮、传输和处理的信息有许多是重要的政府宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、科研数据等重要信息。有的是敏感性信息，有的甚至是国家机密。所以难免会受到各种主动或被动的人为攻击，例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等。同时，通信实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。所以要建立一个安全可靠的网络系统、就必须设计一套完善的安全策略，采用不同的防范措施，并制定相应的安全管理规章制度等。

近年来，计算机犯罪案件也急剧上升，计算机犯罪已经成为普遍的国际性问题。据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一， 每笔犯罪的平均金额为 45000 美元，每年计算机犯罪造成的经济损失高达数十亿美元。任何一个计算机犯罪案件的发生都具有瞬时性、动态性、随机性的特点， 通常一个计算机犯罪案件可在 0．1 秒内发生且往往很难获取犯罪者留下的证据，这大大刺激了计算机高技术犯罪案件的发生。

现有的计算机网络大多数在建设之初都忽略了安全问题，即使考虑了安全，也只是把安全机制建立在物理安全机制上，因此，随着网络的互联程度的扩大，这种安全机制对于网络环境来讲形同虚设。另外，目前网络上使用的协议，比如 TCP / IP 协议，在制订之初也没有把安全考虑在内，所以没有安全可言。开放性和资源共享是计算机网络安全问题的主要根源，它的安全性主要依赖于加密、网络用户身份鉴别、存取控制策略等技术手段。

面对如此严重危害网络信息系统的种种威胁，必须采取有力的措施来保证网络信息的安全与保密，网络的安全措施一般分为三类：逻辑上的、物理上的和政策上的。面对越来越严重危害计算机网络安全的种种威胁，仅仅利用物理上和政策（法律）上的手段来有效地防范计算机犯罪显得十分有限和困难，因此也应采用逻辑上的措施，即研究开发有效的网络安全技术、即使是有了非常完备的安全与保密政策法规，有非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但是如果这些知识得不到普及，那么所有努力都是白费。

随着计算机犯罪案率的迅速增加，各国的计算机系统面临着很大的威胁，并成为严重的社会问题之一，人们已经开始清醒地认识到计算机系统的脆弱性和不安全性。

总之，随着计算机网络技术的发展，计算机网络的安全保密问题已成为日益严重的现实问题。普及网络信息的安全与保密知识，提高人们的法律意识是十分必要的。

2、涉密计算机上互联网为何屡禁不止

涉密计算机上互联网的现象屡禁不止的主要原因有以下几种：

第一，一些单位或部门的保密观念不强，对上互联网造成泄密隐患缺乏足够的认识。一些机关工作人员，甚至有的领导干部，由于保密意识淡薄，缺乏对计算机信息安全保密和互联网脆弱性方面的常识，只注重浏览和下载互联网上的信息，对保存涉密信息的计算机上互联网会造成泄密的危害性认识不足。

第二，保密管理不到位。有的单位没有人对处理涉密信息的计算机进行相应的管理，也缺乏计算机处理涉密信息在保密管理方面相应规定，以至于出现工作人员随意将内部办公用的计算机通过拔号或专线方式与互联网连接，有的工作人员将保存有涉密信息的笔记本电脑带回家供子女上互联网，另外，还有的人将本单位的日常办公网，在没有任何技术防范措施的情况下接入互联网，造成涉密信息通过互联网向外泄密，严重威胁着国家秘密的安全。

第三，定密工作不规范。定密标密随意性大。一些不属于国家秘密的内容被定为了国家秘密，相反真正属于国家秘密的信息却被漏定了密级，致使该定密的没有定密，当作普通内容上了互联网。

第四，缺少对技术管理部门的技术指导和技术检查。当前基层保密机构人员缺乏，不少是兼职保密干部，事务多，工作忙，没有时间和精力做保密工作，对保密工作缺乏系统的规划和管理，难以适应计算机及信息技术发展的要求，不能及时将国家有关信息保密规定传达到计算机管理部门和计算机使用人员。有些地区保密工作部门由于人员少，保密技术检查的技术性又很强，难以安排时间对本地区的计算机使用人员进行保密宣传教育和对涉密计算机进行保密检查。

第五，网络隔离措施如同虚设，违规情况时有发生。一些单位的涉密计算机虽然安装了隔离卡，但有些工作人员不遵守保密规定，不在内网上处理涉密信息，而是图方便直接在外网处理和存储涉密信息。还有的将移动涉密硬盘直接接入外网上的 USB 接口，在外网上直接处理涉密信息。

