ICS 03.040
CCS A 10

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXX—XXXX

灵活用工实时薪酬发放技术规范

Technical Specification for Real-time Salary Distribution in Flexible Employment

（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

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：

灵活用工实时薪酬发放技术规范

1 范围

本文件规定了灵活用工实时薪酬发放的总体要求、薪酬发放方法、系统要求、数据管理、安全与隐私保护。

本文件适用于灵活用工实时薪酬发放技术规范。

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

灵活用工 flexible employment

区别于传统固定用工模式，企业基于用人需求的波峰波谷，灵活地按需雇佣人才，双方不建立正式的全职劳动关系的一种用工形式。包括但不限于兼职、非全日制用工、劳务派遣、业务外包、平台用工等。

3.2

实时薪酬发放 real-time salary distribution

在灵活用工人员完成工作任务或达到约定的薪酬结算节点后，能在极短时间内将应得薪酬支付到其指定账户的过程。

3.3

无卡发薪 salary payment without a bank card

无需劳动者提供银行卡号，通过其他电子支付渠道（如微信、支付宝等）实现薪酬发放的方式。

4 总体要求

4.1 合规性

灵活用工实时薪酬发放系统应严格遵守国家相关法律法规，包括但不限于劳动法律法规、税收法律法规、金融支付监管规定等，保障灵活用工人员的合法权益，确保薪酬发放过程中的税务合规和支付合规。

4.2 准确性

系统应确保薪酬计算的准确性，根据灵活用工人员的工作时长、工作任务完成情况、薪酬标准等信息，精确计算应发薪酬。同时，保证薪酬发放金额、发放对象、发放时间等信息的准确无误，避免出现错发、漏发等情况。

4.3 及时性

实现实时或准实时的薪酬发放，在灵活用工人员完成工作符合结算条件后，尽快将薪酬支付到其账户，满足灵活用工人员对资金及时性的需求。

4.4 安全性

建立完善的安全防护体系，保障系统运行安全、数据安全以及资金安全。防止数据泄露、篡改、丢失，防范支付风险和网络攻击，确保薪酬发放业务的稳定运行。

4.5 可扩展性

系统架构应具备良好的可扩展性，能够适应灵活用工业务规模的增长、业务模式的变化以及新功能的添加。便于与企业其他信息系统、第三方支付机构系统、税务系统等进行对接和集成。

5 薪酬发放方法

5.1 员工信息与考勤管理

5.1.1 企业应建立完善的员工信息录入模块，准确录入灵活用工人员的基本信息，包括姓名、身份证号、联系方式、银行账户信息（如有）、薪酬计算标准等。

5.1.2 采用可靠的考勤模块对员工实际考勤情况进行实时记录，如通过打卡设备、移动应用程序等方式记录员工的工作起始时间、结束时间、工作时长、工作任务完成情况等信息，并将考勤数据及时传输至员工考勤统计模块。

5.1.3 员工考勤统计模块对考勤数据进行汇总、分析和统计，生成员工考勤统计表，为薪酬计算提供准确依据。

5.2 薪酬计算与记录

5.2.1 根据员工考勤统计表以及预先设定的薪酬计算标准，计算每一位员工的工资情况，包括基本工资、加班工资、绩效奖金、补贴等各项薪酬组成部分。

5.2.2 重复上述操作，完成所有员工的薪酬计算，并根据计算结果制作员工薪资记录表，薪资记录表应包含员工姓名、工号、薪酬明细、应发薪酬、实发薪酬等详细信息。

5.3 薪酬确认与发放

5.3.1 将薪资记录表内的员工薪酬信息对应发送至员工手机等终端设备，通过短信、应用程序推送等方式让员工确认薪酬是否有误。

5.3.2 当员工确认薪酬无误后，系统应及时向员工发放薪酬。如采用无卡发薪方式，通过与微信支付、支付宝等第三方支付平台对接，将薪酬发放至员工的微信钱包、支付宝账户等。若员工对薪酬有异议，可通过指定渠道反馈，企业应及时核实并更改薪资记录表内的有误信息，重新计算薪酬后再次发送确认。

5.3.3 在薪酬发放后，系统应及时收集员工薪酬的到账情况，可通过支付平台的反馈信息、银行对账等方式获取到账数据，并根据到账情况制作薪酬发放表，薪酬发放表应记录发放时间、发放金额、员工到账状态等信息。

5.4 薪酬发放表存储与查询

对每月制作的薪酬发放表进行统一存储，可采用数据库、文件存储系统等方式进行存储。存储的数据应便于实时查询员工薪酬的发放情况，企业管理人员、财务人员以及员工本人在授权范围内可随时查询薪酬发放记录。

6 系统要求

6.1 考勤子系统

应具备员工信息录入功能，支持多种信息录入方式；能够准确记录员工考勤数据，并及时传输至其他相关模块；具备数据备份和恢复功能，确保考勤数据的安全性和完整性。

6.2 薪酬计算子系统

应包含薪资计算模块和薪资记录模块。薪资计算模块应能根据预设的计算规则准确计算薪酬，支持多种薪酬计算方式；薪资记录模块应能高效存储和管理薪资计算结果，生成规范的薪资记录表。

