TC260-PG-2026NA

网络安全标准实践指南

——工业企业数据安全能力成熟度模型

（征求意见稿 v1.0-202601）

全国网络安全标准化技术委员会秘书处

2026 年 1 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国网络安全标准化技术委员会
National Technical Committee 260 on Cybersecurity of SAC

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国网络安全标准化技术委员会（以下简称“网安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

本文件起草单位：

本文件主要起草人：

声　明

本《实践指南》版权属于网安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国网络安全标准化技术委员会秘书处”。

摘　要

本实践指南旨在贯彻落实《数据安全法》《网络数据安全管理条例》《工业和信息化领域数据安全管理办法（试行）》中相关要求，引导工业企业逐级提升数据安全能力成熟度水平，支撑主管部门全面了解掌握工业领域数据安全总体态势，带动数据安全技术、产品和服务在工业企业的落地应用。

本实践指南研究提出了工业企业数据安全能力成熟度模型，并结合国际电工委员会面向工业企业提出的通用模型，构建了典型工业企业数据安全风险参考框架，涵盖L0现场设备层、L1现场控制层、L2过程监控层、L3生产管理层和L4企业管理层5个层级，列举了20余类常见工业企业数据，分析了工业企业主要数据流向，并梳理了10余类常见数据安全风险问题，为技术条款编制提供工业企业数据安全事实依据。本实践指南提出了工业企业数据全生命周期安全和通用安全的成熟度等级要求，以及能力成熟度等级评估方法。本实践指南适用于指导工业企业开展数据安全能力建设，以及对工业企业数据安全能力成熟度等级进行评估。

目　录

1 范围

本文件提出了工业企业数据安全能力成熟度模型，给出了工业企业数据安全能力成熟度等级评估方法。

本文件适用于指导工业企业开展数据安全能力建设，以及对工业企业数据安全能力成熟度等级进行评估。

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 29246—2023 信息安全技术 信息安全管理体系 概述和词汇

GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型

YD/T 4982—2024 工业企业数据安全防护要求

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

GB/T 25069—2022、GB/T 32919—2016、GB/T 36323—2018、GB/T 41400—2022、YD/T 4982—2024 和 GB/T 37988—2019 界定的以及下列术语和定义适用于本文件。

3.1

工业控制系统 industrial control system

由各种自动化控制组件以及对实时数据进行收集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。

注：工业控制系统包括监控和数据采集（SCADA）系统、分布式控制系统（DCS）和其他较小的控制系统，如可编程逻辑控制器（PLC）等。

[来源：GB/T 41400—2022，3.1]

3.2

数据安全能力 data security capability

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

[来源：GB/T 37988—2016，3.5]

3.3

能力成熟度 capability maturity

对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

[来源：GB/T 37988—2019，3.6]

3.4

能力成熟度模型 capability maturity model

对一个组织的能力成熟度进行度量的模型，包括一系列代表能力和进展的特征、属性、指示或者模式。

注：能力成熟度模型为组织衡量其当前的实践、流程、方法的能力水平提供参考基准，并设置明确的提升目标。

[来源：GB/T 37988—2019，3.7]

3.5

过程域 process area

实现同一安全目标的相关工业企业数据安全基础实践的集合。

注：一个过程域中包含一个或多个基本实践。

3.6

基础实践 base practice

实现某一安全目标的工业企业数据安全防护相关活动。

3.7

工业企业数据 industrial enterprises data

工业企业数据是指各行业各领域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、收集、存储、使用、加工、传输、提供、公开、销毁的数据。

注：工业企业数据包含生产监测、工业控制、工艺参数、排产计划等数据。

4 缩略语

下列缩略语适用于本文件。

BP：基础实践（Base Practice）

DCS：分布式控制系统（Distributed Control System）

FTP：文件传输协议（File Transfer Protocol）

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

OLE：对象连接与嵌入（Object Linking and Embedding）

OPC：用于过程控制的 OLE（OLE for Process Control）

PA：过程域（Process Area）

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

RTU：远程终端单元（Remote Terminal Unit）

SCADA：监控和数据收集（Supervisory Control And Data Acquisition）

SQL: 结构化查询语言（Structured Query Language）
UPS: 不间断电源（Uninterruptible Power Supply）
USB: 通用串行总线（Universal Serial Bus）
VPN: 虚拟专用网络（Virtual Private Network）

