ICS
CCS

团　　体　　标　　准

T/COSOCC XXXX—XXXX

信息技术应用创新 数据安全通用技术规范

Information technology application innovation—General technical specification for data security

（征求意见稿）

完成时间：2023.12.18

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国基本建设优化研究会　　发 布

COSOCC

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。

本文件由中国基本建设优化研究会提出并归口。

本文件起草单位：。

本文件主要起草人：

COSOCC

引　言

党的十八大以来，围绕习近平总书记建设网络强国、数字中国、智慧社会等重要发展理念，我国全面实施国家大数据战略。与此同时，我国逐步建立了基于自主的IT底层架构和标准，在核心芯片、基础硬件、操作系统、中间件、数据服务器等领域实现国产替代，形成自有开放生态。然而，信创产业数据安全风险问题日益严峻，信创环境下数据安全、企业商业秘密和公民个人信息安全防护需求迫切。通过开展信创数据安全通用技术规范团体标准的研制工作，对信创数据安全进行要求，并提供相应的检测方法，为信创相关设备供应商在产品研发设计、产品生产等在数据安全防护方面提供指导，保障不同信创应用平台、应用软件开发和运维团队提供兼容和信息流通，为信创应用平台、应用软件等使用方在项目招标、项目验收等方面提供技术支撑，为工信部、市场监督管理局等政府监管部门在相关政策制定方面提供依据。

本文件在编制过程中，依据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例（征求意见稿）》等法律法规，以数据处理活动中数据采集、传输、存储、使用、交换和销毁等全生命周期技术管理为目标，制定数据安全要求技术框架，通过顶层设计制定实施细则，提出在数据处理全生命周期各个环节可以实施的技术手段。

COSOCC

信息技术应用创新 数据安全通用技术规范

1 范围

本文件规定了信息技术应用创新环境下，数据处理活动中数据安全的通用安全要求、总体架构和安全技术要求等。

本文件适用于信创相关设备供应商在产品设计、研发过程采取数据安全防护措施，数据运营者基于信创环境的数据安全能力建设等，也可供主管监管部门、重点行业领域制定数据安全相关政策时参考。

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 35273 信息安全技术 个人信息安全规范

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 41479 信息安全技术 网络数据处理安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息技术应用创新 information technology application innovation

面向基础硬件、基础软件、应用软件、网络安全等IT产业链核心技术产品进行自主研发，为我国经济发展、社会运转构建安全可控的信息技术支撑。

3.2

信创环境 environment of information technology application innovation

基于信创基础软硬件平台的软硬件运行环境。

3.3

数据 data

任何以电子或者其他方式对信息的记录。

[来源：GB/T 41479—2022，3.1]

3.4

数据处理活动 data processing activities

数据采集、传输、存储、使用（处理）、交换和销毁等活动。

[来源：GB/T 41479—2022，3.3，有修改]

3.5

数据处理者 data processor

在数据处理活动中自主决定处理目的和处理方式的个人和组织。

3.6

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。

[来源：GB/T 41479—2022，3.4]

3.7

个人信息 personal information

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

[来源：GB/T 41479—2022，3.6，有修改]

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。

[来源：GB/T 41479—2022，3.9，有修改]

3.9

生物特征 biometric feature

利用采集设备获取的诸如人脸、指纹、虹膜等人体样本数据中可用于识别的数字组合或标签。

[来源：GB/T 41786—2022，3.1.3，有修改]

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

5 通用安全要求

5.1 数据处理活动应符合 GB/T 41479 中规定的要求。

5.2 应按照有关要求和标准进行数据分类分级保护,识别信创涉及的核心数据、重要数据、一般数据,对不同级别的数据采取不同的保护措施。

注：国家建立数据分类分级保护制度，按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为核心数据、重要数据、一般数据。

