ICS03.080

|  |
| --- |
| CCSA16 |

DB21

辽宁省地方标准

DB21/TXXXX—XXXX

|  |
| --- |
|  |

工业数据流通 数据安全要求

|  |
| --- |
| 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

辽宁省市场监督管理局　发布

（征求意见稿）

目　次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 数据流通参与方安全要求 3

4.1 数据供方安全要求 3

4.2 数据需方安全要求 3

4.3 数据交易服务机构安全要求 3

5 数据流通安全技术要求 4

5.1 数据采集 4

5.2 数据传输 5

5.3 数据存储 7

5.4 数据处理 14

5.5 数据流通 17

5.6 数据销毁 22

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。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：沈阳华睿博信息技术有限公司、上海数据交易所、北京赛迪时代信息产业股份有限公司、辽宁艾特斯智能交通技术有限公司、东北大学、辽宁省大数据管理中心、国家计算机网络应急技术处理协调中心辽宁分中心等。

本文件主要起草人：邵华、申翔宇、张翔宇、魏国伟、王宇飞、宋宪辉、谭振华、杨成实、李凯等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

本文件起草单位通讯地址和联系电话：通讯地址：辽宁省沈阳市和平区青年大街386号华阳国际大厦2396，联系电话：18698840986

本文件归口部门通讯地址和联系电话：通讯地址：辽宁省沈阳市皇姑区北陵大街45—2号，联系电话：024—86893258

工业数据流通 数据安全要求

1. 范围

本文件规定了工业数据采集、传输、存储、处理以及销毁过程中的安全要求。

本文件适用于工业企业数据流通安全防护工作指导和落实。

1. 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 25069-2022 信息安全技术 术语

GB/T 5271.1-2000 信息技术 词汇 第1部分：基本术语

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

1. 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

[来源：GB/T 5271.1—2000,01.01.02]

1.

工业数据 industrial data

工业领域产生和收集的数据，包括研发设计、生产制造、经营管理、运行维护、平台运营等过程中收集和产生的任何以电子或者其他方式记录的数据。

数据供方　data supplier

数据交易中提供数据的组织机构。

[来源：GB/T 37932-2019，3.2]

数据需方　data acquirer

数据交易中购买和使用数据的组织机构。

[来源：GB/T 37932-2019，3.3]

数据交易　data transaction

数据供方和需方之间以数据商品作为交易对象，进行的以货币或货币等价物交换数据商品的行为。

注1：数据商品包括用于交易的原始数据或加工处理后的数据衍生产品。

注2：数据交易包括以大数据或其衍生品作为数据商品的数据交易，也包括以传统数据或其衍生品作为数据商品的数据交易。

[来源：GB/T 37932-2019，3.1]

数据交易服务机构　data transaction service

为数据供需双方提供数据交易服务的组织机构。

[来源：GB/T 37932-2019，3.4]

个人信息　personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、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：个人信息控制者通过个人信息或其他信息加工处理后形成的信息，例如,用户画像或特征标签,能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,属于个人信息。

[来源：GB/T 35273-2020，3.1，有修改]

1. 数据流通参与方安全要求
	1. 数据供方安全要求

数据供方应满足如下要求：

1. 为一年内无重大数据类违法违规记录的合法组织机构；
2. 完成在数据交易服务机构的注册,并经数据交易服务机构审核通过,才允许参与数据流通业务；
3. 数据供方应证明其具备向数据需方安全交付数据的能力；
4. 向数据交易服务机构提供书面的安全承诺，内容包括但不限于：流通数据来源合法性证明材料、交易数据满足法律法规和政策要求、对流通数据质量评估说明、遵守数据流通安全原则、愿意接受数据交易服务机构安全监督、愿意对数据流通后果负责等；
5. 遵守数据交易服务机构的安全管理制度和流程。
	1. 数据需方安全要求

数据需方应满足如下要求：

1. 为一年内无重大数据类违法违规记录的合法组织机构；
2. 完成在数据交易服务机构的注册,并经数据交易服务机构审核通过,才允许参与数据流通业务；
3. 提供书面的数据流通和使用安全承诺，内容包括但不限于：满足法律法规和政策要求、遵守数据流通安全原则、愿意接受数据交易服务机构安全监督、遵守与数据供方约定的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方等；
4. 按照供需双方约定的使用目的、范围、方式和期限使用数据,禁止进行个人信息的重新识别；
5. 在按照数据流通约定方式完成数据使用后，应及时销毁流通数据；
6. 遵守数据交易服务机构的安全管理制度和流程。
	1. 数据交易服务机构安全要求

数据交易服务机构应满足如下要求：

1. 为一年内无重大数据类违法违规记录的合法组织机构；
2. 完成在数据交易服务机构的注册,并经数据交易服务机构审核通过，才允许参与数据流通业务；
3. 证明具备对流通数据实施安全保护的能力；
4. 提供书面的数据流通和使用安全承诺，内容包括但不限于：满足法律法规和政策要求、遵守数据流通安全原则、愿意接受数据交易服务机构安全监督、遵守与数据供方约定的数据安全要求、对所持有数据提供充分的安全保护、未经明确授权不公开或转交数据给第三方等；
5. 按照供需双方约定的使用目的、范围、方式和期限使用数据,禁止进行个人信息的重新识别；
6. 在按照数据流通约定方式完成数据使用后，应及时销毁流通数据；
7. 遵守数据交易服务机构的安全管理制度和流程。
8. 数据流通安全技术要求
	1. 数据采集
		1. 数据采集安全管理

