ICS 03.060
A11

团　　体　　标　　准

T/CQJR 009—2024

互联网贷款业务数据安全要求

Data security requirements for internet loan business

2024-05-13 发布　　2024-06-12 实施

重庆市金融学会 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的责任。

本文件由重庆蚂蚁消费金融有限公司、重庆富民银行股份有限公司提出。

本文件由重庆市金融学会归口。

本文件起草单位：蚂蚁科技集团股份有限公司、重庆蚂蚁消费金融有限公司、蚂蚁智信（杭州）信息技术有限公司、浙江网商银行股份有限公司、平安银行股份有限公司、重庆富民银行股份有限公司、重庆农村商业银行股份有限公司、汉口银行股份有限公司、中国对外经济贸易信托有限公司、国投泰康信托有限公司、天津信托有限责任公司、马上消费金融股份有限公司、招联消费金融股份有限公司、重庆小米消费金融有限公司。

本文件主要起草人：李士群、胡元美、史艳语、彭晋、白晓媛、陈彬、钱云杰、姜志辉、梅婧婷、刘义、宋铮、赵勇、张园超、谢宗华、王尧、陈晓蓉、孙金绣、王睿、李志、苏毅、杨莹莹、田成志、邓钦心、杨宇杰、李婕、谢颖、李巧、刘晶、杨吉庆、于浩洋、郑煜、赖德泳、刘佳音、陈南。

本文件为首次发布。

互联网贷款业务数据安全要求

1 范围

本文件概述了互联网贷款业务和典型的业务场景，并规定了典型业务场景下的数据安全要求和通用安全要求。

本文件适用于对互联网贷款业务相关方数据安全能力进行评估，也可为互联网贷款业务相关方开展数据安全能力建设时提供参考。

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 25069-2010 信息安全技术 术语

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB 50174-2017 数据中心设计规范

JR/T 0223-2021 金融数据安全 数据生命周期安全规范

JR/T 0044-2008 银行业信息系统灾难恢复管理规范

JR/T0265-2023 金融数据中心能力建设指引

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网贷款 Internet loan

运用信息通信技术，线上自动受理贷款申请并完成授信审批、合同签订、贷款支付、贷后管理等核心业务环节操作，为符合条件的借款人提供的用于消费、日常生产经营周转等的个人贷款和流动资金贷款。

注：互联网贷款通常基于风险数据和风险模型进行交叉验证和风险管理。

3.2

自营贷款 self-operated loan

金融机构通过自主品牌经营贷款产品，利用自身线上渠道为自有客户提供互联网贷款服务。

3.3

联合贷款 cofinancing loan

由两家或两家以上金融机构按约定比例出资，共同经营贷款产品，为客户提供互联网贷款服务。

3.4

助贷 partnership lending

金融机构外的第三方机构发挥自身平台、数据或科技等优势，为金融机构提供引流、营销、获客、催收等互联网贷款的支撑服务。

3.5

合作机构 partner

在互联网贷款业务中，与商业银行在营销获客、共同出资发放贷款、支付结算、风险分担、信息科技、逾期清收等方面开展合作的各类机构。

注：合作机构包括但不限于银行业金融机构、保险公司等金融机构和小额贷款公司、融资担保公司、电子商务公司、非银行支付机构、信息科技公司等非金融机构。

3.6

客户身份基本信息 basic information of customer identity

自然人客户的“身份基本信息”包括客户的姓名、性别、国籍、职业、住所地或者工作单位地址、联系方式，身份证件或者身份证明文件的种类、号码和有效期限。

4 概述

4.1 互联网贷款业务概述

当前互联网贷款业务的开展形式主要包括：自营贷款模式、联合贷款模式和助贷模式。在当前互联网贷款生态中，除了提供互联网贷款服务的金融机构之外，还有支持互联网贷款机构开展业务的各类信息科技和专业服务公司，如提供助贷平台服务、贷后催收服务的公司等。

