ICS
L

团　　体　　标　　准

T/ISC XXXX—XXXX

数据安全技术能力评估要求

Technical specification for data security capability assessment

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中　国　互　联　网　协　会　　发 布

目　　次

前　言

近年来，我国发生了多起重大数据泄露事件，涉及的范围广泛，影响巨大，引发了社会各界的高度关注和广泛讨论；此外，随着我国网络环境的不断发展和壮大，网络安全问题也日益突出，黑客攻击、恶意软件、网络诈骗等种种安全问题层出不穷，给网络安全带来了极大的挑战。为了有效预防和应对这类问题，提升我国数据安全的保障能力，需要制定相应的标准和规范。因此，由中国信息通信研究院牵头，制定了该技术规范。

本技术规范参照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》要求的格式进行编写。

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这些专利的责任。

本技术规范由中国互联网协会归口。

本文件起草单位：中国信息通信研究院、挚理科技(北京)有限公司、北京福田戴姆勒汽车有限公司、北京金山云网络技术有限公司、上海合合信息科技股份有限公司、北京水滴科技集团有限公司、财信证卷股份有限公司、辽宁振兴银行股份有限公司、平安健康互联网股份有限公司、青岛海尔科技有限公司、上海蔚来汽车有限公司、深圳乐信控股有限公司、深圳依时货拉拉科技有限公司、小米汽车科技有限公司、智马达汽车有限公司、中国国际金融股份有限公司、中原消费金融股份有限公司、中证数据有限责任公司、爱康健康科技集团有限公司。

本文件主要起草人：王景尧、吴荻、李玮、王亚宁、张灵通、徐治国、宋宏宇、廖超豪、李晓川、邢悬月、杨志学、夏禹、杨曦、肖红亮、何艺、杨毅、张天力、章文婷、杨湘安、李子超、陈飞彦、章锦成、李斌、袁斯山、白雷、乔智明、单渤凯、郭登海、王丹维、李冬、魏涛亮、杨显哲、李刚、苗夏箐、孙乾。

数据安全技术能力评估要求

1 范围

本文件规定了应具备数据安全能力的企事业单位、政府部门等组织的数据安全技术能力要求。

本文件不仅适用于第三方机构展开数据安全技术能力评估，而且适用于为企业数据安全技术能力自评估提供参考和指导。

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，标注日期的引用文件，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 25069-2022 信息安全技术 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 37973-2019 信息安全技术 大数据安全管理指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 39335-2020 信息技术 个人信息安全评估指南

GB/T 19000-2016 质量管理体系 基础和术语

3 术语和定义

GB/T 41479-2022、GB/T 37988-2019、GB/T 36073-2018、GB/T 25069-2022、GB/T 35273-2020、GB/T 39335-2020、GB/T19000-2016、GB/T 37973-2019等国家标准界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

3.2

数据处理 data processing

对原始数据进行抽取、转换、加载的过程。

3.3

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.4

个人信息 personal information

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

注1：个人信息包括姓名、出生日期、公民身份证号、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。

注2：不包括匿名化处理后的信息。

3.5

个人敏感信息 personal sensitive information

一旦泄露、非法使用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。

3.6

去标识化 de-identification

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

3.7

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：匿名化处理后的信息不属于个人信息。

3.8

重要数据 important data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：重要数据包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

3.9

敏感数据 sensitive data

指包含个人身份信息、医疗记录、支付信息、信用卡号码、社会保险号码等敏感信息的数据类型。

3.10

数据脱敏 data masking

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.11

数据资产 data asset

是指由组织（政府机构、企事业单位等）合法拥有或控制的数据资源，以电子或其他方式记录，例如文本、图像、语音、视频、网页、数据库、传感信号等结构化或非结构化数据，可进行计量或交易，能直接或间接带来经济效益和社会效益。

