ICS
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/XXX XXXX—XXXX

采购计划管理系统技术规范

Technical Specifications for Procurement Plan Management System

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

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。

本文件由全国城市工业品贸易中心联合会归口。

本文件主要起草单位：

本文件主要起草人：

采购计划管理系统技术规范

1 范围

本文件规定了采购计划管理系统技术规范的术语和定义、功能要求、安全要求、性能要去、运维要求、系统验收。

本文件适用于采购计划管理系统。

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。

GB 17859 计算机信息系统 安全保护等级划分准则

GB/T 21052 信息安全技术 信息系统物理安全技术要求

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25000.10系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第10部分：系统与软件质量模型

GB/T 28452 信息安全技术 应用软件系统通用安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

采购计划 Procurement Plan

采购计划是指企业管理人员在了解市场供求情况，认识企业生产经营活动过程中和掌握物料消耗规律的基础上，对计划期内物料采购管理活动所做的预见性的安排和部署。

4 功能要求

4.1 供应商管理

4.1.1 供应商信息管理

系统应能记录和管理供应商的基本信息、组织信息、联系信息、法律信息、财务信息、沟通记录、机会信息、成本信息、产品与服务信息、合约与订单信息等。

4.1.2 供应商资格审核

系统应提供供应商资格审核框架，确保新加入的供应商符合企业的要求。

4.1.3 供应商分类管理

系统应能根据供应商的资格审核状态及绩效，将其归入不同的分类，如尚未进行资格审核、合资格、不合资格、黑名单、高满意度等。

4.2 采购计划管理：

4.2.1 采购计划制定

系统应支持各部门根据各自的费用类别制定采购计划。

4.2.2 采购计划执行

系统应能管理采购完成率并跟踪偏差，同时在整个采购计划和执行过程中提供预警。

4.2.3 采购需求管理

系统应能实现对采购需求的全流程管理，包括采购需求的申请、审批、采购计划的编制和执行情况的跟踪等功能。

4.3 采购订单管理

4.3.1 采购订单生成

系统应能自动生成采购订单，并支持订单的审批、变更和撤销等操作。

4.3.2 采购订单跟踪

系统应能实时监控采购订单的执行情况，确保采购订单的及时执行和供货。

4.4 采购合同管理

4.4.1 系统应对采购合同的签订、履行进行全程跟踪和管理，支持合同台账的建立和合同履行情况的监管。

4.4.2 系统应能提醒合同履行的相关人员关键节点的到来，避免合同漏审、漏执行等风险。

4.5 库存管理

4.5.1 物资入库管理

系统应对采购物资进行入库登记和管理，确保物资信息的准确性和库存的实时监控。

4.5.2 库存跟踪与控制

系统应能实时跟踪物资的采购、配送和入库情况，自动化地计算物资的安全库存、订货点等指标，为企业提供准确的库存控制和管理。

4.6 采购成本管理

4.6.1 系统应对采购成本进行核算和分析，帮助企业控制采购成本，提高采购效率。

4.6.2 系统应支持采购费用的预算、报销和核算等管理，实现采购费用的规范化和透明化。

4.7 报表与分析

4.7.1 系统应能生成各类采购数据报表，为管理决策提供数据支持和依据。

4.7.2 系统应对采购数据进行分析，以发现成本波动的规律和节约成本的空间。

注：特殊采购的特点也需要考虑，如灵活性高、采购成本高和风险较高等。

5 安全要求

5.1 身份安全要求

5.1.1 应具有机密性，可采用对称和非对称加密技术，确保敏感信息不被窃取。

5.1.2 应具有完整性，可采用数字摘要确保身份信息不被篡改。

5.1.3 应具有真实性，身份鉴别可采用数字证书确保身份真实性。

5.1.4 应具有不可抵赖性，可采用数字签名确保数据发送方不可否认自己的信息。

5.2 网络传输安全

5.2.1 应在参与联盟链的节点之间建立安全传输通道，保证数据传输的完整性和不可篡改性。

5.2.2 应对数据和信息采取相应的防护措施，保证其能抵抗篡改、重放等主动或被动攻击。

5.2.3 应保证节点间通信过程中敏感信息字段或整个报文的保密性，宜采用密码学技术。

5.2.4 应确保信息在存储、传输过程中不被非授权用户读取和篡改，可采用有权限的网络访问控制，在参与分布式账本节点之间构建虚拟专用网络（VPN），降低网络攻击造成的危害。

