ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

T/

团 体 标 准

T/XXX XXXX—XXXX

计算机程序运行维护管理系统技术规范

Technical specifications for computer program operation and maintenance management system

草案版次选择

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

全国城市工业品贸易中心联合会 发 布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　一般要求 1
5　运行操作管理 2
6　运行维护管理 2
7　安全机制保障 3

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

计算机程序运行维护管理系统技术规范

1 范围

本文件规定了计算机程序运行维护管理系统技术规范的术语和定义、一般要求、运行操作管理、运行维护管理、安全机制保障。

本文件适用于计算机程序运行维护管理系统技术规范。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语和定义

本文件没有需要界定的术语和定义。

4 一般要求

4.1 系统用户管理

4.1.1 系统用户由数据服务部负责人指定，授权应以满足其工作需要的最小权限为原则。

4.1.2 系统用户应接受审计。对重要信息系统的系统用户，应进行人员的严格审查，符合要求的人员才能给予授权。

4.1.3 系统用户责任到个人，不应以部门或组作为责任人。

4.1.4 在关键信息系统中，对系统用户的授权操作，必须有两人在场，并经双重认可后方可操作，操作过程应自动产生不可更改的审计日志。

4.2 普通用户管理

4.2.1 普通用户应保护好口令（密码）等身份鉴别信息，发现系统的漏洞、滥用或违背安全行为时应及时报告。

4.2.2 不应透露与组织机构有关的非公开信息。

4.2.3 普通用户不应故意进行违规的操作，以及在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息。

4.2.4 不应使用各种非正版软件和不可信的自由软件。

4.2.5 普通用户只能在系统规定的权限内进行操作，必要时某些重要操作应得到批准。

4.3 机构外部用户管理

4.3.1 数据服务部在分配机构外部用户管理权限时，应对机构外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明。外部用户只能是应用层的用户。

4.3.2 机构外部用户可对特定外部用户提供专用通信通道、端口、特定的应用或数据协议、以及专用设备等。在关键部位，一般不允许设置外部用户。

4.4 临时用户管理

4.4.1 临时用户的设置和期限必须经过数据服务部负责人的审批，使用完毕或到期应及时删除，设置与删除均应记录备案。

4.4.2 管理人员应对主要部位的临时用户应进行审计，并在删除前进行风险评估。在关键部位，一般不允许设置临时用户。

5 运行操作管理

5.1 服务器操作管理

对服务器的操作应由授权的系统管理员实施，并按操作规程执行服务器的启动/停止、加电/断电等操作，以及身份鉴别管理。

5.2 终端计算机操作管理

5.2.1 用户在使用自己的终端计算机时，应设置开机、屏幕保护、目录共享口令。

5.2.2 非组织机构配备的终端计算机未获批准，不能在办公场所使用。

5.2.3 用户应及时安装经过许可的软件和补丁程序，不得自行安装及使用其它软件和自由下载软件。

5.2.4 未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其它网络。

5.3 便携机操作管理

5.3.1 便携机需设置开机口令和屏保口令。因工作岗位变动不再需要使用便携机时，应及时办理资产转移或清退手续，并删除机内的敏感数据。

5.3.2 在本地网络工作时应按终端计算机的要求执行。

5.4 网络及安全设备操作管理

对网络及安全设备的操作应由授权的系统管理员实施。授权的系统管理员应按操作规程进行网络设备和安全设备的接入/断开、启动/停止、加电/断电等操作，维护网络和安全设备的运行环境、配置和服务设定，对实施网络及安全设备操作的管理员应进行身份鉴别。

5.5 变更控制和重用管理

5.5.1 任何变更控制和设备重用必须经过申报和审批才能进行，同时还有以下要求：

a) 注意识别重大变更，并进行记录；
b) 评估这些变更的潜在影响；向所有相关人员通报变更细节；
c) 明确中止变更并从失败的变更中恢复的责任和处理方法；
d) 重用设备中原有信息的清除。

