ICS 35.240.99
L67

团　　体　　标　　准

XX/T XXXXX—XXXX

平台生态数据安全基本要求

Basic Requirements for Data Security of Platform Ecological

（草案）

2023 年 03 月

－XX－XX 发布　　XXXX－XX－XX 实施

中国计算机行业协会发布

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。

本文件由中国计算机行业协会提出。

本文件由中国计算机行业协会归口。

本文件起草单位：蚂蚁科技集团股份有限公司、中国软件评测中心、上海交通大学、天弘基金管理有限公司、安恒信息技术有限公司。

本文件主要起草人：郭亮、王庭、宋铮、陈树鹏、冯朝、方超、王昕娅、陆平、王嵩贺、范云龙、赵莹、唐刚、张德馨、杨志、安健、刘思思、谷大武、孙士锋、付婧妍、陈星、何佳、张可菁、林明树、曹思怡、付春红、范孟会、陈中原、张天然、刘兴瑶、肖磊、顾为群、黄山、王少宇、王润、苏芮、迟宇宁。

引　言

随着数字经济的不断发展，数据成为支撑产业发展的生产要素，数据安全的重要性越发凸显。同时数字经济业务模式复杂，数据的使用和保护需要生态参与者共同守护。为落实《网络安全法》《数据安全法》《个人信息保护法》等法律法规的相关规定，促进平台生态个人信息保护和数据安全管理能力提升，本文件为组织如何搭建平台生态数据安全保护能力，履行个人信息保护和数据安全责任提供指导，旨在帮助组织更好满足安全合规要求，提升防数据泄漏和应急溯源能力，发挥数据要素价值，促进数字经济产业发展。

平台生态数据安全基本要求

1 范围

本标准规定了平台生态数据安全的基本要求，具体包括平台运营者数据安全保护、生态合作过程中的数据安全保护，数据防泄漏和应急溯源，为履行个人信息保护和数据安全责任提供参考。

本标准适用于提供互联网平台服务的平台运营者和平台生态机构。

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2019 信息安全技术 网络安全等级保护定级指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 40050-2021 网络关键设备安全通用要求

GB/T 20988-2007 信息系统灾难恢复规范

3 术语和定义

GB/T 17859、GB/T 22240、GB/T 22239、GB/T 25069界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069、GB/T 20988-2007、GB/T 35273-2020中的某些术语和定义。

3.1 平台

即互联网平台，通过网络信息技术，使相互依赖的双边或者多边主体在特定载体提供的规则下交互，以此共同创造价值的商业组织形态。

3.2 平台运营者

向自然人、法人及其他市场主体提供经营场所、交易撮合、信息发布等互联网平台服务的法人及非法人组织。

3.3 平台生态机构

在互联网平台内提供商品或者服务的经营者。

3.4 数据安全网关

可承载跨主体(包含外部主体)数据流通且具备数据管控能力的系统，一般由运行态和管理态共同构成。运行态指数据跨主体流通时实时的数据流动过程，管理态指数据跨主体流通时事前的管理流程和机制。

3.5 敏感个人信息

一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

3.6 特殊数据

指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害公共利益的数据。包括未公开的政务数据，重点行业领域的生产、运行数据，金融业大型或特大型机构、金融交易过程中重要核心节点类机构的关键业务数据，单个生态机构累计被授权获取超过百万量级以上的敏感个人信息等。

3.7 数字水印

将特定的数字信号嵌入数字产品中保护数字产品版权、完整性、防复制或去向追踪的技术。

3.8 资产画像

通过对资产内容、行为对象、防护水平等方面的分析和评估，建立资产分类分级及对应权限、访问控制、加密等安全防护水平的档案。

3.9 数据血缘

一种生命周期的定义，主要包含数据的来源以及数据随时间移动的位置。数据血缘用于分析表和字段从数据源到当前表的血缘路径，以及血缘字段之间存在的关系是否满足，并关注数据一致性以及表设计的合理。

