ICS 35.030
CCS M10

YD

中华人民共和国通信行业标准

YD/T 4982—2024

工业企业数据安全防护要求

Data security protection requirements for industrial enterprises

2024－11－07 发布　　2025－02－01 实施

中华人民共和国工业和信息化部　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这些专利的责任。

本文件由中国通信标准化协会（CCSA）提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、福建省工业信息产业发展研究中心、北京天融信网络安全技术有限公司、深信服科技股份有限公司、福建中信网安信息科技有限公司、北京睿航至臻科技有限公司、烟台中科网络技术研究所、杭州安恒信息技术股份有限公司、华为技术有限公司、长扬科技(北京)股份有限公司、联想(北京)有限公司、北京数安行科技有限公司、中国生物技术股份有限公司、北京奇虎科技有限公司、北京万里红科技有限公司、上海观安信息技术股份有限公司、阳光电源股份有限公司、恒安嘉新（北京）科技股份公司、亚信科技(成都)有限公司、欣旺达动力科技股份有限公司。

本文件主要起草人：孙岩、李俊、王墨、柳彩云、金华松、翁颖、郑丽娜、刘奕彤、李一鸣、宋博韬、姜守义、王海洋、初杰、田丽丹、邵萌、许国章、张亚京、李汝鑫、刘玉红、薛富、赵瑞成、姚一楠、姜国通、谢江、王颖、许道远、廖双晓、孙威。

本文件于2024年首次发布。

工业企业数据安全防护要求

1 范围

本文件规定了工业企业数据安全防护的基础性数据安全防护要求、数据全生命周期安全防护要求、其它防护要求。

本文件适用于指导工业企业开展数据安全防护工作，也可为开展数据安全风险评估工作提供参考。

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 25069-2022 信息安全技术 术语

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

3 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。

3.1

工业企业 industrial enterprise

直接从事工业性生产经营活动（或劳务）的组织。

3.2

工业数据 industrial data

工业企业在研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据。

3.3

核心数据 core data

关系国家安全、国民经济命脉、重要民生、重大公共利益的工业数据（包括原始数据和汇聚、整合、分析等处理中以及处理后的衍生数据）。

3.4

一般数据 general data

其他未纳入重要数据、核心数据目录的工业数据。

3.5

数据载体 data carrier

数据处理活动中使用的系统、平台、设备、媒介等。

3.6

数据安全 data security

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。

4 缩略语

下列缩略语适用于本文件。

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

SCADA：监控与数据采集（Supervisory Control And Data Acquisition）

Telnet：远程登录系统（Telecommunications Network）

PLC：可编程逻辑控制器（Programmable Logic Controller）

VPN：虚拟专用网络（Virtual Private Network）

5 概述

5.1 总体要求

工业企业开展工业领域数据处理活动时应满足以下数据安全防护要求：

a) 基础性数据安全保护要求：工业企业应建立健全数据安全管理机制，配备数据安全技术能力。基础性数据安全保护要求包括安全管理制度、组织机构、人员保障、数据分类分级、权限管理、系统与设备安全管理、供应链数据安全管理、安全评估、日志留存、安全审计，监测预警、信息共享与应急处置等十一个方面的要求；

b) 数据全生命周期安全防护要求：工业企业应规范数据生命周期各阶段的数据处理活动，实施有效的数据安全防护措施。数据全生命周期安全防护要求包括数据收集、数据存储、数据使用加工、数据传输、数据提供、数据出境、数据公开和数据销毁等十个方面；

