信息安全管理制度 投标方案

目 录

第一章 信息安全管理制度 2

1.1. 操作员安全管理制度 4

1.2. 账号的设置与管理 5

1.3. 密码与权限安全管理制度 6

1.4. 数据信息安全管理制度 8

1.5. 独立域控服务器 10

第二章 网络传输安全管理制度 13

2.1. 网络安全 15

2.2. 应用安全 16

2.3. 系统漏洞扫描与安全加固 17

第三章 信息存储安全管理 30

3.1. 数据存储 30

3.2. 数据备份 31

3.3. 终端隔离措施说明 32

3.4. 数据防泄漏措施 33

3.5. 建立文件保密制度 34

3.6. 弥补系统漏洞 36

3.7. 密切监管重点岗位的核心数据 37

第一章信息安全管理制度

为加强公司各信息系统管理，保证信息系统安全，根据《中华人民共和国保守国家秘密法》和国家保密局《计算机信息系统保密管理暂行规定》、国家保密局《计算机信息系统国际联网保密管理规定》,及上级信息管理部门的相关规定和要求，结合公司实际，制定本制度。

信息安全管理，是指数据(包括但不限于委案信息，日常邮件，查询资料，财务等信息)使用过程中传输、运行、维护、废止等操作安全的系列管理活动。

第一条、计算机的使用部门要保持清洁、安全、良好的计算机设备工作环境，禁止在计算机应用环境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备安全的物品。

第二条、非本单位技术人员对我单位的设备、系统等进行维修、维护时，必须由本单位相关技术人员现场全程监督。计算机设备送外维修，须经有关部门负责人批准。

第三条、严格遵守计算机设备使用、开机、关机等安全操作规程和正确的使用方法。任何人不允许带电插拔计算机外部设备接口，计算机出现故障时应及时向电脑负责部门报告，不允许私自处理或找非本单位技术人员进行维修及操作。

第四条、未经批准禁止携带非公司电子设备进入公司生产区域(包括个人电脑、手机、相机、U盘、移动硬盘、光

碟等带入公司，以防止公司网络感染病毒及数据外泄。公司

设备需由专人管理并定期盘点。

第五条、员工不得在互联网上以任何形式张贴涉及公司的保密或者敏感信息，如发现，公司保留追究其法律责任的权利。

第六条、员工在工作过程中未经批准不能通过个人电话、微信、QQ 等通讯工具进行催收及联系客户。

第七条、公司内部设立信息安全专项小组，各部门选举安全专员负责监督、落实安全制度，定期开展安全培训加强员工信息安全意识。

1.1.操作员安全管理制度

1、操作账号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唯一凭证。账号等级分为系统管理员账号、二级管理员账号及普通用户账号。

2、系统管理员账号授权二级管理员账号相应管理权限，二级管理员根据普通用户岗位需求不同授予相应的技能权限组。

3、系统管理员账号必须经过经营管理者授权取得；

4、系统管理员负责各项应用系统的环境生成、维护，负责一般账号的生成和维护，负责故障恢复等管理及维护；

5、系统管理员对业务系统进行数据整理、故障恢复等操作，必须有其上级授权；

6、系统管理员不得使用他人密码进行业务操作；

7、系统管理员及二级管理员调离岗位，上级管理员(或相关负责人)应及时注销其账号并生产新的系统管理员账号。

1.2.账号的设置与管理

1、普通用户账号由系统管理员根据各类应用系统操作要求生成，应按每用户一账号设置。

2、所有用户不得使用其他用户账号进行业务操作。

3、用户调离岗位，系统管理员应及时注销其使用账号或更改到新岗位对于技能权限组。

1.3.密码与权限安全管理制度

1、密码设置应具有安全性、保密性，不能使用简单的数字。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，密码分设为用户密码和操作密码，用户密码是登陆系统时所设的密码，操作密码是进入各应用系统的操作员密码。密码设置不应是名字、生日，重复、顺序、规律数字等容易猜测的数字和字符串；

