天津市地方标准

DB12/T 926—2020

共享经济平台灵活就业人员互联网管理与服务指南

Guidelines of Internet management and service for the Gig Worker in sharing economy platform

2020 - 01 - 21 发布　　2020 - 03 - 01 实施

天津市市场监督管理委员会 发布

共享经济平台灵活就业人员互联网管理与服务指南

1　范围

本标准规定了共享经济灵活就业人员管理与服务机构在开展各项活动及软件平台开发过程中的安全基本要求，包括系统安全、应用安全、数据安全、管理安全。

本标准适用于指导共享经济灵活就业人员管理与服务机构的平台及相关产品在技术、业务、管理等方面的安全过程，可用于共享经济灵活就业人员管理与服务机构。

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 22080 信息技术 安全技术 信息安全管理体系 要求

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 30276-2013 信息安全技术 信息安全漏洞管理规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 36637-2018 信息安全技术 ICT 供应链安全风险管理指南

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/Z 20986-2007 信息安全技术 信息安全事件分类分级指南

JR/T 0095-2012 中国金融移动支付 应用安全规范

JR/T 0197-2020 金融数据安全 金融数据安全数据分级指南

DB12/T 926-2020 共享经济平台灵活就业人员互联网管理与服务指南

3　术语和定义

DB12/T 926-2020 中界定的以及下列术语和定义适用于本文件。

3.1

共享经济平台 the sharing economy platform

指利用互联网现代信息技术，整合海量、分散化资源，通过移动设备、评价系统、支付、基于位置的服务（LBS）等技术手段有效地将需求方和供给方进行最优匹配，对数量庞大的需求方和供给方进行撮合，通过撮合交易达到供需双方收益最大化，具备法人资格的共享经济行业平台型公司。

3.2

共享经济灵活就业人员管理与服务机构（简称：“管理与服务机构”）management and service institute of the Gig Worker in the sharing economy

提供共享经济灵活就业人员平台化服务的组织。

3.3

个人信息 personal information

指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的，属于个人信息。

[来源：GB/T 35273-2020，3.1]

3.4

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇的个人信息。

注：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

个人信息控制者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的，属于个人敏感信息。

[来源：GB/T 35273-2020，3.2]

4 缩略语

下列缩略语适用于本文件。

HIDS：主机入侵检测系统 （Host-based Intrusion Detection System）

CA：证书授权中心 （Certificate Authority）

SDL：安全开发生命周期 （Security Development Lifecycle）

PII：个人可识别信息 （Personal Identifiable Information）

KMS：密钥管理系统 （Key Management System）

5 系统安全

5.1 安全物理环境

应符合 GB/T 22239-2019 中 8.1.1 要求。

5.2 安全通信网络

应符合 GB/T 22239-2019 中 8.1.2 要求。

5.3 安全区域边界

本项要求包括：

a)应符合 GB/T 22239-2019 中 8.1.3 要求。

b)边界设备配置应符合以下条款：

1）按月审核访问控制规则；

2）制定记录、使用边界设备管理的安全策略和操作程序；

3）在便携式计算设备上安装个人防火墙软件或等效功能。

c)安全审计记录应留存至少六个月。

5.4 主机要求

本项要求包括：

a)应符合 GB/T 22239-2019 中 8.1.4.1、8.1.4.2、8.1.4.3、8.1.4.4 要求；

b)如使用云主机，应符合 GB/T 22239-2019 中 8.2.4.1、8.2.4.2、8.2.4.3 要求；

c)应部署 HIDS，对主机的异常操作行为进行安全预警，及时发现并阻止黑客攻击行为；

d)安全审计记录应留存至少六个月。

5.5 系统可用性要求

本项要求包括：

a)应支持高并发请求，自动进行负载均衡；

b)应利用冗余部署消除单点故障；

c)应部署异地灾备环境；

d)应部署主机系统安全监控和业务可用性监控，通过电话、短信、邮件、即时通讯等手段进行报警，快速恢复系统故障。

6 应用安全

6.1 软件开发安全本项要求包括：

a)应根据开发人员类型遵循 GB/T 22239-2019 中 8.1.9.4 或 8.1.9.5 要求；b)开发、测试环境与生产环境中职责分离；

c)开发、测试过程中不使用生产环境数据；

d)在激活系统、系统投入生产前，删除系统组件中的测试数据和账户；

e)开发、测试环境独立于生产环境，并借助访问控制确保两者分离；

f)在系统投入生产前对系统进行安全漏洞扫描，对于测试中发现的安全问题应及时修复。

6.2 密钥安全本项要求包括：a)应符合 JR/T 0095-2012 中的 7.2.2 条款；b)应隔离保管系统中最核心私钥，使用时应保证至少有 2 人同时在场。