c) 其它防护要求：工业企业开展涉及个人信息的数据处理活动，应当符合 GB/T 35273-2020 及 GB/T 41479-2022 相关要求。

5.2 安全防护要求级别

工业领域数据的安全防护要求包括对一般数据、重要数据和核心数据的要求。根据数据处理活动涉及的数据级别，数据处理者应遵循如下防护要求：

a) 一般数据处理活动应按照对一般数据的防护要求开展数据安全防护工作；

b) 重要数据处理活动应在落实对一般数据的防护要求的基础上，按照要求开展重要数据安全防护工作；

c) 核心数据处理活动应在落实对重要数据的防护要求的基础上，按照要求开展核心数据安全防护工作。

6 基础性数据安全防护要求

6.1 安全管理制度

6.1.1 一般数据

本项要求包括：

应结合所属行业领域的数据特征、数据处理场景等，制定数据安全管理制度规范，明确数据安全工作方针、 目标和原则以及管理要求。

6.1.2 重要数据和核心数据

在6.1.1的基础上还应满足以下要求：

a） 应依据重要数据和核心数据目录备案管理要求，开展目录备案和备案变更工作，及时更新重要数据和核心数据目录；

b） 应建立第三方人员安全管理制度，并按照数据全生命周期安全防护要求签署保密协议，定期对第三方人员的数据处理行为进行安全审查；

c） 应建立监督考核机制，落实执行对数据安全管理工作的监督检查和考核制度，定期对数据安全工作相关部门进行安全责任评估。

6.2 组织机构

6.2.1 一般数据

本项要求包括：

宜设置相应的数据安全管理部门或岗位，明确数据安全管理部门或岗位职责，包括但不限于制定企业数据安全管理制度规范、编制年度数据安全工作计划、协调数据安全管理相关部门、建立数据安全防护措施等。

6.2.2 重要数据和核心数据

在6.2.1的基础上还应满足以下要求：

a） 应建立覆盖本企业相关部门的数据安全组织架构，建立常态化沟通与协作机制；

b） 数据安全组织架构宜包括数据安全管理责任部门，采购、审计等职能管理部门，以及研发设计、生产制造、运营维护等业务部门；

c） 应明确数据安全管理责任部门，设置数据安全管理专职岗位。

6.3 人员保障

6.3.1 一般数据

本项要求包括：

a） 宜根据企业和岗位性质，配备数据安全管理人员，负责统筹开展数据安全管理工作，包括但不限于审批数据安全授权事项、组织开展数据安全评估、检查数据安全管理制度规范执行落实情况等；

b） 应定期开展数据安全教育与技能培训，强化重要岗位管理技术人员的技能培训，提高全员数据安全意识和专业技能。

6.3.2 重要数据和核心数据

在6.3.1的基础上还应满足以下要求：

a） 应明确企业数据安全管理负责人，负责指导数据安全管理责任部门、协调各相关部门开展数据安全工作；

b） 应强化研发设计、生产制造等部门的数据处理关键岗位人员管理，将能获知重要数据和核心数据内容的人员确定为关键岗位人员；

c） 应明确数据处理关键岗位人员职责，签署数据安全责任书，责任书内容包括但不限于数据安全岗位职责、义务、处罚措施、注意事项等；

d） 宜制定数据处理关键岗位人员上岗的数据安全教育培训计划，并对培训计划、培养方式、培训内容定期审核和更新。

6.4 权限管理

6.4.1 一般数据

本项要求包括：

a） 宜制定权限管理与审批制度，建立多级审核工作机制和流程；

b） 应对数据处理平台或系统账号的分配、开通、使用、注销等进行严格管理，并按照业务需求、安全防护策略及最小授权原则合理分配数据处理权限；

c） 应按照最小授权原则分配非联网系统、设备的获取、使用权限；

d） 应定期对权限分配情况进行复核，严禁未授权访问数据。

6.4.2 重要数据和核心数据

在 6.4.1 的基础上还应满足以下要求：

a） 应建立内部登记、审批机制，明确数据安全授权审批事项、审批部门和审批人等；

b） 应合理确定数据处理活动的操作权限，严格控制超级管理员权限账号数量，加强数据安全访问控制；

c） 应与所有涉及重要数据和核心数据处理的岗位人员签订安全责任协议，人员调离或终止劳动合同时，及时变更岗位变动人员的数据处理权限，终止离岗人员的所有数据处理权限。

