ICS 01.140
A 14

MZ

中 华 人 民 共 和 国 民 政 行 业 标 准

MZ/T 108—2018

居民家庭经济状况核对信息安全管理规范

Verification service for the family economy information-

Security Management

2018-01-09 发布　　2018-01-09 实施

中华人民共和国民政部 发布

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由民政部社会救助司提出并归口。

本标准起草单位：民政部低收入家庭认定指导中心。

本标准主要起草人：宝力高、李刚、吴镝、王冠、刘珂、张寰

居民家庭经济状况核对信息安全管理规范

1 范围

本标准规定了居民家庭经济状况核对工作的信息安全管理规范，包括术语与定义、场地设备安全管理、人员管理、信息交换、信息使用安全管理、应急预案管理、核对信息系统安全等级保护定级。

本标准适用于各级居民家庭经济状况核对机构。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改版）适用于本文件。

GB/T 20269-2006 《信息安全技术 信息系统安全管理要求》

GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》

GB/T 22240-2008 《信息安全技术 信息系统安全等级保护定级指南》

GB50140-2010 《建筑灭火器配置设计规范》

MZ/T 072-2016 《居民家庭经济状况核对 总则》

3 术语和定义

下列术语和定义适用于本文件。

本标准提及且未单独定义的术语与定义，参考 GB/T 20269-2006 《信息安全技术 信息系统安全管理要求》。

3.1

信息交换场所

用于信息共享单位与核对机构之间或不同核对机构之间信息交换的工作环境。

3.2

核对业务办理场所

用于办理居民家庭经济状况核对业务的工作环境。

3.3

终端

在开展居民家庭经济状况核对业务过程中，所使用的计算机及设备。

4 场地设备安全管理

4.1 工作场所管理

4.1.1 信息交换场所

本项应参考 GB/T22239-2008 相关要求，包括：

a) 工作场所应为独立封闭的工作区域；

b) 重要区域应配置电子门禁系统，鉴别、控制人员进入，记录人员进出情况及在重要区域的行为，记录应至少包含姓名、有效身份证件号码、进出入时间和操作内容，记录应至少保留6个月；

c) 来访人员应提前提出申请，经过审批后方可进入信息交换场所，并在来访过程中遵守信息交换场所的来访限制和活动范围；

d) 应利用光、电等技术设置监控、防盗报警系统，其中监控记录应至少保留6个月；

e) 应采用具有耐火等级的建筑材料，采取区域隔离防火措施，将重要设备与其他设备隔离开，应依据GB50140-2010配备必要的消防器材；

f) 应配置用于销毁文件和光盘的设备。

4.1.2 核对业务办理场所

本项应参考 GB/T22239-2008 相关要求，包括：

a) 工作场所应为独立封闭的工作区域；

b) 应配置用于销毁文件和光盘的设备；

c) 重要区域应配置电子门禁系统，鉴别、控制人员进入，记录人员进出情况及在重要区域的行为，记录应至少包含姓名、有效身份证件号码、进出入时间和操作内容，记录应至少保留6个月；

d) 来访人员应提前提出申请，经过审批后方可进入核对业务办理场所，并在来访过程中遵守核对业务办理场所的来访限制和活动范围，严禁来访人员使用自带的设备接入网络或设备；

e) 应利用光、电等技术设置监控、防盗报警系统，其中监控记录应至少保留6个月；

f) 应采用具有耐火等级的建筑材料，采取区域隔离防火措施，将重要设备与其他设备隔离开，应依据GB50140-2010配备必要的消防器材。

4.2 设备及系统管理

4.2.1 终端使用

本项要求包括：

a) 终端周围不得放置易燃、易爆、强腐蚀、强磁性等有害终端设备安全的物品；

b) 终端应专人专用，设置开机密码，并定期更新，且与最近6个密码不重复；

c) 终端中不得安装与工作无关的软件，工作人员应对终端每周进行1次病毒查杀；

d) 终端中不得保存业务数据,工作人员应对终端每月进行至少1次检查。

4.2.2 核对系统管理

针对用于开展居民家庭经济状况核对的信息系统，安全要求至少包括：

a) 应根据GB/T 20269－2006中的要求，确定应用系统和基础软件的用户管理和访问控制策略；

b) 应及时检测、修复、清除终端及信息系统中的安全隐患，并记录检测、修复、清除的过程，记录应至少保留6个月；

c) 应在保证终端及服务器内部数据不受影响的前提下,安装系统安全防护工具或各类安全补丁；

d) 应使用具有安全专用产品销售许可证的防病毒产品；

e) 应根据GB/T 22239-2008的要求对核对系统进行设计、开发和测试；

f) 应选择具有CMA（检验检测机构资质认定证书）、CNAS（中国合格评定国家认可委员会实验室认可证书）以及“信息安全等级保护测评机构推荐证书”的第三方机构，对信息系统进行验收测试和安全测评；

