* 1. 信息管理系统
     1. 信息管理系统简介

信息管理系统是指本单位利用计算机、网络通信技术，实现信息收集、系统集成、整合分类、信息存储、信息分析的一套专门软件程序。

* + 1. 工作目标

信息管理系统内部控制的目标是促进本单位有效实施内部控制，提高本单位现代化管理水平，将经济业务活动及其内部控制的流程和控制措施嵌入到信息管理系统中，减少人为操纵因素，增强信息安全性、可靠性、合理性及相关信息的保密性、完整性和可用性，为建立有效的信息与沟通机制提供支持保障。单位应对积极推进信息管理系统的开发建设，对信息管理系统建设实施归口管理，在日常办公、财务管理、采购管理、资产管理、预算管理、建设项目和合同管理等领域，尽快实施信息化管理。

* + 1. 组织职能

（1）主管科室

由本单位的key\_fzxxglxtks负责单位信息管理系统、硬件设备、网络环境、系统集成的建立和实施有效的内部控制管理。应对建立健全本单位信息管理系统相关运行管理制度，定期或不定期检查信息管理系统运行情况，及时发现并解决故障。对信息管理系统提出未来建设规划，形成规划方案上报内部控制工作领导小组审议。

负责组织开展信息管理系统的应用培训和技术学习。

（2）各科室的职责

各科室应当相互协作、各尽其责，共同做好信息系统日常运行操作、设备维护与保养等工作。应对在信息系统出现故障或问题及时记录并报至主管科室有关人员，以便及时解决。

* + 1. 信息系统管理制度
       1. 总则

（一）为保证本单位信息网络系统的安全，根据国家有关计算机、网络和信息安全的相关法律、法规和安全规定，结合本单位网络系统建设的实际情况，制定本制度。信息系统归口管理由本单位的牵头key\_fzxxglxtks负责。

（二）本制度所指的信息网络系统，是指由计算机（包括相关和配套设备）为终端设备，利用计算机、通信、网络等技术进行单位内部信息化管理中的数据采集、处理、存储和传输的设备、技术、管理的组合。

（三）信息网络系统安全的含义是通过各种计算机及其他登录终端、网络、密码技术和信息安全技术，在实现网络系统安全的基础上，保护信息在传输、交换和存储过程中的机密性、完整性和真实性。对于终端网络安全特指本机信息系统应用数据、操作系统、身份验证及操作代码的机密性及安全性。

（四）本规定适用于单位内所有计算机硬件、周边设备（如打印机、扫瞄仪、MO存储器、软磁碟、CD碟、数码相机、考勤机终端等）及所有网络设备。单位内所有操作计算机的岗位和与之有关工作的岗位均属此管理之内。

* + - 1. 信息系统安全管理

（一）计算机系统账号与操作员代码

1.操作员代码是进入各类应用系统进行业务操作、分级对数据存取进行控制的代码。操作员代码分为系统管理代码和应用操作代码。代码的设置根据不同应用系统的要求及岗位职责而设置。

2.系统管理操作代码必须经过相应申请经相关系统管理人员授权取得。

3.系统管理员负责各项应用系统的环境生成、维护，负责一般操作员代码的生成和维护，负责故障恢复等管理及维护。

4.系统管理员对业务系统进行数据整理、故障恢复等操作，必须有主管负责人授权。

5.信息部门任何人员不得使用他人操作代码进行业务操作。

6.系统管理员调离岗位，上级管理员（或相关负责人）应及时注销其代码并生成新的系统管理员代码。

7.一般操作码由系统管理员根据各类应用系统操作要求生成，应按每操作用户一码设置。

8.操作员不得使用或盗用他人代码进行业务操作。

9.操作员调离岗位，系统管理员应及时注销其代码并生成新的操作员代码。

（二）密码与权限管理

1.密码是保护系统和数据安全的控制代码，也是保护用户自身权益的控制代码。密码设置应具有安全性、保密性，不能使用简单的代码和标记。

2.重要岗位的用户密码应定期修改，如发现或怀疑密码遗失或泄漏应立即修改，在可能的情况下并相应记记录用户名、修改时间、修改人等内容，及时上报单位信息系统归口部门备案。