6.5 系统与设备安全管理

6.5.1 一般数据

本项要求包括：

a） 应对工业终端设备、工业数据库等数据载体进行安全配置，建立工业终端设备、工业数据库等数据载体的安全配置清单和审计基准要求，定期进行配置审计；

b） 应密切关注重大安全漏洞及其补丁发布，及时采取修补措施，补丁安装前，应对补丁进行安全评估和测试验证；

c） 应对工业控制系统、工业互联网平台等的开发、测试和生产环境进行逻辑或物理隔离；

d） 应强化工控系统、数据库等数据载体的登录账户及口令管理，避免使用默认口令或弱口令，定期更新口令。

6.5.2 重要数据和核心数据

在 6.5.1 的基础上还应满足以下要求：

a） 应对涉及重要数据和核心数据处理活动的数据载体的访问行为进行多因素身份鉴别；

b） 应通过工业防火墙、网闸等防护设备对工业控制网络安全区域边界进行逻辑隔离安全防护；

c） 应对处理重要数据的系统提供不低于 GB/T 22239—2019 第三级要求的防护。

6.6 供应链数据安全管理

6.6.1 一般数据

本项要求包括：

a） 宜制定供应链数据安全管理方案，并明确供应链涉及的数据安全风险控制措施；

b） 在选择供应链涉及的服务商时，应对其资质条件、业务合法性、数据安全防护能力等进行评估核实；

c） 宜加强供应链服务商管理，以合同、协议等明确规定数据安全防护要求和责任落实要求，规范数据使用权限、内容、范围及用途，要求服务商做好数据安全防护工作，防范数据外泄。

6.6.2 重要数据和核心数据

应满足 6.6.1 的要求。

6.7 数据分类分级

6.7.1 一般数据

本项要求包括：

a） 宜制定企业数据资产安全管理规范，梳理相关制度文件，明确数据资产的安全管理目标和原则、维护和使用责任、梳理手段、梳理方式、梳理周期等；

b） 应采用人工核对、 自动化识别等方式，定期梳理本企业电子化数据与以其他方式记录的数据；

c） 应全面掌握数据资产分布、迁移、资产异常等情况，形成数据资产清单并定期更新；

d） 针对数据规模大、挖掘价值高的一般数据，应实施动态管理，及时调整数据分级结果。

6.7.2 重要数据和核心数据

在 6.7.1 的基础上还应满足以下要求：

应按照行业监管部门要求、《工业领域重要数据识别指南》等标准规范及业务需求，开展重要数据和核心数据识别和目录备案工作。

6.8 安全评估

6.8.1 一般数据

本项要求包括：

宜自行或委托第三方评估机构开展数据安全风险评估，评估数据管理能力、数据安全防护能力等内容。

6.8.2 重要数据和核心数据

在 6.8.1 的基础上还应满足以下要求：

a） 应自行或委托第三方评估机构，每年至少开展一次安全风险评估，及时整改风险问题，并向本地区行业监管部门报送风险评估报告；

b） 应在收购或资产剥离、重大流程或系统变更、涉及重要数据和核心数据的新业务上线，以及数据迁移、数据出境、数据提供等过程前，启动数据安全风险评估工作，分析可能存在的风险、造成的问题和影响等，并形成相应的数据安全风险评估报告。

