机关单位网络安全使用管理办法

（经典版）

编制人：_____

审核人：_____

审批人：_____

编制单位：_____

编制时间：____年____月____日

序言

下载提示：该文档是本店铺精心编制而成的，希望大家下载后，能够帮助大家解决实际问题。文档下载后可定制修改，请根据实际需要进行调整和使用，谢谢！

并且，本店铺为大家提供各种类型的经典范文，如管理制度、管理办法、管理规定、规程规范、条例细则、程序标准、岗位职责、管理守则、试题大全、其他范文等等，想了解不同范文格式和写法，敬请关注！

Download tips: This document is carefully compiled by this editor. I hope that after you download it, it can help you solve practical problems. The document can be customized and modified after downloading, please adjust and use it according to actual needs, thank you!

Moreover, our store provides various types of classic sample texts for everyone, such as management systems, management methods, management regulations, rules and regulations, detailed rules and regulations, procedural standards, job responsibilities, management rules, complete test questions, and other sample texts. If you want to learn about different sample formats and writing methods, please pay attention!

机关单位网络安全使用管理办法

日常工作中经常需要参考借鉴网络安全，管理办法，机关，单位相关内容？不知道网络安全，管理办法，机关，单位相关文章写作格式写法？阅读以下为您编辑的机关单位网络安全使用管理办法文章，希望对您能有所帮助。

篇 1:机关单位网络安全使用管理办法

XX机关单位网络安全使用管理办法

第一章

总则

第一条

为加强我单位网络安全使用的管理，实现管理的科学化、规范化和制度化，依据国家对网络系统管理的相关规定，特制定本办法。

第二条

本办法适用于接入本大厦网络的相关单位。

第三条

内网是指使用私网 IP 住址为 XX.XX.XX.XX的整个 B 类住址范围内的机器设备。外网是指使用公网 IP 住址为 XX.XX.XX.XX的整个 C 类住址范围内的机器设备。

第二章

管理机构及其职责

第四条

安全工作委·员会是网络安全使用的管理机构。安全工作委·员会办公室（以下简称办公室）下属单位办公室和接入本大厦网络的相关单位办公室协同负责网络安全使用管理。

第五条

办公室负责网络 IP 住址和无线路由器使用的登记备案管理工作，召集下属单位办公室主任会，及时传达国家互联网管理要求。

第六条

保卫处负责主干网络设备的运营与维护，负责各单位网管员登记备案和技术培训，并依据办公室下发的 IP 住址登记备案表对 IP 住址进行分配管理和上网行为监控。

第七条

各单位办公室要指定网管员负责本单位的 IP 住址分配、登记及本单位网络设备的维护管理，并负责相应的安全管理工作。

第八条

下属单位办公室作为责任部门向办公室负责；办公室向安全工作委·员会及上级管理部门负责。

第三章

内网 IP 住址的管理

第九条

各单位要严格管理现在使用的互联网内网 IP 住址，要做到内网 IP 住址与 MAC 住址及人员一一对应；互联网内网 IP 住址应由各单位指定网管员负责分配，统一管理，并进行备案。备案表要上报办公室

备案管理人。发生内网 IP 住址的增减应及时更改备案表，并及时通知办公室备案管理人进行备案表的更改，内网 IP 住址备案后方可使用。（见附表（1）

第十条

办公室分配给各单位的 VLAN

住址使用及管理权在单位办公室；各单位要加强管理，杜绝违反国家互联网管理条例的事件发生。

第十一条

各单位使用无线网络设备必须向办公室申请，经办公室批准及备案后方可使用；无线网络设备每月要定期更改密码，对使用无线网络人员要有备案；禁止员工私自架设无线网络设备。（见附表（2）

第四章

外网 IP 住址的管理

第十二条

各单位如需设立网站、邮件服务器等公网服务器，必须将服务器统一安置到主机房，并按照保卫处网管人员安排放置入指定机柜中，各单位应当保持服务器清洁、干净，对放置于机柜的服务器必须做好公司标识。

第十三条

各单位使用公网 IP 住址必须向办提出申请，经办同意后，由保卫处网管人员统一分配。IP 住址一经分配后，单位要指定网管员负责管理，及时填好备案表，并上报办公室备案管理人。IP 住址不用