互联网贷款业务工作的开展主要分为贷前管理、贷中管理和贷后管理三个环节。

a)贷前管理主要包括：

- 营销获客：互联网贷款业务提供方面向目标客户开展贷款营销。联合贷款模式和助贷模式下，还涉及到出资发放贷款的合作机构间分配获取到的客户。
- 授信签约：客户为了使用互联网贷款业务而开通互联网线上账号并提交互联网贷款申请，同时客户提供相应授权后，互联网贷款业务提供方对客户开展贷前调查、风险测算并对贷款申请给出审批结果，最终双方完成一笔贷款合作的签约。

b)贷中管理主要包括：

- 放款还款：互联网贷款业务提供方基于客户需求完成贷款金额的放款支用，并对客户的资金使用用途及资金流向进行监控或抽样核查，客户根据贷款合约的还款计划进行还款。

c)贷后管理主要包括：

- 逾期催收：针对客户逾期还款的贷款进行催收。
- 呆账核销：针对客户逾期还款的贷款且符合核销条件的进行核销。

另外，在贷款业务运营管理中，还包括风险管理、资产管理、监管报送、合作机构的管理。

a)风险管理：实现贷款业务过程中的反洗钱、反欺诈等风险管控。

b) 资产管理：主要为互联网贷款业务资产的管理和转让，实现互联网贷款业务的负债风险管理和融资。

c) 监管报送：根据人行、金融监督管理局的监管合规报送要求，整理报送数据并及时上报。

d) 合作机构管理：基于互联网贷款开展的业务合作需求，完成合作机构的准入、日常管理和退出管理。

4.2 互联网贷款业务典型场景概述

互联网贷款业务各环节典型场景中涉及的数据及处理活动如下表1所示。

表 1 互联网贷款业务各环节典型场景中涉及的数据及处理活动

业务环节	典型场景	涉及数据	数据处理活动
营销获客	a) 通过互联网平台、电销等推广渠道以及目标客群的属性数据进行互联网贷款营销 b) 联合贷款模式和助贷模式下，将营销推广获得的客群在合作机构间进行客户的分配	客户个人属性数据、客户行为数据、手机号码、营销推广内容、机构的客群偏好数据，如属地、年龄等	a) 使用客户的个人属性数据进行客群洞察、客群圈定、广告投放、活动准入、权益推荐、效果分析等 b) 根据合作机构的客群偏好数据和客户的属性数据向合作机构分配客户
授信签约	a) 客户注册互联网贷款业务的账号 b) 客户申请贷款时提交贷款申请相关信息，如身份证等相关证件信息 c) 针对贷款客户开展的人脸核身、反洗钱及反欺诈风控 d) 客户签订服务协议、授信协议、贷款合同等 e) 基于业务的实际情况进行额度、利率以及授信状态的变更管理	a) 客户个人信息：姓名、证件类型、证件号码、性别、国籍、职业、证件到期日、联系地址、联系方式、身份证影印件、人脸照片等 b) 客户信贷业务数据：授信额度、本金、利率、利息、余额、逾期金额、还款金额、业务通知短信等	a) 针对采集和生成的敏感数据在客户端、服务端的传输、存储、处理和展示 b) 在互联网贷款运营平台对客户个人信息和贷款业务数据的计算、处理和使用
放款还款	a) 根据用户需求展示本次贷款信息，包括额度、息费、收款账户、还款计划以及对应的合同信息 b) 根据用户需求进行核身(包括人脸识别、密码验证等方式)以及必要的反洗钱及反欺诈风控，并进行贷中风控审批 c) 根据用户需求完成合同签署、贷款资金发放、贷款入账等 d) 根据用户的贷款合约进行还款提醒、还款批扣，以及用户主动还款操作 e) 根据用户的贷款合约，对支用资金的使用用途及流向进行监控或抽样核查 f) 根据用户需求或风控，进行贷款合同以及还款计划的调整		客户个人信息、业务数据、资金数据的查询、计算、使用和传输
贷后管理	a) 筛选出逾期的还款并根据催收策略启动催收 b) 通过催收平台由专业的催收人员或系统自动化能力触达客户进行催收 c) 对于满足呆账核销条件的贷款，贷款提供方可按照相关规定对其进行核销	a) 逾期还款信息：客户的个人信息、逾期天数、逾期利息、逾期贷款余额、逾期本金、应催金额、应催余额等 b) 催收记录：催收案件编号、催收人员、催收结果、催收客户信息、催收录音等 c) 呆账核销信息：客户基本信息、合同及身份	a) 对催收客户相关的基础信息和贷款记录进行融合加工，制定催收策略，并形成催收案件 b) 基于催收案件，催收人员使用催收平台进行催收作业 c) 催收作业相关的录音数据的传输、使用和存储 d) 根据呆账核销条件和核销信息对客户贷款进行核