6.9 日志留存

6.9.1 一般数据

本项要求包括：

a） 应对数据处理日志及系统运行日志进行记录；

b） 日志记录信息应包括操作时间、操作地点、操作人员、操作 IP、操作对象、操作账号及权限、处理方式和处理结果等，并确保日志记录完整、准确；

c） 日志的留存时间应满足国家相关法律法规要求，不低于六个月；

d） 应对日志操作进行权限控制，配备日志审计员，加强日志访问和处理管理。

6.9.2 重要数据和核心数据

在 6.9.1 的基础上还应满足以下要求：

应对高风险操作（如批量复制、批量传输、批量销毁等操作）日志进行备份，对日志的备份文件定期进行完整性校验，以保证日志备份文件的可用性和真实性。

6.10 安全审计

6.10.1 一般数据

本项要求包括：

应对数据的访问权限进行定期审计，至少每半年一次对访问权限规则和已授权清单进行复核，定期清理已失效的账号和授权。

6.10.2 重要数据和核心数据

在 6.10.1 的基础上还应满足以下要求：

a) 应配备日志审计技术能力，将重要数据和核心数据处理活动全量纳入审计范围；

b) 宜每半年形成一份重要数据处理活动审计报告，每季度形成一份核心数据处理活动审计报告。

6.11 监测预警、信息共享与应急处置

6.11.1 一般数据

本项要求包括：

a) 宜对工业数据泄露、违规传输、流量异常等安全风险进行监测分析，研判其原因、过程、范围、影响等，增强数据安全风险监测预警能力；

b) 宜采用技术手段对互联网出入口的工业数据进行实时安全监测；

c) 应及时排查数据安全隐患，采取必要措施防范数据安全风险；

d) 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，并与行业主管部门数据安全事件应急预案进行衔接，组织开展应急演练并保存演练记录；

e) 应在数据安全事件发生后，按照应急预案及时开展应急处置；

f) 对损害用户合法权益的数据安全风险或事件，应及时告知用户，并提供减轻危害的措施；

g) 事件处置完成后，应形成总结报告，每年向本地区行业监管部门报告数据安全事件处置情况，总结报告内容包括但不限于事件原因、事件后果、影响范围、事件责任、处置过程和结果、工作经验等。

6.11.2 重要数据和核心数据

在 6.11.1 的基础上还应满足以下要求：

a) 涉及重要数据和核心数据的安全风险，应向本地区行业监管部门报告；

b) 涉及对重要数据和核心数据的未经授权访问操作，宜具备自动化识别和实时预警能力；

c) 应及时将可能造成较大及以上安全事件的安全风险向本地区行业监管部门报告。

7 数据全生命周期安全防护要求

7.1 数据收集安全

7.1.1 一般数据

本项要求包括：

a） 应遵循合法、正当、必要的原则开展数据收集，明确数据收集的目的、方式、流程、范围、类型等，以及数据格式、质量准则和评价方式等要求，不得窃取或者以其他非法方式收集数据；

b） 应加强对收集人员、设备、环境的管理，确保工业企业现场的 SCADA、工业数采网关、PLC 等数据采集系统及组件处于受防护状态；

c） 在开展数据收集时，宜采用技术措施对外部数据的真实性、有效性、安全性进行鉴别，避免收集不明来源的数据；

d） 通过移动存储介质收集数据并导入系统前，应对介质设备进行标签化管理，确定接入安全策略，实现移动介质接入控制；

e） 对涉及工业通信协议的数据，应通过受防护的上位机或组态软件完成收集。

7.1.2 重要数据

在 7.1.1 的基础上还应满足以下要求：

a） 应对数据收集的来源、时间、类型、数量、频度、流向等信息进行记录和审计，避免出现超范围数据收集活动；

b） 应对数据收集所涉及的软硬件工具、设备、系统、平台、接口以及收集技术等，采取必要的测试、认证、鉴权等措施，并进行内部审批；

c） 应具备对数据收集行为进行监测的技术能力，确保数据收集的合规性和执行上的一致性，并能够在发现异常时进行告警；

d） 应采用与数据提供方签署相关协议、数据源合法性书面承诺等方式，明确通过间接途径获取数据的双方的法律责任。

7.1.3 核心数据

在 7.1.2 的基础上还应满足以下要求：

应具备数据收集行为实时监控能力，在发现异常时及时终止数据收集行为，并采用技术手段确保所有收集行为可溯源。

7.2 数据存储安全

7.2.1 一般数据

本项要求包括：

a） 应对存储数据的使用进行身份鉴别和访问控制；

b） 宜采用加密技术、数字签名、完整性校验等方式，实现存储数据的保密性、不可抵赖性和完整性；

c） 应建立数据备份制度，定期开展全量数据、增量数据备份；

d） 宜建立工业数据本地及异地灾难恢复机制，定期开展灾难恢复演练，根据演练情况修订灾难恢复预案等业务连续性计划，检查工控系统容灾备份和灾难恢复预案的有效性；

e） 对于非联网独立控制单元，如传感、控制或执行单元等，应采用物理安全措施保障生产环境的设备数据访问或调试接口不暴露在外，采用机密性和完整性防护措施，保障现场存储数据不被泄露、篡改或破坏。

