# 信息与网络管理中心信息安全保密管理办法

来源：网络 作者：空山新雨 更新时间：2025-07-25

*第一篇：信息与网络管理中心信息安全保密管理办法信息与网络管理中心信息安全保密管理办法为加强信息化建设安全保密工作，维护集团安全和利益，结合信息化建设工作实际，特制定本管理办法。一、信息安全与保密1、建立信息系统安全等级保护制度，建立人员权...*

**第一篇：信息与网络管理中心信息安全保密管理办法**

信息与网络管理中心信息安全保密管理办法

为加强信息化建设安全保密工作，维护集团安全和利益，结合信息化建设工作实际，特制定本管理办法。

一、信息安全与保密

1、建立信息系统安全等级保护制度，建立人员权限控制表，进行信息分级管理，不同级别的人员只能查看相应级别的数据；

2、发布任何信息必须经过合法的工作程序或主管领导的审批；

3、记录敏感数据的操作日志，并长期保存；

4、对数据中心的运行拓扑结构、服务器软硬件信息，包括操作系统和应用软件的配置等信息应分级管理并严格保密；

5、在开发、运行、维护过程中，每位成员要有保密意识，不该看的不看，不该说的不说；

6、禁止在自己管理的计算机（工作用机、服务器）上开设与工作无关的服务；

7、禁止在个人用机（笔记本电脑、台式 PC 机）上存放敏感数据；

8、系统管理员、数据库管理员、信息系统开发人员及相关人员不得对外宣扬本职工作所从事的具体内容；

9、所有上互联网的人员必须遵守国家有关法律法规的规定

10、如发生信息安全与保密事故，当事人立即向信息中心主任汇报，相关信息不得向无关人员透露。

二、数据安全

1、对存放敏感数据的运行服务器须严格管理。系统账号必须登记并定期检查；

2、严格控制对运行数据库和试运行库的直接访问。原则上只有运行服务室数据库管理人员、技术支持人员可以直接访问，其他人员访问数据库必须得到相关领导批准并备案；

3、建立数据备份制度，对数据进行定期备份，包括数据容灾备份；备份的数据应注意保密，不得随意存放；

4、运行数据库不得用于系统的开发调试；

5、测试数据库和开发数据库中不得存放敏感数据；

6、所有管理员（数据库系统、应用系统）应严格管理自己的帐号和密码，并定期更换密码；

7、管理员登录系统应采用加密方式；

8、不得利用邮件、移动存储介质、笔记本电脑等将数据中心的涉密资源带出办公室。

三、网络和服务器安全

1、设立信息系统安全保密责任人，加强对信息安全工作的组织落实；

2、设立信息安全管理员岗位，并制定相应的岗位职责；

3、建立数据中心网络信息安全防范体系，保证服务器特别是关键服务器的安全；

4、凡用于对外提供服务的服务器必须保留至两年的日志。

四、数据中心机房安全

1、对存放服务器的数据中心机房建立机房管理制度和严密的保安措施，无关人员严禁入内，相关人员进出机房必须有相应登记；

2、对信息备份的介质要专人保管，定期检查，防止丢失或受损；

3、加强机房日常管理，制定数据中心机房值班制度；

4、对于进出数据中心机房的设备必须经过严格的审批和登记手续。

五、办公环境安全

1、对于新装的计算机必须严格按照规范进行；

2、每位成员在其办公用机安装操作系统后，必须安装补丁程序、防病毒软件并进行安全检查。每位成员负责自己使用的办公用机的安全，及时更新补丁，升级相关软件及病毒库；

3、所有成员都有责任和义务保管好所使用的网络设施和计算机设备，非管理人员禁止随意更改设备配置，确保设备的正常稳定运行；

4、禁止未授权的其他人员接入中心的计算机网络以及访问网络中的资源；

5、IP 地址为计算机网络的重要资源，使用者应在管理员的规划下使用这些资源，不能擅自更改。某些系统服务对网络产生影响，使用者应在安全管理员的指导下使用，禁止随意开启计算机中的系统服务，保证计算机网络畅通运行；

6、计算机使用者应保管好分配给自己的用户账号和密码。禁止随意向他人泄露、借用自己的账号和密码，严禁不以真实身份登录系统。计算机使用者应定期更改密码、使用复杂密码。不得猜测他人的密码，不得使用黑客程序进行密码破解，不得窃取系统管理员的密码；