		证影印件信息、放还款记录、催收记录等	销
风险管理	对互联网贷款业务的数据和外部引入的数据进行融合计算，围绕贷款业务的全生命周期提供风险控制能力	姓名、证件号码、人行征信信息、外部个人数据、风控模型及模型结果数据等	a) 用于风控的各类数据的引入 b) 基于风控模型进行的数据融合加工计算
资产管理	a) 根据互联网贷款中产生的资产信息进行汇总分析管理 b) 围绕着资产的转让，在转让前签订协议并对待转让资产进行抽样检查，检查通过后基于协议进行资产转让，并将相关的资产数据提供给受让机构	资产数据、客户个人数据、资产交易明细数据	a) 外部数据引入用于资产管理 b) 基于转让对外提供资产数据
监管报送	基于监管要求，完成各类监管数据的定期报送	用于监管报送的各类数据	报送数据的采集、加工、处理和报送传输
合作机构管理	a) 合作机构准入时，对合作机构进行准入评估和合同签订 b) 业务合作期间，开展合作业务运营管理和定期评估等 c) 合作机构退出时，开展合作退出的评估和治理	合作机构名称、合作业务范围、联系人清单、合同协议、合作机构的安全评估报告及安全能力证明信息	围绕合作的业务和数据交互，进行合作过程中的安全评估和安全保障

5 典型场景数据安全要求

5.1 营销获客

本项要求包括但不限于：

a)对客户推广营销时，为进行客群洞察、客群圈定、广告投放等而使用的客户属性数据和联系方式，应通过合法渠道最小化的采集获取，并获得客户的授权；

b)通过电销渠道触达客户时，应通过营销系统的功能实现，避免直接使用客户明文的手机号码。特殊场景下，业务确需使用客户明文联系方式的，应通过额外的报备审批、权限管控、监控审计等补充措施加强安全管理，防范特殊场景下的数据泄漏风险；

c)推广营销如需要使用从外部引入的数据，应对数据来源的合法合规性进行评估，评估内容包括数据源主体资质、数据共享授权情况等，并对使用范围进行限定，防止被用于其他非授权的场景；

d)通过自动化决策方式向个人进行信息推送、推广营销时，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

5.2 授信签约

本项要求包括但不限于：

a)客户注册登陆时，应采用技术措施保障客户的账号安全，如引导客户设置高强度的账号密码、使用验证码等多因素认证方式或结合指纹识别、人脸识别等成熟的生物信息认证方式；

b)对客户身份核验时，应基于业务需要最小化地采集使用客户的身份信息，采集使用客户个人信息应通过隐私协议的形式获得客户的充分授权，应采取技术措施保障用户身份信息在传输、处理、存储、使用等场景下的安全，如权限控制、安全协议、数据加密、数据脱敏等；

c)客户使用互联网贷款服务时，应通过服务协议的形式向客户清晰展示服务内容、服务方式等信息，并通过客户主动勾选或点击同意按钮的方式签署服务协议，确保客户基于真实意愿自主选择地开通；

d)对客户授信审批时，应通过个人信用报告查询授权书的形式向客户清晰展示个人征信的处理目的、处理方式、保存期限等信息，并通过客户主动勾选或点击同意按钮的方式签署征信授权协议；

e)授信审批需要使用的客户身份、信用等数据，应基于客户授权和业务需要最小化地采集使用，个人不良征信信息应自不良行为或者事件终止之日起保存5年，超过5年的应当予以删除；

f)授信审批如需要使用从外部引入的数据，应对数据来源的合法合规性进行评估，评估内容包括数据源主体资质、数据共享授权情况等，并对使用范围进行限定，防止被用于其他非授权的场景；

g)授信合同签署时，应通过充分的措施，如账号密码、指纹识别、人脸识别等方式进行身份核验，确保客户的真实身份和真实意愿，并记录和存储完整的签署日志；

h)在数据处理、授信流程等需要人工介入的环节，应通过权限管控、数据脱敏、页面水印、下载限制等方式控制数据的泄漏风险。

5.3 放款还款

本项要求包括但不限于：

a)客户申请贷款时，应向客户清晰展示本次贷款的可用额度、收款账户、还款计划、息费信息、贷款合同协议等信息，并在申请提交时通过充分的措施，如账号密码、指纹识别、人脸识别等方式进行二次验证，确保客户的真实身份和真实意愿，并记录和存储完整的签署日志；