3.10 链路刻画

描述数据从收集，生产到服务的全链路的变化和存在形式。

3.11 蜜罐

在威胁狩猎过程中，蜜罐旨在主动收集甚至勾引外部威胁进入组织设计的陷阱中，以提升捕获威胁主体，定位威胁源头，打击威胁本体的实际能力。

3.12 电子证据

最终达成并满足资政情报能力的关键，也是可以对外部公开，可以经受挑战和验证的证据材料。

3.13 威胁狩猎

也称威胁搜索、网络狩猎或者网络威胁搜索，不同于APT攻击或者红蓝军渗透测试这类网络应用环境安全的测试，属于模拟攻击者开展寻找黑入IT环境中安全威胁的行为。

3.14 灾难恢复预案

定义信息系统灾难恢复过程中所需的任务、行动、数据和资源的文件。用于指导相关人员在预定的灾难恢复目标内恢复信息系统支持的关键业务功能。

[来源：GB/T 20988—2007，定义3.10]

3.15 业务连续性管理

为保护组织的利益、声誉、品牌和价值创造活动，找出对组织有潜在影响的威胁，提供组织建设有效反应恢复能力框架的管理过程。包括组织在面临灾难时对恢复或连续性的管理，以及为保证业务连续计划或灾难恢复预案的有效性的培训、演练和检查的全部过程。

[来源：GB/T 20988—2007，定义3.4]

4 平台运营者安全要求

4.1 基本要求

平台应满足网络安全等级保护安全要求，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理、安全运维管理等要求。具体参照GB/T 22239-2019《网络安全等级保护基本要求》。

4.2 组织保障

4.2.1 管理制度

制度体系应包括数据安全方针，数据安全工作各关键领域的管理要求，针对具体环节落地实施的操作规范、指南，管理制度集体执行过程中产生和使用的过程性文档。

4.2.2 组织建设

本项要求包括：

a) 应明确架构层级、职责划分以及人员的具体分工，数据安全应建立清晰的岗位职责、奖惩制度、考核机制；
b) 数据安全组织架构应包括决策层、管理层、执行层和监督层。同时，组织应建立数据安全接口人机制，进一步加强各层级、各部门的沟通协调与工作协同。

4.2.3 人员能力

本项要求包括：

a) 安全人员应具备实现组织、制度和技术工具的建设和执行能力；
b) 人员核心能力应包括数据安全管理能力、数据安全运营能力、数据安全技术能力及数据安全合规能力，具体参照 GB/T 37988-2019《信息安全技术—数据安全能力成熟度模型》。

4.3 能力建设

4.3.1 数据资产管理

4.3.1.1 分类分级

本项要求包括：

a) 应基于现有标准建立适当的数据分类分级标准；
b) 应建立自动化的分类分级检测能力，确保分散在组织各处各层面的各类数据能够被及时发现和快速管控；
c) 应支持自动化数据分类分级服务，应包含全面资产扫描、智能数据分类和统一数据定级。

4.3.1.2 资产画像

本项要求包括：

a) 应支持将组织内部数据及其流转信息进行串联、合并、加工和处理，建立全域数据的关系图谱；
b) 应支持数据处理生命周期各环节进行多角度、多维度的透视观察能力，向各类业务场景提供全方位的数据服务。

4.3.1.3 链路刻画

应通过数据库解析、代码解析等方式建立数据链路分析能力，形成数据血缘，实现每个节点的数据流动清晰可见，可分析、可监控，降低数据安全的风险管控成本。

4.3.2 权限管理

4.3.2.1 凭据管理

应建立身份管理系统，通过身份鉴别信息的可用不可见、统一应用身份颁发和验证，统一管控账号和口令等身份凭据。

4.3.2.2 认证管理

应支持全场景认证机制，支持人和应用的身份认证，并实现认证和记录用户身份。

4.3.2.3 授权管理

应遵循权限最小化原则，权限互斥隔离，具备完善的权限生命周期管理，并建立了行列级鉴权能力来保护个人信息。

4.3.2.4 操作审计

应建立端边云的全链路审计能力。

4.3.3 数据防泄漏

4.3.3.1 标识管理

本项要求包括：

a) 应定义用户在应用下的唯一标识；
b) 同一个用户应在不同应用的标识不同，实现了用户数据在应用维度的隔离，避免数据拼图风险；
c) 应只有用户授权应用才能使用该用户的标识，即使数据扩散也无法直接使用。

4.3.3.2 数字水印

本项要求包括：

a) 应根据实际场景采用不同数字水印技术；
b) 应在文档、图片中增加明水印用以标识文档的权属信息、使用范围，限制数据的违规使用和外发；
c) 应在人员通过网页访问敏感信息的场景下，在网页中增加水印，对人员的图片截取等行为进行一定程度的防范；
d) 应在数据库导出数据、重要文件中增加暗水印，用于在数据发生泄漏时进行溯源，快速定位数据的来源与流转。