第六，对笔记本电脑的使用缺乏有效的监督管理。多数笔记本电脑存在一机两用的情况，一方面在笔记本电脑硬盘上保存有涉密信息，另一方面又有上互联网。

第七，违反保密规定使用涉密载体。有的工作人员通过软盘、可移动硬盘、优盘在涉密网和互联网之间交替使用，把保存有涉密信息的存储介质接入互联网，存在严重的泄密隐患。

第八，纵向网络的安全保密要求存在上下不统一的情况。有一些部委的涉密网络，从部委到省的连接要求很严，而省到地市的连接则有很明显的放松，有的地市将上连的网络间接与互联网连接，虽然采取了防火墙措施，但没有实现物理隔离，这对整个涉密网络的安全保密带来严重的威胁。

来 源：《保密工作》

3、计算机泄密的主要途径

做好计算机信息处系统的保密工作是我们面临的新课题，突出表现是计算机系统容易泄密和被窃密。

1、计算机电磁波辐射泄漏

一类传导发射，通过电源线和信号线辐射。

另一类是由于设备中的计算机处理机、显示器有较强的电磁辐射。

计算是靠高频脉冲电路工作的，由于电磁场的变化，必然要向外辐射电磁波。这些电磁波会把计算机中的信息带出去，犯罪分子只要具有相应的接收设备，就可以将电磁波接收，从中窃得秘密信息。据国外试验，在 1000 米以外能接收和还原计算机显示终端的信息，而且看得很清晰。微机工作时，在开阔地带距其 100 米外，用监听设备就能收到辐射信号。

这类电磁辐射大致又分为两类：

第一类是从计算机的运算控制和外部设备等部分辐射，频率一般在 10 兆赫到 1000 兆赫范围内，这种电磁波可以用相应频段的接收机接收，但其所截信息解读起来比较复杂。

第二类是由计算机终端显示器的阴极射线管辐射出的视频电磁波，其频率一般在 6．5 兆赫以下。对这种电磁波，在有效距离内，可用普通电视机或相同型号的计算机直接接收。接收或解读计算机辐射的电磁波，现在已成为国外情报部门的一项常用窃密技术，并已达到很高水平。

2．计算机网络化造成的泄密

由于计算机网络结构中的数据是共享的，主机与用户之间、用户与用户之间通过线路联络，就存在许多泄密漏洞。

（1）计算机联网后，传输线路大多由载波线路和微波线路组成，这就使计算机泄密的渠道和范围大大增加。网络越大，线路通道分支就越多，输送信息的区域 也越广，截取所送信号的条件就越便利，窃密者只要在网络中任意一条分支信道上或某一个节点、终端进行截取。就可以获得整个网络输送的信息。

（2）黑客通过利用网络安全中存在的问题进行网络攻击，进入联网的信息系统进行窃密。

（3）INTERNET 造成的泄密。在 INTERNET 上发布信息把关不严；INTERNET 用户在 BBS、网络新闻组上网谈论国家秘密事项等；使用 INTERNET 传送国家秘密信息造成国家秘密被窃取；内部网络连接 INTERNET 遭受窃密者从 INTERNET 攻击进行窃密；处理涉密信息的计算机系统没有与 INTERNET 进行物理隔离，使系统受到国内外黑客的攻击；间谍组织通过 INTERNET 搜集、分析、统计国家秘密信息。

（4）在 INTERNET 上，利用特洛尹木马技术，对网络进行控制。

（5）网络管理者安全保密意识不强，造成网络管理的漏洞。

3、计算机媒体泄密

越来越多的秘密数据和档案资料被存储在计算机里，大量的秘密文件和资料变为磁性介质和光学介质，存贮在无保护的介质里，媒体的泄密隐患相当大。

（1）用过程的疏忽和不懂技术。存储在媒体中的秘密信息在联网交换被泄露或被窃取，存储在媒体中的秘密信息在进行人工交换时泄密。

（2）大量使用磁盘、磁带、光盘等外存储器很容易被复制。

（3）处理废旧磁盘时，由于磁盘经消磁十余次后，仍有办法恢复原来记录的信息，存有秘密信息的磁盘很可能被利用磁盘剩磁提取原记录的信息。这很容易发生在对磁盘的报废时，或存贮过秘密信息的磁盘，用户认为已经清除了信息，而给其它人使用。