5 工业企业数据安全能力成熟度模型

5.1 能力成熟度模型

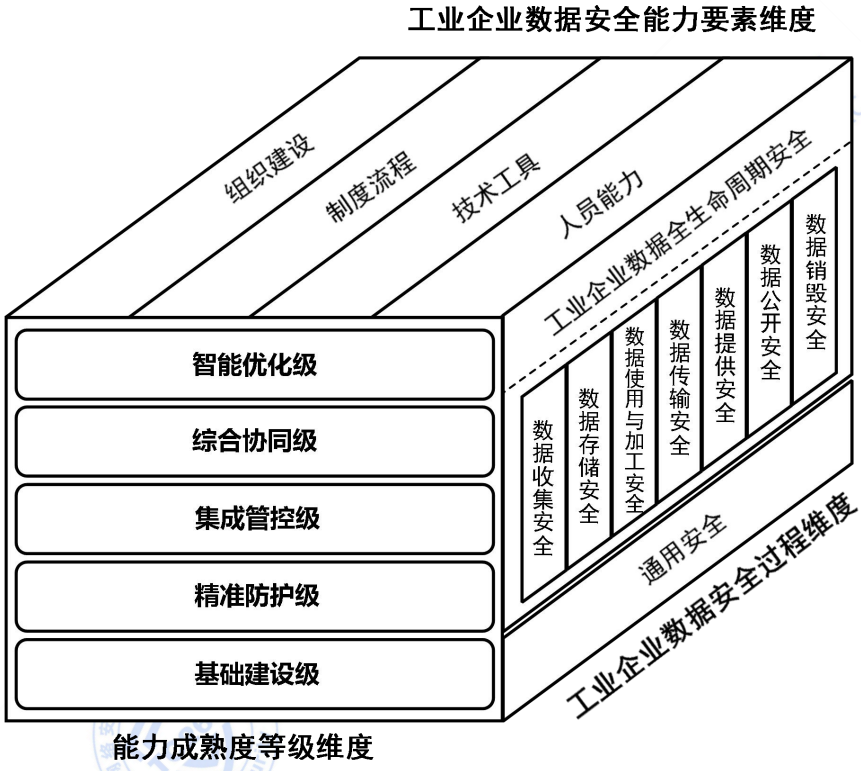

图 1 工业企业数据安全能力成熟度模型

工业企业数据安全能力成熟度模型的架构由以下三个维度构成。

a) 工业企业数据安全能力要素维度
组织工业企业数据安全能力要素包括组织建设、制度流程、技术工具和人员能力。

b) 能力成熟度等级维度
组织工业企业数据安全能力成熟度等级划分为五级，由低至高分别为基础建设级、精准防护级、集成管控级、综合协同级和智能优化级。

c) 工业企业数据安全过程维度
组织工业企业数据安全能力建设过程包括工业企业数据全生命周期安全和通用安全：
1) 工业企业数据全生命周期安全包括：工业企业数据收集安全、数据存储安全、数

据使用与加工安全、数据传输安全、数据提供安全、数据公开安全、数据销毁安全7个过程类；

2)通用安全包括：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、数据供应链安全、数据分类分级、安全风险评估、日志留存、监控与安全审计、监测预警、信息共享与应急处置、数据出境12个过程类。

5.2 能力要素维度

5.2.1 能力构成

通过对组织工业企业数据安全防护过程应具备安全能力的量化，进而评估每项安全过程的实现能力。组织工业企业数据安全能力要素包括：

a) 组织建设：工业企业数据安全机构的设立、职责分配和沟通协作；
b) 制度流程：组织工业企业数据安全领域相关制度制定和流程执行；
c) 技术工具：通过技术手段和产品工具落实安全要求或自动化实现安全工作；
d) 人员能力：执行工业企业数据安全防护工作的人员的安全意识及相关专业能力。

5.2.2 组织建设

从承担工业企业数据安全防护工作的组织应具备的组织建设能力角度，根据以下方面进行能力等级区分：

a) 工业企业数据安全架构对组织业务的适用性；
b) 工业企业数据安全机构承担的工作职责的明确性；
c) 工业企业数据安全机构运作、沟通协调的有效性。

5.2.3 制度流程

从组织工业企业数据安全防护制度流程的建设以及执行情况角度，根据以下方面进行能力等级区分：

a) 工业企业数据安全关键节点授权审批流程的明确性；
b) 相关制度流程的制定、发布、修订的规范性；
c) 制度流程实施的一致性和有效性。

5.2.4 技术工具

从组织用于开展工业企业数据安全防护工作的安全技术、应用系统和工具角度，根据以下方面进行能力等级区分：

a) 工业企业数据安全防护技术在工业企业中的利用情况，针对数据安全风险的应对能力；
b) 利用技术工具对工业企业数据安全防护工作的自动化支持能力，对工业企业数据安全防护制度流程固化执行的实现能力。

5.2.5 人员能力

从组织承担工业企业数据安全防护工作的人员应具备的能力角度，根据以下方面进行能力等级区分：

a) 工业企业数据安全人员所具备的安全技能是否能够满足复合型能力要求(对工业企业数据相关业务的理解程度以及工业企业数据安全专业能力)；

b) 工业企业数据安全人员的安全意识以及对关键工业企业数据安全岗位员工安全能力的培养。

5.3 能力成熟度等级维度

组织工业企业数据安全能力成熟度等级共分为 5 级，见图 2。

图 2 工业企业数据安全能力成熟度等级

根据组织开展安全防护的能力分为 5 个能力成熟度等级，自低向高分别是基础建设级、精准防护级、集成管控级、综合协同级、智能优化级。各能力成熟度等级的特征描述如下：

a) **基础建设级：**
组织建立并记录工业企业数据安全能力建设工作，能够制定规范化安全防护制度、规章，使得组织能够以重复的方式执行，采用适当的安全防护技术手段开展企业数据资产保护工作。

b) **精准防护级：**
组织能够在建章立制基础上，采用数字化装备、信息技术手段等，有针对性地开展安全防护，面向各方面形成独立、可复制的安全能力，初步形成数据安全能力提升自驱力。

c) **集成管控级：**
组织能够在已有工作基础上，通过集成化工具、系统等，对相对独立的单点防护设备进行集中统一管控，同时整合相关防护规章制度文件，形成体系化制度，实现组织内部工业企业数据安全的集中管理、统一控制的安全能力。

d) **综合协同级：**
组织能够面向不同产线、厂区、工厂及产业链上下游相关单位，统筹考虑数据安全风险和需求，开展安全防护建设，建立多级协同的安全管理体系，并通过态势感知、统一管控等技术手段实现综合决策、协同防护的安全能力。

e) **智能优化级：**
组织能够采用人工智能、主动防御、内生安全等先进技术，与已有安全防护设备、系统、制度体系深度融合，通过知识学习、智能建模分析等技术，构建可智能化演进的安全防护系统，形成具有自决策、自进化能力的安全防护体系。