b)客户主动还款时，应向客户清晰展示本次还款的本金、息费等信息，并在客户还款支付时通过充分的措施，如账号密码、指纹识别、人脸识别等方式进行二次验证，确保客户的真实身份和真实意愿；

c)在支用、还款等资金交易环节，应采取加密、完整性校验和电子签名等技术手段，防止资金交易过程中的数据泄漏、篡改和抵赖；

d)在支用、还款等资金交易环节所使用和产生的客户身份基本信息，应采用国密或行业通用的安全算法实现加密存储，加密方式采用表级加密或字段级加密。

5.4 贷后管理

本项要求包括但不限于：

a)催收及呆账核销业务应基于真实的业务账单数据，按照最小必要原则进行数据的处理和使用，保证数据来源的合法合规性，且通过权限控制等措施保证相关数据仅在催收业务范围使用；

b)催收业务应依托于专业的催收业务系统，催收业务的案件整合、策略制定、案件分配、催收作业等均应通过系统化的能力实现，减小从业人员工作过程中的数据接触面和获取面；

c)催收业务系统应基于催收业务开展中的岗位划分，实现基于岗位职责的权限管理，具备权限申请分配、权限回收的能力；

d)催收业务系统应在客户个人敏感数据的展示页面实现默认脱敏和默认水印能力。特殊业务场景下无法脱敏的，如催收过程中需要向催员展示明文数据以核实客户身份、需要展示客户逾期减免材料以进行减免审核，则应通过严格的管控措施限制敏感数据的泄漏风险，如权限管控、禁止数据复制、数据下载等；

e)催收作业中触达客户时，包括但不限于发短信、打电话等，应通过催收业务系统的功能实现，避免催员直接使用客户明文的手机号码等联系方式。使用即时通讯软件触达客户的，应针对潜在风险开展全面的安全管理，如能够对即时通讯软件进行统一管理，加强使用人员的账号身份验证，规范添加用户为聊天好友的过程，关闭不必要的数据发布发送功能，限制聊天内容的下载转发，记录访问操作日志并定期审计等。特殊场景下，业务确需催员使用客户明文联系方式的，应通过额外的补充措施加强安全管理，防范特殊场景下的数据泄漏风险，如报备审批、权限管控、监控审计等；

f)催收业务系统应具备日志和审计能力，对系统上的数据操作均有详细的日志记录，并能根据日志记录开展定期的安全审计，以及时发现潜在的针对敏感信息的高危操作风险；

g)催收业务中所使用或生成的与客户相关的数据，包括但不限于客户的基础信息、授信记录、用信记录、逾期记录、催收记录、短信内容、电话录音等，均应通过权限管理、脱敏水印、下载限制等实现严格的安全管控，涉及到客户身份基本信息在存储环节应采用国密或行业通用的安全算法进行加密保护，加密方式采用表级别加密或字段级加密；

h)呆账核销业务应根据法规要求并基于真实的业务账单数据，按照最小必要原则进行数据的处理和使用，在数据的加工处理、计算分析、展示使用等环节，应采用技术措施保障各环节下的数据安全，如权限控制、查询管控、加密脱敏、页面水印、下载控制等。

5.5 风险管理

本项要求包括但不限于：

a)风险管理中需要使用到的客户信息等数据，在采集前应通过隐私协议等形式征得客户的充分授权，通过外部引入的数据应进行合法合规性评估且引入数据仅能用于风险管理场景；

b)风险管理中使用的风险模型和风险策略等配置信息，应基于最小化原则进行严格的访问控制，防止风险管理信息泄露导致风控策略被绕过；同时针对风控模型、风控策略的变更发布应建设严格的测试审批机制，控制变更发布过程中的业务影响；

c)风险管理中涉及到的客户身份基本信息，在存储环节应采用国密或行业通用的安全算法进行加密保护，加密方式采用表级别加密或字段级加密。

5.6 资产管理

本项要求包括但不限于：

a)互联网贷款资产管理过程中，贷款资产涉及贷款业务的基础明细数据和统计汇总数据，在数据的加工处理、计算分析、展示使用等环节，应采用技术措施保障各环节下的数据安全，如权限控制、查询管控、加密脱敏、页面水印、下载控制等；

b)互联网贷款资产转让过程中，贷款资产涉及资产数据、债务人信息等数据在买方、卖方、技术服务机构等之间传输时，数据输出方应对数据接收方开展安全保障能力的评估，通过签名验签、报文加密等方式保障资产转让过程中的信息传输安全。涉及资产数据、债务人信息的披露时应按照最小必要原则并采用技术措施保障数据安全，如权限控制、查询管控、加密脱敏、页面水印、下载控制等。