数据供方数据采集应满足如下要求：

1. 组织开展数据采集活动的过程中应满足权责一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与等原则；
2. 应设立数据采集安全管理团队，负责制定和推动实施整体的数据采集安全合规管理制度；
3. 应设立数据采集风险评估团队，负责对不同业务或项目场景的数据采集提供安全评估服务支持，并制定相应的改进方案，评估内容包括但不限于合规安全性、技术安全性等；
4. 定义采集数据的目的和用途，明确数据来源、采集方式、采集范围等内容，并制定标准的采集模板、数据采集方法、策略和规范；
5. 遵循合规原则，确保数据采集的合法性、正当性和必要性；
6. 设置专人负责信息生产或提供者的数据审核和采集工作；
7. 对于初次采集的数据，应采用人工与技术相结合的方式进行数据采集，并根据数据的来源、类型或重要程度进行分类；
8. 最小化采集数据，仅需要完成必须工作即可，确保不收集与提供服务无关的个人信息和重要数据；
9. 对采集的数据进行分级分类标识，并对不同类别、级别的数据实施相应的安全管理策略和保障措施，对数据采集环境、设施和技术采取必要的安全管理措施；
10. 部署数据采集系统或相关工具，制定数据采集策略（如采集周期、频率、采集内容等）对数据进行采集；
11. 在采集过程中对被采集方授权同意采集的过程和信息进行日志记录；
12. 实施数据采集过程的数据防泄漏安全技术措施：如采集数据的加密、采集链路加密、敏感信息和字段的脱敏、权限的访问控制等。
	* 1. 数据源鉴别及记录管理

数据供方开展数据源鉴别及记录活动的过程中应遵循如下基本要求，防止数据仿冒和伪造：

1. 设立负责数据源鉴别和记录的岗位和人员，负责对数据源进行鉴别、记录和追溯，检测数据是否被仿冒、伪造，同时提供统一的数据源管理策略和方案；
2. 采取标注法、反向查询法等技术手段对外部收集的数据和数据源进行识别和记录；
3. 对关键溯源数据进行备份，并采取数据加密、访问控制及数据备份等技术手段对溯源数据进行安全保护；
4. 确保负责该项工作的人员理解数据源鉴别标准和组织内部的数据采集业务，并结合实际情况执行标准要求；
5. 通过身份鉴别、数据源认证等安全机制确保数据来源的真实性。
	1. 数据传输
		1. 数据加密传输

在数据进行传输时，应满足如下要求：

1. 应设立数据加密管理部门，负责整体的数据加密管理和密钥管理、制定整体的数据加密制度和原则，指定统一采用的数据加密算法、技术等，并推动落实相关要求。
2. 在数据传输前，首先进行风险评估，评估内容包括重要程度、数据对机密性和完整性的要求程度以及其安全属性破坏后可能导致系统受到的影响程度。
3. 根据风险评估结果，确定加密算法的类型、属性，以及所用的密钥长度，采用合理的加密技术。
4. 选择的加密技术应符合国家有关加密技术的法律法规。
5. 对生成、存储、归档保存密钥的设备采取物理保护。
6. 使用经过业务平台部门批准的加密机制进行密钥分发，并记录密钥的分发过程，以便审计跟踪，统一对密钥、证书进行管理。
7. 密钥的管理应基于以下流程：
8. 密钥产生：密钥的产生包括为不同的密码系统和不同的应用生成密钥。密钥采用人工产生或加密机产生的方式；
9. 密钥分发：向目标用户分发密钥，包括在收到密钥时如何将之激活。
10. 密钥分发管理应满足如下要求：
11. 密钥存取：为当前或近期使用的密钥或备份密钥提供安全存储，包括授权用户如何访问密钥；
12. 密钥更新：应制定密钥更新方案，包括密钥变更时机、变更规则以及被泄露的密钥的处置方法等；
13. 密钥备份：应对密钥进行备份，防止密钥丢失；
14. 密钥销毁：需要销毁的密钥包括过期密钥、废除密钥、泄露密钥、被攻破密钥，密钥销毁前，应确认不再需要由此密钥保护的数据信息。
	* 1. 网络可用性管理

网络可用性管理应满足如下要求：

1. 应设立网络可用性管理部门负责网络可用性管理，制定整体的网络可用性管理方案和标准，包括制定可用性的标准数值、故障指标、故障处理方案等，对网络节点、传输链路进行考察，并部署相应设备保障网络可用性、防止出现数据泄露等风险。
2. 在网络规划设计阶段，应细致分析业务模型，确定基础网络拓扑，对影响网络可用性的关键节点和链路应做充分的冗余设计，并根据网络结构，在各个层次、各个节点部署合适的高可用性技术。
3. 网络配置应遵循如下原则：
4. 层次化：分层次设计网络结构，严格定义各层次的功能；
5. 模块化：根据区域划分拓扑结构；
6. 可扩展：根据业务发展需要，通过简单复制模块单元来拓展网络；
7. 冗余设计：提供设备和链路的冗余保护。
8. 在组件或设备选型时，除保证技术指标外，也要有足够高的可靠性指标。
9. 持续进行网络维护和优化。利用高效的网络设备管理工具持续监控、分析、预测、优化，最大限度的规避网络拥塞。
10. 在进行软硬件版本升级或新设备，新业务上线时，应事先详细规划，制定应急预案。
11. 定期对主机系统和网络系统进行安全评估。
12. 做好业务系统和网络系统的协调。积极分析业务模型，并适当的进行调整。
13. 设定网络可用性管理部门，负责网络及其组件设备的日常维护以及网络故障的应急工作，全面负责可能出现的各种突发事件处置工作，并协调解决网络故障处置工作中的重大问题。
14. 网络可用性管理部门应预先对网络故障预警预报体系进行建设，编制网络故障防治规划。
15. 网络可用性管理部门应加强对网络及各组件的日常监测及其日志保存工作，发现险情时，应及时向领导小组报告。
16. 网络可用性管理部门应执行值班制度，以保障最先发现网络故障并及时处置次突发事件。
17. 建立健全网络故障速报制度，保障突发性网络故障信息可立即发布预警。
18. 网络故障发生时，立即启动应急预案，采取应急处置程序，判定网络故障级别，并立即向网络可用性管理部门报告。在网络故障处置过程中，应及时报告网络故障处置工作的进展情况，直至故障修复。
19. 网络故障消除后，由网络可用性管理部门向领导小组宣布网络故障应急期结束，并予以公告，同时预案终止。
	1. 数据存储
		1. 物理存储安全