3.12

数据分类 data classification

将具有某种共同属性或特征的数据，根据应用场景、数据来源、共享属性、开放属性等属性或特征，按照一定的原则和方法进行归类。

3.13

结构化数据 structural data

能够用数据或统一结构加以表示，一般存储在数据库中，如客户资料、销售记录等。

3.14

非结构化数据 unstructured data

无法用数字或统一的结构表示，如办公文档、图像、声音、网页、设计图纸等。

3.15

半结构化数据 semi-structured data

介于结构化和非结构化之间的数据，结构隐含在数据中，如HTML，XML，JSON，RDF等。

3.16

数据分级 data staging

根据数据的敏感程度和数据遭受篡改、泄露或非法利用后对受侵害客体的影响程度，按照一定的原则和方法进行定级。

3.17

用户端 client side

指数据处理或计算发生在用户设备上的计算机处理方式。

4 数据安全技术能力要求

数据安全技术能力是指组织机构或企业在保护其所有数据的机密性、完整性和可用性方面所具备的技术能力，包括数据资产与数据识别、权限管理与操作规范、数据防泄漏与溯源、敏感数据保护、业务流量风险监控、敏感操作发现、数据提取分发安全等方面。为满足数据安全技术能力的要求，实施所确定的措施，实现数据安全目标，组织应至少建立健全以下数据安全技术能力，对所需的数据安全技术实现过程进行实施和控制：

4.1 数据资产与数据识别

a) 确定企业拥有或控制的所有数据资产；

b) 明确数据资产内容、数据量、数据来源、存放位置、使用范围、责任主体、数据共享情况等；

c) 按照分类分级法，确定组织的数据资产类别、敏感等级；组织应建立数据分类分级管理过程，并保持成文信息。覆盖的范围应包括数据处理活动涉及的所有平台系统。

数据分类分级应满足国家法律法规及相关标准的要求，综合考虑数据的类别属性、级别、使用目的等，明确数据分类策略；建立数据资产分类分级清单；根据数据不同类别、级别，明确安全防护措施，实现对数据的精细化管控与防护，同时满足数据安全法对于数据分类分级制度的合规性要求。

在数据分类的基础上，对每一类数据类型制定数据分级标准。分级标准应考虑以下因素：

- 数据重要及敏感程度；
- 数据的安全保护需求；
- 数据泄露、丢失或破坏可能造成的危害程度。

d) 在数据资源识别时，应配备技术能力，定期对相关平台系统数据库中的结构化与半结构化数据进行自动化梳理，发现识别敏感数据信息；需要配备技术管控手段，对数据识别以及分类分级的过程进行管控，如样本数据查看二次授权、数据资产权限隔离等，保障过程安全。

4.2 权限管理与操作规范

a) 组织应明确关键系统的用户账号申请、审批、分配、开通、使用、变更、注销等安全保障要求，明确账号权限最小化可用原则，对于权限申请应联动数据分类分级结果，判定权限敏感级别，实现权限申请差异化审批流程。

b) 涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），组织应采取多人审批授权或操作监督，并实施日志审计，需与操作审计技术能力对应。日志记录信息要素应具备完整性，日志保存期限应至少为六个月。

c) 组织应具备一定的账号权限分配；从而实现对离职/转岗人员账号回收、账号权限变更、沉默账号等安全问题的处理。

d) 组织应视内部安全风险威胁情况，对数据安全相关审批采用自动化审批流程，保障管控有效。无法实现自动化审批的，应加入人工控制手段，实现与数据级别联动，实现差异化审批保护。

e) 组织应对高风险用数场景应实施操作过程监督，监督过程应完整记录，定期审计。

4.3 数据防泄漏与溯源

涉及非结构化数据资产的存储、处理、展示敏感数据的，应配备数据防泄露与水印溯源能力，依据自身实际业务风险情况，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。

组织应依据自身实际业务情况，具备对网络文件储存服务（网盘）、邮件、FTP、USB及即时通讯工具等多种数据导入导出渠道进行实时监控的能力，可及时对异常数据操作行为进行预警或拦截，以防范数据泄露风险。对于已经发生的数据泄露事件，应采取有效的日志审计、水印等方式追溯。

4.4 敏感数据保护

a) 对授权收集到的敏感数据信息，应采取去标识化、关键字段加密安全存储措施。根据相关方要求，删除、销毁的个人信息可进行匿名化处理，不可继续使用；

b) 在跨安全域或通过互联网传输敏感数据信息时，采用加密传输措施；

注:适宜的加密传输措施，例如可确保安全的加密算法或传输通道。

c) 在用户端显示敏感数据信息时，应采取措施防止未授权人员获取敏感数据信息。组织应配备技术能力有效防止脱敏失效，如伪脱敏、弱脱敏等情况；

d) 组织应根据数据的敏感级别，以及操作人员的数据权限，建立统一的数据交付策略，实现同一级别数据在不同平台系统中，管控措施的一致、可靠及高效。

注：在用户端显示敏感数据信息时，应根据敏感数据级别，采取动态脱敏策略防止未授权人员获取敏感数据信息。对于权限较高人员，在不存在合规风险的情况下，应采用可逆脱敏，支持查看脱敏数据的明文。查看明文的操作行为应进行详细记录，并易于查询、审计。