5.4 过程维度

5.4.1 PA 体系

PA 体系分为工业企业数据全生命周期安全过程域和工业企业通用安全过程域两部分，共包含 31 个 PA，见图 3。

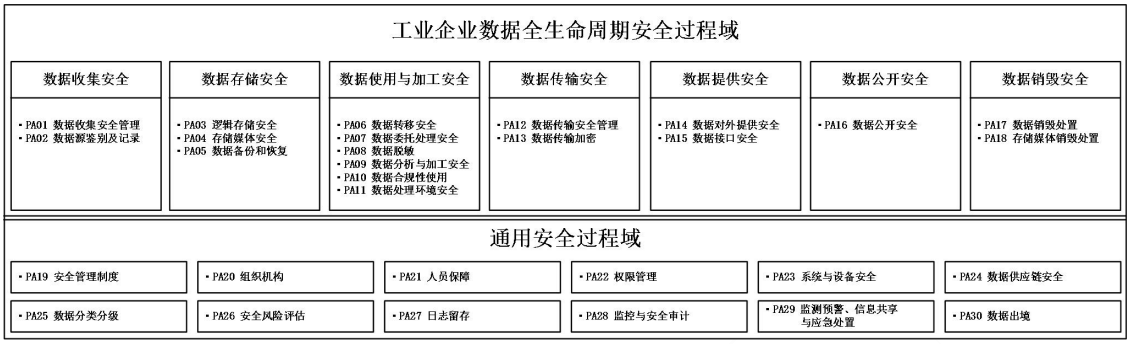

图 3 工业企业数据安全 PA 体系

工业企业数据全生命周期安全包括以下 7 个过程类：

a) 数据收集安全的 PA（PA01-PA02）包括：数据收集安全管理、数据源鉴别及记录 2 个 PA；

b) 数据存储安全的 PA（PA03-PA05）包括：逻辑存储安全、存储媒体安全、数据备份和恢复 3 个 PA；

c) 数据使用与加工安全的 PA（PA06-PA11）包括：数据转换安全、数据委托处理安全、数据脱敏、数据分析与加工安全、数据合规性使用、数据处理环境安全 6 个 PA；

d) 数据传输安全的 PA（PA12-PA13）包括：数据传输安全管理、数据传输加密 2 个 PA；

e) 数据提供安全的 PA（PA14-PA15）包括：数据对外提供安全、数据接口安全 2 个 PA；

f) 数据公开安全的 PA（PA16）包括：数据公开安全 1 个 PA；

g) 数据销毁安全的 PA（PA17-PA18）包括：数据销毁处置、存储媒体销毁处置 2 个 PA。

通用安全包括以下 12 个过程类：

h）通用安全过程域的 PA（PA19-PA30）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、数据供应链安全、数据分类分级、安全风险评估、日志留存、监控与安全审计、监测预警、信息共享与应急处置、数据出境 12 个 PA。

5.4.2 编码规则

工业企业数据安全防护 PA 编码规则如下：

a) 每个 PA 有对应的编号，分别采用递增的数值 01，02，…，表示；

b) 每个 PA 由若干 BP 组成，BP 用 BP.XX.XX 进行编号，第一组编码表示所在 PA 的序号，第二组编码表示具体 BP 的序号，具体 BP 的序号采用递增的数值 01，02，…，表示；

c) 对于每个 PA 的每个级别，组织需同时实现该级别和所有低于该级别的 BP，才能达到该级别的能力水平。

5.4.3 关系描述

能力成熟度等级与 PA、BP、能力要素的关系如下：

a) 组织在每个 PA 的能力成熟度划分为 5 级，对每个等级下组织应具备的能力要求，结合附录 A 中典型工业企业数据安全风险参考框架梳理的数据类型、数据流向和安

全风险，从 4 个能力要素提出具体的 BP;

b) 并非每个 PA 的能力成熟度等级都包含完整的 4 个能力要素;

c) **对于每个 PA，高等级的能力要求应不低于所有低等级能力要求;**

d) 在确定目标成熟度等级的前提下，组织机构根据数据全生命周期所覆盖的业务场景挑选适用于组织机构的数据安全 PA 和 BP;

e) **工业企业数据安全能力成熟度等级判定规则详见附录 B;**

f) 工业企业数据安全基线要求映射说明详见附录 C。

注：针对某一具体 PA，如某级的能力要求中未涉及某一能力要素的内容，则默认应实现在较低级的能力要求中该能力要素的内容。

6 全生命周期安全能力成熟度评估

6.1 数据收集安全

6.1.1 PA01 数据收集安全管理

6.1.1.1 PA 描述

在收集数据的过程中，组织应明确收集数据的目的和用途，确保满足数据源的真实性、有效性和最少够用等原则要求，并明确数据收集渠道、规范数据格式以及相关的流程和方式，从而保证数据收集的合规性、正当性、一致性。