7、上网时必须将杀毒软件的实时监测功能打开；

8、接到可疑邮件时不要随意打开，以免感染病毒；

9、禁止利用扫描、监听、伪装等工具对网络和服务器进行恶意攻击，禁止非法侵入他人网络和服务器系统，禁止利用计算机和网络干扰他人正常上课和工作的行为。

**第二篇：网络与信息管理中心岗位职责**

网络与信息管理中心岗位职责

1、保障网络信息安全，通过网络信息系统为学校的教学、科研、管理及校园文化建设提供良好的服务；

2、建立和完善网络信息管理的各项规章制度，实现管理的规范化和制度化，认真履行，严格遵守；

3、负责学校级别网站的建设、管理与维护等工作，保证网站内容的及时性、准确性和有效性；

4、负责各部门二级网站的统一部署和维护，协助相关部门进行网页内容和源代码的更新修改；

5、负责校内各应用系统的配置、维护、调整及更新，对各部门管理员分配相应权限，并提供技术支持，解决校园网应用和管理中的关键技术；

6、负责学校信息的安全管理，提出和执行具体措施保障校园网络信息设备和信息系统的安全、高效、平稳运行；

7、定期检查设备的运转情况，做好设备维护记录，落实责任制，明确责任人和职责，保证设备高效稳定的运行；

8、负责校内各类信息网站和应用系统的数据备份、资料整理和归档，定期对服务器防护软件进行更新升级，保证数据的安全；

9、对于服务器等设备的故障和信息网站受到的恶意攻击，及时响应并采取应急预案，最短时间内恢复正常的网络信息服务。并查找确认故障源或攻击源，采取有效措施预防；

10、完成领导交办的其它相关工作。

**第三篇：信息保密管理办法**

信息保密管理办法

第一章 总 则

第一条 为切实加强股份有限公司（以下简称“公司”）的信息保密工作，防范和杜绝各种泄密事件的发生，保护和合理利用公司秘密，确保公司信息披露的公平、公正，保障公司、股东及其他利益相关者的合法权益不受侵犯，根据有关法律、法规及《公司章程》的规定，结合公司实际，制定本管理办法。

第二条 保密信息是指不为公众所知悉，关系公司利益，具有实用性并经公司采取保密措施保护的技术信息、经营信息和管理信息等，在一定时间内只限一定范围人员知悉的信息。

第三条 公司董事、监事及中高层管理人员及公司各部门、子公司以及全体职员都有保守公司秘密的义务，都应做好信息保密工作。

第四条 信息保密工作，实行积极防范、突出重点、既确保秘密又便于工作，并充分履行信息披露义务的方针。

第二章 保密信息范围和密级确定

第五条 保密信息包括但不限于以下事项和行为：

（一）可能对公司股票及其衍生品种交易价格产生重大影响，但尚不具备公开披露条件的信息；

（二）涉及公司经营管理、运作和决策，或对公司利益有重大影响，一旦泄密将给公司带来损失或失去潜在收益的信息；

（三）包括以书面和电子等方式存在的各种信息；

（四）其他与公司相关的需要保密的信息。

第六条 保密信息的密级分为“绝密”、“机密”、“秘密”三个等级。

（一）绝密是最重要的公司秘密，泄露会使公司的利益遭受特别严重的损害，对公司股票及其衍生品种交易价格可能产生重大影响且尚未公开披露的信息，主要包括：公司的发展规划、经营战略、商务谈判内容及载体，正式合同和协议文书、未开标的投标文件、未公开的重大投资决策、尚未确定的公司重要人事调整及安排等，以及按《档案法》规定属于绝密级别的各种档案；

（二）机密是重要的公司秘密，泄露会使公司利益遭受到严重的损害，如、财务报表、统计资料、重要会议记录、公司经营情况等，以及按《档案法》规定属于机密级别的各种档案；

（三）秘密是一般的公司秘密，泄露会使公司的利益遭受损害，如公司人事档案、合同、协议、薪金制度，人力资源对管理人员的考评材料等，以及按《档案法》规定属于秘密级别的各种档案。

第七条 定级方法 由文件生成部门负责人确定文件的密级程度、保密期限和起止日期，并在文件的右上角标明。属公司秘密事项但不能标明密级的，由涉密部门负责人口头通知接触范围内的人员。保密期限届满，自行解密或经批准，提前解密。