g) 安全测评每年至少进行1次，并根据测评结果进行整改。

4.2.3 数据库安全管理

本项要求包括：

a) 应指定专人负责数据库用户管理、权限管理、数据库日常维护和备份操作，限定相关帐户有效期限和权限范围，不可直接使用ROOT或DBA用户进行应用和数据库运维；

b) 对数据库的关键操作，应建立审批备案制度，并保留创建用户、更改用户等权限操作的记录，记录应至少保留6个月；

c） 应对数据库操作日志每周进行1次巡检，防止用户非法操作数据库，日志保存不少于6个月；

d） 应指定专人保管数据库服务器开机密码，并定时更新；

e） 应对姓名和有效证件号等敏感数据进行加密；

f） 应采用数据库审计系统，对数据库进行安全审计。

4.2.4 数据备份与恢复

本项应参考 GB/T22239-2008 相关要求，包括：

a） 应提供本地数据备份与恢复功能，备份介质场外存放应不少于2份，备份数据应加密存储；

b） 应对核对系统的业务数据、系统数据和重要软件进行备份；

c） 核对系统数据应进行每月全备份、每日增量备份，用于备份数据的存储介质保存期至少为5年；

d） 应对备份过程进行记录，所有文件和记录应妥善保存，记录应至少保留六个月；

e） 应每月至少开展一次数据备份与恢复的抽检工作，检查和测试备份介质的有效性，抽样率应不低于10%；

4.2.5 用户身份鉴别

本项应参考 GB/T22239-2008 相关要求，包括：

a) 应提供专用的登录控制模块，对登录用户进行身份标识和鉴别；

b) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

c) 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能（登录失败处理措施至少包括，结束会话、限制非法登录次数和自动退出等功能），并根据安全策略配置相关参数；