6.1.1.2 等级描述

6.1.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程:

1) 应遵循合法、正当的原则收集数据，不得窃取或者以其他非法方式收集数据（BP.01.01）;

2) 在开展数据收集时，宜采用人工核查或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（BP.01.02）。

6.1.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程：涉及个人信息收集的（主要涉及 L3、L4 层），应明确收集的目的、方式和范围，并经被收集者同意（BP.01.03）。

6.1.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 制度流程:

1) 应加强数据收集人员、设备的管理，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（BP.01.04）;

2) 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（BP.01.05）；

b) 技术工具：

1) 涉及工业通信协议的数据，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、鉴权等安全防护措施，并进行内部审批（BP.01.06）；

2) 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（BP.01.07）；

6.1.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：工业企业核心业务团队应设专人负责工业生产和管理运维等数据（涉及L0至L4各层）的收集安全管理（BP.01.08）；

6.1.1.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：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，并采用技术手段实现所有收集行为可溯源（BP.01.09）。

6.1.1.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1) 应依据工业企业数据收集流程建设工业生产和管理运营数据（涉及L0至L4各层）收集相关的工具，以保证组织数据收集流程实现的一致性，同时WMS、MES、ERP等相关系统应具备详细的日志记录功能，确保数据收集授权过程的完整记录（BP.01.10）；

2) 应采取技术手段保证数据收集过程中工业企业重要数据（涉及L0至L4各层）不被泄露（BP.01.11）。

6.1.1.2.7 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应明确工业企业数据收集安全管理效果的评估方式（涉及L0至L4各层），如数据收集安全管理在业务的覆盖率、制度流程执行效果、数据收集授权率等（BP.01.12）。

b) 技术工具：应采取必要的技术手段对收集的工业企业数据（涉及L0至L4各层）进行校验（BP.01.13）。

6.1.1.2.8 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：工业企业数据收集安全管理应持续优化（涉及L0至L4各层），持续跟踪数据收集安全管理执行效果、新业务产生的需求、行业新技术和最佳实践、合规新要求新变化等（BP.01.14）。

b) 技术工具：应根据制度流程的更新，应用人工智能等前沿技术（主要涉及L3、L4各层）不断升级优化工业企业数据收集工具（BP.01.15）；

6.1.2 PA02 数据源鉴别及记录

6.1.2.1 PA 描述

对产生数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造。

6.1.2.2 等级描述

6.1.2.2.1 基础建设级——一般增强要求

该等级的数据安全能力要求描述如下：

制度流程：工业生产等相关核心业务系统的在线数据收集和外部第三方收集（主要涉及L2、L3、L4层），均应建立了相应机制执行数据源的鉴别和记录（BP.02.01）；

6.1.2.2.2 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由工业生产、管理运维等业务团队相关人员负责数据源（涉及L0至L4各层）鉴别和记录（BP.02.02）；
b) 技术工具：应具有技术工具支持对工业生产和管理运营数据源（涉及L0至L4各层）的鉴别和记录（BP.02.03）。

6.1.2.2.3 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 技术工具：
   1) 组织应采取技术手段对外部收集的数据和数据源（主要涉及L3、L4层）进行识别和记录（BP.02.04）；
   2) 应对关键追溯数据进行备份（涉及L0至L4各层），并采取技术手段对追溯数据进行安全保护（BP.02.05）。
b) 人员能力：负责该项工作的人员应理解数据源（涉及L0至L4各层）鉴别标准和组织内部数据收集的业务，能够结合实际情况执行（BP.02.06）。

6.1.2.2.4 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
   1) 组织应定义了工业生产和管理运营数据追溯策略要求、追溯数据格式、追溯数据安全存储与使用的管理制度等（涉及L0至L4各层）。根据组织内的业务梳理数据源的类型，并明确在数据管理系统中对数据源类型标记的要求（BP.02.07）；
   2) 应明确基于追溯数据的数据业务与法律法规合规性审核的机制（涉及L0至L4各层），并依据审核结果增强或改进与数据服务相关的访问控制与合规性保障机制和策略（BP.02.08）。
b) 技术工具：组织关键的数据管理系统中应提供了标记工业生产和管理运营数据的数据源类型的功能（涉及L0至L4各层），从而实现对组织内部各类数据源的统计和分析（BP.02.09）。

6.1.2.2.5 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应对数据源鉴别方式和分类方法进行持续的改进（涉及 L0 至 L4 各层），基于业务的发展变化以及行业最佳实践，提升数据源管理的成效（BP.02.10）。

b) 技术工具：应使用人工智能等前沿技术（主要涉及 L3、L4 层）面向制度流程的更新持续改进工具在工业生产和管理运营数据鉴别、记录和追溯等方面的服务能力（BP.02.11）；

6.2 数据存储安全

6.2.1 PA03 逻辑存储安全

6.2.1.1 PA 描述

基于组织内部的业务特性和数据存储安全要求，建立针对数据逻辑存储、存储容器等对象的有效安全控制。

6.2.1.2 等级描述

6.2.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

a) 制度流程：应按照法律、行政法规规定和用户约定的方式、期限进行数据存储（BP.03.01）。

b) 技术工具：

1) 对于非联网独立控制单元，例如传感、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，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（BP.03.02）；