第八条 属于公司秘密的载体（如图纸、资料、录音、录象、软盘、光盘等），应当依据本制度第六条、第七条的规定进行相应标注。保密期限届满，自行解密或经批准，提前解密。

第三章 主要涉密部门、人员范围及管理权限

第九条 公司主要涉密部门包括：董事会秘书处、事务部、财务部、企划部、营运部、技术工程部、审计部，以及下属企业主要涉密部门。

第十条 公司主要涉密人员包括：

（一）公司董事、监事、中高级管理人员；

（二）列入主要涉密部门的全体员工；

（三）负责保密事项制作、保管的人员；

（四）公司主要涉密部门根据需要临时或专门指定的部门或岗位人员；

（五）公司临时聘用的接触涉密工作的外部工作人员，如法律顾问、财务顾问等。公司可根据保密信息的具体情况，要求涉密人员签署保密协议。

第十一条 各部门负责人为本部门的保密工作负责人，公司事务部为公司保密工作管理部门，负责监督和检查各部门的保密工作；组织解决密级不明确或者有争议的事项并负责组织处理公司的泄密事件。

第十二条 保密工作管理权限：

（一）绝密事项（含载体），由绝密事项生成部门指定专人负责做好标识，妥善保管，并建好记录、台帐。绝密事项的发放、传阅均需经相关公司领导批准，并应限制在一定时间内返还保管。绝密事项允许知悉的范围是公司董事、监事、中高级管理人员、绝密事项形成的相关人员，及董事、监事、高级管理人员认为需要让其知悉的对象；

（二）机密事项（含载体），由机密事项生成部门指定专人负责做好标识，妥善保管，并建好记录、台帐。机密事项的发放，传阅需经相关公司领导或其授权的部门经理批准，并应限制在一定时间内返还保管。机密事项允许知悉的范围是公司董事、监事、高级管理人员、机密事项形成的相关人员，及董事、监事、高级管理人员、机密事项形成的负责人认为需要让其知悉的对象；

（三）秘密事项（含载体），由秘密事项生成部门指定专人负责做好标识，妥善保管，并建好记录、台帐。机密事项的发放，传阅需经部门经理或部门经理以上领导批准，并应限制在一定时间内返还保 管。秘密事项允许知悉的范围是公司董事、监事、高级管理人员、秘密事项形成的相关人员，及董事、监事、高级管理人员、秘密事项形成的负责人认为需要让其知悉的对象。

第四章 保密管理

第十三条 传阅保密材料由机要人员统一掌握，划定传阅范围，不得自行扩大，不得让无关人员查看，控制传阅文件的交接，以防丢失。

第十四条 不得擅自翻印、复印、传抄秘密文件、资料；不得在公共场所谈论秘密事项，不得在私人通讯中涉及秘密内容。保密材料复印件应视同原件管理，复印过程的废页应及时销毁。

第十五条 保密材料严格按照批准的份数打印，不得擅自多印多留，草稿视同原件一样管理，打印过程形成的废页、废件应及时销毁。

第十六条 传递保密材料要有保密措施，传递应专送，不得办理无关事项，密件不得携入不利于保密的场所。

第十七条 做好通讯中的保密工作，不在无保密措施的电话、传真机上传递保密材料。第十八条 做好公司重要会议的保密工作，会址应选择有利于保密的地方，严格控制无关人员进入，严禁滥发会议文件，会后检查有无遗漏材料。

