

T/ACCEM

团 体 标 准

T/ACCEM XXXX—XXXX

数字化日结薪酬管理系统技术要求

Technical Requirements for the Digital Daily Settlement Salary Management System

（征求意见稿）

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

中国商业企业管理协会 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 系统架构 1

5 系统功能要求 1

6 系统性能要求 2

7 系统安全要求 3

8 数据管理 3

9 系统兼容性要求 4

10 系统维护与支持要求 4

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。

本文件由重庆辉烨人力资源管理有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：重庆辉烨人力资源管理有限公司。

本文件主要起草人：

数字化日结薪酬管理系统技术要求

1 范围

本文件规定了数字化日结薪酬管理系统的系统架构、系统功能要求、系统性能要求、系统安全要求、数据管理、系统兼容性要求、系统维护与支持要求。

本文件适用于数字化日结薪酬管理系统技术要求。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

日结薪酬

以日为单位进行薪酬结算的支付方式，员工每日工作结束后，依据当天的工作时长、工作成果等因素核算并发放薪酬。

4 系统架构

4.1 总体架构

采用模块化分层架构，分为表现层、业务逻辑层、数据访问层和基础设施层。各层相互协作，实现系统的各项功能。表现层负责与用户交互，提供操作界面；业务逻辑层处理核心业务；数据访问层管理数据存储与查询；基础设施层提供基础支撑。

4.2 系统模块

4.2.1 合同生成模块：基于预设规则和算法生成薪酬计算方案。包括数据采集子模块（获取工作时长、任务量等数据）和计算生成子模块（根据薪酬标准计算薪酬）。

4.2.2 签署验证模块：对薪酬发放进行验证和处理。包含下发子模块（向财务等相关部门发送薪酬信息）、审核子模块（审核薪酬数据准确性）和发放子模块（执行薪酬发放操作）。

4.2.3 加密验证模块：保障数据和支付安全。由加密处理子模块（对薪酬数据加密）、密钥管理子模块（生成和管理密钥）以及安全校验子模块（验证支付安全和用户身份）组成。

4.2.4 存储管理模块：存储和管理薪酬数据。分为存储子模块（采用分布式存储技术存储数据）和管理子模块（管理数据访问权限，验证访问人员身份）。

4.3 模块连接关系

合同生成模块生成薪酬数据后，传递给签署验证模块；签署验证模块审核通过后，将数据交给加密验证模块加密处理；加密验证模块处理完成后，数据进入存储管理模块存储；各模块间通过内部接口进行数据交互，确保数据传输准确、高效。

5 系统功能要求

5.1 员工信息管理

5.1.1 信息录入：支持批量导入和单个录入员工基本信息，涵盖姓名、身份证号、联系方式、银行账号等，同时关联员工所属项目、工种等信息。

5.1.2 信息更新：员工信息变更时，可实时更新，确保数据准确及时。

- 5.1.3 信息查询与筛选：能依据多种条件（如姓名、身份证号、项目等）快速查询和筛选员工信息，便于管理人员进行数据统计与分析。
- 5.2 考勤管理
 - 5.2.1 考勤记录采集：对接多种考勤设备或考勤软件，自动采集员工上下班打卡时间、加班时长等考勤数据，确保数据准确完整。
 - 5.2.2 考勤异常处理：自动标记迟到、早退、旷工等考勤异常情况，提供异常原因录入和审核功能，保证考勤数据合规。
 - 5.2.3 考勤统计分析：按日、周、月等周期生成考勤报表，统计员工出勤天数、加班时长、缺勤情况等，为薪酬核算提供数据支持。
- 5.3 薪酬核算管理
 - 5.3.1 薪酬规则设定：根据不同工种、项目，设置薪酬计算规则，包括基本工资、加班工资、奖金、补贴等计算方式，支持设置扣款项，如社保代扣、罚款等。
 - 5.3.2 自动核算：依据考勤数据和薪酬规则，自动计算员工日结薪酬，生成薪酬明细，确保薪酬核算准确高效。
 - 5.3.3 薪酬审核：提供薪酬审核功能，审核人员可查看薪酬明细，标记和调整异常数据，审核通过后才能发放薪酬。
- 5.4 薪酬发放管理
 - 5.4.1 发放渠道对接：支持与主流银行、第三方支付平台对接，实现薪酬批量发放，确保发放及时准确。
 - 5.4.2 发放记录管理：详细记录每笔薪酬发放的时间、金额、发放渠道、员工接收状态等信息，便于查询追溯。
 - 5.4.3 发放异常处理：自动提醒薪酬发放失败情况，提供重新发放和原因查询功能，确保员工及时收到薪酬。
- 5.5 报表管理
 - 5.5.1 薪酬报表生成：生成各类薪酬报表，如日结薪酬报表、月度薪酬汇总表、项目薪酬成本报表等，报表格式支持自定义，满足不同管理需求。
 - 5.5.2 数据导出：支持将报表数据导出为 Excel、PDF 等常见格式，方便与其他系统进行数据交互或深度数据分析。
 - 5.5.3 报表权限管理：根据用户角色设置报表查看权限，保障敏感数据安全。
- 5.6 系统管理
 - 5.6.1 用户管理：管理系统用户，包括添加、删除、修改用户信息，分配用户角色和权限，确保系统操作安全合规。
 - 5.6.2 角色与权限管理：定义不同角色（如管理员、财务人员、项目负责人等）的操作权限，实现精细化权限控制，防止越权操作。
 - 5.6.3 数据备份与恢复：定期对系统数据进行备份，保障数据安全可恢复。数据异常时，能快速恢复操作。