2) 应对存储数据的使用进行身份鉴别和访问控制（BP.03.03）。

6.2.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应明确工业生产和管理运营数据的存储管理安全规范和配置规则（主要涉及 L2、L3、L4层），确立数据存储系统在权限管理、访问控制、日志管理、加密管理、版本升级等方面的要求，并予以实施（BP.03.04）。

6.2.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：在中华人民共和国境内收集和产生的重要数据，法律、行政法规有境内存储要求的，应当在境内存储（BP.03.05）。

b) 技术工具：

1) 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（BP.03.06）；

2) 应能够监测到数据在存储过程中机密性、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（BP.03.07）。

6.2.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应设立负责工业生产和管理运营数据存储的（主要涉及L2、L3、L4层）一体化安全管理岗位，岗位人员负责明确数据存储系统一体化安全管理要求，并推进相关要求的实施（BP.03.08）。

b) 制度流程：应明确工业生产和管理运营数据的存储隔离授权与操作要求（主要涉及L2、L3、L4层），实现多用户数据存储隔离（BP.03.09）。

c) 技术工具：应配备工业生产和管理运营数据存储系统安全配置扫描工具（主要涉及L2、L3、L4层），并定期进行扫描（BP.03.10）。

d) 人员能力：负责该项工作的人员应熟悉工业生产和管理运营数据存储系统架构（主要涉及L2、L3、L4层）（BP.03.11）。

6.2.1.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：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，并采用技术手段实现所有存储操作行为可溯源（BP.03.12）。

6.2.1.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 技术工具：应配备一体化数据存储系统安全配置管理工具，实现对工业生产和管理运营数据存储系统安全配置情况的一体化管理和控制（主要涉及L2、L3、L4层）（BP.03.13）。

b) 人员能力：该项工作负责人员应具备分析数据存储安全风险的专业能力，能够针对各类存储系统自行采取有效的安全防护措施（BP.03.14）。

6.2.1.2.7 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应明确工业生产和管理运营数据的分片和分布式存储安全规则（主要涉及L2、L3、L4层），如数据存储完整性规则、多副本一致性管理规则、存储转移安全规则等，以满足分布式存储下分片数据完整性、一致性和保密性安全要求（BP.03.15）。

b) 技术工具：应针对工业生产和管理运营数据建立可伸缩存储架构（主要涉及L2、L3、L4层），实现存储动态调整功能（BP.03.16）。

6.2.1.2.8 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应使用人工智能等前沿技术定期审核实时数据库、历史数据库等数据库系统的安全配置情况和权限分配情况（主要涉及L2、L3、L4层），并改进优化相关配置和角色权限（BP.03.17）。

6.2.2 PA04 存储媒体安全

6.2.2.1 PA 描述

针对组织内需要对数据存储媒体进行访问和使用的场景，提供有效的技术和管理手段，

防止对媒体的不当使用而可能引发的数据泄露风险。存储媒体包括终端设备及网络存储。

6.2.2.2 等级描述

6.2.1.2.1 基础建设级——一般增强要求

该等级的数据安全能力要求描述如下:

制度流程: 业务团队应明确工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)使用,购买、标记的安全制度(BP.04.01)。

6.2.1.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上,该等级还应满足的数据安全能力要求描述如下:

制度流程: 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,并对介质进行分类和标识管理,根据存档目录清单,定期盘点(BP.04.02)。

6.2.1.2.3 精准防护级—重要增强要求

在满足前序级别要求的基础上,该等级还应满足的数据安全能力要求描述如下:

a) 组织建设:应由业务团队相关人员根据工业企业实际业务需求负责执行工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)安全管理工作(BP.04.03)。
b) 人员能力:业务团队中负责相关工作的人员,应熟悉工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)安全管理的相关制度要求(BP.04.04)。

6.2.1.2.4 集成管控级—核心增强要求

在满足前序级别要求的基础上,该等级还应满足的数据安全能力要求描述如下:

a) 组织建设:组织应设立统一负责工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)安全管理的岗位和人员(BP.04.05)。
b) 制度流程:
   1) 应明确工业生产和管理运营数据存储媒体访问和使用的安全管理规范,建立存储媒体(主要涉及 L2、L3、L4 层)使用的审批和记录流程(BP.04.06);
   2) 应明确购买或获取工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)的流程,要求通过可信渠道购买或获取存储媒体,并针对各类存储媒体建立格式化规程(BP.04.07);
   3) 应建立工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)资产标识,明确存储媒体存储的数据(BP.04.08);
   4) 应对工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)进行常规和随机检查,确保存储媒体的使用符合机构公布的关于存储媒体使用的制度(BP.04.09);
a) 技术工具:
   1) 组织应使用技术工具对工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)性能进行监控,包括存储媒体的使用历史、性能指标、错误或损坏情况,对超过安全值的存储媒体进行预警(BP.04.10);
   2) 应对工业生产和管理运营数据存储媒体(主要涉及 L2、L3、L4 层)访问和使用行为进行记录和审计(BP.04.11)。
b) 人员能力:负责该项工作的人员应熟悉工业生产和管理运营数据存储媒体(主要涉