4.3.3.3 接口脆弱性检测

本项要求包括：

a) 应建立接口脆弱性检测能力，多维度分析接口在使用过程中是否存在无鉴权、越权、可遍历等泄露敏感信息的风险；
b) 应对已发现的脆弱接口，给出安全加固方案，消除原接口的脆弱性。

4.3.3.4 流量攻击防护

本项要求包括：

a) 应对全部的网关进行全流量数据采集，快速识别流量内容，对数据进行标准化沉淀，构建边界链路、接口画像、请求行为等信息，为风险检测及挖掘提供坚实的数据基础；
b) 应对接口、应用、账户、设备、环境等进行多维度分析检测，挖掘存在的风险，最终形成以流量为基础，以接口为中心，以接口关联主体为对象发现未知风险场景，构建风险主体的业务自助分析能力，实现风险主体的业务运营分析和检测策略的双向驱动；
c) 应实现流量数据采集到风险处置的闭环。流量处置中心具备接口、账号、IP 等多维度处置能力，构建封禁、限权、降频等多种处置手段，对不同的风险类型进行分层处置，提高黑产攻击成本。

4.3.3.5 流通与计算环境管控

本项要求包括：

a) 应对企业内部数据做统一受控流转治理与管控，应涉及流通申报、数据安全网关、流通策略三个核心特性；
b) 应对多源数据融合计算场景建立整体安全解决方案体系，通过数据流入，安全受控计算和流出安全管控，保障大规模多源数据计算过程安全可控。

5 生态机构管理要求

5.1 基本要求

5.1.1 生态机构管理原则

本项要求包括：

a) 对涉及平台机构和生态机构之间的数据流通场景，平台应对生态机构开展接入和过程管理。
b) 应明确数据流通基本原则，包括目的明确最小必要、用户数据明示授权、流通主体权责一致、流通安全清白可证等。

5.1.2 数据流通规范

本项要求包括：

a) 应基于数据、组织、数据安全网关，三维构建数据流通标准。
b) 为实现数据安全流通，如涉及个人信息、重要数据等敏感数据，生态机构应周期性参与平台组织的安全合规评价工作，生态机构也可提交满足平台机构要求的第三方安全测评认证、安全保险等凭证，平台审核通过后视为有效。

5.1.3 安全合规评价

平台应基于标准开展对生态机构数据流通的安全合规性评价，包括生态机构准入评估、生态机构评级、生态机构安全认证等维度。

5.2 组织管理

5.2.1 管理制度

本项要求包括：

a) 应在合法、合理范围内与生态机构实现稳定的业务合作与数据合作；
b) 应针对不同生态合作场景，从多个维度提出安全管理制度，规范生态机构数据处理行为。对于涉及个人信息处理的生态机构，应制定安全能力分级要求，生态机构应满足对应等级要求。
c) 管理制度还应包含规范合作机构新增入驻管理流程的生态机构准入管理规则、保障用户个人信息权益的用户信息处理规范、横跨数据安全全生命周期管控的生态机构安全管理规范、约束服务商对商户提供运营/推广/开发服务的服务商管理规范、针对特殊应用类型生效的小程序/生活号运营规范、以及定义生态机构违规处置的违规处理规范等。

5.2.2 组织建设

本项要求包括：

a) 应建立系统化的长效机制协助企业建立并提升自身数据安全能力，共同维护安全清朗的网络环境；
b) 宜通过行业性组织共同提升整个行业的数据安全水平，共同推动行业透明、规范发展。

5.3 合作过程管理

5.3.1 生态机构准入

本项要求包括：

a) 生态机构应保证，在为用户提供产品和服务的过程中涉及个人信息处理时，严格遵守中华人民共和国相关法律法规的要求；
b) 应参照相关国家标准，规范个人信息处理行为，保障用户的合法权益和社会公共利益；
c) 应制定安全能力分级要求，生态机构应满足对应等级要求；
d) 对未达到对应安全能力要求或未按时完成安全能力评估的生态机构，应限制获取个人信息接口权限及相关服务。