5.7 监管报送

本项要求包括但不限于：

a)应严格遵守监管单位的报送要求和报送标准，建立固定的数据加工报送链路，采用技术措施保障报送数据在采集加工、质量控制、提交报送等环节的安全，如权限控制、查询管控、加密脱敏、页面水印、下载管控、安全通道等；

b)应设置报送专员负责监管报送工作，根据监管要求在监管单位完成报送专员备案，并对报送专员开展报送操作和安全意识的培训；

c)应采取技术措施对报送使用的终端进行安全加固，如网络隔离、病毒防护、补丁更新、权限控制等，严格限制报送终端的访问和使用，仅为报送专员开通终端的访问和操作权限；

d)监管有要求或者安全风险防护有需要的，应设置专用的报送间，并建立配套的管理机制、执行规范、技术措施等，如制定报送间管理办法和行为规范、明确报送间管理和使用人员职责、设置报送间门禁权限控制、妥善保管和安全使用移动存储介质、执行网络隔离措施、建立全覆盖的视频监控等。

5.8 合作机构管理

本项要求包括但不限于：

a)应建立合作机构的安全管理制度，明确业务、安全、技术等相关部门的职责，制定面向合作全过程的安全管理要求，并基于管理制度开展业务合作中的动态管理。

b)合作机构准入时应满足以下要求：

1) 业务合作中如涉及数据的共同处理、委托处理等，应清晰定义数据处理的场景，并通过合作协议条款明确数据处理场景下双方的安全管理责任和义务；

2) 业务合作中如涉及数据的共同处理、委托处理等，应在合作机构准入流程中加入对合作机构安全评估的环节，评估合作机构的安全保障能力和数据安全风险，合作机构满足安全保障要求方可开展业务合作。

c)合作机构合作期间应满足以下要求：

1) 应建立与合作机构的应急响应联动机制和应急预案，定期开展联合演练，发生安全事件后应及时与合作机构联动，开展事件的应急响应处置；

2) 宜建立安全情报监测机制，持续监测业务合作中的安全风险，提升安全风险的及时感知能力和响应处置时效；

3) 应建立对合作机构定期的安全评估机制，开展频次不低于年度的安全评估，以保证合作机构的安全能力持续满足要求；

4) 与合作机构的合作范围发生变化时，应面向新的合作范围再次开展安全评估，可基于合作变化适当地调整评估内容，以保证新的合作业务满足安全要求；

5) 应完整地留存与合作机构合作中的各项信息，包括但不限于合同协议、合作准入记录、数据传输记录、系统调用日志、评估审计记录、合作退出记录，留存期限应遵循相关法律法规要求，以满足事后检查和审计的需要。

d)合作机构退出时应满足以下要求：

1) 应基于数据处理关系的变化，根据实际情况对合作机构提出明确的数据删除要求，以保证提供给合作机构的数据在业务合作结束后不会被超范围的使用；

2) 应基于业务合作关系的变化，根据实际情况及时断开相应的网络访问、关停相应的系统接口、回收相应的账号权限、销毁相应的密钥证书以及停止相应的数据同步等。

6 通用安全要求

6.1 安全管理

本项要求包括但不限于：

a)应设置明确的信息安全管理部门和人员承担安全管理工作，并设置安全管理领导组织负责安全战略和重大决策工作；

b)应建立体系化的安全管理制度，覆盖数据安全、网络安全、应用安全、物理安全等关键领域；
c)应加强人员的安全管理，包括员工入职背景调查、保密协议签署、安全培训、权限管理等；
d)应获得法规要求或行业通用的安全资质，如等级保护认证、信息安全管理体系认证等。

6.2 数据安全

本项要求包括但不限于：
a)应建立数据资产目录、数据分类分级管理制度和执行规范，并进行动态管理维护，开展数据的分类分级保护；
b)宜使用自动识别工具，结合企业定义的数据分类分级策略自动识别和标记数据的类型和级别；
c)应满足JR/T 0223-2021要求；
d)个人信息应满足GB/T 35273及JR/T 0171-2020要求。