及 L2、L3、L4 层）安全管理的相关合规要求，熟悉不同存储媒体访问和使用的差异性（BP. 04. 12）。

6. 2. 1. 2. 5 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：应建立工业生产和管理运营数据存储媒体（主要涉及 L2、L3、L4 层）管理系统，确保存储媒体的使用和传递过程得到严密跟踪（BP. 04. 13）。

6. 2. 1. 2. 6 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：应使用人工智能等前沿技术持续更新优化组织的工业生产和管理运营数据存储媒体（主要涉及 L3、L4 层）管理系统和净化工具，以保证存储媒体的安全使用（BP. 04. 14）。

6. 2. 3 PA05 数据备份和恢复

6. 2. 3. 1 PA 描述

通过执行定期的数据备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。

6. 2. 3. 2 等级描述

6. 2. 3. 2. 1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：宜建立数据备份制度，根据需要定期开展数据备份（BP. 05. 01）。

6. 2. 3. 2. 2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：工业生产和管理运维等业务团队应明确数据（主要涉及 L2、L3、L4 层）备份和恢复的制度（BP. 05. 02）；

6. 2. 3. 2. 3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应建立数据容灾备份机制，定期开展数据恢复测试，并对备份进行安全管理，备份数据的防护要求不应低于源数据的防护要求（BP. 05. 03）。

6. 2. 3. 2. 4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：工业生产和管理运维等业务团队应明确负责数据（主要涉及 L2、L3、L4 层）备份和恢复的岗位和人员（BP. 05. 04）。

b) 技术工具：应建立工业生产和管理运维数据（主要涉及 L2、L3、L4 层）备份与恢复的技术工具（BP. 05. 05）。

6. 2. 3. 2. 4 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：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（BP.05.06）。

6.2.3.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应明确负责组织统一的工业生产和管理运维数据（主要涉及L2、L3、L4层）备份和恢复管理工作的岗位和人员，负责建立相应的制度流程并部署相关的安全措施（BP.05.07）。

b) 制度流程：

1) 应明确工业生产和管理运维数据（主要涉及L2、L3、L4层）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（BP.05.08）；

2) 应明确工业生产和管理运维数据（主要涉及L2、L3、L4层）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（BP.05.09）；

3) 应明确工业生产和管理运维数据（主要涉及L2、L3、L4层）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，（BP.05.10）；

4) 应依据工业生产和管理运维数据（主要涉及L2、L3、L4层）全生命周期和业务规范，建立数据全生命周期各阶段数据归档的操作流程（BP.05.11）；

5) 应明确归档工业生产和管理运维数据（主要涉及L2、L3、L4层）的压缩或加密要求（BP.05.12）；

6) 应明确归档工业生产和管理运维数据（主要涉及L2、L3、L4层）的安全管控措施，非授权用户不能访问归档数据（BP.05.13）；

7) 应识别组织适用的合规要求，按监管部门的要求对相关工业生产和管理运维数据（主要涉及L2、L3、L4层）予以记录和保存（BP.05.14）；

8) 应明确工业生产和管理运维数据（主要涉及L2、L3、L4层）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（BP.05.15）；

9) 应明确工业生产和管理运维过期存储数据（主要涉及L2、L3、L4层）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（BP.05.16）；

c) 技术工具：

1) 应建立工业生产和管理运维数据（主要涉及L2、L3、L4层）备份与恢复的统一技术工具，保证相关工作的自动执行（BP.05.17）；

2) 应建立工业生产和管理运维备份和归档数据安全（主要涉及L2、L3、L4层）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（BP.05.18）；

3) 应定期采取必要的技术措施查验工业生产和管理运维备份和归档数据（主要涉及L2、L3、L4层）完整性和可用性（BP.05.19）；

4) 应建立工业生产和管理运维过期存储数据（主要涉及L2、L3、L4层）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（BP.05.20）；

5) 应通过风险提示和技术手段避免非过期工业生产和管理运维数据（主要涉及L2、L3、L4层）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（BP.05.21）；
6) 应确保存储架构具备数据存储跨机柜或跨机房容错部署（主要涉及L2、L3、L4层）能力（BP.05.22）。

d) 人员能力：
1) 负责该项工作的人员应了解工业生产和管理运维数据（主要涉及L2、L3、L4层）备份媒体的性能和相关数据的业务特性，能够确定有效的数据备份和恢复机制（BP.05.23）；
2) 负责该项工作的人员应了解工业生产和管理运维数据（主要涉及L2、L3、L4层）存储时效性相关的合规性要求，并具备基于业务对合规要求的解读能力和实施能力（BP.05.24）。