6.3 电子签约本项要求包括：

a)服务机构应支持与灵活就业人员在线签署具备法律效应的电子合同；

b)电子合同应具有时效性，通过实名身份认证，做防篡改、防止复制签名技术处理；

c)输入密码过程应做实时加密处理。

6.4 身份验证根据不同共享经济灵活就业人员管理与服务和场景需求，应进行身份信息要素验证的分级管理。至少应满足以下要求：

a)签约服务：应进行姓名、身份证号、银行卡号、手机号四要素认证；

b)自主签约批量结算服务：应进行姓名、身份证号、银行卡号、手机号四要素认证；

c)批量结算到银行卡服务：应进行姓名、身份证号、银行卡号三要素认证；

d)预签约服务：应进行姓名、身份证号二要素认证。

7 数据安全

7.1 总述应保证所服务的灵活就业人员、共享经济平台和管理与服务机构本身的数据安全。

7.2 数据分级个人信息和个人敏感信息分级应按照 GB/T 35273-2020 中附录 A 和附录 B 执行。客户、业务、经营管理、监管数据分级宜参考 JR/T 0197-2020 中附录 A 执行，应根据管理与服务机构的实际情况，对敏感数据进一步分级。敏感数据的分级宜以下列内容为准：

a)一级敏感数据包括个人敏感信息(如银行账户、手机号、身份证号)、系统级配置信息(如数据库认证配置、商户通信密钥、系统间通信密钥、数字证书认证配置)、系统级账户密码(如服务器最高权限密码) 、系统的源代码等；

b)二级敏感数据包括脱敏的订单和用户数据等；c)三级敏感数据包括统计类数据，如用户画像数据等。

7.3 数据加密 7.3.1 数据加密规则

个人敏感信息加密规则应满足：

a)数据全生命周期加密；

b)采取 KMS 管理密钥全生命周期；

c)采取的加密算法包括但不局限于对称加密算法、非对称加密算法和摘要加密算法，并应满足以下要求：

1）选择符合国家行业主管部门要求的算法；

2）支持对称加密算法包括但不限于 SM4、3DES、AES (128 位或更高)；

3）支持非对称加密算法包括但不限于 SM2、RSA (2048 位或更高)；

4）支持摘要加密算法包括但不限于 SM3、SHA-2。

d)至少采取数据加密、密钥加密二层加密。

7.3.2 一级敏感数据加密应符合本标准 7.3.1 要求。

7.3.3 二级及以下敏感数据加密方式应符合本标准 7.3.1 中的 a)、b)、c)要求。

7.4 数据访问管理与服务机构管理人员访问灵活就业人员信息应符合 GB/T 22239-2019 中 8.1.4.2 和 8.1.4.3 的相关要求。

7.5 数据处理数据处理活动的主要操作包括但不限于数据查询、数据读取、数据索引、批处理、交互式处理、数据统计分析、数据可视化等。根据管理与服务机构为灵活就业人员提供共享经济综合服务时的实际情况，数据处理在符合 GB/T 37973-2019 中 8.4.1 的同时，应满足以下条款：

a)灵活就业人员 PII 处理应征得用户明示同意；注：明示同意是指个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”、“注册”、“发送”等。

b)灵活就业人员 PII 处理应在高安全性的桌面虚拟化环境进行；注：桌面虚拟化环境指将操作系统桌面安装、运营环境，操作和显示环境相分离，利用客户端访问虚拟化平台上的操作系统桌面。客户端只传输鼠标键盘动作和接受显示画面，实现数据和使用相分离。高安全性是指虚拟桌面终端本地不存储任何用户数据，本地终端对应的硬件接口可被禁用，如 USB、CD-ROM 等外设接口。外发网络数据应接受白名单限制。

