工业企业数据安全防护要求

（草案）

编制单位：国家工业信息安全发展研究中心

2022 年 3 月

目　录

1 范围

本文件规定了工业企业数据安全防护的管理要求和全生命周期保护要求,针对不同安全级别的工业数据确立分级防护的原则。

本文件可供工业企业等数据处理者开展数据安全防护作参考。同一工业企业可能存在不同级别的数据，需要在通用安全防护的基础上，专门针对数据开展分级安全防护。

2 规范性引用文件

本文件无规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业企业 Industrial Enterprise

工业企业包括原材料工业、装备工业、消费品工业、电子信息制造业、软件和信息技术服务业、民爆等工业领域的数据处理者。

3.2

工业数据 Industrial Data

工业数据是指工业各行业各领域，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

工业数据全生命周期 Life Cycle of Industrial Data

包括工业数据收集、存储、使用加工、传输、提供、公开、销毁等环节。

3.4

数据收集 Data Collect

获取工业数据的行为。

3.5

数据存储 Data Store

工业数据以某种格式记录在计算机内部或外部存储介质上。

3.6

数据使用加工 Data Processing

包括对工业数据进行分析、加工等过程。

3.7

数据传输 Data Transfer

工业数据从一个系统、设备、平台、企业传送到另一个系统、设备、平台、企业的通信过程。

3.8

数据提供 Data Provide

工业数据所有者向其他主体共享、转移、委托处理数据。

3.9

数据公开 Data Disclosure

将工业数据向社会或不特定人群公开发布的行为。

3.10

数据销毁 Data Destruction

对工业数据进行彻底删除，使其无法复原的过程。

4 概述

工业企业数据安全防护内容包括安全管理要求和全生命周期保护要求。其中，安全管理要求包括安全管理制度、组织机构、人员保障、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、日志留存和审计，监测预警、信息共享与应急处置等；全生命周期安全保护要求包括一般、重要、核心三级数据在收集、存储、使用加工、传输、提供、公开、销毁等全生命周期各环节中的安全防护要求。

不同级别数据同时被处理且难以分别采取保护措施的，应按照其中级别最高的要求实施保护。

5 数据安全管理要求

5.1 安全管理制度

应结合所属行业领域的工业数据特征、工业数据处理场景等，制定数据安全管理制度和业务相关的数据安全策略和规程，明确数据安全工作方针、目标和原则，并对管理制度执行落实情况进行监督检查和考核问责，管理制度包括但不限于数据安全管理办法，数据分类分级规范、数据安全审计办法、数据安全评估办法、数据安全应急管理制度、数据内部登记审批制度等，并及时进行修订。

5.2 组织机构

a) 应根据需要设置数据安全管理相关部门和岗位，明确相关职责。
b) 重要数据和核心数据处理者，应明确数据安全管理责任部门，负责统筹开展数据安全管理工作，其职责包括但不限于制定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保护措施、审批数据安全授权事项、组织开展数据安全评估、提出数据保护对策建议、检查数据安全管理制度规范执行落实情况等。

c) 重要数据和核心数据处理者，应建立覆盖本单位相关部门的数据安全工作体系，建立常态化沟通与协作机制。工作体系应当包括数据安全管理责任部门，采购、法务、审计、人力、财务等职能管理部门，以及研发设计、生产制造、运营维护、销售营销等业务部门。

d) 重要数据和核心数据处理者，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。

5.3 人员保障

a) 应根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，协助行业（领域）监管部门开展工作。

b) 应在人员录用、调离等过程中，对涉及数据安全工作的人员身份、背景、专业资质、涉密情况等开展审查。

c) 应定期开展数据安全宣传教育与技能培训，提高人员数据安全意识和专业技能。

d) 应根据人员角色（包括内部人员、外部合作人员、运维人员等），加强对数据的访问控制。

e) 应强化研发设计、生产制造、运营维护、销售营销等部门数据处理关键岗位的管理，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，明确数据处理行为规范和安全保护责任，签署责任书。

f) 重要数据和核心数据处理者，应在数据安全管理责任部门中配备专门的数据安全管理和技术人员，其他部门应按照数据安全职责及分工要求，明确专职或兼职的数据安全管理和技术人员。应明确企业数据安全管理责任人，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，本单位法定代表人或者主要负责人是数据安全第一责任人，领导团队中分管数据安全的成员是直接责任人。