（4）计算机出故障时，存有秘密信息的硬盘不经处理或无人监督就带出修理，或修理时没有懂技术的人员在场监督，而造成泄密。

（5）媒体管理不规范。秘密信息和非秘密信息放在同一媒体上，明密不分，磁盘不标密级，不按有关规定管理秘密信息的媒体，容易造成泄密。

（6）媒体失窃。存有秘密信息的磁盘等媒体被盗，就会造成大量的国家秘密外泄其危害程度将是难以估量的。各种存贮设备存贮量大，丢失后造成后果非常严重。

（7）设备在更新换代时没有进行技术处理。

4．内部工作人员泄密

（1）无知泄密。如由于不知道计算机的电磁波辐射会泄露秘密信息，计算机工作时未采取任何措施，因而给他人提供窃密的机会。又如由于不知道计算机软盘上剩磁可以提取还原，将曾经存储过秘密信息的软盘交流出去或废旧不作技术处理而丢掉，因而造成泄密。不知道上 INTERNET 网时，会造成存在本地机上的数据和文件会被黑客窃走。网络管理者没有保密安全知识。

（2）违反规章制度泄密。如将一台发生故障的计算机送修前既不做消磁处理，又不安排专人监修，造成秘密数据被窃。又如由于计算机媒体存储的内容因而思想麻痹，疏于管理，造成媒体的丢失。违反规定把用于处理秘密信息的计算机，同时作为上 INTERNET 的机器。使用 INTERNET 传递国家秘密信息等。

（3）故意泄密。外国情报机关常常采用金钱收买、色情引诱和策反别国的计算机工作人员。窃取信息系统的秘密。如程序员和系统管理员被策反，就可以得知计算机系统软件保密措施，获得使用计算机的口令或密钥，从而打入计算机网络，窃取信息系统、数据库内的重要秘密；操作员被收买，就可以把计算机保密系统的文件、资料向外提供。维修人员被威胁引诱，就可对用进入计算机或接近计算机终端的机会，更改程序，装置窃听器等。

4、注意涉密磁盘的剩余磁效应

计算机磁盘属于磁介质，所有磁介质都存在剩磁效应的问题，保存在磁介质中的信息会使磁介质不同程序地永久磁化，所以磁介质上记载的信息在一定程度上是抹除不净的，使用高灵敏度的磁头和放大器可以将已抹除信息的磁盘上的原有信息提取出来。据一些资料介绍，即使磁盘已经改写了 12 次，第一次写入的信息仍有可能被恢复出来。这使涉密和重要磁介质的管理、废弃磁介质的处理，都成为很重要的问题。国外甚至有一些这样的规定：记录绝密级资料磁盘只准用一次，不用时就必须销毁，不准抹后重录。

磁盘是用于拷贝和存储文件的，它常被重新使用，有时要删除其中某些文件，有时又要拷贝一些文件进去。在许多计算机操作系统中，用 DEL 命令删除一个文件，仅仅是删除该文件的文件指针，也就是删除了该文件的标记，释放了该文件的存储空间，而并没有真正将该文件删除或覆盖。在该文件的存储空间未被其他文件覆盖之前，该文件仍然原封不动地保留在磁盘上。计算机删除磁盘文件的这种方式，可提高文件处理的速度和效率，也可方便误删除文件的恢复，但却给窃密者留下了可乘之机。他只要查阅一下磁盘上最近删除的文件目录，就可以轻而易举地找到和恢复对他有价值的信息。

因此如果将曾经记载过秘密信息的磁盘留做它用，必须将原记载的信息彻底清除，具体清除办法和技术有很多种，但实质上可分为直流消磁法和交流消磁法两种。

直流消磁法是使用直流磁头将磁盘上原先记录信息的剩余磁通，全部以一种形式的恒定值所代替。通常，我们操作计算机用完全格式化方式格式化磁盘就是这种方法。

交流消磁法是使用交流磁头将磁盘上原先记录信息的剩余磁通变得极小这种方法的消磁效果比直流消磁法要好得多，消磁后磁盘上残留信息强度可比消磁前下降 90 分贝。实用中一般是使用大电流的交流强力消磁器进行的，对一些曾记载过较高密级的磁盘，使用这种消磁技术进行处理后，才能从保密环境中释放做其他使用。