工业数据的物理存储应满足如下要求：

1. 存储介质由存储介质安全管理部门进行统一采购，选择可靠的品牌，并遵循申报、审批、采购、标识、入账的流程，采购中应进行防病毒等安全性检测，在确保安全的情况下入账；
2. 数据存储介质由存储介质安全管理部门进行统一管理；
3. 存储介质的存放环境应有防火、防盗、防水、防尘、防震、防腐蚀及防静电等措施，防止其被盗、被毁、被未授权修改以及其信息的非法泄露，对于磁带、磁盘等带有磁性的介质应注意其保存环境，保证其长期有效；
4. 根据数据的容量和重要性合理选择数据存储介质；
5. 数据存储介质必须具有明确的分类标识，标识须包括存储数据的内容、归属、大小、存储期限、保密程度等，并结合数据类型和管理策略统一命名，存储介质的标识必须醒目；
6. 建立数据存储介质保管清单，由存储介质安全管理部门定期根据保管清单对介质的使用现状进行检查，检查内容包括完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏），任何存储介质盘点出现差异时，必须及时报告给上级领导部门；
7. 存储介质在运输过程中，必须采取密封处理；
8. 应选取可靠的速递公司承担介质的传递工作，介质传递时间、安全保障（防火、防震、防潮、防磁、防盗）等方面的要求应在与速递公司的合同中加以约定。速递公司的资质、介质传递流程、速递合同须经存储介质安全管理部门批准；
9. 当存有敏感业务信息的介质进行异地传输时，应选择本单位可靠人员进行传递，并且使用专用安全箱包进行包装；
10. 移动存储介质的接收应履行登记、入账等手续，存储介质安全管理部门需对存储介质的运输过程进行详细记录；
11. 新启用的存储介质或使用移动存储介质时，应进行安全检查和查杀病毒处理；
12. 存储介质的使用需在受控的办公场所的指定计算机上进行；
13. 非本单位的移动存储介质不应和涉密计算机连接；
14. 不应在高温、强磁场的环境下使用存储介质；
15. 涉密和非涉密的存储介质不应交叉使用；
16. 因公务需要携带存储介质外出时，应经存储介质安全管理部门审批同意并登记；
17. 如使用移动介质转移存储敏感数据，应在使用前格式化，并在使用后立即删除敏感数据；
18. 复制移动存储介质中的信息应经过存储介质安全管理部门批准并履行登记手续，复制件应视同原件进行管理，复制移动存储介质中的信息时，不得改变其知悉范围，并由存储介质安全管理部门进行监督；
19. 移动存储介质需要送外维修时，应经过存储介质安全管理部门审批，对送出维修的介质应首先清除介质中的敏感数据，必须到存储介质安全管理部门制定的单位进行维修，由存储介质安全管理部门全程陪同监督；
20. 存储介质的维修由存储介质安全管理部门负责，并对维修人员、维修对象、维修内容、维修前后状况进行监督和记录；
21. 为防止敏感信息泄露给未经授权的人员，各部门应将需要废弃的存储介质送到存储介质安全管理部门，由存储介质安全管理部门统一进行安全销毁，存储介质销毁应经过存储介质安全管理部门审批，不得自行销毁；
22. 存储介质销毁前，存储介质安全管理部门须对所含信息进行风险评估；
23. 任何含有敏感信息的中间存储介质，都需要销毁其中的信息，任何存储介质不再用于存储保密信息之前，必须进行格式化，存储介质上删除敏感的信息后，必须执行重复写操作防止数据恢复；
24. 应采用粉碎或烧毁的方式对含有硬拷贝形式的敏感信息存储介质进行报废处理；
25. 存储介质安全管理部门需对存储介质的处置做记录、以备审查；
26. 被销毁介质上的备份内容如果未到备份保存期限，应将备份内容复制到较新的介质上，并将复制后的介质归档。
	* 1. 逻辑存储安全

工业数据的逻辑存储应满足如下要求：

1. 应设立数据逻辑存储安全管理部门负责管理整体的数据逻辑，制定数据逻辑安全存储管理制度，建立数据逻辑存储隔离与授权操作标准等，包含认证授权、账号管理、权限管理、日志管理、加密管理、版本管理、安全配置、数据隔离等要求点，搭建整体的数据逻辑存储系统，维护数据逻辑存储系统和存储设备；
2. 普通账号应使用同一而规范的申请表提出用户账号创建、修改、删除、禁用等申请；
3. 在受理申请时，逻辑存储管理部门根据申请配置权限，在系统条件具备的情况下，给用户分配独有的用户账号和权限。用户不得使用他人账号或者允许他人使用自己的账号；
4. 当用户岗位和权限发生变化时，应主动申请所需逻辑存储系统过的账号和权限；
5. 只有经逻辑存储安全管理部门授权的用户才可以使用特权账号和超级用户账号，严禁共享账号；