3.服务器、路由器、交换机等单位重要信息设备的超级用户密码由信息系统归口部门负责人指定专人设置和管理，并由密码设置人员将密码装入密码信封，在骑缝处加盖印章并签字标注封存日期后交由信息系统归口部门存档并登记。如遇特殊情况需要启用封存的密码，必须经过相关负责人同意，由密码使用人员向密码管理人员索取，使用完毕后，须立即更改并封存，同时在“密码管理登记簿”中登记。

4.系统维护用户的密码应至少由两人共同设置、保管和使用。有关密码授权工作人员调离岗位，主管负责人须指定专人接替并对密码立即修改或用户删除，同时在“密码管理登记簿”中登记并备档留存。

* + - 1. 数据安全管理

（一）存放备份数据的介质必须具有明确的标识。备份数据在条件允许情况下实行异地存放，并保证重要系统的数据备份要有两份。

（二）注意计算机重要信息资料和数据存储介质的存放、运输安全和保密管理，保证存储介质的物理安全。

（三）任何非应用性业务数据的使用及存放数据的设备或介质的调拨、转让、废弃或销毁必须严格按照程序进行逐级审批，以保证备份数据安全完整。

（四）数据恢复前，必须对原环境的数据进行备份，防止有用数据的丢失。数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。

（五）数据清理前必须对数据进行备份，在确认备份正确后方可进行清理操作。历次清理前的备份数据要根据备份策略进行定期保存或永久保存，并确保可以随时使用。数据清理的实施应避开业务高峰期，避免对联机业务运行造成影响。

（六）需要长期保存的数据，数据管理部门需与相关部门制定转存方案，根据转存方案和查询使用方法要在介质有效期内进行转存，防止存储介质过期失效，通过有效的查询、使用方法保证数据的完整性和可用性。转存的数据必须有详细的文档记录。

（七）非本单位技术人员对本单位的设备、系统等进行维修、维护时，必须由本单位相关技术人员或相关负责人现场全程监督。计算机设备送外维修，须经资产管理归口部门负责人批准。

（八）设备使用部门应对报废设备中存有的程序、数据资料进行备份后清除，并妥善处理废弃无用的资料和介质，防止泄密。

（九）信息系统归口管理部门需指定专人负责计算机病毒的防范工作，建立本单位计算机病毒防治管理制度，经常进行计算机病毒检查，发现病毒及时清除。

（十）单位内所有计算机未经信息系统归口管理部门的允许不准安装与其业务无关的软件、不准使用来历不明的载体（包括软盘、光盘、移动硬盘、MP3等其他存储介质）。

* + - 1. 网络安全及防病毒管理

（一）任何人员不得盗用他人账号或操作员代码、单位内部网络安全管理密码进行操作。

（二）严禁在工作计算机上安装BT、P2P等类型的多线程或占用带宽流量的下载软件，所有下载均采用单线程下载。保证单位的带宽有效利用。

（三）计算机内电子邮件收发均通过单位内部邮件系统进行，条件允许的情况下可以使用本单位内部办公自动化平台。

（四）计算机均采用域管理方式进行登录，在工作期间必须登录单位域服务器，并严格按照域管理下的操作说明进行文档及其他相关文件的传递。

（五）防病毒系统均采用单位统一布署的网络防病毒系统，由信息系统归口管理部门统一对防病毒服务器进行升级和下载，不得擅自登录非本病毒软件官方以外的下载站点下载并进行病毒库代码更新。

（六）为保证单位Internet的带宽流量，信息系统归口管理部门必须对访问Internet权限进行管控，若有访问外部Internet公网其他特别需求的，可提出申请，经本部门负责人及信息系统归口管理部门审核，报经分管领导批准后，使申请人享受访问Internet的特别需求权力。未通过此程序审批而私自设定其他方法访问外部网络，一经发现，将做严责。如因此给单位带来损失的，责成责任人承担相应损失。

* + - 1. 机房安全管理

（一）进入信息主机房至少应当有两人在场，并登记“机房出入管理登记簿”，记录出入机房时间、人员和操作等内容。

（二）信息管理人员进入机房必须在“机房出入管理登记簿”签字登记，其他人员进入机房必须经信息系统归口管理部门的许可，并由有关人员陪同（特殊情况除外）。机房当日值班人员必须如实记录来访人员名单、进出机房时间、来访内容等。非信息系统归口管理部门工作人员原则上不得进入机房对系统进行操作。如遇特殊情况必须操作时，经信息系统归口管理部门负责人批准同意后并在有关人员陪同情况下进行。对操作内容进行记录，由操作人和监督人签字后备案。