7.2.2 重要数据

在 7.2.1 的基础上还应满足以下要求：

a） 应采用校验技术、加密技术、数字签名等手段实现数据安全存储，不得直接提供存储系统的公共信息网络访问；

b） 应对重要数据存储介质进行安全管理，将介质存放在安全环境中，实行存储环境专人管理；

c） 宜根据所承载数据和软件的重要程度对介质进行分类和标识管理，根据存档目录清单，定期盘点；

d） 应能够监测到数据在存储过程中保密性、完整性、可用性受到破坏的风险，并向授权用户提供告警信息；

e） 应对备份进行安全管理，定期对重要数据进行本地备份，备份介质场外存放，备份数据的防护要求不应低于源数据的防护要求；

f） 对涉及工业生产的实时数据，可根据实际情况转储成关系型数据，再实行安全防护与数据备份；

g） 应定期进行重要数据恢复演练，确保能够及时、完整、准确地恢复数据；

h） 应制定重要数据本地化存储操作规程，存储重要数据的数据中心、云平台等不应设置在境外。

7.2.3 核心数据

在 7.2.2 的基础上还应满足以下要求：

a） 应对历史数据库、时序数据库、实时数据库等核心数据存储设备进行硬件冗余，启用实时数据备份功能，并实施异地容灾备份，保证主设备出现故障时冗余设备可以及时切换并恢复数据；

b） 应具备数据存储行为实时监控能力，在发现异常时及时终止数据访问、删除、修改等操作行为，并采用技术手段确保所有存储操作行为可溯源；

c） 应制定核心数据本地化存储操作规程，存储核心数据的数据中心等不应设置在境外。

7.3 数据使用加工安全

7.3.1 一般数据

本项要求包括：

a） 对涉及自动化决策的数据使用加工行为，应建立数据分析相关数据源的数据获取、汇聚及使用操作规范，明确数据获取、汇聚及使用方式、访问接口、授权机制等，保障决策的透明度；

b） 应对数据挖掘、关联分析等数据使用行为进行记录；

c） 原则上严格禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet 等高风险通用网络服务；

d） 确需远程访问工业控制系统的，宜采用数据单向访问控制等策略进行安全加固，对访问时限进行控制，并采用加标锁定策略；

e） 确需远程维护工业控制系统的，宜采用虚拟专用网络（VPN）等远程接入方式进行。

7.3.2 重要数据

在7.3.1的基础上还应满足以下要求：

a） 应对数据的使用加工进行授权和验证，遵循最小化访问原则；

b） 应明确原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容，并周期性地检查用户操作数据的情况，统一管理数据使用权限；