5.3.2 数据流通评审

本项要求包括：

a) 应对开放平台/服务商平台获取的敏感信息进行加密；
b) 不得通过任何方式未授权留存用户的敏感个人信息；
c) 应配合平台方委托的第三方机构进行数据流通场景下的安全评审；
d) 应保证获得的敏感信息经过用户明示同意授权，规范使用；
e) 应保证仅限在其申明的范围内使用；
f) 应接受服务商平台、监管机构、行业自律组织及公检法等有关部门调查，协查商户的违法违规行为，督促商家整改并及时通知开放平台/服务商平台。

5.3.3 数据接收方安全能力评估

本项要求包括：

a) 应对涉及重要数据流通合作的生态伙伴，周期性组织进行数据安全能力及个人信息保护评估工作，确保数据接收方在达到相应安全能力要求后平台放行企业准入或数据开放过程；

b) 应对数据接收方的安全能力评估整体涵盖组织管理与机制、数据安全生命周期管理、系统安全、网络安全、终端安全、安全运营、应急保障等部分；
c) 应对未能满足安全能力要求的生态机构，约束数据权限或服务。

5.3.4 风险巡检与尽责通知

本项要求包括：
a) 应从数据安全网关、流量、数据接收方等多维度，基于重点关注风险，建立定期风险评估机制；
b) 当生态机构出现安全风险或安全事件时，平台应对生态机构进行风险揭示与告知，敦促生态机构尽快对风险进行响应并处置修复；
c) 当生态机构出现安全风险或安全事件时，平台应具备对生态机构告警、拦截、处置、阻断能力，按需实现风险快速止血；
d) 生态机构出现例如数据泄露、舆情事件或其他重大数据安全风险时，平台方应尽责通知的基础上，视具体情况对生态机构采取额外限制措施，包括但不限于版本下架、隐藏、应用下线、终止业务等。

5.3.5 数据流通过程

本项要求包括：
a) 若生态机构在数据流通过程中存在违规行为，致平台用户、其他生态机构或社会公众的合法权益受到侵害，平台应按需给予相应的处罚，严重时应启动清退机制，终止向生态机构提供服务；
b) 平台应对未授权访问、水平权限校验失效、身份认证机制不健全、用户敏感信息透出造成用户信息被批量爬取等风险做安全检测；
c) 当平台发现数据流通过程出现安全或合规风险时，应立即启动应急流程，并按需启动回收与退出机制流程。

5.3.6 回收与退出机制

本项要求包括：
a) 生态机构在合作过程中，存在违规行为，导致平台用户、其他生态机构或社会公众的合法权益受到侵害时，应给予相应的处罚；
b) 应视风险情况及情节严重程度，对应用或接口采取以下措施，包括但不限于：个人信息接口调用限流/限频、调用权限封禁/回收，应用隐藏或下线。并取消或调整小程序开发者部分服务权限，包括但不限于：警告、版本下架、隐藏、应用下线、终止小程序业务。

5.4 数据安全网关管理

5.4.1 风险评估管控

本项要求包括：
a) 应对数据安全网关进行安全风险评估，确保数据传输安全风险处于可接受水平；
b) 应建设安全评估能力，包括可识别出数据传输数据的资产类型、敏感等级的资产识别能力；数据交互各方的身份识别认证能力；传输敏感数据，业务合理性判断能力；异常流量的监测，告警能力和机制；阻断违规数据传输的拦截能力等；
c) 应明确重点关注风险，包括：调用方身份冒用风险；数据传输过程中被窥探、被篡改风险；传输字段超出约定范围，过多地传输信息；业务合作变更时，（如合作合同结束，范围变化等）传输数据未做调整；数据爬取风险等；

d) 评估现有防护能力，应重点关注数据传输安全加密技术，接口调用认证鉴权方式，应有相应的安全产品支持基于业务场景的访问控制，应有安全产品阻止爬虫爬取数据；
e) 应建立数据安全网关的风险巡检机制，根据数据传输安全管控策略，对可能引发风险的操作进行告警、拦截等动作。

5.4.2 最小输出管控

应基于最小必要原则，在数据传输过程中，采用字段裁剪，行级鉴权，敏感信息脱敏等技术。仅传输业务实现必需的最少字段，最少数据量，不传递业务不相关数据。

5.4.3 管控效果度量

应通过收集、分析数据安全网关的配置数据和流量数据，通过指标体系和风险评估提供度量报告和洞察结果以辅助安全治理决策，从而降低数据传输安全风险发生的可能性和损失。

6 生态机构安全要求

6.1 基本要求

生态机构应满足网络安全等级保护安全要求，包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全建设管理、安全运维管理等要求。具体参照GB/T 22239-2019《网络安全等级保护基本要求》。