注：特权账号指在系统中有专用权限的账号，如备份账号、权限管理账号、系统维护账号等。超级用户账号指系统中最高权限账号，如administrator、root等管理员账号。

1. 逻辑存储安全管理部门需监督特权账号和超级用户账号的使用情况并记录；
2. 尽量避免特权账号和超级用户账号的临时使用，确需使用时必须提交申请及审批流程；临时使用超级用户账号必须有逻辑存储安全管理部门在场监督，并记录其工作内容；超级用户账号临时使用完毕后，逻辑存储安全管理部门需立即更改账号密码；
3. 应按照用户角色分配不同的权限的账号，删除或锁定可能无用的账户；
4. 用户账号口令的发放应严格保密，用户应及时更改初始口令，账号口令最小长度为6位，并应具有一定的复杂度，账号口令应定期更改，账号口令的更新周期不得超过90天，不应共享个人用户账号口令，超级用户账号需通过保密形式由逻辑存储安全管理部门留存一份；
5. 逻辑存储管理部门应建立逻辑存储系统账号及权限的文档记录，记录用户账号和相关信息，并在账号变动时及时更新记录；
6. 员工离职后，逻辑存储管理部门应及时禁用或删除离职人员所使用的账号，如果离职人员是系统管理员，则及时更改特权账号或超级用户口令；
7. 逻辑存储安全管理部门应制定逻辑存储系统的访问规则；
8. 应保证在进入逻辑存储系统前必须执行登录操作，并且记录登录成功与失败的日志；
9. 逻辑存储系统的管理员应确保用户的权限被限定在许可的范围内，同时能够访问到有权访问的信息；
10. 访问控制权限设置的基本规则是除明确允许执行的情况外，其余必须禁止，访问控制的规则和权限应结合实际情况，并记录在案；
11. 逻辑存储安全管理部门应具备较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理并通知上级领导部门或专职人员，采用国家许可的正版防病毒软件并及时更新软件版本，逻辑存储系统应及时升级或安装安全补丁，弥补系统漏洞；应为逻辑存储服务器做好病毒及木马的实时监测，及时升级病毒库；
12. 未经逻辑安全管理部门许可，不应在逻辑存储系统上安装新软件；若确为需要安装，安装前应进行病毒检查；经远程通信传送的程序或数据，必须经过检测确认无病毒后方可使用；
13. 定期对逻辑存储系统上的安全日志进行检查，对错误、异常、警告等日志进行分析判断，并将判断结果进行有效解决处理并记录存档；逻辑存储系统上的日志应定期备份；
14. 逻辑存储安全管理部门应定期检查并记录逻辑存储系统的存储情况，如果发现存储容量超过70%，应及时删除不必要的数据，必要时申报新的存储；
15. 当逻辑存储系统出现故障时，由逻辑存储安全管理部门督促和配合厂商工作人员尽快维修，并对故障现象及解决全过程进行详细记录；

注：逻辑存储系统的故障包括：软件故障、硬件故障、入侵与攻击，以及其他不可预料的未知故障等。

1. 逻辑存储系统需外出维修时，逻辑存储安全管理部门应删除系统中的敏感数据；
2. 对于不能尽快处理的故障，逻辑存储安全管理部门应立即通知上级领导，并保护好故障现场；
3. 逻辑存储系统在上线前应遵循统一的配置要求进行有效的安全配置，同时采用配置扫描工具和漏洞扫描系统对数据存储系统进行定期扫描，尽可能地消除或降低逻辑存储系统的安全隐患。
	* 1. 云存储安全

工业数据云存储应满足如下要求：

1. 应保证云计算基础设施位于中国境内；
2. 应保证云计算平台不承载高于其安全保护等级的业务应用系统；
3. 应实现不同云服务客户虚拟网络之间的隔离；
4. 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
5. 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略，提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；
6. 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则，在不同等级的网络区域边界部署访问控制机制，设置访问控制规则；
7. 应能检测到云服务客户发起的、对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等，应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量，应在检测到网络攻击行为、异常流量情况时进行告警；
8. 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启，保证云服务商对云服务客户系统和数据的操作可被云服务客户审计；
9. 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制；
10. 应保证当虚拟机迁移时，访问控制策略随其迁移，应允许云服务客户设置不同虚拟机之间的访问控制策略；
11. 应能检测虚拟机之间的资源隔离失效，并进行告警，应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警，应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警；
12. 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务，应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改，应采用密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；
13. 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定，应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限，应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施，应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程；
14. 云服务客户应在本地保存其业务数据的备份，应提供查询云服务客户数据及备份存储位置的能力，云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之的内容应保持一致，应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程；
15. 应保证虚拟机所使用的内存和存储空间回收时得到完全清除，云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除；
16. 应能对物理资源和虚拟资源按照策略做统一管理调度与分配，应保证云计算平台管理流量与云服务客户业务流量分离，应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计，应根据云服务商和云服务客户的职责划分，实现各自控制部分包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测；
17. 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力，应在服务水平协议中规定云服务的各项服务内容和具体技术指标，应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等，应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除，应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据；
18. 应确保供应商的选择符合国家有关规定，应将供应链安全事件信息或安全威胁信息及时传达到云服务客户，应将供应商的重要变更及时传达到云限务客户，并评估变更带来的安全风险，采取措施对风险进行控制；
19. 云计算平台的运维地点位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。
	* 1. 数据备份和恢复