6.3 发薪子系统

应由确认模块、支付模块和反馈模块组成。确认模块负责将薪酬信息发送给员工确认；支付模块支持多种支付渠道，确保薪酬准确、及时发放；反馈模块能及时收集薪酬到账信息，并反馈给存储子系统。

6.4 存储子系统

应具备强大的数据存储能力，能够存储大量的薪酬发放表等数据；提供高效的数据查询接口，满足不同人员的查询需求；具备数据加密和访问控制功能，保障数据安全。

7 数据管理

7.1 数据准确性

确保员工信息、考勤数据、薪酬计算标准、薪酬发放记录等数据的准确性，在数据录入、传输、计算等过程中应进行严格的数据校验和审核。

7.2 数据完整性

保证数据的完整性，防止数据丢失或损坏。对重要数据应进行定期备份，备份数据应存储在不同地理位置，以应对可能出现的灾难事件。

7.3 数据更新

当员工信息、薪酬计算标准等数据发生变化时，应及时更新相关数据，确保薪酬计算和发放的准确性。

8 安全与隐私保护

8.1 身份认证与授权

8.1.1 采用多种身份认证方式相结合，确保用户身份的真实性和合法性。如用户名 / 密码认证、短信验证码认证、指纹识别认证、面部识别认证等，根据用户的使用场景和安全级别要求，为用户提供合适的身份认证方式。

8.1.2 建立完善的授权管理机制，根据用户的角色和职责，为用户分配相应的系统操作权限。权限管理应细化到功能模块、数据对象和操作行为，确保用户只能在授权范围内进行操作，防止越权访问和操作风险。同时，定期对用户的权限进行审查和更新，确保权限的合理性和有效性。

8.2 数据加密

8.2.1 对系统中的敏感数据进行加密处理，包括用户数据、薪酬数据、支付数据、税务数据等。在数据存储阶段，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存储，防止数据被非法读取。在数据传输阶段，采用 SSL/TLS 等加密协议对数据进行加密传输，确保数据在网络传输过程中的安全性，防止数据被窃取、篡改或劫持。

8.2.2 加密算法应采用符合国家标准和行业规范的安全加密算法，如 AES、RSA 等，并定期对加密算法和密钥进行更新和管理，保障加密的强度和安全性。同时，建立密钥管理系统，对加密密钥的生成、存储、分发、使用和销毁等环节进行严格管理，确保密钥的安全性和保密性。

8.3 网络安全防护

8.3.1 构建完善的网络安全防护体系，包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）、防病毒系统等安全设备和软件。通过防火墙设置访问控制策略，限制外部非法网络访问，防止网络攻击和恶意软件入侵。利用 IDS 和 IPS 实时监测网络流量，及时发现和阻止入侵行为。部署防病毒系统，对系统中的文件和数据进行病毒查杀，保障系统的安全运行。

8.3.2 定期对网络安全防护设备和软件进行更新和维护，确保其防护功能的有效性。同时，开展网络安全漏洞扫描和渗透测试，及时发现和修复系统中的安全漏洞，防范潜在的网络安全风险。

8.4 支付安全

8.4.1 在薪酬支付过程中，与合规的支付渠道进行合作，确保支付过程的安全可靠。支付渠道应具备完善的支付安全保障机制，如支付风险监控、支付密码验证、支付限额管理等功能。系统应与支付渠道进行安全对接，采用安全的支付接口和通信协议，保障支付数据的传输安全。

8.4.2 建立支付风险防控机制，对支付过程中的异常交易进行实时监控和预警。例如，监测支付金额

异常、支付频率异常、支付对象异常等情况，及时发现和防范支付欺诈风险。对于异常交易，系统应自动采取暂停支付、人工审核等措施，确保支付资金的安全。同时，加强对支付数据的管理和保护，防止支付数据泄露导致支付风险。

8.5 安全审计与监控

8.5.1 建立安全审计系统，对系统中的用户操作行为、数据访问行为、系统运行状态等进行全面审计和记录。审计日志应包括详细的操作信息，如操作时间、操作人、操作内容、操作结果等，便于追溯和分析安全事件。定期对审计日志进行审查和分析，及时发现潜在的安全问题和违规行为，并采取相应的措施进行处理。

8.5.2 实施安全监控措施，实时监测系统的运行状态、网络流量、安全设备状态等信息。通过监控系统及时发现系统故障、网络攻击、数据泄露等安全事件，并发出警报通知相关人员进行处理。同时，对安全监控数据进行分析和统计，为系统的安全优化和风险评估提供数据依据。

8.6 应急响应与处置

制定完善的应急响应预案，针对可能出现的安全事件（如系统故障、网络攻击、数据泄露等）制定相应的应急处置流程和措施。