5.3 数据安全保护措施应覆盖数据的全生命周期，且针对不同类型数据对象特点采取相应技术手段。

5.4 应结合数据处理活动的实际情况，按照有关国家标准定期开展数据安全风险评估，并根据评估结果持续、动态优化数据安全保护措施。

5.5 信创数据处理活动应符合国家网络安全等级保护相关标准要求。

5.6 数据安全保护中使用的密码算法、技术和产品应符合法律法规的规定和密码相关国家标准、行业标准的有关要求。

6 总体架构

信创数据安全总体框架基于信创环境，面向受保护对象，采用数据安全技术实现数据全生命周期安全。总体框架应符合图1的规定。

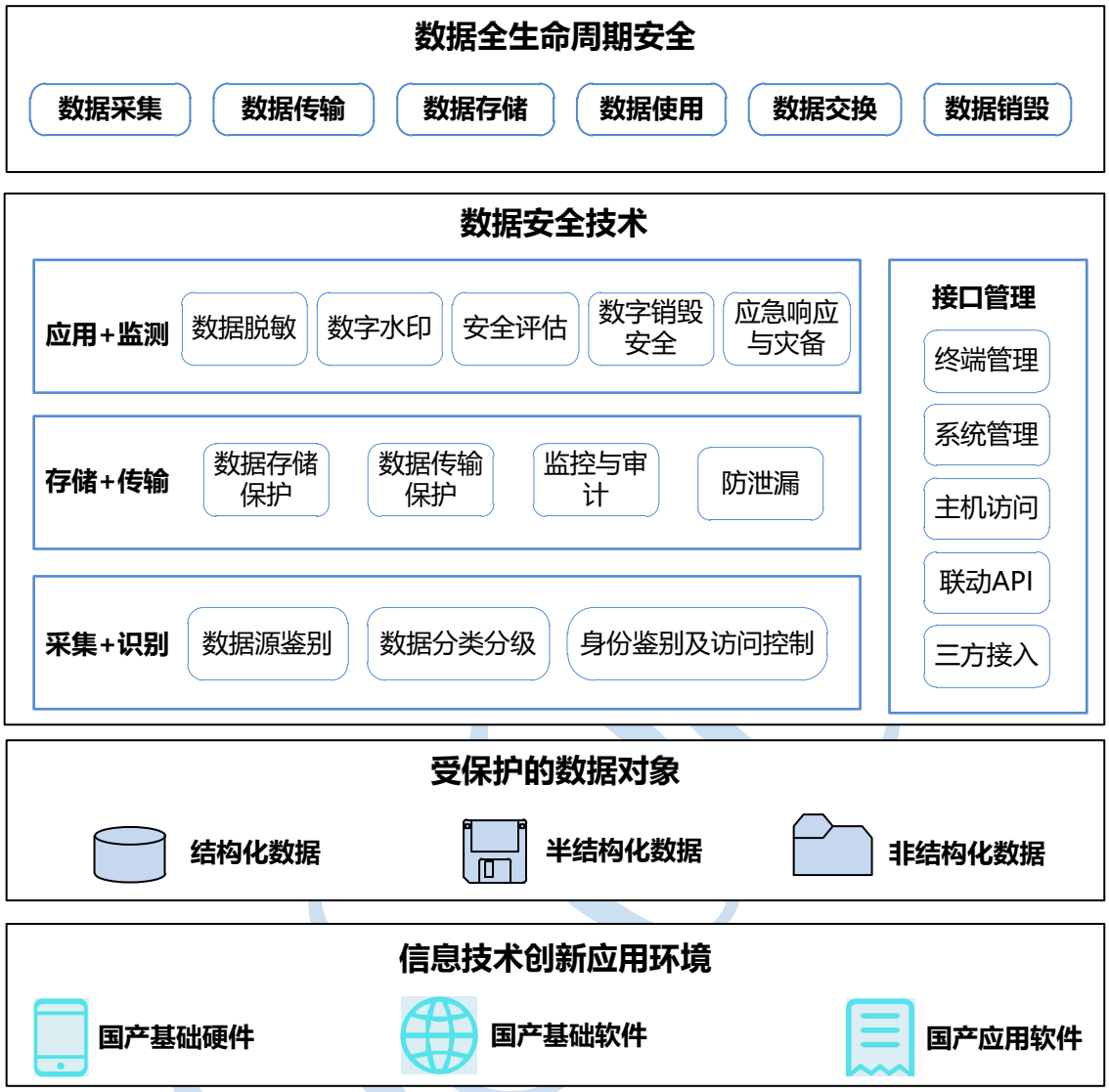

图1　信创数据安全总体框架

信创数据安全总体框架底层基于信创环境，包括国产基础硬件、基础软件和应用软件等。

数据安全总体框架支持多种数据形态，受保护的数据对象包括结构化数据、半结构化数据和非结构化数据。

数据安全技术由采集及识别层、存储及传输层、应用及监测层、管理及接口层等组成，采集及识别层包括数据源鉴别、数据分类分级和身份鉴别及访问控制；存储和传输层包括数据存储保护、数据传输保护、监控与审计和防泄漏；应用及监测层包括数据脱敏、数字水印、安全评估、数据销毁安全和应急响应与灾备；系统及接口层包括终端管理、系统管理、主机访问、联动API和三方接入。