工业数据备份和恢复应满足如下要求：

1. 应设立数据备份和恢复管理部门负责制定整体的数据备份和恢复制度、建立数据备份和恢复的标准操作流程，并推动以上相关要制度确实可靠的落地执行；
2. 应制定完备的数据备份管理制度，以保证数据备份工作的规范性；
3. 应明确数据备份与恢复的管理制度，以满足数据服务可靠性、可用性等安全目标；
4. 应明确数据备份与恢复的操作规程，明确定义数据备份和恢复的范围、频率、工具、过程、日志记录、数据保存时长等；
5. 应明确数据备份与恢复的定期检查和更新工作程序，包括数据副本的更新频率、保存期限等；
6. 应依据数据生存周期和业务规范，建立数据生存周期各阶段数据归档的操作流程；
7. 应明确归档数据的压缩或加密要求；
8. 应明确归档数据的安全管控措施，非授权用户不能访问归档数据；
9. 应识别组织适用的合规要求，按监管部门的要求对相关数据予以记录利保存；
10. 应明确数据存储时效性管理规程，明确数据分享、存储、使用和删除的有效期、有效期到期时对数据的处理流程、过期存储数据的安全管理要求；
11. 应明确过期存储数据的安全保护机制，对超出有效期的存储数据应具备再次获取数据控制者授权的能力；
12. 应建立数据备份与恢复的统一技术工具，保证相关工作的自动执行；
13. 应建立备份和归档数据安全的技术手段，包括但不限于对备份和归档数据的访问控制、压缩或加密管理、完整性和可用性管理，确保对备份和归档数据的安全性、存储空间的有效利用、安全存储和安全访问；
14. 应定期采取必要的技术措施查验备份利归档数据完整性和可用性；
15. 应建立过期存储数据及其备份数据彻底删除或匿名化的方法和机制，能够验证数据已被完全删除、无法恢复或无法识别到个人，并告知数据控制者和数据使用者；
16. 应通过风险提示和技术手段避免非过期数据的误删除，确保在一定的时间窗口内的误删除数据可以手动恢复；
17. 应确保存储架构具备数据存储跨机柜或跨机房容错部署能力。
	1. 数据处理
		1. 数据脱敏

工业数据脱敏应满足如下要求：

1. 应设立数据脱敏部门并配置专职的技术人员和管理人员，负责制定整体的数据脱敏原则和制度，并推动相关要求确实可靠的落地执行。
2. 应根据实际业务场景，结合行业法规的要求，制定相应的数据脱敏策略。
3. 应确保经过数据脱敏处理后，原始信息中包含的敏感信息已被移除，无法通过处理后的数据得到敏感信息；
4. 脱敏后的数据应尽可能的体现原始数据的特征，且应尽可能多的保留原始数据中的有意义信息，以减小对使用该数据的系统的影响；
5. 应保证数据脱敏的过程可通过程序自动化实现，可重复执行；
6. 数据脱敏时需保证对相同的原始数据，在各输入条件一致的前提下，无论脱敏多少次，其最终结果数据是相同的；
7. 可通过配置的方式，按照输入条件不同生成不同的脱敏结果，从而可以方便的按数据使用场景等因素为不同的最终用户提供不同的脱敏数据；
8. 在数据脱敏之前，应结合数据分级分类表对敏感数据进行识别和定义，明确需要脱敏的数据信息，一般包括个人信息数据、组织敏感信息、国家重要数据等，并根据识别出的敏感数据的具体情况，确定合适的脱敏方法；
9. 在数据脱敏的各个阶段需加入安全审计机制，严格、详细记录数据处理过程中的相关信息，形成完整的数据处理记录；
10. 设置专人定期对脱敏相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常。
	* 1. 数据分析安全

工业数据分析应满足如下要求：

1. 应设立数据分析部门，负责为公司提供必要的数据分析技术支持，负责为制定整体的数据分析安全方案和相关制度，并推动相关要求确实可靠的落地执行；
2. 应明确数据分析过程的安全规范，覆盖构建数据仓库、建模、分析、挖掘、展现等方面的安全要求，明确个人信息保护、数据获取方式、访问接口、授权机制、分析逻辑安全、分析结果安全等内容；
3. 应明确数据分析安全审核流程，对数据分析的数据源、数据分析需求、分析逻辑进行审核，以确保数据分析目的、分析操作等当面的正当性；
4. 应采取必要的监控审计措施，确保实际进行的分析操作与分析结果使用与其声明的一致，整体保证数据分析的预期不会超过相关分析团队对数据的权限范围；
5. 应明确数据分析结果输出和使用的安全审核、合规评估和授权流程,防止数据分析结果输出造成安全风险；
6. 在针对个人信息的数据分析中，组织应采用多种技术手段以降低数据分析过程中的隐私泄漏风险
7. 应记录并保存数据分析过程中对个人信息、重要数据等敏感数据的操作行为；
8. 应提供组织统一的数据分析系统，并能够呈现数据分析前后数据间的映射关系。
	* 1. 数据处理环境安全