5.4 权限管理

a) 应制定权限管理与审批制度，根据实际建立多级审核工作机制和流程。

b) 应分别设置数据安全管理人员、数据处理人员、安全审计人员的权限，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、安全保护策略及最小授权原则合理分配数据处理权限。

d) 应定期对权限分配情况进行复核，严禁非授权访问数据。

e) 涉及处理重要数据和核心数据、授权特定人员超权限处理数据、数据批量复制、数据公开、数据销毁等数据处理活动的，应由数据安全管理责任部门或者数据安全责任人审批。

5.5 系统与设备安全管理

a) 做好工业终端设备、边缘计算设备、边缘平台、工业互联网平台、工业软件、工业数据库等的安全配置，建立系统与设备配置清单，定期进行配置审计。

b) 对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试。

c) 密切关注重大安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需

对补丁进行严格的安全评估和测试验证。

d) 分离工业控制系统等的开发测试和生产环境，以及工业互联网平台等的开发测试和运行环境。

e) 对工业控制网络安全区域之间及工业控制网络与企业网或互联网之间的边界进行安全防护。禁止没有防护的工业控制网络与互联网连接。

f) 对关键设备、系统和平台的访问进行多因素认证。

g) 合理分类设置账户权限，以最小特权原则分配账户权限。

h) 强化工业控制设备、SCADA 软件、工业通信设备、工业互联网平台、工业软件、工业数据库等的登录账户及口令，避免使用默认口令或弱口令，定期更新口令。

5.6 供应链数据安全管理

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

b) 在选择服务商时，应以合同等方式明确服务商承担的数据安全责任和义务，以合同、协议等方式要求服务商做好数据安全保护工作，防范敏感数据外泄。

c) 应加强合作方管理，对合作方的资质条件、业务合法性、数据安全保护能力等进行评估核实，并以合同、协议等方式，明确数据安全保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。应通过管理或技术手段，对合作方数据使用情况进行监督管理，一旦发现异常及时进行终止，并于合作结束后及时关闭数据接口。

5.7 安全评估

a) 重要数据和核心数据处理者，应自行或委托第三方评估机构，每年至少开展一次安全评估，及时整改风险问题，并向地方工业和信息化主管部门报送评估报告。评估的内容包括但不限于处理的重要数据和核心数据种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施，数据安全管理能力、数据安全防护能力等情况，形成相应的数据安全评估报告，并针对评估发现的重大安全风险，制定整改方案，落实整改措施。

b) 重要数据和核心数据处理者，应在收购或资产剥离、重大流程或系统变更、新业务上线，以及数据迁移、数据出境、数据提供、委托处理等过程前，启动数据安全评估工作，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评估报告。

5.8 日志留存和审计

a) 应对数据收集、存储、使用加工、传输、提供、公开、销毁等环节实施日志留存管理。

b) 日志记录信息应包括执行时间、操作地点、操作人、操作账号、处理方式、授权情况、登录信息等，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 6 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。

e) 应明确数据安全审计的内容，包括但不限于企业内部权限控制、企业数据流动跟踪情况、数据安全事件、数据安全防护措施有效性等。

f) 应定期开展数据安全审计，记录并形成数据安全审计报告，及时整改审计发现的问

题。

5.9 监测预警、信息共享与应急处置

a) 应根据实际情况建设数据安全风险监测预警能力，面向工业控制系统、工业交换机、工业数据服务器、工业网络边界、工业软件、工业数据库、工业云平台等开展数据安全风险监测，对数据泄露、违规传输、流量异常等安全风险及安全事件进行监测分析，及时排查安全隐患，采取必要措施防范数据安全风险。
b) 应及时将可能造成较大及以上安全事件的或涉及重要数据和核心数据的安全风险向地方工业和信息化主管部门报告。
c) 应制定数据安全事件应急预案，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。
d) 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，涉及重要数据和核心数据的安全事件，应第一时间向地方工业和信息化主管部门报告。对可能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。
e) 事件处置完成后，应在规定期限内形成总结报告，每年向地方工业和信息化主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 数据全生命周期安全保护要求

6.1 一般数据全生命周期安全保护

6.1.1 数据收集安全

a) 应当遵循“合法正当、目的明确、最小够用”的原则开展数据收集，不得窃取或者以其他非法方式收集数据。
b) 数据收集过程中，应加强对收集人员、设备的管理。

6.1.2 数据存储安全

a) 对确需加密的数据，可采用加密技术、数字签名、校验等技术，实现存储数据的保密性、不可抵赖性和完整性。
b) 应依据法律规定或与用户约定的方式和期限存储数据，并根据实际情况开展数据备份。

6.1.3 数据使用加工安全

a) 利用数据进行自动化决策的，应保证决策的透明度和结果公平合理。
b) 应对数据挖掘、关联分析等数据使用行为进行记录。

6.1.4 数据传输安全

应根据实际需求，可采用密码技术、数据脱敏、校验技术、安全传输通道或者安全传输协议等措施保证数据传输安全。

6.1.5 数据提供安全

应明确数据提供的范围、数量、条件、程序等，并与数据获取方签订数据安全协议。

6.1.6 数据公开安全

应在数据公开前对数据公开的必要性、范围、规模、方式等进行分析研判，研判结果为可以公开的，应根据数据特点、应用场景等采取合适方法对数据进行必要的脱敏处理，确保数据公开安全。

6.1.7 数据销毁安全

应明确数据销毁对象、规则、流程技术等要求，对销毁活动进行记录和留存。

6.1.8 数据出境安全

应结合实际开展数据出境安全自评估和安全管理。

6.1.9 数据转移安全

应明确数据转移方案，并通过电话、短信、邮件、公告等方式通知受影响用户。

6.1.10 数据委托处理安全

应通过签订合同协议等方式，明确数据安全保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，对合作方数据使用情况进行监督管理。