6.2 敏感个人信息管理

6.2.1 安全管理机制

本项要求包括：

a) 应指定数据安全负责人，负责日常数据安全事件响应与应急处置；
b) 应建立必要的数据安全管理制度，在研发、生产、办公及业务运营等环节规范数据使用，保障个人信息的安全；
c) 应在员工（含外包）录用前，进行必要的背景调查，并与涉及个人信息处理的关键岗位人员需签署关于数据安全的责任协议；
d) 应在员工调岗或终止劳动合同时，及时调整或终止权限，回收门禁卡，强化终端管控等，避免用户个人信息产生泄漏。

6.2.2 数据生命周期管理

本项要求包括：

a) 收集个人信息应遵循最小化要求，应用系统在收集个人信息前，须对外部数据来源的合法性进行确认，确保数据安全网关的合法性和正当性；并向个人信息主体明确告知收集的个人信息类别，并获得个人信息主体的明示同意后，方可进行信息收集；并向个人信息主体提供更正或补充个人信息的方法；
b) 应采用安全通道、通道加密、数据加密等措施保护数据，如：HTTPS、VPN 等，并采用国家认证的加密算法及认证产品，如：SM2、SM3 等；
c) 应通过平台官方接口获得涉及用户个人信息的数据及相关密钥、凭证，须做好加密存储。禁止代码中明文编码，防控泄漏；

d) 不同商户、应用须分别做好隔离，不同应用间数据独立存储，不可混用；个人信息进行有效加密存储，按业务所需设置存储时限；
e) 涉及数据跨境业务，应遵循国家数据跨境相关的法律法规；
f) 涉及个人信息数据销毁时，应采取有效技术手段进行完全删除，确保数据不可恢复；
g) 个人信息主体主动要求删除个人信息或与用户终止服务时，必须立即删除全部因使用本服务而获得的数据（包括各种备份），且不得再以任何方式继续使用，除非法律法规要求必须，有权保留。

6.2.3 网络与系统安全

本项要求包括：
a) 应对登录系统的用户分配帐号和权限，并重命名或删除默认帐号，修改默认帐号的默认口令；
b) 应制定明确的密码策略，确保设备&帐号的密码规则满足策略要求，禁止密码设置为空或使用默认密码，定期更换密码，帐号初始密码禁用固定密码，应随机生成。密码强度要求满足包含字母大写、字母小写、数字、特殊字符其中的三种或以上组合，且长度至少 8 位以上；
c) 应及时删除或停用多余的、过期的帐号，避免帐号多人流通；
d) 业务系统应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

6.2.4 终端安全

办公终端应制定相应的操作系统和必要应用程序的补丁管理计划，及时修补漏洞。

6.2.5 安全运维管理

本项要求包括：
a) 应用、系统、数据库等涉及个人信息操作场景，应做日志记录并保存，以支持有效的审核、安全取证分析等；
b) 应建立数据安全应急处置机制，制定数据安全事件应急预案，发生数据安全事件时能及时启动应急响应机制，进行风险排查处置，采取措施防止危害扩大，并上报处置结果；
c) 生态机构应向平台提供完整的企业基础信息、包括但不限于涉及企业相关业务资产清单（应用名称、服务器 IP 等）、数据安全负责人信息（姓名、手机、邮箱等），如有变更须在 3 天内完成信息更新；
d) 生态机构应周期性参与平台组织的安全能力评估工作，也可自行提交由第三方安全机构完成的安全评估，安全评估需提交平台运营者审核，审核通过后视为有效。

6.3 特殊数据管理

本项要求除敏感个人信息管理中的各项要求外，应包含以下额外要求。

6.3.1 安全管理机制

本项要求包括：
a) 应成立数据安全管理机构，有明确数据安全管理负责人，数据安全管理负责人应当具备数据安全专业知识和相关管理工作经历；
b) 涉及存在与第三方合作场景（包含外包服务），应就数据合作签订协议，明确处理范围、权利及义务。确保从平台获取的任何信息，限制关联三方对相关信息的使用并保持信息的保密性。