5.3 物理安全

应符合GB/T 21052的要求。场地安全部署物理数据中心及附属设施的，用于业务运行、数据存储和处理的物理设备需符合国家监管要求。

5.4 节点部署安全

5.4.1 应保证承担共识的节点冗余部署，保证系统可用性；避免将所有承担共识的节点部署在同一机房内，能在单一机房节点不可用时保证系统整体的可用性。

5.4.2 确保部署节点的硬件设备存储容量可扩展，避免因数据容量达到上限而无法同步数据。

5.5 硬件设备

5.5.1 应对设备运行状态、资源使用情况等进行监控，能在发生异常时发出告警。

5.5.2 设备和存储介质在重用、报废或更换时，能对其承载的数据进行清除且不可恢复。

6 性能要求

6.1 安全性

安全性技术要求如下:

——应符合 GB/T 28452 中应用软件系统安全技术要求第三级及以上要求；

——不应存在隐蔽接口,不应加载能够禁用安全机制或绕过安全机制的组件；

——应在用户明示同意后,方可收集用户相关信息,并在收集用户相关信息时显示提示信息；

——在软件系统维护升级更新活动中,不得侵害用户信息安全。

6.2 可靠性

可靠性技术要求如下:

——系统应支持 7×24 h 的稳定无故障运行；

——系统应支持数据有效性检验功能,保证输入的数据格式或长度符合系统设定的要求；

——对于用户“非法”的输入或操作,系统不崩溃、不退出；

——系统应支持自动保护功能,当故障发生时能自动保护当前所有状态,保证系统能够进行恢复。

6.3 易用性

技术要求如下:

——系统应提供用户使用手册,且手册中的功能描述与软件的实际功能一致；

——系统研制过程中形成的所有文档,语言简练、前后一致、易于理解以及语句无歧义；

——系统页面布局要合理,不宜过于密集或过于空旷,合理利用空间；

——系统的提示、警告或错误说明应该清楚、明了、恰当,避免歧义；

——编辑页面中的必输项应给出标识；

——对于用户非法的输入或操作，系统应给予提示信息,且提示信息能引导用户进行正确输入或操作；

——对可能造成数据无法恢复的操作,系统应给予提示信息,给用户放弃选择的机会；

——日期类型数据输入应提供日历选择功能；

——系统应支持 Ctrl+A 全选、Ctrl+C 拷贝、Ctrl+V 粘贴、Ctrl+X 剪切、Ctrl+Z 撤消等快捷操作；

——对于有多个输入框的页面,系统应支持通过 Tab 键变更光标焦点,按照从左到右、从上到下的原则。

7 运维要求

7.1 系统监控

7.1.1 应具备对系统状态实时监控的能力，包括物理服务器状态、虚拟机状态、数据库服务状态、节点同步状态等。

7.1.2 应支持自定义设置监控采集数据资料库保存时间。
7.1.3 应支持自动警告推送功能。
7.1.4 宜具备系统状态监控结果实时可视化展示的能力。

7.2 设备管理

7.2.1 加密机应放于专门区域，指定专人管理，并定期进行维护管理。
7.2.2 应采用白名单机制控制对加密机的访问，阻止非授权设备访问加密机。
7.2.3 在报废加密机前，应将加密机内的密钥完全清除，确保加密机内的密钥等敏感数据无法被恢复重用。
7.2.4 严格控制加密机的变更操作，经过审批后才可进行变更操作，并须留下变更相关的审计日志。
7.2.5 加密机以外的设备应遵循 GB/T 22239 中的相关要求。
7.2.6 对网络中的节点性能，需要根据实际承载的业务场景协商接入标准。
注：网络中节点性能指标包括CPU、内存、带宽等指标。

7.3 数据/漏洞维护管理

7.3.1 漏洞发现/修复要求

7.3.1.1 涵盖节点服务器自身漏洞、软件漏洞、智能合约漏洞等不同层次漏洞至少每月扫描一次。扫描时可合理采用第三方扫描工具。
7.3.1.2 漏洞扫描记录保持与扫描策略一致，发现漏洞及时提出修改方案并修复，对于无法修复的漏洞及时报告，如果漏洞修复影响到账本数据，则应通过共识协议进行数据的修正。系统日志留存记录，达到漏洞修复可追溯的效果。

7.3.2 数据备份/恢复要求

7.3.2.1 数据备份策略根据业务需要进行实时备份。
7.3.2.2 密钥等关键数据备份策略根据业务需要进行定期备份。
根据密钥等关键数据的恢复策略定期进行恢复演练，最近一次恢复记录表明备份数据的可用性，保证在出现重大事件时能够及时的进行数据恢复。

8 软件验收

按照GB/T 25000.10、GB 17859的规定进行验收。