对一些经消磁后仍达不到保密要求的磁盘，或已经损坏需废弃的涉密磁盘，以及曾经记载过绝密级信息的磁盘，必须作销毁处理。磁盘销毁的方法是，将磁盘碾碎后放入焚化炉熔为灰烬和铝液。

第二部分：网络安全保密法律法规

计算机信息系统保密管理暂行规定

（1998 年 2 月 26 日国家保密局发布）

第一章 总 则

第一条 为保护计算机信息系统处理的国家秘密安全，根据《中华人民共和国保守国家秘密法》制定本规定。

第二条 本规定适用于采集、存储、处理、传递、输出国家秘密信息的计算机信息系统。

第三条 国家保密局主管全国计算机信息系统的保密工作。

各级保密部门和中央、国家机关保密工作机构主管本地区、本部门的计算机信息系统的保密工作。

第二章 涉密系统

第四条 规划和建设计算机信息系统，应当同步规划落实相应的保密设施。

第五条 计算机信息系统的研制、安装和使用，必须符合保密要求。

第六条 计算机信息系统应当采取有效的保密措施，配置合格的保密专用设备，防泄密、防窃密。所采取的保密措施应与所处理信息的密级要求相一致。

第七条 计算机信息系统联网应当采取系统访问控制、数据保护和系统安全保密监控管理等技术措施。

第八条 计算机信息系统的访问应当按照权限控制、不得进行越权操作。未采取技术安全保密措施的数据库不得联网。

第三章 涉密信息

第九条 涉密信息和数据必须按照保密规定进行采集、存储、处理、传递、使用和销毁。

第十条 计算机信息系统存储、处理、传递、输出的涉密信息要有相应的密级标识，密级标识不能与正文分离。

第十一条 国家秘密信息不得在与国际网络联网的计算机信息系统中存储、处理、传递。

第四章 涉密媒体

第十二条 存储国家秘密的计算机媒体，应按所存储信息的最高密级标明密级，并按相应密级的文件进行管理。

存储在计算机信息系统内的国家秘密信息应当采取保护措施。

第十三条 存储过国家秘密信息的计算机媒体不能降低密级使用。不再使用的媒体应及时销毁。

第十四条 存储过国家秘密信息的计算机媒体的维修应保证所存储的国家秘密信息不被泄露。

第十五条 计算机信息系统打印输出的涉密文件，应当按相应密级的文件进行管理。

第五章 涉密场所

第十六条 涉密信息处理场所应当按照国家的有关规定，与境外机构驻地、人员保持相应的安全距离??

第十七条 涉密信息处理场所应当根据涉密程度和有关规定设立控制区，未经管理机关批准无关人员不得进入。

第十八条 涉密信息处理场所应当定期或者根据需要进行保密技术检查。

第十九条 计算机信息系统应采取相应的防电磁信息泄漏的保密措施。

第二十条 计算机信息系统的其它物理安全要求应符合国家有关保密标准。

第六章 系统管理

第二十一条 计算机信息系统的保密应实行领导负责制，由使用计算机信息系统的单位的主管领导负责本单位的计算机信息系统的保密工作，并指定有关机构和人员具体承办。

各单位的保密工作机构协助本单位的领导对计算机信息系统的保密工作进行指导、协调、监督和检查。

第二十二条 计算机信息系统的使用单位应根据系统所处理的信息涉密等级和重要性制订相应的管理制度。

第二十三条 各级保密部门应依照有关法规和标准对本地区的计算机信息系统进行保密技术检查。

第二十四条 计算机信息系统的系统安全保密管理人员应经过严格审查，定期进行考核，并保持相对稳定。

第二十五条 各单位保密工作机构应对计算机信息系统的工作人员进行上岗前的保密培训，并定期进行保密教育和检查。

第二十六条 任何单位和个人发现计算机信息系统泄密后，应及时采取补救措施，并按有关规定及时向上级报告。

第七章 奖 惩

第二十七条 对在计算机信息系统保密工作中做出显著成绩的单位和人员应给予奖励。

第二十八条 违反本规定，由保密部门和保密机构责令其停止使用，限期整改，经保密部门、机构审查、验收合格后，方可使用。

第二十九条 违反本规定泄露国家秘密，依据《中华人民共和国保守国家秘密法》及其实施办法进行处理，并追究单位领导的责任。

第八章 附 则

第三十条 军队的计算机信息系统保密工作按军队的有关规定执行。

第三十一条 本规定自发布之日起施行。