时应当及时上报撤销。

第五章

上网行为管理

第十四条

各单位必须严格按照国家互联网相关规定规范员工的上网行为，对违反国家互联网规定的行为必须严格禁止，一经发现将按国家互联网相关规定及相关规定进行处罚。违反法律规定，构成犯罪的，将依法追究刑事责任。

第十五条

上班时间禁止玩网络游戏，禁止使用多线程下载工具，禁止在网络上做有关部门明令禁止的网络行为。管理系统将对所有网络用户进行实时监控，并保留用户的上网行为日志，以备日后查询。

第十六条

科研测试系统如需接入大厦网络，须经保卫处审查同意后，报办公室审批。

第十七条

所有网络用户不得制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬X和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色·情、赌·博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的。

第六章

主机房管理

第十八条

各单位网管员要严格管理机房门禁密码，禁止将机房门密码透露给其它人员，禁止带领与工作无关的人员进入机房。

第十九条

工作人员、到访人员出入要进行登记。（附表3、机房出入登记单）。进入机房后，在指定的工作区作业，禁止操作非本单位的设备、设施。机房视频监控系统对机房内所有活动进行24小时监控，以备日后查询。

第二十条

各单位网管员必须严格遵守著作权法，禁止使用盗版软件、非法软件、淫秽软件，并负有对网络用户的监督职责。一经发现上述违法行为，立即销毁软件、并追究行为人的法律责任。

第二十一条

禁止在服务器上进行试验性质的软件调试，禁止在服务器上随意

安装软件。需要对服务器进行配置的，必须在其它可进行试验的机器上调试通过并确认可行后，才能在服务器上实施。

第七章

汇聚层机房管理

第二十二条

机房由所在层网管人员负责管理和维护，无关人员未经许可不得进入机房。

第二十三条

机房内交换机和通信配线柜是大厦网络通信系统的关键设备，任何单位和个人不得擅自更改或挪动。

第二十四条

保持场地清洁、卫生，不得存放易燃易爆和强磁物品及其它与机房工作无关的物品，杜绝安全隐患。

第八章

附则

第二十五条

凡违反网络管理办法的单位和个人，将依情节轻重给予批评教育，责令整改；对情节特别严重的或造成经济损失的，将通报批评、追究责任并禁止接入网络;对违反国家法律法规，构成犯罪的，依法追究刑事责任。

第二十六条

本办法自发布之日起执行。

附表 1IP 住址备案表

单位名称:

责任人:

联系电话:

所属部门

使用者

IP 住址

MAC 住址

联系电话

制表人（网管员）：年

附表 2 无线网络备案表

单位名称:

责任人:

联系电话:

所属部门

设备管理人

无线设备 IP 住址

DHCP 住址池

联系电话

附表 3 机房出入登记单

年度

月/日

来宾姓名

来宾单位

携带物品

工作内容

进入时间

离开时间

陪同人（签字）

备注

时分

篇 2:校园网网络安全方案设计

网络安全设计

1、网络病毒的防范

病毒产生的原因：某校园网很重要的一个特征就是用户数比较多，会有很多的 PC 机缺乏有效的病毒防范手段，这样，当用户在频繁的访问 INTERNET 的时候，通过局域网共享文件的时候，通过 U 盘，光盘拷贝文件的时候，系统都会感染上病毒，当某个学生感染上病毒后，他会向校园网的每一个角落发送，发送给其他用户，发送给服务器。

病毒对校园网的影响：校园网万兆、千兆、百兆的网络带宽都被大量的病毒数据包所消耗，用户正常的网络访问得不到响应，办公平台不能使用；资源库、VOD 不能点播；INTERNET 上不了，学生、老师面临着看着丰富的校园网资源却不能使用的尴尬境地。

2、防止 IP、MAC 地址的盗用

IP、MAC住址的盗用的原因：某校园网采用静态 IP 住址方案，如果缺乏有效的 IP、MAC住址管理手段，用户可以随意的更改 IP 住址，在网卡属性的高级选项中可以随意的更改 MAC住址。如果用户有意无意的更改自己的 IP、MAC住址，会引起多方冲突，如果与网关住址冲突，同一网段内的所有用户都不能使用网络；如果恶意用户发送虚假的 IP、MAC的对应关系，用户的大量上网数据包都落入恶意用户的手中，造成 ARP欺骗攻击。