5.5.2 数据服务部应形成书面规定，以对操作系统、数据库、应用系统、人员、服务等的变更进行标准控制。信息系统的任何变更都必须考虑全面的安全性。

5.6 信息交换管理

5.6.1 在公众网站、内部网站发布的信息，以及提供查询的信息应符合国家有关政策法规的规定。

5.6.2 对所公布的信息应采取适当的安全措施，以保护其完整性。

5.6.3 应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的情况发生。

6 运行维护管理

6.1 运行维护管理内容

运行维护管理包括四个方面：

a) 日常运行安全管理；
b) 运行状况监控；
c) 软件硬件维护管理；
d) 外部服务方访问管理。

6.2 日常运行安全管理

6.2.1 数据服务部应通过正式授权程序委派专人负责系统运行的安全管理。

6.2.2 建立运行值班等有关安全规章制度。

6.2.3 正确实施为信息系统可靠运行而采取的各种检测、监控、审计、分析、备份及容错等方法和措施。

6.2.4 定期对运行安全进行监督检查。

6.2.5 明确各个岗位人员对信息系统各类资源的安全责任，明确信息系统安全管理人员和普通用户对信息系统资源的访问权限。

6.2.6 按风险管理计划和操作规程定期对信息系统的运行进行风险分析与评估，并向管理层提交正式的风险分析报告。

6.3 运行状况监控

6.3.1 所有的系统日志应保留一定期限，日志不能更改，只允许授权用户访问。

6.3.2 日志应有脱机保存的介质。

6.3.3 信息系统应使用统一的时间，以确保记录日志准确。

6.3.4 定期清理日志，并形成日志清理报告。

6.3.5 审计日志须经数据服务部负责人授权方可查阅，并告知用户某些行为会被审计。

6.4 软件硬件维护管理

6.4.1 由数据服务部明确信息系统的软件、硬件维护的人员和责任，规定维护的时限，以及设备更新和替换的办法。

6.4.2 制定有关软件、硬件维修的制度。

6.4.3 对需要外出维修的设备，应经过综合部、数据服务部审批，磁盘数据应进行删除。

6.4.4 外部维修人员进入机房维修，应经过综合部审批，并有数据服务部专人负责陪同。

6.5 外部服务方访问管理

6.5.1 对外部服务方访问的要求，应经过总经理审批，由数据服务部备案。

6.5.2 由数据服务部主导，必要时综合部协助，对外部服务方访问建立相应的安全管理制度。

6.5.3 外部服务方访问应签署保密合同。

6.5.4 数据服务部应对外部服务方访问进行风险分析和评估。

6.5.5 对外部服务方访问实施严格控制，必要时实施监视。

7 安全机制保障

7.1 身份鉴别机制管理

7.1.1 对网络、操作系统、数据库系统等系统管理员和应用系统管理员以及普通用户，应明确使用和保护身份鉴别机制的责任，采用不可伪造的鉴别信息进行身份鉴别，采用有关身份鉴别和认证系统的管理维护措施。

7.1.2 应指定安全管理人员定期进行检查，鉴别信息应进行相应的保护。

7.2 访问控制机制管理

7.2.1 应根据自主访问控制机制的要求，由授权用户为主、客体设置相应访问的参数。

7.2.2 应将自主访问控制与审计密切结合，实现对自主访问控制过程的审计，使访问者为自己的行为负责，并保证最高管理层对自主访问控制管理的掌握。

7.3 系统安全管理

7.3.1 应对操作系统和数据库管理系统按其安全技术和机制的不同要求实施相应的安全管理。

7.3.2 数据服务部应通过正式授权程序委派专人负责系统安全管理。

7.3.3 建立系统安全配置、备份等安全管理规章制度，按规章制度的要求及时进行补丁升级。

7.3.4 严格按照要求进行日常安全管理，包括对用户安全使用进行指导和审计等。

7.3.5 应根据访问控制安全策略的要求，全面考虑和统一设置、维护用户及主、客体的标记信息。