6.3 系统安全

承载互联网贷款核心业务系统的网络、主机和应用应满足等保三级或以上安全要求，核心业务系统如互联网贷款业务系统、互联网贷款运营系统、互联网贷款合作机构管理系统等。

6.4 物理安全

本项要求包括但不限于：
a)数据中心建设应满足GB50174-2017和JR/T0265-2023要求；
b)承载互联网贷款核心业务系统的数据中心应满足等保三级或以上安全要求，核心业务系统如互联网贷款业务系统、互联网贷款运营系统、互联网贷款合作机构管理系统等。

6.5 日志安全

a)应制定相应的操作流程规范，确保日志的安全收集、存储和访问控制，保障日志数据的安全性与合规性；
b)禁止在系统运维日志中记录明文的敏感信息，包括个人金融信息、客户身份基本信息等；
c)系统运行维护类日志应至少保存6个月，特定情况下需延长至1年或3年。商业银行类交易日志根据国家会计准则要求保存，通常不少于1年。金融机构客户交易记录至少保存5年，涉及反洗钱调查时保存期限应延长至调查工作结束。

6.6 信息科技外包安全

本项要求包括但不限于：
a)面向服务提供商的安全管理应满足以下要求：
1) 应建立信息科技外包的安全管理制度，明确科技外包的安全管理组织架构，制定面向外包服务全过程的安全管理要求，并基于管理制度开展外包服务中的动态管理；
2) 应对信息科技外包活动及相关服务提供商进行分级管理，对重要外包和一般外包采取差异化管控措施；
3) 应明确服务提供商的准入标准，准入前开展尽职调查，评估服务提供商的网络和信息安全保障能力，在合同或协议中明确服务提供商的安全管理责任和义务；
4) 应对外包服务过程中的安全和业务连续性保障进行持续监控，建立风险事件的应急预案，开展频次不低于年度的安全评估和应急演练；

5) 应开展信息科技外包及其风险管理的审计工作，定期对信息科技外包活动进行审计，至少每三年覆盖所有重要外包，发生重大外包风险事件后应当及时开展专项审计；
6) 服务提供商退出时应基于业务服务和数据处理关系变化，根据实际情况对服务提供商提出明确的数据删除要求，关停相应网络访问、系统接口，回收相应账号权限等。

b)面向服务提供商人员的安全管理应满足以下要求：

1) 应对引入的服务提供商人员开展背景调查、签订保密协议、组织安全教育培训，增强网络和信息安全意识；
2) 应按照最小必要原则对引入的服务提供商人员审慎开放访问权限，严格管理和监控服务过程中的安全风险，涉及核心系统开发维护、敏感数据操作处理等场景还应采取针对性措施做进一步安全保障，如采取隔离办公职场、职场视频监控、云办公桌面、网络访问控制等。

6.7 业务连续性

本项要求包括但不限于：

a)应建立业务连续性的管理制度，明确业务连续性的管理组织架构和职责，制定面向业务运行全过程的连续性管理要求，并基于管理制度开展业务连续性的动态管理；

b)应根据JR/T 0044-2008要求建立灾难备份中心，并对灾难备份中心开展常态化运行维护和有效性验证，确保灾难发生后备份中心可以继续保障业务运行或使用备份数据能够进行业务的恢复；

c)应制定重要事件的安全应急预案，预案内容包括安全应急处理流程、系统恢复流程等内容，应急预案场景包括但不限于物理安全、网络安全、主机安全、应用安全、数据安全、人员安全、消费者权益保障等方面；

d)应根据制定的安全应急预案定期开展应急演练，对相关人员进行教育培训，留存培训记录，记录包括培训对象、培训内容等；

e)应建立安全应急响应必要的工具集合，包括木马查杀、漏洞检测、网络扫描、渗透测试、防护阻断等安全应急工具，定期检查工具集合的可用性及版本情况，及时升级维护。

参 考 文 献

[1] 中国人民银行[2007]第2号 金融机构客户身份识别和客户身份资料及交易记录保存管理办法

[2] 中国人民银行[2018]第102号 关于进一步加强征信信息安全管理的通知

[3] 中国人民银行[2020]第5号 金融消费者权益保护实施办法

[4] 中国人民银行[2023] 中国人民银行业务领域数据安全管理办法（征求意见稿）

[5] 银监会[2006]第63号 商业银行信息科技风险管理指引

[6] 银保监[2020]第9号 商业银行互联网贷款管理暂行办法

[7] 银保监[2021]第141号 银行保险机构信息科技外包风险监管办法

[8] 银保监[2022]第14号 关于加强商业银行互联网贷款业务管理 提升金融服务质效的通知