IP、MAC住址的盗用对校园网的影响：在用户看来，校园网络是一个很不可靠是会给我带来很多麻烦的网络，因为大量的 IP、MAC冲突的现象导致了用户经常不能使用网络上的资源，而且，用户在正常工作和学习时候，自己的电脑上会经常弹出 MAC住址冲突的对话框。由于担心一些机密信息比如银行卡账户、密码、邮箱密码泄漏，用户会尽量减少网络的使用，这样，学生、老师对校园网以及网络中心的信心会逐渐减弱，投入几百万的校园网也就不能充分发挥其服务于教学的作用，造成很大程度上的资源浪费。

3、安全事故发生时候，需要准确定位到用户

安全事故发生时候，需要准确定位到用户原因：

国家的要求：2002 年，X签署了 282 号令，要求各大 INTERNET 运营机构（包括高校）必须要保存 60 天的用户上网记录，以待相关部门审计。

校园网正常运行的需求：如果说不能准确的定位到用户，学生会在网络中肆无忌弹进行各种非法的活动，会使得校园网变成“黑客”

更严重的是，如果当某个学生在校外的某个站点发布了大量涉及政治的比如法X的言论，这时候公安部门的网络信息安全监察科找到我们的时候，我们无法处理，学校或者说网络中心只有替学生背这个黑锅。

安全事故发生时候，不能准确定位到用户的影响：

一旦发生这种涉及到政治的安全事情发生后，很容易在社会上广泛传播，上级主管部门会对学校做出处理；同时也会大大降低学校在社会上的影响力，降低家长、学生对学校的满意度，对以后学生的招生也是大有影响的。

5、用户上网时间的控制

无法控制学生上网时间的影响：如果缺乏有效的机制来限制用户的上网时间，学生可能会利用一切机会上网，会旷课。学生家长会对学校产生强烈的不满，会认为学校及其的不负责任，不是在教书育人。这对学校的声誉以及学校的长期发展是及其不利的。

6、用户网络权限的控制

在校园网中，不同用户的访问权限应该是不一样的，比如学生应该只能够访问资源服务器，上网，不能访问办公网络、财务网络。办公网络的用户因该不能访问财务网络。因此，需要对用户网络权限进行严格的控制。

7、各种网络攻击的有效屏蔽

校园网中常见的网络攻击比如MAC FLOOD、SYN FLOOD、DDOS攻击、扫描攻击、ARP欺骗攻击、流量攻

非法 DHCP服务器及 DHCP攻击、窃取交换机的管理员密码、发送大量的广播报文，这些攻击的存在，会扰乱网络的正常运行，降低了校园网的效率。

2.4.3.2 网络攻击的防范

1、常见网络病毒的防范

对于常见的比如冲击波、振荡波等对网络危害特别严重的网络病毒，通过部署扩展的 ACL，能够对这些病毒所使用的 TCP、UDP的端口进行防范，一旦某个用户不小心感染上了这种类型的病毒，不会影响到网络中的其他用户，保证了校园网网络带宽的合理使用。

2、未知网络病毒的防范

对于未知的网络病毒，通过在网络中部署基于数据流类型的带宽控制功能，为不同的网络应用分配不同的网络带宽，保证了关键应用比如 WEB 课件资源库、邮件数据流有足够可用的带宽，当新的病毒产生时，不会影响到主要网络应用的运行，从而保证了网络的高可用性。

3、防止 IP 住址盗用和 ARP攻击

通过对每一个 ARP报文进行深度的检测，即检测 ARP报文中的源 IP 和源 MAC是否和端口安全规则一致，如果不一致，视为更改了 IP 住址，所有的数据包都不能进入网络，这样可有效防止安全端口上的 ARP欺骗，防止非法信息点冒充网络关键设备的 IP（如服务器）造成网络通讯混乱。

4、防止假冒 IP、MAC发起的 MAC

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/728122143051007011