第十九条 做好办公自动化中的保密工作，对保密材料加设浏览和下载权限。

第五章 泄密的处理

第二十条 泄密是指下列行为之一：

（一）使公司秘密被不应知悉者知悉的；

（二）使公司秘密超过了限定的接触范围，而不能证明未被不应知悉者知悉的。

第二十一条 公司发生或者发现泄密事件，应当在知悉泄密事件后及时报告事务部和董事会秘书处。遇重大特殊情况时，可直接向分管领导上报。

第二十二条 发生泄密事件的部门，应根据情况及时采取补救措施，最大限度减少泄密造成的损失。处置泄密事件，应做到如下几点：

（一）任何部门和个人应积极配合有关部门查明事发原因；

（二）应对责任人进行处理，以增强保密意识；

（三）采取纠正和预防措施，防止类似泄密事件的再次发生。

第六章 责任与奖惩

第二十三条 符合下列情形之一者，公司对有关部门或人员给予表彰或奖励：

（一）及时举报泄密事件，且避免可能由此造成公司损失的；

（二）非责任人及时采取补救措施，避免或最大限度减少泄密造成损失的；

（三）在改进保密技术、保密措施等方面取得显著成绩的。

第二十四条 出现下列情况之一者，给予警告，或采取适当的经济处罚：

（一）泄露公司秘密，尚未造成严重后果或经济损失的；

（二）已泄露公司秘密但采取了补救措施的。

第二十五条 出现下列情况之一者，应予以辞退，情节严重的，将依法追究相关法律责任：

（一）故意或过失泄露公司秘密，造成严重后果或重大经济损失的；

（二）违反本制度规定，为他人窃取、刺探、收买或提供公司秘密的；

（三）利用职权强制他人违反保密规定的。

第七章 附则

第二十六条 本管理办法未尽事宜，按国家相关法律规定办理。

第二十七条 本管理办法解释权属公司事务部 第二十八条本办法自印发之日起施行。8

**第四篇：网络和信息安全保密责任书**

网络和信息安全保密责任书

为坚决杜绝计算机违规事件发生，进一步做好网络安全工作，为信息化建设工作提供强有力的网络安全保障，为提高网络和应用系统使用人员的安全保密意识，增强责任感，确保网络和信息安全保密，根据“谁使用、谁负责”的管理责任制，结合实际，制定了《网络和信息安全保密责任书》，并要求所有使用计算机的干警签订。

一、办公专网与国际互联网完全物理隔离，不使用任何其他网络设备造成“一机两用”。

二、原则上办公用的电脑不得安装软驱、光驱和开放USB接口，因工作需要必须安装软驱、光驱和开放USB接口，的计算机。不得使用外来和自用的移动存储设备。外来的软盘、光盘和移动存储设备必须由计算机信息安全管理组查杀病毒和登记后，转入办公专网才能使用。全面防止移动存储设备使用中“公私不分”。

三、计算机安全日常防范

1、管理好本人使用的计算机，不准外来和无关人员使用和乱动计算机。

2、任何人不得随意安装软件，如有需要安装与工作相关的软件。应由计算机信息安全管理组指定人员协助安装。

3、计算机均应设置开机热启动、网络登陆及屏幕保护密码，暂时离开电脑要确保正在编辑的文件已关闭或正在使用的应用系统已退出且屏幕保护已启动。

4、重要文件要设置开启密码。

5、电脑系统或文件设置的密码或口令其长度不得少于8个字符；应采用组成复杂、不易猜测的口令，一般应是：大小写英文字母、数字、特殊字符中两者以上的组合；口令更换周期不得长于一个月。

6、每个用户必须妥善管理自己的密码、口令，要定期更换并不得随意泄露。

四、本责任书一式三份，自签订之日起生效，计算机信息安全管理组与责任人各执一份。

管理机构：计算机信息安全管理组 责任人签名：

负 责 人：

联系电话 ：

签订日期 ：

年 月 日 签订日期 ：

年 月 日

**第五篇：网络信息安全和保密责任制**

网络信息安全和保密责任制

为加强企业信息安全，维护企业合法权益，明确员工对企业所负的信息安全与保密责任，根据国家相关法规、制度要求，特制定本责任制：

一、监控中心负责对相关系统所涉及资料重点档案的各种存储载体、收集、登记、存档等管理工作。

二、加强计算机系统的保密安全管理，对涉密与非保密计算机予以明确区分，涉密机必须完全与局域网脱离连接，并禁止上因特网以防泄密，做到上网信息不涉密，涉密信息不上网。

三、信息收集、整理和加工应分别由专人负责，互相监督，不得编造或篡改信息，各部门或个人所提供信息应在显著位置标明信息保密等级。

四、为保护知识产权和防止信息泄密，任何部门和个人不得私自向他人提供互联网发布的信息。

如确需要时，由各部门报分管副矿批准后，同时报监控中心记录备案后方可。

五、存储于计算机设备及媒体中的信息，低于保密等级及无关人员不得私自调阅。

六、接触机密信息的有关人员，应严格执行保密制度，未经领导批准，不得向低于保密等级无关人员传播。

七、存储过秘密信息的计算机媒体委外维修应保证所存储的信息不被泄露，同时报监控中心备案。

记载有机密信息的报废磁介质和纸张，必须进行销毁。

八、对外来参观人员，不经领导批准，任何部门和个人均不得通过屏幕显示和打印方式输出机密信息，更不得进行磁介质拷贝。

九、任何部门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。

十、发现信息泄密、利用单位机密信息进行违法犯罪、发布有害信息等违法犯罪行为，任何部门和个人均有义务及时向监控中心及有关部门进行汇报，并协助有关部门或管理人员对上述人或事进行调查、取证、处理，向调查人员如实提供所需证据。

部门负责人： 责任人：

二○一一年一月

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！