6.2 重要数据全生命周期安全保护

6.2.1 数据收集安全

在6.1.1的基础上还应满足以下要求：

a) 数据收集前，应根据业务需求，明确收集来源、目的、方式、数量、精度、频率、周期、范围、用途等规则。
b) 数据收集前，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) 应对数据收集的时间、范围、类型、数量、频度、流向、级别等信息进行记录和审计，避免出现超范围数据收集活动。
d) 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。
e) 通过间接途径获取数据的，应与数据提供方通过签署相关协议、数据源合法性书面承诺等方式，明确双方法律责任。

6.2.2 数据存储安全

在6.1.2的基础上还应满足以下要求：

a) 应对存储数据的使用进行身份鉴别和访问控制。
b) 应采用存储介质安全管控、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。
c) 应能够检测到数据在存储过程中保密性、完整性、可用性受到破坏，在数据受到破坏时，应向授权用户提供告警信息。
d) 应加强数据备份管理，增加备份冗余度和备份介质的种类。
e) 应定期进行数据恢复演练，全量数据备份至少每周一次，增量数据备份至少每天一次，确保能够及时、完整、准确地恢复数据。

6.2.3 数据使用加工安全

在6.1.3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。

b) 应避免将挖掘算法产生的中间过程数据与原始数据存储于同一逻辑空间。
c) 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，并周期性的检查用户操作数据的情况，统一管理数据使用权限。
d) 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。
e) 应对数据挖掘、关联分析等数据使用行为的时间、范围、数量、级别、行为等信息进行记录和审计。
f) 应对原始数据和挖掘结果进行标识，防止数据被恶意删除、篡改、滥用。
g) 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。

6.2.4 数据传输安全

在6.1.4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) 应在数据导入导出过程中配备安全技术手段，防止在数据导入导出过程中发生数据的可用性和完整性遭到破坏，降低可能存在的数据泄露等风险。

6.2.5 数据提供安全

在6.1.5的基础上还应满足以下要求：
a) 应具备数据提供安全监控技术能力，确保提供的数据合理规范使用，未超出授权范围。
b) 应在数据上云等活动中开展数据安全监测。
c) 应对数据获取方的数据安全保护能力进行评估或核实，并根据评估情况采取相应的保护措施，确保数据提供过程安全。
d) 在数据提供过程中，采取必要的保护措施，包括但不限于数据脱敏、数据标注、数据水印等技术手段。

6.2.6 数据公开安全

在6.1.6的基础上还应满足以下要求：

研判结果为可以公开的重要数据，应根据实际情况，采取数据脱敏、数据水印等必要措施保证数据公开安全。

6.2.7 数据销毁安全

在6.1.7的基础上还应满足以下要求：
a) 应设置数据销毁相关监督人员，对销毁过程进行监督等。
b) 应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，原则上不得以任何理由、任何方式对销毁数据进行恢复。
c) 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。
d) 应及时向地方工业和信息化主管部门更新重要数据目录备案。

6.2.8 数据出境安全

在6.1.8的基础上还应满足以下要求：

a) 确需出境的，应依法依规进行数据出境安全评估。

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。

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。

6.2.9 数据转移安全

在6.1.9的基础上还应满足以下要求：

应及时向地方工业和信息化主管部门更新备案。

6.2.10 数据委托处理安全

在6.1.10的基础上还应满足以下要求：

应对被委托方的数据安全保护能力、资质进行评估或核实。

6.3 核心数据全生命周期安全保护

6.3.1 跨主体处理数据

a) 跨主体提供、转移、委托处理核心数据的，应事先向地方工业和信息化主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跨主体传输、提供、转移、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。

6.3.2 数据收集安全

在6.2.1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。

6.3.3 数据存储安全

在6.2.2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。

6.3.4 数据使用加工安全

在6.2.3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、分析等行为可溯源。

6.3.5 数据传输安全

在6.2.4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。

6.3.6 数据提供安全

在6.2.5的基础上还应满足以下要求：
提供核心数据应事先向地方工业和信息化主管部门提出审批申请。

6.3.7 数据公开安全

在6.2.6的基础上还应满足以下要求：
原则上不允许公开。

6.3.8 数据销毁安全

在6.2.7的基础上还应满足以下要求：
应及时向地方工业和信息化主管部门更新核心数据目录备案。

6.3.9 数据出境安全

在6.2.8的基础上还应满足以下要求：
核心数据出境应事先向地方工业和信息化主管部门提出审批申请。

6.3.10 数据转移安全

在 6.2.9 的基础上还应满足以下要求：
核心数据转移应事先向地方工业和信息化主管部门提出审批申请。

6.3.11 数据委托处理安全

在6.2.10的基础上还应满足以下要求：
核心数据委托处理应事先向地方工业和信息化主管部门提出审批申请。