（三）保持机房整齐清洁，机房设备按维护计划定期进行保养。计算机机房中要保持恒温、恒湿、电压稳定，做好静电防护、防雷、防尘等项工作，保证主机系统的平稳运行，定期对机房运行的各项环境指标（如温度、洁净度、温度上升率等）进行测试，并做好记录，通过实际测量各项参数发现问题及时解决，保证机房各项设备的正常运行。

（四）机房内严禁吸烟、进食、会客、聊天等与业务无关的活动。严禁携带液体和食品进入机房，严禁携带与上机无关的物品，特别是易燃、易爆、有腐蚀等危险品进入机房。如因需要携带移动计算机进入机房需报经信息系统归口管理部门批准方可。

（五）机房工作人员严禁违章操作，严禁私自将外来软件带入机房使用。

（六）严禁在未采取安全措施或通电的情况下拆卸、移动机房内等相关设备、部件及网络。在进行机房硬件更换或维修时，必须进行静电释放方可进行。

（七）定期检查机房消防设备器材，做好检查登记。

（八）机房内不准随意丢弃存储介质和有关业务保密数据资料，对废弃存储介质和业务保密资料要及时销毁（碎纸），不得作为普通垃圾处理。严禁机房内的设备、存储介质、资料、工具等私自出借或带出。

（九）服务器等所在的机房后备电源（UPS）除了电池自动检测外，每年必须深充放电一次到两次。

* + - 1. IT设备购置、维修及报废管理
         1. IT设备购置

1.所有IT设备均由本单位采购归口部门负责采购。设备购置由使用部门提出申请，由信息系统归口管理部门进行核定后上报分管领导审批后进行采购。属于政府采购范畴内的设备购置必须严格执行本单位的政府采购业务流程。

2.大型、高端的IT设备的采购验收工作必须由信息系统归口管理部门参与共同完成。

3.IT设备的采购严格遵守单位采购流程及政府采购业务管理规定。

* + - * 1. IT设备故障维修

1.信息系统归口管理部门负责本单位所有IT设备的故障及维修。

2.信息系统归口管理部门对本单位的IT设备故障做鉴定和维修，并出具鉴定结果，并对鉴定结果负责。

3.对于一般故障和影响到部门工作业务开展的，必须在当天工作日内完成处理。对于重大故障必须及时维护及维修的，如超出工作时限部分按照实际情况酌情处理。必须建立维修记录。

4.IT设备硬件故障经信息系统归口管理部门人员鉴定在其范围内无法维修的，如在三包范围内的，由信息系统归口管理部门联系销售厂家进行维修。超出三包范围的，信息系统归口管理部门填报维修申请单，由信息系统归口管理部门负责人核准上报单位分管领导审批后交由外包维修单位进行维修。

5.对于IT硬件设备故障在鉴定后无维修价值的，转入IT设备报废管理流程进行处理。

* + - * 1. IT设备报废管理

1.IT设备的报废鉴定统一由信息系统归口管理部门完成，特殊IT设备（如服务器、磁带存储设备、核心路由器、核心交换机）的故障鉴定由厂家、单位委托第三方IT设备鉴定机构、信息系统归口管理部门共同完成。

2.信息系统归口管理部门对IT设备报废鉴定报告上报单位分管领导审批后，对报废IT设备统一进行存放管理，并按国有资产管理制度严格执行资产报废处置业务流程。

3.对IT设备报废鉴定为人为原因造成的，由责任人承担此IT设备的全额损失，并按照单位相关管理规定进行从严处罚。

* + - 1. 信息化系统项目管理

（一）本管理规定适用于单位内部信息化建设过程中的所有信息管理系统项目招标、采购及实施。

（二）信息化建设过程的系统建设要从单位中长期规划出发，结合本单位实际发展情况，根据先进性、必要性、合理性、经济性、兼容性原则实施。

（三）信息化系统的建立过程中的调研与可行性论证、实施采购、合同签定、项目实施、项目验收等均由信息系统归口管理部门与建设部门共同配合完成，信息系统归口管理部门主导上述工作各环节。