工业数据处理环境应满足如下要求：

1. 应由业务团队相关人员负责数据处理环境安全管控；
2. 数据处理环境的系统设计、开发和运维阶段应制定相应的安全控制措施，实现对安全风险的管理；
3. 应明确数据处理环境的安全管理要求；
4. 应基于数据处理环境建立分布式处理安全要求，对外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识利用户身份鉴权、数据副本节点更新检测及防止数据泄漏等方面进行安全要求和控制；
5. 组织应明确适合数据处理环境的数据加解密处理要求和密钥管理要求；
6. 应建立数据分布式处理节点间可信连接策略和规范，例如：采用Kerberos、可信模块等节点认证机制以确保数据分布式处理节点接入的可信性；
7. 应建立数据分布式处理每个计算节点和用户安全属性的周期性确认机制，确保分布式处理预定义安全策略的一致性；
8. 应建立分布式处理过程中数据文件鉴别和认证的策略和规范，确保分布式处理数据文件的可访问性；
9. 应建立分布式处理过程中不同数据副本节点的更新检测机制，确保这些结点数据拷贝的真实性；
10. 应建立分布式结算过程中数据泄露控制规范和机制，防止数据处理过程中的调试信息、日志记录、不受控制输出等泄露受保护的个人信息或重要数据；
11. 应建立分布式处理外部服务组件审核机制，防止外部服务组件泄漏受保护的个人信息或重要数据；
12. 应建立数据分布式处理节点的自动维护策略和管控措施，提供虚假结点监测、故障用户结点确认和自动修复的技术机制，避免云环境或虚拟环境下潜在的安全攻击；
13. 基于员工工作岗位和角色，遵循最小权限和职责分离原则，授予员工有限的资源访问权限；
14. 应建立数据处理环境的数据加密和解密处理策略和密钥管理规范。在风险评估的基础上采用合理的加密技术；
15. 使用自动化监控系统对数据处理平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控；
16. 应制定数据处理溯源策略和溯源机制、溯源数据存储和使用的管理制度，并制定溯源数据表达方式和格式规范，以规范化组织、存储和管理溯源数据；
17. 应建立基于溯源数据的数据业务与法律法规合规性审计机制，并依据审计结果增强或改进数据服务相关的访问控制与合规性保障工作；
18. 应采取校验码、加密、数字签名等技术手段，保证溯源数据真实性和机密性。并采用必要的技术手段，确保溯源数据能重现数据处理过程，如追溯操作发起者及发起时间。
	* 1. 数据导入导出安全

工业数据导入导出应满足如下要求：

1. 应设立数据导入导出安全管理部门，负责提供必要的技术支持，负责导入导出数据的安全，负责制定整体的数据导入导出制度，并推动相关要求在组织内业务中确实可靠的落地执行；
2. 在进行数据导入导出操作之前，操作人员应明确数据导入导出的目的，范围，内容和格式等；
3. 在明确数据导入导出的目的之后，应向数据导入导出安全管理部门提出申请；
4. 数据导入导出安全管理部门在收到数据导入导出申请后，应对所申请的数据导入导出范围及内容进行风险评估及合规性审查等工作；
5. 当导出数据中的内容包含个人信息时，应先征得个人信息主体的明示同意；
6. 数据导入导出安全管理部门在授权过程中应采取“最小够用”原则，即为数据使用者提供完成业务处理活动所需的最小数据集；
7. 数据导入导出安全管理部门应对导入导出数据的范围和内容进行审查，确认无误后方可对数据使用者进行授权；
8. 数据导入导出安全管理部门应设置负责数据导入导出工作的专职人员，并对数据导入导出安全负责；
9. 对数据导入导出的专职人员采取必要的认证措施，防止假冒；
10. 对导入导出的数据采取必要的安全技术措施，如木马检测，加密传输，加密存储，完整性校验等，以确保导入导出数据的安全性；
11. 对导入导出的数据进行机器和人工双重校验，以保证数据的完整性和可用性；
12. 对导出数据的存储介质进行标识，明确介质的命名规则，统一编号格式，定期对数据的完整性和可用性进行验证；
13. 导出的数据存储介质的存放环境应有防火，防盗，防水，防尘，防震，防腐蚀及防静电等措施，防止其被盗，被毁，被未授权修改，以及其中所存信息的非法泄露；
14. 如果导出的数据将不再使用，应销毁该数据，以避免数据泄露；
15. 在数据导入导出的各个阶段都应加入安全审计机制，严格，详细地记录数据导入导出过程中的相关信息，形成完整的数据导入导出记录；
16. 数据导入导出安全管理部门应设置专人定期对数据导入导出相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常问题。
	1. 数据流通
		1. 数据共享安全

工业数据共享应满足如下要求：

1. 应设立数据交换安全管理部门，负责为数据交换提供必要的技术支持，负责制定整体的数据共享安全策略及安全规范，负责为技术人员制定数据共享审计策略和审计日志管理规范，并推动相关要求确实可靠的落地执行；
2. 应明确数据共享的安全规范，从国家安全、组织机构的核心价值保护、个人信息保护等方面对数据共享的风险控制提出要求；
3. 明确相应的权限审批和授权流程，并根据不同场景下数据共享制定细化的规范要求，以降低数据共享场景下的安全风险；
4. 应建立数据共享的审核流程，包括共享的数据内容、涉及的部门和组织、授权审批同意/否决、归档记录等；
5. 数据共享前应提出数据共享申请，明确数据共享所涉及的数据范围、内容及格式等；
6. 数据交换安全管理部门在收到数据共享申请后，要对数据共享所涉及的数据范围、内容及格式等进行评估；
7. 应设置专门的人员负责数据共享，并对数据共享安全负责；
8. 应在数据共享的各个阶段加入安全审计机制，严格、详细地记录并保存数据共享的所有操作和行为；
9. 数据共享安全管理部门应设置专人定期对数据共享相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常。
	* 1. 数据开放安全