c） 应采用恶意代码检测、身份鉴别、访问控制等技术手段，确保数据在使用加工中的环境安全；

d） 应在不影响数据使用加工的情况下，对数据脱敏后再进行处理；

e） 应对测试过程中产生的数据进行防护，杜绝未授权获取及使用测试数据。

7.3.3 核心数据

在7.3.2的基础上还应满足以下要求：

应具备数据使用加工行为实时监控能力，在发现异常时及时终止数据使用加工行为，并采用技术手段确保所有数据挖掘、使用、加工、分析行为可溯源。

7.4 数据传输安全

7.4.1 一般数据

本项要求包括：

a） 应根据工业应用场景、数据类型、数据级别和时效要求等因素，制定数据传输安全策略；

b） 应区分安全域内、跨安全域的数据传输场景，建立安全域内、跨安全域的不同场景的数据传输安全策略；

c） 针对受条件限制无法通过网络传输的工业现场数据，应采用受控加密的移动存储介质实现数据安全传输；

d） 工业设备间通信、设备与平台通信时，应对通信端身份、安全策略、安全状态进行双向鉴别，并建立数据安全传输信道，保证工业网络通信的安全性；

e） 对于在非联网的局域网络或控制总线中传输的数据，应采用安全传输协议和身份鉴别等措施，保障工业控制网络不被非法访问，所传输的数据不被泄露、篡改或破坏。

7.4.2 重要数据

在7.4.1的基础上还应满足以下要求：

a） 应采用数据加密、数据校验、安全传输通道、安全传输协议等措施保证数据传输安全，必要时可采用单向隔离传输等技术手段；

b） 应在数据迁移前进行备份和安全评估，保证数据迁移不影响业务应用的连续性；

c） 应具备数据传输异常检测技术能力，对陌生 IP 地址、数据库异常连接（如在设定时间内，某 IP 与实时数据库无任何数据交互或异常交互）等进行实时告警，在检测到数据遭破坏时及时采取恢复措施；

d） 涉及跨组织机构或者使用公共信息网络进行数据传输的，应建立内部登记、审批机制；

e） 应采取流量限速、阻断、违规外联监测等必要措施，对工控协议数据包进行深度解析，仅允许符合安全策略的数据通过安全域边界。

7.4.3 核心数据

在7.4.2的基础上还应满足以下要求：

a） 应具备数据传输实时监测处置能力，保证能够及时告警并阻断违规传输；

b） 应具备数据溯源能力，确保所有数据传输路径可恢复，数据传输行为可溯源；

c） 应采用技术手段实现数据传输的真实性、不可抵赖性和可控性。

7.5 数据提供安全

7.5.1 一般数据

本项要求包括：

a） 应明确数据提供的范围、数量、条件、程序、时间等，建立跨网、跨安全域的数据提供安全操作规范，保障数据提供安全；

b） 应采用数据加密、安全通道等手段，保障数据提供安全；

c） 应建立工业数据交换共享的安全监控措施，对交换共享的数据及数据交换共享行为等进行监控，确保交换共享的数据合理规范使用。

7.5.2 重要数据

在7.5.1的基础上还应满足以下要求：

a） 应与数据获取方签订数据安全协议，并对数据获取方的数据安全防护能力进行评估或核实，根据评估情况采取相应防护措施，确保数据提供过程安全；

b） 应具备数据提供的安全监控技术能力，对提供的数据及数据提供行为进行监控，确保数据合理规范提供，未超出授权范围；

c） 在数据对外提供前，应采取关键字检测、正则表达式检测、数据标识符检测，以及非结构化数据、结构化数据、图片指纹检测等技术实现数据内容的深度识别和过滤，防止生产系统相关重要数据对外泄漏；