d) 应使用强密码策略，强密码策略参见附录 A；

e) 用户信息和密码应加密保存。

4.2.6 系统操作管理

本项要求包括：

a） 核对系统用户采用实名制方式管理，登录密码应至少每个季度修改一次，并妥善保存，登录用户名和密码不应交给运维人员保管；

b） 核对系统使用完毕后应及时退出，如15分钟内无操作应自动退出；

c） 应建立密码遗失和泄漏应急处理机制；

d） 核对系统用户权限申请，应制定申请和审批流程；

e） 工作人员离岗，应及时删除系统账号。

5 人员管理

5.1 人员录用

本项应参考 GB/T22239-2008 相关要求，包括：

a) 应指定或授权专门的部门或人员负责人员录用；

b) 应严格规范人员录用过程，对被录用人的政治、社会因素及专业资格和资质等进行审查，对其所具有的业务技术水平进行考核；

c) 核对机构应与被录用人员签署保密协议。

d) 应设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查。

5.2 人员离岗

本项应参考 GB/T22239-2008 相关要求，包括：

a) 确定人员离岗时，应立刻注销离岗人员所有核对信息系统访问账号和权限，终止文件查阅权限；

b) 应收回离岗人员工作证件、钥匙及其个人持有的软硬件设备；

c) 应办理严格的调离手续，如关键岗位人员要离岗，须签订保密协议，明确保密义务后方可离岗。

5.3 人员考核

本项应参考 GB/T22239-2008 相关要求，包括：

a) 应对各岗位人员每季度至少进行 1 次安全技能及安全知识的考核；

b) 应对所有能够接触到核对数据的人员进行全面、严格的安全审查和技能考核，并对考核结果进行记录并保存。

5.4 人员培训

本项应参考 GB/T22239-2008 相关要求，包括：

a) 新录用人员上岗前，应进行信息安全培训，明确岗位应遵守的信息安全制度和技术规范；

b) 应每季度开展至少 1 次安全技术教育培训，并针对不同岗位制定不同的培训计划；

c) 应对安全教育和培训的情况和结果进行记录并归档保存。

5.5 外部人员访问管理

针对非从事核对业务的外部人员，应参考 GB/T22239-2008 相关要求，包括：

a) 外部人员访问受控区域应先提出书面申请，经批准后由专人全程陪同或监督，并登记备案；

b) 对外部人员允许访问的区域、设备、系统和文件应进行书面的规定，并在各区域明示访问权限。

6 信息交换

6.1 在线交换

本项要求包括：

a) 使用电子政务外网进行互联的，应采用电子政务外网进行数据传输，未使用政务外网互联的，采用专线网络传输数据；

b) 在传输过程中应对数据进行加密；

c) 应通过前置服务器用于发送和接受信息，在确认交换完成后，前置服务器数据应及时清除，如确需保留，应依据“4.2.4数据备份与恢复”中要求进行单独备份；

d) 应建立防止抗抵赖机制，确保所有操作具有可追溯性；

e) 应建立问题定位、数据恢复的回滚机制；

f) 在交换过程中如发现有异常情况应立即暂停在线数据交换直至排除安全隐患。

6.2 离线交换

本项要求包括：

a) 通过核对信息系统导入导出数据时，应至少2人同时在场，其中1人负责操作，1人负责监督；

b) 针对不同信息共享单位制定操作规范，至少应对交接手续、交接场所、交接周期、人员要求做出规定；

c) 存储介质应使用不可修改的光盘或可加密存储设备；

d) 针对不同信息共享单位，应使用专用存储介质；

e) 每次运送数据前，应对以安全U盘为存储介质的数据采用全新密钥加密技术对可加密存储设备重新设定密码，新密钥或密码应在1月内未被使用；

f) 应通过机要用车或国家规定的正规社会用车指定专人负责运送，除驾驶人员外，不应让其他无关人员同乘交通工具；

g) 负责运送数据的人员不得掌握被运送数据的加密密码和加密存储设备的密码；

h) 除不可抗力原因，数据运送过程中应直接送至目的地；

i) 数据交换结束后，应清除用于数据交换的存储介质中数据，销毁用于交换数据的光盘，如彻底清除不了，必须加强管理。

7 信息使用安全管理

本项要求包括：

a) 除工作需要外，工作人员不得擅自保存核对信息系统的数据；

b) 在核对信息系统开发、测试、培训、交流过程中，不得使用真实数据；

c) 在数据分析过程中，应对能够识别人员身份或无统计意义的信息进行剔除或转换处理。

8 监测预警与应急处置

本项应参考 GB/T22239-2008 相关要求，包括：

a) 各级核对机构应建立网络安全监测预警和信息通报制度，统筹协调本行政区内有关部门加强网络安全信息收集、分析和通报工作。

b) 建立网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织

演练。

c) 省级核对机构应成立信息安全委员会，负责审批和组织相关信息安全活动；

d) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

e) 应对系统管理和操作人员进行应急预案培训，应急预案的培训应至少每年举办1次；

f) 应定期对应急预案进行演练，根据不同的事件，确定演练的周期；

g) 应急预案应定期审查，并根据实际情况进行更新。

h) 当出现网络安全事件时，应及时收集、报告有关信息，加强对网络安全风险的监测；立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

9 核对信息系统安全等级保护

应根据GB/T 22239-2008 《信息安全技术 信息系统安全等级保护基本要求》和GB/T 22240-2008 《信息安全技术 信息系统安全等级保护定级指南》的规定，对核对系统进行信息系统等级保护定级、备案、测评和整改。

附录 A

（规范性附录）

强密码策略

A.1 强密码策略

密码类别	最小强度规定
安全管理员帐号密码	■ 最小密码长度不小于 10 位 ■ 密码中必须包含大写字母、小写字母、数字和其他特殊符号 ■ 和个人信息无关 ■ 最近 20 个密码不得重复
安全审计员	■ 最小密码长度不小于 10 位 ■ 密码中必须包含大写字母、小写字母、数字和其他特殊符号 ■ 和个人信息无关 ■ 最近 20 个密码不得重复
系统管理员帐号密码	■ 最小密码长度不小于 8 位 ■ 密码中必须包含大写字母、小写字母和数字 ■ 和个人信息无关 ■ 最近 10 个密码不得重复
普通用户帐号密码	■ 最小密码长度不小于 8 位 ■ 密码中必须包含字母和数字 ■ 和个人信息无关 ■ 最近 6 个密码不得重复
用户帐号初始密码	■ 最小密码长度不小于 6 位 ■ 密码中必须包含字母和数字 ■ 和个人信息无关 ■ 最近 6 个密码不得重复