6 系统性能要求

6.1 响应时间

系统操作响应时间控制在 3 s 以内，确保用户快速获取操作结果，提高工作效率。高并发情况下（如薪酬核算、批量发放时），响应时间也应在可接受范围内，不影响系统正常使用。

6.2 吞吐量

系统支持至少 1 000 个用户同时在线操作，满足企业不同规模使用需求。高并发场景下，系统稳定处理数据，不出现卡顿、崩溃等情况。

6.3 准确性

薪酬核算准确率达 99.9% 以上，确保员工薪酬计算准确，避免薪酬错误引发纠纷。数据存储和传输过程中，保证数据完整一致，防止数据丢失或错误。

6.4 可靠性

系统具备 7×24 h 不间断运行能力，年故障停机时间不超过 24 h，确保薪酬管理工作连续。系统具备容错能力，部分组件故障时，能自动切换或降级运行，保证关键功能可用。

7 系统安全要求

7.1 数据加密

对系统中的敏感数据（如员工身份证号、银行账号、薪酬数据等）进行加密存储和传输，防止数据泄露。采用行业标准加密算法（如 AES、RSA 等），保障数据安全。加密强度不低于 128 位。

7.2 身份认证与授权

采用多因素身份认证方式（如用户名 + 密码 + 验证码），确保用户身份真实。严格授权管理，根据用户角色和权限控制对系统功能和数据的访问，防止未经授权的访问和操作。密码复杂度要求为至少 8 位，包含数字、字母和特殊字符，且定期更换。

7.3 访问控制

设置防火墙，阻止外部非法网络访问。监控和审计内部网络访问，记录用户操作行为，及时发现和处理异常访问行为。防火墙具备至少 10 种安全防护策略，审计日志保存期限不少于 3 年。

7.4 数据备份与恢复

定期对系统数据进行异地备份，备份数据保存期限不少于 5 年。制定完善的数据恢复计划和流程，确保数据丢失或损坏时能快速恢复，保证业务连续性。数据恢复成功率不低于 99%。

7.5 安全审计

系统具备安全审计功能，记录系统操作日志，包括用户登录、数据修改、薪酬发放等操作。审计日志保存不少于 3 年，方便事后安全分析和追溯。审计日志记录详细程度应包含操作时间、操作人、操作内容、操作结果等信息。

8 数据管理

8.1 数据分类与存储

8.1.1 对薪酬管理系统涉及的数据进行分类管理，主要包括用户数据、任务数据、薪酬数据、支付数据、税务数据、系统日志数据等。不同类型的数据应采用合适的存储方式进行存储，如关系型数据库、非关系型数据库、文件系统等。

8.1.2 用户数据应包括企业用户和用工人员用户的基本信息、身份信息、联系方式、账户信息、权限信息等，应存储在安全可靠的数据库中，并进行加密处理，保障用户信息安全。