d） 应在数据接入互联网等活动中，开展数据安全风险监测，对安全风险高的网络出口和资产，加强网络边界的身份认证和访问控制；

e） 应在数据提供过程中采取必要防护措施，包括数据加密、数据标注、数据水印等；

f） 通过移动存储介质提供数据时，应对介质进行安全监控，确保过程受控；

g） 应采用数据标注、水印等溯源技术，对数据流经节点及共享流转过程中的篡改、泄露、滥用等行为进行溯源；

h） 应根据交换共享的数据特点、应用场景等选择合适的脱敏方法，并对数据脱敏有效性进行评估，保证数据脱敏完全以及脱敏后数据的可用性。

7.5.3 核心数据

在7.5.2的基础上还应满足以下要求：

跨主体提供核心数据的，应当评估安全风险，采取必要的安全防护措施，并事先向本地区行业监管部门提出审批申请。

7.6 数据公开安全

7.6.1 一般数据

本项要求包括：

应结合数据公开场景，明确数据公开范围、类别、条件、流程等数据公开安全策略和操作规程。

7.6.2 重要数据

在7.6.1的基础上还应满足以下要求：

a）应采取数据脱敏、数据水印等必要措施，保证数据公开安全；

b）应在重要数据公开前，分析研判可能对国家安全、公共利益产生的影响，存在重大影响的不得公开。

7.6.3 核心数据

在7.6.2的基础上还应满足以下要求：

核心数据原则上不允许公开。

7.7 数据销毁安全

7.7.1 一般数据

本项要求包括：

a） 应建立数据销毁制度，明确销毁数据对象、规则、流程、技术等要求；

b） 应建立存储媒介安全销毁的操作规程，存储媒介的销毁包括但不限于物理销毁、存储介质消磁、格式化技术等；

c） 应对数据销毁活动进行记录和留存，记录数据销毁的审批、实施过程，以及被销毁数据的情况等。

7.7.2 重要数据

在7.7.1的基础上还应满足以下要求：

a） 可实现存储介质物理销毁，保证在数据完全删除后再销毁存储介质；

b） 应完全清除缓存中的数据，并在数据存储空间被释放或重新分配前完全清除数据，防止数据被恶意恢复；

c） 数据销毁后，应及时向本地区行业监管部门报备更新的重要数据目录。

7.7.3 核心数据

在7.7.2的基础上还应满足以下要求：

核心数据销毁后，应及时向本地区行业监管部门报备更新的核心数据目录。

7.8 数据委托处理安全

7.8.1 一般数据

本项要求包括：

宜在数据委托处理前，通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务。

7.8.2 重要数据

在 7.8.1 的基础上还应满足以下要求：

应在数据委托处理前，对受托方的数据安全防护能力、资质进行评估或核实，并与数据接收方通过合同、协议等形式明确双方的数据安全防护责任和义务。

7.8.3 核心数据

在7.8.2的基础上还应满足以下要求：

a） 跨主体委托处理核心数据的，应当评估安全风险，采取必要的安全防护措施，并事先向本地区行业监管部门提出审批申请；

b） 应采用数据溯源系统、审计系统等技术工具对数据跨主体委托处理行为进行全流程监控、审计、存证，确保数据活动的操作行为、传输路径可溯源，并确保溯源数据的真实性和保密性。

7.9 数据出境安全

7.9.1 一般数据

本项要求包括：

a） 应根据数据出境相关法律法规要求，对个人信息出境采取订立个人信息出境标准合同等措施；

b） 宜通过与境外获取方签订合同或其他具有法律效力的文件，充分约定数据安全防护责任义务，明确境外获取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，并采取加密技术措施保障数据出境安全。

7.9.2 重要数据

在7.9.1的基础上还应满足以下要求：

a） 确需出境的，数据出境前，应依法依规开展数据出境安全评估；

b） 应具备数据出境安全监测能力，对通过评估的数据出境的行为、内容开展安全监测，加强数据出境安全风险防范和处置；

c） 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。

7.9.3 核心数据

应满足7.9.2的要求。

7.10 数据转移安全

7.10.1 一般数据

本项要求包括：

因兼并、重组、破产等原因转移数据的，应在数据转移前明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。

7.10.2 重要数据

在7.10.1的基础上还应满足以下要求：

数据转移后，涉及重要数据备案内容发生变化的，应当履行备案变更手续。

7.10.3 核心数据

在 7.10.2 的基础上还应满足以下要求：

a) 跨主体转移核心数据的，应当评估安全风险，采取必要的安全防护措施，并事先向本地区行业监管部门提出审批申请；

b) 应采用数据溯源系统、审计系统等技术工具对数据跨主体转移进行全流程监控、审计、存证，确保数据活动的操作行为、传输路径可溯源，并确保溯源数据的真实性和保密性。

参 考 文 献

[1] 《中华人民共和国网络安全法》
[2] 《中华人民共和国数据安全法》
[3] 《中华人民共和国个人信息保护法》
[4] 《工业和信息化领域数据安全管理办法（试行）》，工信部网安〔2022〕166号
[5] 《数据出境安全评估办法》，国家互联网信息办公室令第11号