工业数据开放应满足如下要求：

1. 应对工业数据按照数据开放属性进行分类。
2. 对于分类属性为禁止开放的数据，不得开放。
3. 对于分类属性为受限开放、无条件开放的数据应满足以下要求：
4. 在开放前，对开放的必要性、范围、规模、方式等进行分析研判。
5. 数据安全管理责任部门应会同业务部门，对拟开放数据的合规性、业务需求、数据脱敏方案等进行审核与审批，业务部门应对开放渠道、开放时间、拟开放数据的真实性，以及数据脱敏效果进行确认。
6. 应采取合适方法对数据进行脱敏处理，保证工业数据开放安全。
7. 应确保工业数据开放内容的真实性、规范性、实效性和准确性。
8. 应采取数据水印等必要措施保证工业数据开放安全。
9. 应在数据分类分级的基础上，建立工业数据开放管理制度，针对可对外公开和开放的数据进行开放前、开放中、开放后安全管理，具体包括开放前的数据内容、开放范围等审核，开放中对定期审查，以及开放后可能出现不良影响的应急处理机制。
10. 应制定工业数据开放审核制度，包括数据待开放内容、涉及的部门和组织、审核批准/否决、工业数据开放应急处理流程等，确保开放内容是可以公开并且符合法律法规要求的。工业数据开放的审核由工业数据开放安全管理部门负责，严格审核和管理开放的数据，确保已开放数据的合法性、真实性、准确性。
11. 应采取密码技术措施对开放数据的机密性、完整性和可用性进行安全防护。如通过官网开放数据时，采取包括网页防篡改等技术，防范披露数据篡改风险。
12. 对数据开放全链路各环节的权限最小化控制，如进行白名单控并对异常进程监控。
13. 应采取必要的防泄漏技术或手段，防止工业数据在开放过程中发生泄露。
14. 原则上核心数据不允许开放。
	* 1. 数据交易安全
			1. 交易申请

数据交易申请环节应满足如下要求：

1. 数据供方应明确界定交易数据的内容范围、使用范围，以确保符合国家相关法律法规的要求；
2. 数据供方应按数据交易服务机构要求,提供对交易数据的概要描述,并提供样本数据；
3. 数据交易服务机构对数据供方提供的样本数据进行内容审核,确认数据合法合规。对于不符合要求的,数据交易服务机构应要求数据供方重新提交样本数据进行审核；
4. 数据需方应披露数据需求内容、数据用途，以确保符合国家法律法规的要求；
5. 数据交易服务机构对数据需方的数据需求进行审核通过后方可发布。
	* + 1. 交易磋商

数据交易磋商环节应满足如下要求：

1. 供需双方应对交易数据的用途、使用范围、交易方式、使用期限和交易价格等协商和约定,形成交易订单；
2. 数据交易服务机构应遵循国家法律,对交易订单从数据出境安全、个人信息保护安全等方面进行审核,确保符合相关法律法规和标准等合规性要求,撤销不符合要求的交易订单；
3. 数据交易服务机构应对审核通过的订单进行登记备案，并对供需双方发出交易确认通知。
	* + 1. 交易实施

数据交易实施环节应满足如下要求：

1. 数据交易服务机构应审核数据需方的数据安全能力成熟度，确保不低于数据供方的数据安全能力成熟度；
2. 数据交易服务机构应为数据交易与数据供方和数据需方签订三方合同,明确数据内容、数据用途、交付质量、交付方式、交易金额、交易参与方安全责任、保密条款等内容；
3. 数据交易服务机构应对交付数据内容进行监测和核验,如发现违法违规事件,应及时中断数据交易行为，同时依法依规进行处理；
4. 数据交易服务机构应对交易过程中的违法违规数据具有追溯能力；
5. 对于在线数据交付模式,数据交易服务机构应在供需双方的数据传输链路上部署交易数据监控工具，具有完备的数据保护机制和数据泄露检测能力；
6. 对于托管数据交付模式,数据交易服务机构应为数据需方建立安全的数据使用环境,并分配相应的权限；
7. 数据供方在数据需方未完全获取数据内容前,有义务保证交易数据质量和数量符合数据成交9时的相关描述；
8. 在托管数据交付模式下,数据需方在数据使用完成后，应向数据交易服务平台提供提取结果数据请求，核准后由数据交易服务平台发放给数据需方。
	* + 1. 交易结束

数据交易结束环节应满足如下要求：

1. 数据交付完成后,数据供方应立即关闭数据访问接口,数据供方发出数据交付完成确认；
2. 数据交付完成后，数据需方发出数据接收完成确认；
3. 在托管数据交付模式下,数据交易服务机构应在交易结束后立即销毁残余数据；
4. 数据交易服务机构应为交易过程形成完整的交易日志并安全保存。
	* 1. 数据接口安全