（四）信息化系统项目立项申请原则上由建设部门提出，信息系统归口管理部门也可以根据本单位发展提出。所有信息化系统立项均报单位上会研究决定后方可着手实施。

（五）信息化系统项目一经确定立项实施，必须成立项目小组，确定项目小组负责人及成员，原则上项目小组负责人由单位分管领导担任，小组成员由单位各相关部门的负责人组成。信息系统归口管理部门在项目实施过程中对项目小组负责。

（六）项目小组成员要根据项目要求，极积主动高质量完成项目实施过程中专项工作。工作实施专管专责，不得中途转手他人（特殊情况除外）。

（七）信息系统归口管理部门在项目实施过程中负责协调、组织、沟通和实施过程中的衔接工作。及时解决处理项目实施过程中的技术和其他问题。

（八）信息系统归口管理部门全程跟踪、管理项目实施过程中的所有环节，并对项目进度及质量负责。信息化系统项目实施过程中的技术文档、项目需求、知识文档等信息系统归口管理部门要建立完整的项目文档管理体系。

（九）信息化系统项目验收由项目小组评审验收，信息系统归口管理部门具体负责项目验收评估及项目验收报告并上报单位领导审批。

（十）信息系统归口管理部门负责信息化系统项目验收完成后的具体运行维护工作，并依据运行情况出具相关运行报告。

* + - 1. 计算机使用管理

（一）信息系统归口管理部门负责单位各部门的计算机软件、硬件、上网行为及系统运行的统一维护和管理。

（二）信息系统归口管理部门负责对单位各部门使用的计算机做日常定期、不定期使用监督检查，对于检查中发现的违规全权处理。对于检查中发现的重大违规应及时上报单位分管领导。

（三）单位全体职工对违规使用计算的行为有互相监督和举报的权利。

（四）严禁外来人员使用本单位电脑。

（五）单位所有计算机实行封签管理。计算机的维修权在信息系统归口管理部门，任何人不得擅自更改计算机硬件配置或打开计算机，非信息系统归口管理部门人员对计算机故障原因的确定无任何效力。

（六）下班后各部门必须关闭计算机及处围设备，检查电源情况，确保安全方可离开。

（七）在办公期间，长时间不用电脑必须采取人离机锁定，防止信息数据及秘密泄露。

（八）计算机使用人员不得擅自更改系统软件设置，安装与工作无关的即时通讯、炒股、游戏、BT下载、P2P、在线流媒体音视频播放等第三方软件。

（九）单位接入互联网的网络参数及设备参数严格实行保密，信息系统归口管理部门对此项保密负责。

（十）任何人不得利用单位计算机和网络从事违法犯罪活动，一经查处落实，将从严处罚。

（十一）工作时间内严禁使用计算机或互联网做与工作无关的事。

（十二）工作时间除工作需要打开的互联网指定访问外（包含下载），其他网络访问及网络应用信息系统归口管理部门一律采用技术手段处理，确保各部门工作正常开展不受影响。

（十三）任何部门和个人不得从事下列活动：

1.利用计算机信息网络制作、传播、复制有害信息；

2.非法侵入计算机信息网络，非法窃取计算机信息系统中信息资源；

3.未经授权查阅他人电子邮箱，冒用他人名义发送电子邮件；

4.故意干扰计算机信息网络畅通，故意输入计算机病毒以及其他有害数据危害计算机信息系统安全；

5.违反规定，对计算机信息系统功能进行增加、删除、修改、干扰，对信息系统中存储、处理或者传输的数据和应用程序进行增加、删除、修改、复制，影响计算机信息系统正常运行；

6.刊登、出版、发行、销售、出租有关计算机病毒源程序的书刊资料和其他媒体；

7.传播、制造、销售、运输、携带、邮寄含有计算机病毒及危害单位及社会公共安全的有害数据；

8.危害计算机信息系统安全的施工，从事其它危害计算机信息系统安全的活动。

* + - 1. 附则

（一）本制度由key\_fzxxglxtks负责制定和解释。

（二）本制度在颁布之日起施行。