应对关联三方整体的资质进行审核，涉及数据交互的三方应包含必要的安全资质（如 ISO27001、等保），并在合作期间持续监控评估三方的安全能力；

c) 应定期组织开展数据安全教育培训，特别是针对涉及用户个人信息处理人员的安全规范与心智教育；

d) 应制定数据安全培训计划，每年组织开展全员数据安全教育培训，数据安全相关的技术和管理人员每年教育培训时间不得少于二十小时。

6.3.2 数据生命周期管理

本项要求包括：

a) 生态机构应对数据资产进行分类分级管理；

b) 应根据实际职责严格限定可访问或使用个人信息的权限及数量，严格限制数据拷贝权限及批量导出行为；

c) 系统开发环境、测试环境应使用脱敏的或经过去标识化处理的个人信息。

6.3.3 网络与系统安全

本项要求包括：

a) 应授予管理帐号所需的最小权限，实现管理用户的权限分离；

b) 业务系统应关闭不必要的系统服务、默认流通和高危端口，仅开放必须的端口、服务。（如：80，443 端口）；

c) 核心业务系统应具备脆弱性检测的能力，能对常见的主机入侵、恶意代码攻击、系统漏洞进行监测并告警；

d) 应具备帐号风控管控能力，保护和管理平台帐号的安全（登录风控、弱密码监测、登陆认证行为管控等），识别帐号的异常风险并进行管控；

e) 应划分不同的网络区域，独立的生产、开发测试和办公网络区域等，重要网络区域及各网络区域应采取可靠的技术或方案隔离。

6.3.4 终端安全

本项要求包括：

a) 办公终端应设置登录口令保护、屏幕保护及安装防病毒软件，并定期进行病毒库更新及全盘杀毒；

b) 涉及用户个人信息的办公终端应采取必要的数据防泄漏措施，如：防病毒软件、网络访问限制、DLP、终端准入等。

6.3.5 安全运维管理

本项要求包括：

a) 应用、系统、数据库等涉及个人信息操作场景，应做日志记录并保存，并定期对日志进行审计，审计报告至少保留三年；

b) 生态机构应建立漏洞管理机制，定期对业务系统进行漏洞扫描；

c) 生态机构应对漏洞进行跟踪管理，及时修复漏洞，高危漏洞 24 小时内修复，中危漏洞 3 天内修复，低危漏洞 7 天内修复；

d) 发生重大信息泄露、毁损、丢失等数据安全事件处置完毕后，应由专业的第三方安全机构进行安全测评，并将测评报告提交平台；

e) 应制定实施数据安全保护计划，定期组织演练，保障所处理的个人信息的安全。

7 应急溯源安全要求

7.1 溯源能力

7.1.1 情报集散

本项要求包括：

a) 情报采集应满足合规要求基础上全面完整采集，不得违规采集其他组织的非公开或保密信息；
b) 情报流转分配应符合最小分享原则，避免被滥用和扩散；
c) 情报消费应明确消费方式和目的，最终消费的结果应各方确认后反馈给情报分发者；
d) 情报销毁存档应建立处置准则，确保有记录留存。

7.1.1.1 事件情报

本项要求包括：

a) 消费者应是情报直接关联处置方；
b) 应有明确的事件指向性，如组织相关，数据样本等；
c) 在内部流转消费过程中，应根据实际应用场景及使用数据，转化为具体事件；
d) 最终的反馈应是事件处置的结果。

7.1.1.2 漏洞情报

本项要求包括：

a) 所有公开漏洞信息的获取应公开透明；
b) 禁止私自采集传播 0-day 等非公开漏洞信息；
c) 漏洞情报的消费主体应落实到漏洞上；
d) 在组织内部的消费处置对象应逐渐转化为漏洞修复处置；
e) 最终的反馈应是漏洞处置的结果。

7.1.1.3 舆情情报

本项要求包括：

a) 公开舆情的监控应明确边界，对于禁止批量获取的舆情信息，不得违规获取；
b) 应对公开舆情信息明确并定义多维度的挖掘分析能力，采集并分析境内外舆情差异和聚合性；
c) 应通过灵活策略配置，根据组织需求制定预警机制，实时监控舆情走向，及时预警出发到关联方，做到及时应对处置；
d) 应做到快速采集，快速分析，实时传递。