8.1.3 任务数据应包括任务发布信息、任务执行信息、任务完成情况信息等，可根据任务的特点和查询需求选择合适的存储方式。薪酬数据应详细记录薪酬计算的过程和结果，包括各项薪酬组成部分的计算明细、应发薪酬、实发薪酬、代扣税费等信息，存储在关系型数据库中，便于进行财务核算和数据分析。

8.1.4 支付数据应记录每一笔支付交易的详细信息，包括支付订单号、支付金额、支付时间、支付对象、支付渠道、支付状态等，存储在支付管理相关的数据库表中，并与薪酬数据进行关联。税务数据应包括税务计算规则、税务申报信息、税务缴纳记录等，存储在税务管理相关的数据库表中。系统日志数

据应记录系统运行过程中的各类操作日志、异常日志等，采用文件系统或日志管理数据库进行存储，便于进行系统运维和问题排查。

8.2 数据备份与恢复

8.2.1 制定完善的数据备份策略，定期对系统中的重要数据进行备份，备份频率应根据数据的重要性和变化频率进行合理设置，如每日备份、每周备份等。数据备份应采用多种备份方式相结合，如全量备份、增量备份、差异备份等，确保数据的完整性和可恢复性。

8.2.2 备份数据应存储在异地安全的存储设备中，防止因本地灾难（如火灾、地震、硬件故障等）导致数据丢失。同时，应定期对备份数据进行恢复测试，确保备份数据的可用性和完整性。当系统出现数据丢失或损坏时，能够及时从备份数据中进行恢复，保障系统的正常运行和业务的连续性。

8.3 数据安全性与隐私保护

8.3.1 加强数据安全防护，采用数据加密技术对敏感数据进行加密存储和传输，如用户的身份证号、银行卡号、密码等信息。在数据存储环节，使用数据库加密技术对存储在数据库中的敏感数据进行加密；在数据传输环节，采用 SSL/TLS 等加密协议对数据进行加密传输，防止数据在传输过程中被窃取或篡改。

8.3.2 建立严格的数据访问控制机制，根据用户的角色和权限，对系统中的数据进行访问授权。只有经过授权的用户才能访问和操作相应的数据，防止未经授权的数据访问和滥用。同时，对用户的数据操作行为进行审计和记录，便于追溯和发现潜在的数据安全问题。

8.3.3 尊重用户的隐私，严格遵守相关法律法规和隐私政策，不得将用户数据用于未经用户同意的其他用途。在数据收集、使用和共享过程中，应向用户明确告知数据的使用目的、方式和范围，并获得用户的明确同意。对涉及用户隐私的数据进行严格管理和保护，防止数据泄露对用户造成不良影响。

9 系统兼容性要求

9.1 操作系统兼容性

系统兼容主流操作系统，包括 Windows 7 及以上版本、Linux、Mac OS 等，确保不同操作系统用户正常使用系统。在不同操作系统下，系统功能的兼容性测试通过率不低于 99%。

9.2 浏览器兼容性

支持主流浏览器，如 Chrome、Firefox、Edge、Safari 等，确保在不同浏览器上系统功能正常，页面显示完整。在不同浏览器下，页面布局差异不超过 5%。

9.3 移动设备兼容性

系统具备良好的移动设备兼容性，支持在手机和平板上通过浏览器或移动应用进行访问和操作，满足用户随时随地管理薪酬的需求。移动应用的适配分辨率不少于 5 种常见尺寸，操作响应时间不超过 2 s。

10 系统维护与支持要求

10.1 维护服务

供应商提供至少 3 年的免费维护服务，包括系统升级、漏洞修复、故障排除等。维护期内，及时响应企业技术支持请求，确保系统正常运行。紧急问题响应时间不超过 1 h，一般问题响应时间不超过 4 h。

10.2 技术支持

供应商提供 7×24 h 的技术支持服务，通过电话、邮件、在线客服等方式为企业提供技术咨询和问题解决服务。技术支持人员的专业资质认证率不低于 80%。

10.3 培训服务

供应商提供系统使用培训服务，包括操作培训、维护培训等，确保企业员工熟练使用系统。培训方式可采用线上培训、线下培训或现场指导等，满足企业不同培训需求。培训覆盖率不低于 95%，培训后员工操作熟练程度测试通过率不低于 90%。