6.2.3.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
1) 应明确工业生产和管理运维数据（主要涉及L2、L3、L4层）冗余强一致性、弱一致性等控制要求，以满足不同一致性水平需求的数据副本多样性和多变性存储管理要求（BP.05.25）；
2) 应对组织内工业生产和管理运维数据（主要涉及L2、L3、L4层）备份的场景、数量、频率进行了定期的统计，了解组织内部数据备份工作的开展情况（BP.05.26）。

b) 技术工具：
1) 应建立在线/离线的多级工业生产和管理运维数据（主要涉及L2、L3、L4层）归档方式，支持海量数据的有效归档、恢复和使用（BP.05.27）；
2) 应为不同时效性的工业生产和管理运维数据（主要涉及L2、L3、L4层）建立分层的数据存储方法，具备按时效性自动迁移数据分层存储的能力（BP.05.28）；
3) 应具备工业生产和管理运维数据（主要涉及L2、L3、L4层）副本或数据备份存储的多种压缩策略和实现技术，确保压缩数据副本或数据备份的完整性和可用性（BP.05.29）；
4) 存储系统应具备工业生产和管理运维数据（主要涉及L2、L3、L4层）存储跨地域的容灾能力（BP.05.30）；
5) 应通过工具对需要符合数据存储合规要求的数据（主要涉及L2、L3、L4层）进行标识（BP.05.31）；
6) 应具备工业生产和管理运维数据（主要涉及L2、L3、L4层）时效性自动检测能力，包括但不限于告警、自动删除和拒绝访问等，以保证数据的及时删除、更新和有效性（BP.05.32）。

6.2.3.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应密切关注国内外数据备份和恢复的优秀解决方案，使用人工智能等前沿技术生成适用于本组织的解决方案并用于组织内部的数据（主要涉及L3、L4层）备份和恢复工作（BP.05.33）。

6.3 数据使用加工安全

6.3.1 PA06 数据转移安全

6.3.1.1 PA 描述

通过对数据转移过程中对数据的安全性进行管理，防止数据转移过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的数据泄露风险。

6.3.1.2 等级描述

6.3.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

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（BP.06.01）。

6.3.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

应明确工业生产等核心业务数据导入导出安全制度或审批流程（BP. 06.02）；

6.3.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：数据转移后，涉及重要数据目录备案内容发生变化的，应当履行备案变更手续（BP.06.03）。

6.3.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由业务团队相关人员负责对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的数据导入导出执行安全管理（BP.06.04）。

b) 人员能力：负责数据导入导出的人员应具备对数据导入导出业务的理解能力，掌握数据导入导出规程，并能够针对生产现场监控、仓储管理等具体场景提出有效的解决方案（BP.06.05）。

c) 技术工具：应记录组织内部的数据导入导出行为，确保生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的数据导入导出行为追溯（BP.06.06）。

6.3.1.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
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（BP.06.07）。

b) 技术工具：
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，实现数据活动的操作行为、传输路径可溯源，并实现溯源数据的真实性和保密性（BP.06.08）。

6.3.1.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应针对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层），设立统一的数据导入导出安全管理岗位和人员，负责制定规则和提供技术能力，并推动在组织内业务落地执行（BP.06.09）。

b) 制度流程：
1) 应依据数据分类分级要求建立符合工业生产、管理运营等业务规则的数据导入导出安全策略，如授权策略、流程控制策略、不一致处理策略等（BP.06.10）；
2) 应明确生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）导出安全评估和授权审批流程，评估数据导出的安全风险，并对大量或敏感数据导出进行授权审批（BP.06.11）；
3) 导出生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）时，如采用存储媒体导出数据，应建立针对导出存储媒体的标识规范，明确存储媒体的命名规则、标识属性等重要信息，定期验证导出数据的完整性和可用性（BP.06.12）；
4) 应针对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）制定导入导出审计策略和日志管理规程，并保存导入导出过程中的出错数据处理记录（BP.06.13）；

c) 技术工具：
1) 应记录并定期审计组织内部的工业数据导入导出行为，确保未超出数据授权使用范围（BP.06.14）；
2) 应对工业数据导入导出终端设备、用户或服务组件执行有效的访问控制，实现对其身份的真实性和合法性的保证（BP.06.15）；
3) 在导入导出完成后应对工业数据导入导出通道缓存的数据进行删除，以保证导入导出过程中涉及的数据不会被恢复（BP.06.16）。

d) 人员能力：负责数据导入导出安全工作的人员应能够充分理解组织的生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出规程，并根据数据导入导出的业务执行相应的风险评估，从而提出实际的解决方案（BP.06.17）。

6.3.1.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1) 应采取多因素鉴别技术对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出操作人员进行身

份鉴别（BP.06.18）；

2) 应为生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出通道提供冗余备份能力（BP.06.19）；

3) 应对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出接口进行流量过载监控（BP.06.20）；

4) 应建立组织统一的生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）导入导出管理系统，提示数据导入导出的安全风险并进行在线审核（BP.06.21）；

5) 应配置规范的生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出机制或服务组件，明确数据导入导出最低安全防护要求（BP.06.22）。

6.3.1.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

组织应及时跟进业务相关的法律法规的更新和产业内的优秀做法，使用人工智能等前沿技术定期评估导入导出服务组件和导入导出通道的安全性，对生产监测、工业控制等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的导入导出的风险控制方案进行持续的优化调整（BP.06.23）；

b) 技术工具：

应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.06.24）；

6.3.2 PA07 数据委托处理安全

6.3.2.1 PA 描述

通过对数据委托处理流程的规范化管理，降低数据被违规使用、篡改或泄露的风险。

6.3.2.2 等级描述

6.3.2.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

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（BP.07.01）。

6.3.2.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应在数据委托处理前，对受托方的数据安全能力、资质进行评估，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（BP.07.02）。

6.3.2.2.3 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

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（BP.07.03）。

b) 技术工具：
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，实现数据活动的操作行为、传输路径可溯源，并实现溯源数据的真实性和保密性（BP.07.04）。