工业数据接口管理应满足如下要求：

1. 应建立数据接口安全管理部门，负责提供必要的技术支持，负责制定整体的数据接口安全控制策略，负责为数据使用者制定统一的、标准的数据接口开发规范，并推动相关要求确实可靠的执行；
2. 制定接口开发规范，对涉及的接口类型、编码格式、变量名称、变量类型、长度、大小等内容进行规范定义。同时，采用不安全参数限制、时间戳超时机制、token授权机制、签名机制、安全传输协议HTTPS等安全措施，降低数据在接口调用过程中的安全风险；
3. 应建立数据接口管理平台，实现对数据接口的管理和审核，保障开放的接口符合安全规定要求；
4. 组织机构因内部系统建设或者功能完善需要申请或者变更数据接口的，由组织内部信息化专员登录数据接口管理平台提出相应的申请与变更需求，经上级领导审批同意后，提报数据接口安全管理部门审批；
5. 组织机构接到外部数据接口使用申请时，由数据接口安全管理部门在数据接口管理平台上进行提报与登记，登记内容包括数据接口调用者的使用目的、使用方式等。并组织数据接口相关技术人员与数据接口调用者共同评审数据接口的实施可行性以及制定实施与测试方案。在实施前，需与接口调用者签订安全责任声明书，包括双方权利义务、数据使用目的、调用频次、责任归属等；
6. 在数据接口调用的各个阶段都应加入安全审计机制，严格、详细地记录接口调用过程中的相关信息，包括日期、时间、调用人、IP地址、状态、返回内容等；
7. 数据接口安全管理部门应设置专人定期对接口调用相关的日志记录进行安全审计，发布审计报告，并跟进审计中发现的异常。
	* 1. 数据出境安全
8. 应结合实际开展数据出境安全自评估和安全管理。自评估至少应包含以下几个方面：
9. 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；
10. 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；
11. 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；
12. 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；
13. 与境外接收方拟订立的数据出境相关合同等法律文件是否充分约定了数据安全保护责任义务；
14. 其他可能影响数据出境安全的事项。
15. 确需出境的，应依法依规进行数据出境安全评估。
16. 应具备数据出境安全监测能力，对通过评估的数据的出境行为、内容开展安全监测，加强数据出境安全风险防范和处置。
17. 应预留数据安全监测、检查等技术接口，为数据出境安全管理提供技术支持。
18. 应采取必要的防泄漏技术或手段，防止工业数据在出境过程中发生泄露。
19. 原则上核心数据不允许出境，确需出境的，应当依法依规进行数据出境安全评估。
	1. 数据销毁
		1. 数据销毁处置

工业数据销毁处置应满足如下要求：

1. 应设立数据销毁安全管理部门，负责提供必要的技术支持，负责制定整体的数据销毁处置策略和管理制度，负责为技术人员建立规范的数据销毁流程和审批机制，并推动相关要求确实可靠的落地执行；
2. 应依照数据分类分级建立数据销毁策略和管理制度，明确数据销毁的场景、销毁对象、销毁方式利销毁要求；
3. 应建立规范的数据销毁流程和审批机制，设置销毁相关监督角色，监督操作过程,并对审批和销毁过程进行记录控制；
4. 应按国家相关法律和标准销毁个人信息、重要数据等敏感数据；
5. 对于在工作中形成的个人临时性草稿及文字废纸，由组织人员通过碎纸机自行进行破碎销毁；
6. 对于工作过程中形成的日常办公作废的文件，需要上级领导部门鉴定确已无保存价值，待上级部门审核通过后，由数据销毁安全管理部门现场监督组织人员使用碎纸机进行破碎销毁；
7. 对于日常办公过程中形成的作废数据，需遵循如下销毁流程：
8. 组织人员根据实际情况，结合业务和数据的重要性，明确需要销毁的数据，并在数据销毁平台上提出相应的数据销毁申请，此申请需要填写的内容包括申请人、销毁内容，涉及部门、销毁原因等。经上级领导审批后，提报数据销毁安全管理部门审批；
9. 数据销毁安全管理部门接到数据销毁申请后，组织相关人员开展数据销毁评审会议，对所申请的数据进行合理性和必要性评估，并根据数据分类分级的结果，评审数据销毁的手段和方法，其中包括物理销毁和逻辑销毁等，比如覆写法、消磁法、捣碎法/剪碎法、焚毁法，或者配置必要的数据销毁工具等，确保能以不可逆的方式销毁数据内容。对于已通过评审的数据销毁申请，数据销毁安全管理部门应在数据销毁管理平台上录入数据销毁实施期限并确认销毁申请审核。若评审结果为否决销毁，则由数据销毁安全管理部门在数据销毁管理平台进行否决需求操作；
10. 为防止机密数据泄露给未经授权的人员，各部门人员应将需要销毁的数据送到数据销毁安全管理部门，由存储介质安全管理部门按照评审通过的销毁方法统一进行安全销毁。注意，未经审核和评审的机密数据，组织人员不得擅自销毁。
	* 1. 存储媒体销毁处置

工业数据存储媒体销毁处置应满足如下要求：

1. 应设立介质销毁安全管理部门，负责提供必要的技术支持，负责制定整体的介质销毁处置策略和管理制度，负责为技术人员建立规范的介质销毁监督流程和审批机制，并推动相关要求确实可靠的执行。
2. 组织内的人员必须严格遵守组织所制定的介质销毁安全管理制度，根据实际情况，明确需要销毁的介质。对于以下情形之一的存储介质可以提出介质销毁申请：
3. 备份数据的保存实际时间已经超过部门的制度要求，部门上级领导确认该数据无保留价值；
4. 存储介质因过频使用、自然老化而无法使用的；
5. 因水灾、火灾等其他事故造成的存储介质损坏而无法使用的；
6. 因特殊原因或工作需要销毁存储介质。
7. 组织人员明确需要销毁的介质后，在介质销毁平台上提出相应的介质销毁申请，需要填写的内容包括申请人、销毁介质清单、介质类型、销毁原因等。经上级领导审批后，提报介质销毁安全管理部门审批。
8. 介质销毁安全管理部门接到介质销毁申请后，组织相关人员开展介质销毁评审会议，对所申请的介质进行合理性和必要性的评估，并根据实际的数据保密性要求。
9. 对于评审通过的介质销毁申请，介质销毁安全管理部门在介质销毁管理平台上录入介质销毁实施期限并确认销毁申请审核。若评审结果为否决销毁，则由介质销毁安全管理部门在介质销毁管理平台进行否决需求操作。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_