2、管理员密码应定期修改，间隔时间不得超过一个月，如发现或怀疑密码遗失或泄漏应立即修改，并在相应登记簿记录用户名、修改时间、修改人等内容。

3、服务器、路由器等重要设备的超级用户密码由运行机构负责人指定专人(不参与系统开发和维护的人员)设置和管理，并由密码设置人员将密码装入密码信封，在骑缝处加盖个人名章或签字后交给密码管理人员存档并登记(暂时放在经理办公室的保管箱中)。如遇特殊情况需要启用封存的密码，必须经过经理同意，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、催收系统维护用户的密码只能一个人知道，每次更改密码需要将密码装入密码信封，有密码保管员存档保存。如遇特殊情况需要启用封存的密码，必须经过经理同意，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。

5、有关密码授权工作人员调离岗位，有关部门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。

1.4.数据信息安全管理制度

1、存放备份数据的介质必须具有明确的标识。备份数据必须双机备份，设置自动备份。

2、催收录音，监控录像储存时间不得少于3年。

3、任何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审批，以保证备份数据安全完整。

4、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。数据恢复过程中要严格按照数据恢复手册执行，出现问题时由技术部门进行现场技术支持。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。

5、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。

6、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。

7、非本单位技术人员对本公司的设备、系统等进行维修、维护时，必须由本公司相关技术人员现场全程监督。计算机

设备送外维修，须经设备管理机构负责人批准。送修前，需将设备存储介质内应用软件和数据等信息备份后删除，并进行登记。对修复的设备，设备维修人员应对设备进行验收、病毒检测和登记。

8、 管理部门应对报废设备中存有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。

9、运行维护部门需指定专人负责计算机病毒的防范工作，建立本单位的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。

10、用于生产计算机未经有关部门允许不准私自安装其它软件。如工作需要必须使用其它软件，需向部门负责人审批后，由相关技术人员安装正规渠道软件。

1.5.独立域控服务器

1、权限管理集中、管理成本下降

1.1、 域环境，所有网络资源，包括用户，均是在域控制器上维护，便于集中管理。所有用户只要登入到域，在域内均能进行身份验证，管理人员可以较好的管理计算机资源，管理网络的成本大大降低。

1.2、 防止公司员工在客户端随意安装软件，能够增强客户端安全性、减少客户端故障，降低维护成本。

1.3、 通过域管理可以有效的分发和指派软件、补丁等，实现网络内的一起安装，保证网络内软件的统一性。

1.4、配 合ISA的话就可以根据用户来确定可不可以上网。不然只能根据 IP。

2、安全性能加强、权限更加分明

2.1、有利于企业的一些保密资料的管理，比如说某个盘允许某个人可以读写，但另一个人就不可以读写；哪一个文件只让哪个人看；或者让某些人可以看，但不可以删/改/移等。

2.2、 可以封掉客户端的 USB 端口，防止公司机密资料的外泄。

2.3、安全性完全与活动目录(Active Directory) 集成。不仅可在目录中的每个对象上定义访问控制，而且还可在每个对象的属性上定义。活动目录(Active Directory)提供安全策略的存储和应用范围。安全策略可包含帐户信息：如域

范围内的密码限制或对特定域资源的访问权；通过组策略设置下发并执行安全策略。

3、账户漫游和文件夹重定向

3.1、个人账户的工作文件及数据等可以存储在服务器上，统一进行备份、管理，用户的数据更加安全、有保障。当客户机故障时，只需使用其他客户机安装相应软件以用户帐号登录即可，用户会发现自己的文件仍然在“原来的位置”(比如，我的文档),没有丢失，从而可以更快地进行故障修复。

3.2、 卷影副本技术可以让用户自行找回文件以前的版本或者误删除的文件(限保存过的32个版本)。在服务器离线时(故障或其他情况),“脱机文件夹”技术会自动让用户使用文件的本地缓存版本继续工作，并在注销或登录系统时与服务器上的文件同步，保证用户的工作不会被打断。

4、方便用户使用各种共享资源

4.1、 可由管理员指派登录脚本映射分布式文件系统根目录，统一管理。用户登录后就可以像使用本地盘符一样，使用网络上的资源，且不需再次输入密码，用户也只需记住一对用户名/密码即可。

4.2、 各种资源的访问、读取、修改权限均可设置，不同的账户可以有不同的访问权限。即使资源位置改变，用户也不需任何操作，只需管理员修改链接指向并设置相关权限即

可，用户甚至不会意识到资源位置的改变，不用像从前那样，

必须记住哪些资源在哪台服务器上。

5、SMS 系统管理服务 (System Management Server)