c)数据处理过程应遵循可审计原则，记录删除数据的操作时间、操作工具、操作方式、数据内容等，并符合 GB/T 22239-2019 中 8.1.4.3 的要求。

7.6 数据存储数据存储应符合以下条款：

a)符合 GB/T 37973-2019 中 8.3 要求；

b)建立防火墙保护平台数据；

c)提供异地实时备份功能，并具有相应的恢复功能以便在发生故障时恢复；

d)对运行关键业务的服务器采用集群结构，有主备机制，实现业务系统不间断运行；

e)在提供服务前对服务器进行安全漏洞扫描和渗透测试，服务提供过程中应每年至少进行一次渗透测试，对于测试中发现的安全问题应及时修复；

f)数据库应具备接入相关监管机构监管信息交互平台的能力。

7.7 数据删除应符合 GB/T 37973- 2019 中 8.6 要求。

8　管理安全 8.1 信息安全人员组织设置应设置信息安全高层管理机构、信息安全日常管理机构、信息安全技术团队等信息安全管理组织。

8.1.1 信息安全高层管理机构信息安全高层管理机构应由管理与服务机构的最高管理层组成，负责决策、监督、推动整体信息安全体系建设，对管理与服务机构及其所有发生活动负责。

8.1.2 信息安全日常管理机构信息安全日常管理机构应由管理与服务机构内部的各部门骨干成员组成，负责统一协调、监督各项安全制度和策略在不同职责部门内统一实施。

8.1.3 信息安全技术团队信息安全技术团队应由管理与服务机构内部的技术人员组成，负责生产环境安全和办公环境安全的保障工作。信息安全团队中技术人员应具备信息安全相关工作经验。

8.2 运维管理安全要求 8.2.1 安全运维管理应符合 GB/T 22239-2019 中 8.1.10 要求。在使用云计算环境时，应符合 GB/T 22239-2019 中 8.2.6、8.2.7 要求。

8.2.2 服务器运维安全基线本项要求包括：

a)运行在生产环境操作系统上的软件，应统一由管理与服务机构内部的运维人员从可信环境下载和安装。对于通用软件和组件，统一制定安全配置策略和规范；

b)根据功能和安全级别，应在不同模块间使用网络隔离或者虚拟安全组进行隔离。生产环境的入口统一使用堡垒机作为唯一入口，堡垒机应具备审计功能，便于事后追踪。核心系统对外应只提供必须开放的端口，无关端口应全部关闭。

8.2.3 安全漏洞的识别和修复本项要求包括：

a) 安全漏洞的生命周期和漏洞管理应符合 GB/T 30276-2013 中 4.5 要求；

b) 应具备识别潜在的编码漏洞的能力，应在投入生产或向客户发布前审核自定义代码。自定义代码审核应包括但不限于以下内容：

1）应由代码原作者以外的人员以及熟悉代码审核方法和安全编码实践的人员审核代码变更；

2）代码审核应确保代码的开发符合安全编码指南；

3）代码发布前应已经进行修正和测试；

4）代码审查结果在发布前应已经由管理人员审核并批准。

c) 应制定服务中间件和操作系统漏洞升级机制，一旦有操作系统或者各种服务组件的零日漏洞预警，应及时进行安全预警和补丁升级，预防潜在的安全风险。

8.2.4 病毒查杀应确保所有病毒查杀机制病毒库保持为最新，执行定期扫描，生成检查日志。

8.2.5 应急预案本项要求包括：a)应制定统一的应急预案框架，包括但不限于应急事件分级、启动应急预案条件、应急事件处理流程、应急组织及职责以及事前事后培训等，事件分类分级宜参考 GB/Z 20986-2007；b)应至少每季度开展 1 次应急预案模拟演练。

8.3 员工安全意识培养要求

8.3.1 全员安全培训管理与服务机构应对全体员工在入职初期和安全规则发生重大变化时，实施培训，包括但不限于信息安全防护的基本方法和注意事项、预防网络欺诈的技巧、信息安全相关的法律法规。

8.3.2 开发和运维安全培训管理与服务机构应对信息系统开发和维护人员在入职初期和安全规则发生重大变化时，实施培训，包括但不限于不同开发栈的安全编码培训和安全运维培训。

8.4 系统供应链安全要求应按 GB/T 36637-2018 实施供应链安全风险管理。

8.5 安全体系要求本项要求包括：

a)应符合网络安全等级保护第三级；

b)应建立符合 GB/T 22080 标准的安全管理体系；

c)宜通过 PCI DSS 安全认证；d)应设置与信息安全监管机构及第三方安全服务提供商之间的联络员，制定实施程序。