4.5 业务流量风险监控

a) 具备对内外部访问流量的自动化分析能力，发现数据处理平台系统的接口资产，并根据接口资产的采集、输出的数据级别和自身业务风险实际情况，定义接口资产的敏感级别，对使用接口的风险行为进行记录并告警；

b) 具备对API接口的脆弱性（安全性漏洞，业务逻辑性漏洞）及外部攻击行为的自动化发现能力;

c) 具备应用系统的安全合规性进行检查，对于业务系统未经加密直接传输的敏感信息，可进行告警，并记录相关信息的传输途径和位置。

4.6 敏感操作发现

组织应具备对重要业务系统的用户操作行为进行实时监控的能力，对操作安全基线进行定义，可基于用户历史行为、同属用户群行为基线进行对比，分析当前用户行为偏差，对偏离基线的异常用户行为进行告警及拦截。

可依据自身业务风险实际情况分批次将重要业务系统进行管控。应与企业内部数据分级管控措施规则为基础，对风险策略进行统一配置。

5 数据安全管理能力要求

为满足数据安全管理能力的要求，实施所确定的措施，实现数据安全目标，组织应至少建立完善以下数据安全管理能力，对所需的数据安全管理实现过程进行实施和控制：

5.1 组织架构及人员保障

组织应当明确数据安全第一负责人，并建立组织内部数据安全工作职能部门或机构，设立数据安全管理相关岗位，实现对组织数据安全风险的有效管理。数据安全第一责任人应确保组织与数据安全管理相关的职责、权限得到分配、沟通和理解。

数据安全第一责任人应分配职责和权限，以：

a) 确保数据安全管理能力符合本技术规范的要求；

b) 确保各过程获得其预期输出；

c) 报告数据安全管理能力的绩效以及改进机会，特别是向最高管理者报告；

d) 确保在整个组织中推动数据安全管理；

e) 确保在策划和实施数据安全管理能力变更时保持其完整性。

应明确数据安全岗位人员、职责划分，落实数据安全管理工作。

5.2 数据使用分级管控

a) 组织应在数据分类分级的基础上制定不同级别数据的通用管控原则，包括但不限于据使用审批、数据权限管理、数据脱敏、数据加密等。

b) 组织应识别并确定内部所有用数场景，并针对不同场景制定明确的审批流程，形成对应审批流程图。包括但不限于以下使用数据场景：

- 数据查看
- 数据导出
- 数据外发、共享
- 数据接口调用
- 数据删除、销毁
- 系统权限申请

5.3 合作方管理

应加强第三方数据合作的管理，落实合作方安全准入机制，应根据合作的业务重要程度及交互数据敏感程度，对第三方进行分级分类管理。

应明确对外合作中数据安全保护方式和合作方责任落实要求，合作结束后数据删除要求，合作方违约责任和处罚等。

应建立合作方台账管理机制，形成并定期更新合作方清单。清单的内容应包含合作方名称、相关资质、合作业务或系统、合作形式、合作期限、合作方联系人等。

根据合作方共享数据的不同级别来制定不同的资质以及数据保护能力要求；对于接收的数据，则需对数据来源进行判定。最终由内部评审后通过。

5.4 数据安全工作自评估

最高管理层应按计划的时间间隔评审组织的数据安全工作开展情况，以确保其持续的适宜性、充分性和有效性。

自评估应考虑：

a) 自评内容应覆盖企业主体数据安全相关工作；

b) 应考虑与数据安全管理能力相关的外部和内部事项的变化；

c) 有关数据安全负责人的反馈，包括以下方面的趋势：

1) 不符合和纠正措施；

2) 数据安全目标完成情况。

3) 数据安全风险评估结果及应对措施的状态；
4) 持续改进的机会。