通过能够分发应用程序、系统补丁等，用户可以选择安装，也可以由系统管理员指派自动安装。并能集中管理系统补丁（如 Windows Updates),不需每台客户端服务器都下载同样的补丁，从而节省大量网络带宽。

6、灵活的查询机制

用户和管理员可使用“开始”菜单、“网上邻居”或″Active Directory 用户和计算机”上的“搜索”命令，通过对象属性快速查找网络上的对象。例如，您可通过名字、姓氏、电子 邮件名、办公室位置或用户帐户的其他属性来查找用户。通过使用全局编录来优化查找信息。

7、扩展性能较好

WIN2K 的活动目录具有很强的可扩展性，管理员可以在计划中增加新的对象类，或者给现有的对象类增加新的属性。计划包括可以存储在目录中的每一个对象类的定义和对象类的属性。

8、方便在 MS 软件方面集成

如 ISA、Exchange、Team Foundation Server、SharePoint、SQL Server 等。

第二章网络传输安全管理制度

第一条、公司网络的安全管理，应当保障网络系统设备和配套设施的安全，保障信息的安全，保障运行环境的安全。

第二条、任何单位和个人不得从事下列危害公司网络安全的活动：

1、任何单位或者个人利用公司网络从事危害公司计算机网络及信息系统的安全。

2、对于公司网络主结点设备、光缆、网线布线设施，以任何理由破坏、挪用、改动。

3、未经允许，对信息网络功能进行删除、修改或增加。

4、未经允许，对计算机信息网络中的共享文件和存储、处理或传输的数据和应用程序进行删除、修改或增加。

5、故意制作、传播计算机病毒等破坏性程序。

6、利用公司网络，访问带有“黄、赌、毒”、反动言论内容的网站。

7、 向其它非本单位用户透露公司网络登录用户名和密码。

8、其他危害信息网络安全的行为。

第三条、各单位信息管理部门负责本单位网络的安全和信息安全工作，对本单位单位所属计算机网络的运行进行巡

检，发现问题及时上报信息中心。

第四条、连入公司网络的用户必须在其本机上安装防病

毒软件， 一经发现个人计算机由感染病毒等原因影响到整体网络安全，信息中心将立即停止该用户使用公司网络，待其计算机系统安全之后方予开通。

第五条、严禁利用公司网络私自对外提供互联网络接入服务， 一经发现立即停止该用户的使用权。

第六条、对网络病毒或其他原因影响整体网络安全的子网，信息中心对其提供指导，必要时可以中断其与骨干网的连接，待子网恢复正常后再恢复连接。

2.1.网络安全

1、生产和作业网络均部署单独VLAN并部署相关防火墙策略且断开和互联网的连接。

2、存放服务商敏感数据均部署单独VLAN并部署相关防火墙策略且断开和互联网的连接，防止数据外泄。

3、 已通过防火墙策略关闭所有外部开放端口，只开放生产必须端口。

4、 已安装监控和端口监听系统及 syslog 日志审计系统，对各网络和硬件设备进行监控和监听，并按时对机房物理设备进行巡检。

2.2.应用安全

1、对生产PC统一部署杀毒软件，实际病毒的查杀和监控。定期自动更新病毒库和制定查杀策略。

2、购买并部署杀毒软件同时部署相关策略。

3、针对敏感数据终端设备，封锁必要的网络传输端口，禁止安装传输软件。

2.3.系统漏洞扫描与安全加固

1、身份鉴别

1.1、 密码安全策略

要求：操作系统和数据库系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

目的：设置有效的密码策略，防止攻击者破解出密码。

操作步骤：

【位置】开始—管理工具—本地安全策略—帐户策略—密码策略，加固设置为下图所示：

策略 ▲	安全设置
密码必须符合复杂性要求	已启用
密码长度最小值	8个字符
密码最短使用期限	2 天
密码最长使用期限	90 天
强制密码历史	5个记住的密码

010

用可还原的加密来储存密码已禁用

1.2、 帐号锁定策略

要求：应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

目的：遭遇密码破解时，暂时锁定帐号，降低密码被猜解