数据安全总体框架覆盖数据全生命周期，包括数据采集、数据传输、数据存储、数据使用（处理）、数据交换和数据销毁。

7　安全技术要求

7.1　数据源鉴别

7.1.1　概述

信创数据处理者应对收集或产生数据的来源进行身份识别，在数据采集过程中应对数据源进行记录，对采集的数据进行数据来源的标识，以防止采集到其它不被认可的或非法数据源产生的数据，避免采集到错误的或失真的数据，必要时应对数据源进行追踪和溯源。

7.1.2 技术要求

信创数据源鉴别技术应符合下列要求：

a) 应对数据采集来源进行管理，包括明确采集源识别和管理、采集源的安全认证机制、采集源安全管理要求等内容；
b) 应对采集的数据在数据生命周期过程中进行数据溯源管理，保留数据流路径上的日志记录不少于六个月。

7.2 数据分类分级

7.2.1 概述

信创数据处理者在数据采集阶段应做好数据分类分级工作，满足分类分级安全技术要求。对数据分类分级并进行标记，根据标记可对数据安全等级进行识别，并保留标记记录，明确数据处理活动全生命周期必要的安全管理策略和保障措施。

7.2.2 技术要求

信创数据分类分级技术应符合下列要求：

a) 应定期梳理数据资产,形成并及时更新数据资产清单，按照有关规定开展数据分类分级工作；
b) 应根据业务需求、数据来源和用途等因素，划分组织机构数据类别，并根据数据资产变动和分类分级要求变动情况，及时更新数据资产清单；
c) 应定期更新重要数据和核心数据目录，按照有关规定开展目录备案工作。

7.3 身份鉴别与访问控制

7.3.1 概述

信创数据处理活动应采用设置身份标识与鉴别、访问控制与权限等技术，对数据处理者身份进行标识与鉴别，明确访问控制及权限的分配、变更、撤销等权限，以及系统账户、数据权限的申请审批流程等。

7.3.2 技术要求

信创身份鉴别与访问控制技术应符合下列要求：

a) 应采用口令、密码技术、生物特征（或生物特征属性）等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应为密码技术；
b) 应对用户、登录的进程、应用进行身份标识和鉴别，保证用户身份标识具有唯一性，身份鉴别信息应具有复杂度要求并且定期更新；
c) 应授予管理用户所需的最小权限，实现管理用户的权限分离；
d) 应定期删除或停用多余的、过期的账户及数据权限；
e) 宜建立统一的身份与访问管理系统，支持人员、数据资源、应用系统的统一纳入。

7.4 数据存储保护

7.4.1 概述

信创数据处理活动过程中可采用符合GB/T 39786规定的密码技术，保证存储过程中数据的保密性和完整性，对敏感数据进行加密存储。

7.4.2 技术要求

信创数据存储保护技术应符合下列要求：

a) 应对数据存储环境进行分域分级设计；

b） 应根据数据安全级别、重要性、量级、使用频率等因素进行分类分级存储保护，采用保密性、完整性、可恢复性等数据安全保护机制。

7.5 数据传输保护

7.5.1 概述

信创数据处理活动过程中对传输的安全要求应采用符合GB/T 39786规定的密码技术要求，保证通信过程中数据的保密性和完整性，同时应具备监控数据传输过程的能力，发现问题时及时告警并进行阻断。

7.5.2 技术要求

信创数据传输技术应符合下列要求：

a） 应根据数据传输的应用场景，采用接口安全管理与保护措施；
b） 应根据传输的数据类型、级别和应用场景等，明确数据安全策略并采取保护措施；
c） 应在数据交换不完整时清除传输缓存数据，交换完成后清除传输历史缓存数据。

7.6 监控与审计

7.6.1 概述

信创数据处理者应对数据处理活动中数据流转的全过程进行监控与审计，明确数据安全审计统筹部门，配备安全审计员，对权限分配审批、数据处理日志等开展安全审计工作。

7.6.2 技术要求

信创监控与审计技术应符合下列要求：

a） 应配备视频监控等基础安全设施，并留存视频监控记录材料；
b） 应确定必要的数据安全审计策略，明确审计对象、审计内容和实施周期，开展数据重大操作越权访问数据和远程访问数据等重点场景安全审计和数据分析；
c） 应针对审计发现的问题及时处置、整改、跟踪复核，按照有关规定定期形成数据安全审计报告。

7.7 防泄漏

7.7.1 概述

信创数据处理活动防泄措施可从文档安全与外发安全管控、终端数据安全管理两方面开展。数据处理者应建立文档数据防泄漏环境，防范有意、无意的泄密行为以及对行为的具体管控，同时建立终端数据防泄漏环境，防范内部信息和个人身份信息泄漏。