7.1.2 威胁感知

7.1.2.1 态势监控

本项要求包括：

a) 应具备日常运行状态的监控体系；
b) 应定义日常常规运行监控模式，可快速定位并发现异常状态，并可第一时间处置；
c) 应提炼出关键指标和数字指标，便于整体和细节状态展示；
d) 应 100%覆盖面向基础设施的监控；
e) 应对底层的监控确保数据的采集没有被篡改或刻意删除。

7.1.2.2 异动跟踪

本项要求包括：

a) 应能快速定位到异常，并可快速透视，可看到当前异常的具体异常内容以及其联动项目异常；
b) 应对异常的监控维度，包含业务、安全、数据。

7.1.2.3 常态化度量

本项要求包括：

a) 应对常态化以指标化的形式，可实时跟踪态势的波动和变化；
b) 应提炼出针对性的指标，指标应具备易读性和公信力；
c) 应明确计算过程和原始数据的采集积累；
d) 应对过程和结果都能做出实时的数字化判定。

7.1.2.4 风险联动

7.1.3 威胁狩猎

7.1.3.1 蜜罐

应具备蜜罐设置能力及安全管理要求，包含但不限于，系统蜜罐、数据蜜罐、载体蜜罐、存储蜜罐、心智蜜罐、钓鱼体系。

7.1.3.2 电子证据

应具备电子证据取证能力及安全管理要求，包含但不限于，电子取证采集要求、电子取证保存要求、电子取证过程要求、电子取证销毁转移要求。

7.1.4 威慑反制

7.1.4.1 专案打击

应包含但不限于，专案人员资质要求、专案报备要求、专案上报要求。

7.1.4.2 联合办案

应包含但不限于，生态业务方联动规范、生态业务方联动备案、生态业务方联动风险评估、生态业务伙伴证据/数据流通拼接要求。

7.2 应急管理

7.2.1 应急预案

7.2.1.1 应急组织

本项要求包括：

a) 管理决策者，应出自组织的高层管理人员，在应急过程中起到决策重要输入的作用；
b) 执行保障者，应出自组织的中层管理人员，是风险事件处置环节中的风险管理者，对于具体风险的处置判断和修复行为负责；
c) 应急执行者，应出自各风险域的实操人员，在应急处置过程中接收风险处置意见，落实止血动作；

d) 资源保障者，应出自横向支持团队，在应急处置及灾后重建过程中提供人力资源，硬件资源，物质资源的支持和保障。

7.2.1.2 灾难恢复预案

灾难恢复预案旨在风险的暂时性或彻底根除，消除掉当前风险或威胁对于组织的影响，应包含但不限于，事件处置规范、生态呼叫树、生态伙伴联动排查。

7.2.1.3 业务连续性管理

应包含但不限于，生态业务风险评估、生态伙伴风险评估、生态威胁处置规范。

7.2.2 事件处置

7.2.2.1 自动化处置

7.2.2.2 风险复核

应包含但不限于，风险发生的原因、风险处置过程、风险处置结果评估，风险修复完全情况，未完全修复或风险接受项目评估、风险二次发生评估，可能性及危害等级、风险修复成本核算等。

7.2.2.3 防御体系补漏

应包含但不限于,当前风险防御体系疏漏或薄弱项目、防御建设优化方案、防守能力建设成本评估、防守能力建设后风险评估。

7.2.3 归因溯源

7.2.3.1 日志完整性

应包含但不限于，日志存储备份、日志数据全量/抽样digest、日志数据加密存贮、日志数据acl、日志数据本地/异地采集传输。

7.2.3.2 日志全面性

应包含但不限于，日志采集覆盖、日志采集方式、日志存储时长、日志采集规范。

7.2.4 对抗演练

本项要求包括：

a) 攻防两方的隔离与独立性；
b) 扮演攻击的一方，不同于传统渗透，只负责发现漏洞，需要更进一步了解业务和防守者痛点；
c) 不论攻击者还是防守者，都需要明确关键核心指标，用以判断每一次攻防演练对业务和技术的价值。

7.2.5 自证清白

当出现由于生态导致数据泄露事件时，组织应明确举证非自身导致的全部证据，所有证据应被公正第三方接受并采纳，应自证生态事件风险事件与组织无关。

7.2.5.1 自动化策略

本项要求包括：

a) 数据输出判断，当前数据是否归属数据组织，且是否合法合规输出给了生态生态机构；
b) 证据链拼接；
c) 证据防篡改；
d) 自动化取证，应急溯源过程中可以自动化取证留痕，关联的辅证可以自动化选择并参与拼接为证据链。

