ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/XXX XXXX—XXXX

企业品牌策划营销系统技术规范

Technical specifications for enterprise brand planning and marketing system

－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：

企业品牌策划营销系统技术规范

1 范围

本文件规定了企业品牌策划营销系统技术规范的术语和定义、基本要求、功能要求、性能要求、安全要求、运维要求。

本文件适用于企业品牌策划营销系统。

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/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 20273 信息安全技术 数据库管理系统安全技术要求
GB/T 20988 信息安全技术 信息系统灾难恢复规范
GB/T 28452 信息安全技术 应用软件系统通用安全技术要求
GB/T 37095 信息安全技术 办公信息系统安全基本技术要求

3 术语和定义

本文件没有需要界定的术语和定义。

4 基本要求

4.1 硬件环境

硬件环境要求如下：

——开发硬件环境：

1) CPU 主频：3.0G Hz；
2) CPU 核心数：四核心；
3) 内存容量：4 GB、8 GB；
4) 显存容量：2 GB。

——运行硬件环境：

1) CPU：Intel i7；
2) CPU 核心数：六核心；
3) CPU 主频：3.0 GHz 及以上。

4.2 软件环境

软件环境要求如下：

——操作系统：Windows 8.1 Pro 64 位操作系统；
——开发工具：eclipse；
——运行平台：Windows7/8/Linux 数据库：Sql；
——支持软件：Windows Server 2008 网络协议：TCP/IP 协议。

4.3 信息安全

符合 GB/T 37095、GB/T 20273、GB/T 20988 的相关要求。

5 功能要求

5.1 市场调研与分析

系统应具备强大的市场调研和分析功能，能够收集和分析市场数据、竞争对手信息、目标客户需求等，为品牌策划和营销活动提供数据支持。

5.2 品牌定位与策略制定

系统应能够帮助企业确定清晰的品牌定位，包括品牌形象、品牌文化、品牌价值观等，并根据市场调研结果制定有效的品牌策略。

5.3 营销计划制定与执行

系统应支持制定详细的营销计划，包括产品定价、促销策略、渠道策略、广告策略等，并能够跟踪计划的执行情况，及时调整策略以提高营销效果。

5.4 客户管理与沟通

5.4.1 系统应建立客户数据库，对客户进行分类管理，并跟踪客户的购买行为和偏好。
5.4.2 系统应支持通过多种渠道与客户进行沟通和互动，如短信、邮件、社交媒体等，以提高客户满意度和忠诚度。

5.5 销售管理与跟踪

5.5.1 系统应对销售过程进行管理和跟踪，包括建立销售线索、跟进客户、提供报价和合同管理等。
5.5.2 系统应能够分析销售数据，提供销售趋势、业绩评估、销售预测等信息，为制定销售策略提供参考。

5.6 营销效果评估与优化

5.6.1 系统应对营销活动的效果进行评估，包括销售额、市场份额、客户满意度等指标。
5.6.2 系统应能根据评估结果，提出优化建议，以改进品牌策划和营销活动的效果。

5.7 团队协作与项目管理

5.7.1 系统应支持团队协作和项目管理功能，确保团队成员能够高效地协作完成品牌策划和营销活动。
5.7.2 系统应提供任务分配、进度跟踪、成果展示等功能，以便团队成员及时了解项目进展和完成情况。

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 安全要求

7.1 物理安全

7.1.1 确保服务器和数据中心位于安全的环境中，有适当的访问控制和物理防护措施。
7.1.2 使用防盗报警系统、视频监控和门禁系统来监控和记录物理访问。

7.2 网络安全

7.2.1 实施防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）来抵御网络攻击。
7.2.2 定期更新和修补网络设备和应用程序的安全漏洞。
7.2.3 部署网络隔离和访问控制策略，限制对系统的非法访问。

7.3 系统安全

7.3.1 使用强密码策略，并定期更换系统密码。
7.3.2 限制系统管理员的访问权限，并遵循最小权限原则。
7.3.3 实施定期的安全审计和日志审查，以检测异常行为。

7.4 数据安全

7.4.1 使用加密技术（如 TLS/SSL）来保护数据传输过程中的机密性。
7.4.2 在数据库中实施数据加密，保护敏感信息的存储。
7.4.3 遵循数据备份和恢复策略，确保数据的可靠性和可恢复性。

7.5 访问控制

7.5.1 实施基于角色的访问控制（RBAC），确保用户只能访问其所需的数据和功能。
7.5.2 使用多因素身份验证（MFA）来提高用户登录的安全性。
7.5.3 定期审计和审查用户账户和权限，删除不再需要的账户和权限。

7.6 灾难恢复和业务连续性

7.6.1 部署灾难恢复计划，确保在发生灾难时能够迅速恢复系统的正常运行。
7.6.2 实施备份和恢复策略，包括定期备份数据和关键系统组件。
7.6.3 测试灾难恢复计划的有效性，并定期进行更新和修订。

8 运维要求

8.1 系统监控

8.1.1 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。

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

8.2 设备管理

8.2.1 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。
8.2.2 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。
8.2.3 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。
8.2.4 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。
8.2.5 加密机以外的设备应遵循 GB/T 22239 中的相关要求。
8.2.6 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。

8.3 数据/漏洞维护管理

8.3.1 漏洞发现/修复要求

8.3.1.1 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。
8.3.1.2 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。

8.3.2 数据备份/恢复要求

8.3.2.1 数据备份策略根据业务需要进行实时备份。
8.3.2.2 密钥等关键数据备份策略根据业务需要进行定期备份。
8.3.2.3 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。