7.7.2 技术要求

信创数据防泄漏技术应符合下列要求：

a） 应以文件透明加密的方式对局域网计算机进行加密管理，加密后的文件只能在局域网下正常打开；
b） 应记录局域网计算机打开文件后修改、删除的行为，并在文件修改或删除时进行自动备份；
c） 内外部数据传输应使用加密措施确保传输过程的安全；
d） 应部署相关设备监测网络可用性及防范数据泄漏风险。

7.8 数据脱敏

7.8.1 概述

信创数据处理者应对敏感数据建立数据脱敏安全策略并按照安全策略进行脱敏，同时制定密钥管理制度，并严格按照密钥管理制度实施数据处理活动中密钥的管理。

7.8.2 技术要求

信创数据脱敏技术应符合下列要求：

a） 应根据应用需要保留敏感数据的原始数据格式、属性或关联；

b) 应对数据脱敏操作过程进行记录,记录内容至少包括操作时间、操作人、操作对象等；
c) 有条件的情况应使用对应安全级别的密钥存储模块，对密钥分发和传输过程中采用防窃听技术。

7.9 数字水印

7.9.1 概述

信创数据处理者应对交换的敏感数据添加数字水印，防止数据被非法复制和盗版，同时维护数据的版权和完整性。

7.9.2 技术要求

信创数字水印技术应符合下列要求：
a) 应支持根据数据格式，添加相应的水印，包括文档水印、图像水印、视频水印、音频水印等；
b) 应支持基于数字水印进行数据的追踪溯源。

7.10 安全评估

7.10.1 概述

信创数据处理者应定期对数据和数据处理活动进行安全评估，掌握数据安全总体状况，发现存在的数据安全风险和违法违规问题，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力奠定基础。

7.10.2 技术要求

信创数据安全评估技术应符合下列要求：
a) 应定期对所在组织整体数据安全保护水平、重点业务与平台系统数据安全保障情况进行梳理和自查；
b) 应对自查总结过程进行记录,形成总结报告，对发现的问题进行原因分析、明确改进措施和计划；
c) 应开展重要数据和核心数据风险评估，对于评估中发现的安全风险隐患，结合重要数据处理场景，及时采取有效应对措施化解风险隐患。

7.11 数据销毁安全

信创数据处理活动过程中数据销毁应符合GB/T 35273的要求。

7.12 应急响应与灾备

7.12.1 概述

信创数据处理者应开展数据安全风险监测，对数据资产、数据处理环境、网络与系统设备、数据处理账号和内外部数据流动等实施监测巡查，对异常流动等行为进行排查和预警，及时采取补救措施。

7.12.2 应急响应与灾备技术要求

信创应急响应与灾备技术应符合下列要求：
a) 应制定数据安全事件应急预案，根据事件等级明确应急响应责任分工、工作流程和处置措施等；
b) 应制定数据安全事件应急演练计划，针对数据泄露、丢失、窃取、损坏、滥用、篡改、非法访问和违规传输等典型数据安全事件定期开展演练,形成演练总结报告；
c) 发生数据安全事件后，应按照应急预案及时开展应急处置，事件处置完成后，应按照有关规定进行整改，形成总结报告并及时上报；
d) 应制定所在组织备份策略和规程，包括备份的范围、备份方式和数据格式、验证备份数据完整性和可用性的规程、从备份数据恢复的规程等。

7.13 接口管理

7.13.1 概述

信创数据处理活动应采用符合GB/T 39786要求的密码技术对系统间的级联接口进行安全防护，保障通过级联接口传递数据的保密性和完整性。

7.13.2 接口管理技术要求

信创接口管理技术应符合下列要求：

a) 应采取终端准入控制、终端鉴别等安全技术措施，防止非法或未授权终端接入内部网络；
b) 应采取系统鉴权策略，例如 IP 地址过滤、会话管理技术、反射攻击防御技术等；
c) 应设置主机访问安全策略，禁止非系统管理员以及外来入侵用户对系统的任意篡改、删除、格式化等操作，对主机的安全实行完整性检测，监控非法篡改资源的情况等；
d) 应对 API 库存表进行定期维护更新，采取强制 API 身份验证策略，为用户设置 API 访问密钥并限制 API 密钥可能被使用的次数；
e) 应对第三方嵌入或接入的自动化工具收集个人信息的行为进行审计，发现超出约定的行为，及时切断接入。

COSOCC

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语
[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 37988—2019 信息安全技术 数据安全能力成熟度模型
[4] GB/T 39477—2020 信息安全技术 政务信息共享数据安全技术要求
[5] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[6] GB/T 41786—2022 公共安全 生物特征识别 术语

COSOCC