7.2.5.2 证据链完整

本项要求包括：
a) 完整性，组织应确保证据链未被组织本身，生态伙伴或任何第三方篡改；
b) 全面性，证据链应验证一个事件过去至少半年直至出现的完整链路及过程；
c) 最小披露，在面向生态伙伴及外部三方时，组织所提供的证据链应满足最小使用原则，同时在取证过程中，组织只能取证风险相关的数据，不能越界采集；
d) 保密性，证据链的保存传输过程应使用可信的加密算法，以确保证据不会被三方直接读取。

8 社会责任要求

8.1 个人人身、财产利益保护

8.1.1 安全要求

若有充分证据表明，现已存在能够显著提高数据安全和个人信息保护水平的更高要求，组织不宜仅仅满足于较低的要求。

8.1.2 产品或服务设计开发

本项要求包括：
a) 应确保在正常和合理可预见的使用情况下,提供的产品或服务,对消费者的人身、财产是安全的；
b) 应考虑并顾忌消费者的需求差异、能力差异或局限性（尤其是了解信息所需时间的差异或局限性）来确保对产品或服务的合理设计；
c) 应评估产品或服务在所有使用阶段和条件下可能致使的人身、财产损害风险；
d) 应通过遵循以下优先顺序来降低风险:首先考虑采用完全消除风险的安全设计;然后考虑增设保护性装置;最后才考虑向消费者提供警示信息。

8.1.3 产品或服务使用

本项要求包括：
a) 产品或服务的使用过程中，宜建立能够识别消费者风险行为的特征库；
b) 识别消费者存在风险行为的，宜通过复合措施核验消费者的身份；
c) 或通过显著方式向消费者警示可能出现的风险，并经消费者确认；
d) 消费者遭受或可能遭受人身、财产损害的，组织宜为消费者提供简捷、迅速的反馈处置方式；
e) 消费者使用产品或服务前组织宜使用文字信息，说明与使用有关的风险及预防措施；
f) 还宜尽可能使用符号、图片向消费者传递告知重要信息；
g) 避免使用敏感个人信息。如产品或服务使用敏感个人信息的，应遵守相关法律法规的要求，并脱敏展示；

h) 产品或服务使用过程中，如出现重大漏洞，或者包含有误导或错误的信息，应中止提供服务，通知受影响的消费者并采取补救措施；
i) 建立能够识别违法违规行为的特征库，并持续监测、打击违法行为。

8.2 消费者投诉及争议处理

本项要求包括：

a) 应以清晰、显著的方式公示投诉、处理方式及反馈时限；
b) 公示的投诉应有效且高效，尽可能从组织内部实现处理的转换，不得频繁要求消费者更换投诉方式；
c) 应建立投诉处理流程，并完善有效的操作规范，形成从投诉到反馈的闭环，避免消费者投诉无人处理、无人反馈等情况；
d) 应建立投诉处理库，记录投诉处理的时间、原因、处理情况等，便于组织定期评审并改进；
e) 应建立投诉处理满意度的反馈途径，消费者可通过该途径反馈意见或建议，便于组织定期评审并改进；
f) 应提供充分和有效的人工客服支持；
g) 应处理投诉时不向消费者收取不合理费用，不要求消费者放弃其法律上的权利。

8.3 消费者教育和意识培养

本项要求包括：

a) 应在运营的产品或服务的显著界面、位置、步骤设置消费者教育和意识培养相关的宣传活动；
b) 应面向消费者就有关数据安全和个人信息保护的适用法律法规、投诉举报途径、消费者保护机构与组织等开展教育活动；
c) 应面向消费者就产品和服务相关的数据安全和个人信息保护功能等开展教育活动；
d) 应面向消费者就与使用有关的风险信息以及所有必要的警示信息开展教育活动；
e) 应面向消费者就相关数据和个人信息泄露导致的风险和案例开展教育活动。

参 考 文 献

[1] GB/T 35273-2020 信息安全技术 个人信息安全规范

[2] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

[3] GB/T 37932-2019 信息安全技术 数据交易服务安全要求

[4] GB/T 37973-2019 信息安全技术 大数据安全管理指南

[5] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

[6] NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations