

团 体 标 准

T/ACCEM XXXX-XXXX

智能柜用户交易视频隐私保护规范

Smart cabinet user trading video privacy protection standards

(征求意见稿)

20XX-XX-XX 发布

20XX-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 权限管理 1

5 视频管理 2

6 人员管理 3

7 应急处理 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。

本文件由深圳市丰宜科技有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：

本文件主要起草人：

智能柜用户交易视频隐私保护规范

1 范围

本文件规定了智能柜用户交易视频隐私保护的权限管理、视频管理、人员管理、应急处理。
本文件适用于智能柜用户交易视频隐私保护。

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 39335 信息安全技术 个人信息安全影响评估指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

用户交易视频隐私保护 User trading video privacy protection

指在用户进行视频交易过程中，平台或服务提供商采取一系列技术措施和管理措施，确保用户隐私信息不被泄露或滥用。对用户个人信息、视频内容以及交易过程安全进行的全面保护。

3.2

云平台 Cloud platform

基于云计算技术的计算机平台，提供各种云服务，如云存储、云计算、云数据库等。

3.3

数据完整性校验 Data integrity check

是一种验证数据完整性的技术，通过特定的算法对数据进行计算，生成一个校验值，用以检验数据在传输或存储过程中是否发生篡改。校验值通常是一串特定的字符，与原始数据进行比对，若相同则说明数据未被篡改，否则数据完整性受到破坏。

4 权限管理

4.1 基本要求

用户交易视频属于个人敏感信息，应划分权限范围进行管理。权限管理应遵守“合理最小必要”原则。

注：“合理”是指申请的权限范围及理由合理，“最小”是指申请最小化权限完成对应工作所需。“必要”是指必须查看用户交易视频才可完成后续工作。

4.2 权限申请

4.2.1 进行用户交易视频查阅、加工处理的人员应统一签订保密协议书，同时知晓保密责任、违反保密协议的行为及相关处罚、违约责任。

4.2.2 内部申请人员提交申请流程时，应说明权限范围、时间目的及使用人员。

4.3 权限使用

使用人申请相关权限后，应妥善保管账号密码，不得将账号外借，不得使用未经允许的通道登录，使用完后应及时退出账号。

4.4 权限关闭

4.4.1 使用人因工作变动调整或需求变动无需查看用户交易视频时，应主动向管理员汇报并关闭权限；使用人员办理离职时，使用人员上级或供应商对接人应主动向管理员汇报关闭权限。

4.4.2 管理员应定期对人员权限进行评审，包括权限有效期及当前权限范围能否适用于该人员岗位，对于权限范围不适用的，管理员应及时沟通并关闭相应权限。

5 视频管理

5.1 视频采集管理

5.1.1 摄像头位置应由上至下、固定朝向某一位置，应仅采集人脸特征数量最少的交易视频，不得朝向出入口、人流密集区域等，不得过度采集周围人员信息。

5.1.2 用户扫码前不得开始视频录像，不得开启麦克风进行录音。

5.2 视频传输管理

应采取数据完整性校验、数据加密（Https 协议）、加签验签、密钥等措施保障视频传输安全。

5.3 视频处理管理

5.3.1 应对所有原用户交易视频进行人脸特征、敏感部位等进行打码处理。

5.3.2 应对已处理的交易视频添加水印以便查阅展示，水印内容应包含：

- a) 操作人姓名；
- b) 工号；
- c) 操作时间。

5.3.3 应在安全可靠的环境中通过身份认证进行视频加工处理，避免非授权访问。

5.4 视频使用管理

5.4.1 除客服售后审核等必须进行查阅视频外，任何人未经审批，不得以任何方式拍摄、下载，不得外带、外传、外发。

5.4.2 智能柜补货人员及一线商务拓展人员不得查阅、下载、转发、存储用户交易视频。

5.4.3 各类小程序或 APP 不得提供用户交易视频查阅、下载、转发等功能。

5.4.4 应用系统应隐藏视频播放地址，取消下载按钮，并对网页前端可获取到的视频地址进行加密。

5.4.5 视频查阅完毕后，使用人员应及时退出视频查阅页面。

5.4.6 用户查阅视频行为及操作进行记录，记录保存时间应不少于 60 天。

5.5 视频存储管理

5.5.1 采用云平台存储视频，应采取加密存储或视频人脸特征打码等措施存储视频数据，并采用身份认证机制及权限控制，获取相应视频数据应对其进行安全审计，对用户行为及操作进行记录，记录保存时间不少于 60 天。

5.5.2 原交易视频数据与已加工处理视频数据应分开存储，对原交易视频应采取加密保护存储，保留时间不超过 1 个月。

5.5.3 已投入使用的智能柜应当关闭现场调试功能。

5.6 视频数据提供、公开管理

5.6.1 除非经用户书面同意，不得公开视频数据。

5.6.2 不宜向第三方提供或委托处理视频数据，因业务需要确需提供或委托处理的，应满足的安全要求包括但不限于：

- d) 按 GB/T 39335 的规定对数据接收方开展安全评估，并通过合同等方式约定提供或委托处理的目的、期限、方式、保护措施等，并对数据接收方的处理活动进行监督；
- e) 在提供或委托处理前，单独告知用户主体数据接收方身份、接收方数据安全能力、数据类别、可能产生的影响等相关信息，并征得用户主体单独同意或书面同意；
- f) 数据接收方应按约定处理视频数据，不得超出约定的目的、方式等处理视频数据，不得转委托。

5.7 视频数据删除管理

5.7.1 视频数据处理目的已实现、无法实现或者为实现处理目的不再必要应进行删除并不可恢复；原始视频存储期限到期后也应进行不可逆删除。

5.7.2 数据处理者停止提供视频采集业务时进行删除并不可恢复。

6 人员管理

6.1 内部人员管理

6.1.1 账号密码安全

内部人员具备查阅下载用户交易视频的权限的，应保护好各应用系统的账号、口令，不得私自外借，在发现任何非法使用本人账号而导致用户交易视频信息系统安全的事件时，必须立即报告信息安全部门。

6.1.2 安全意识及保密协议

内部人员应参与安全意识培训并完成考试，签订保密协议。

6.1.3 保密行为准则

内部员工的保密行为准则如下：

- a) 仅在公司分配的办公终端中查阅使用用户交易视频；
- b) 不通过其他渠道（网盘、邮件、U 盘等）外发或私自存储用户交易视频；
- c) 对所查阅的交易视频进行保密，不得进行截图、拍照、录像或口头传播相关视频信息。

6.2 外包人员管理

6.2.1 账号密码安全

外包人员具备查阅下载用户交易视频的权限的，应保护好各应用系统的账号、口令，不得私自外借，在发现任何非法使用本人账号而导致用户交易视频信息系统安全的事件时，必须立即报告信息安全部门。

6.2.2 安全意识及保密协议

- 6.2.2.1 外包人员应提高安全意识，由外包负责人进行信息安全意识宣导，并要求签订保密协议。
- 6.2.2.2 外包人员所导致的用户交易视频信息安全事件，按照所签订的具体服务合同规定进行处理。

6.2.3 保密行为准则

外包员工的保密行为准则如下：

- a) 外包员工应当对商业秘密和客户的隐私信息进行分类和标识，妥善保管和管理，不得擅自更改或删除保密标识；
- b) 不通过其他渠道（网盘、邮件、U 盘等）外发或私自存储用户交易视频；
- c) 对所查阅的交易视频进行保密，不得进行截图、拍照、录像或口头传播相关视频信息。

6.3 供应商管理

- 6.3.1 参与视频采集、处理、传输、存储等环节的供应商应按照相关文件进行管理。
- 6.3.2 应具备防止对摄像头、麦克风等传感器非授权访问和使用的机制。
- 6.3.3 应具备关闭、禁止或限制使用设备上与实际应用无关的端口、协议和服务的机制。
- 6.3.4 应建立持续性安全保障机制，当出现信息安全缺陷时，及时通知用户，并提供修复方法或者应急处置方案。
- 6.3.5 供应商所导致的用户交易用户交易视频信息安全事件，应按所签订的合作合同规定及保密协议进行处置。
- 6.3.6 原始视频只进行商品识别、识别完成后应删除。
- 6.3.7 设备管理平台应符合等级保护三级要求，具备一定的安全防护措施。

7 应急处理

7.1 紧急措施

当发现有交易视频数据泄露时，应立即报告信息安全及隐私管理委员会，由委员会协调人员进行检查，及时通过审计日志定位视频泄露链条、视频来源、视频查阅操作日志，并关闭账号权限。

7.2 抑制处理

应排查系统及数据库、应用系统等相关日志，根据情况及时下线或切断相关业务系统外联网络，并保留证据，定位人员、还原事件过程。

7.3 闭环总结

信息安全及隐私管理委员会应组织协调相关部门、供应商人员对业务系统和相关日志进行检查，分析事件原因及总结，并根据实际情况进行通告处罚。