6.3.3 PA08 数据脱敏

6.3.3.1 PA 描述

根据相关法律法规、标准的要求以及业务需求，给出敏感数据的脱敏需求和规则，对敏感数据进行脱敏处理，保证数据可用性和安全性的平衡。

6.3.3.2 等级描述

6.3.3.2.1 基础建设级——一般增强要求

该等级的数据安全能力要求描述如下：
制度流程：在核心业务中，应对业务中涉及的工业生产和管理运维数据（主要涉及 L2、L3、L4 层）脱敏需求进行分析，明确脱敏的流程和方法（BP.08.01）。

6.3.3.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：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（BP.08.02）；

6.3.3.2.3 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由业务团队相关人员负责工业生产和管理运维数据（主要涉及 L2、L3、L4 层）脱敏工作（BP.08.03）。
b) 人员能力：负责该项工作的人员应了解工业生产和管理运维数据（主要涉及 L2、L3、L4 层）脱敏的常用技术，并能够基于数据脱敏的具体场景保证业务和安全之间的需求平衡（BP.08.04）。
c) 技术工具：应通过一定的技术工具（如敏感字段屏蔽等方式），实现对工业生产和管理运维相关核心业务的（主要涉及 L2、L3、L4 层）数据脱敏（BP.08.05）。

6.3.3.2.4 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：
1) 组织应设立统一的工业生产和管理运维数据安全岗位和人员，负责制定数据（主要涉及 L2、L3、L4 层）脱敏的原则和方法，并提供相关技术能力（BP.08.06）；
2) 在数据权限的申请阶段，有相关人员应评估使用真实数据的必要性，以及确定该场景下适用的工业生产和管理运维数据（主要涉及 L2、L3、L4 层）脱敏规则及方法（BP.08.07）。
b) 制度流程：

1) 应明确组织的工业生产和管理运维数据脱敏规范，明确数据（主要涉及 L2、L3、L4 层）脱敏的规则，脱敏方法和使用限制等（BP. 08. 08）；
2) 应明确需要脱敏处理的应用场景、脱敏处理流程、涉及部门及人员的职责（涉及 L0 至 L4 各层）分工（BP. 08. 09）。

c) 技术工具：
1) 组织应提供统一的工业生产和管理运维数据脱敏工具（主要涉及 L2、L3、L4 层），实现数据脱敏工具与数据权限管理系统的联动，以及数据使用前的静态脱敏（BP. 08. 10）；
2) 应提供面向不同数据类型（涉及 L0 至 L4 各层）的脱敏方案，可基于场景需求自定义脱敏规则（BP. 08. 11）；
3) 工业生产和管理运维数据脱敏后应保留原始数据格式和特定属性（涉及 L0 至 L4 各层），满足开发与测试需求（BP. 08. 12）；
4) 应对工业生产和管理运维数据脱敏处理过程相应的操作进行记录（主要涉及 L2、L3、L4 层），以满足数据脱敏处理安全审计要求（BP. 08. 13）。

d) 人员能力：
1) 应熟悉常规的工业生产和管理运维数据（主要涉及 L2、L3、L4 层）脱敏技术，能够分析数据脱敏过程中存在的安全风险，基于数据脱敏的具体场景保证业务和安全之间的需求平衡（BP. 08. 14）；
2) 应具备对工业生产和管理运维数据（涉及 L0 至 L4 各层）脱敏的技术方案定制化的能力，能够基于组织内部各级别的数据建立有效的数据脱敏方案（BP. 08. 15）。

6. 4. 3. 2. 5 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
1) 应明确列出需要脱敏的工业生产和管理运维数据（涉及 L0 至 L4 各层）资产，给出不同分类分级数据的脱敏处理流程（BP. 08. 16）；
2) 应明确脱敏数据（主要涉及 L2、L3、L4 层）治理要求在评估方法等方面反映脱敏治理效果（BP. 08. 17）。

b) 技术工具：
1) 应配置脱敏数据识别和脱敏效果验证服务组件或技术手段（主要涉及 L2、L3、L4 层），确保数据脱敏的有效性和合规性（BP. 08. 18）；
2) 应提供工业生产和管理运维数据脱敏组件或技术手段（主要涉及 L2、L3、L4 层），支持泛化、抑制、假名化等数据脱敏技术（BP. 08. 19）；
3) 应针对特定的数据使用场景和数据脱敏的策略（主要涉及 L2、L3、L4 层），部署数据的动态脱敏方案（BP. 08. 20）。

c) 人员能力：应定期对工业生产和管理运维数据脱敏工作人员（主要涉及 L2、L3、L4 层）的脱敏操作能力进行考核评估（BP. 08. 21）。

6. 4. 3. 2. 6 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1) 应持续跟踪业务新需求、数据脱敏新技术和最佳实践、合规新要求新变化等，

使用人工智能等前沿技术动态调整数据（主要涉及L2、L3、L4层）脱敏规则和手段（BP.08.22）；

2) 应实现对非结构化数据、组合数据的数据（主要涉及L2、L3、L4层）脱敏（BP.08.23）

6.3.4 PA09 数据分析与加工安全

6.3.4.1 PA 描述

通过在数据分析与加工过程采取适当的安全控制措施，防止数据挖掘、分析与加工过程中有价值信息和个人隐私泄露的安全风险。

6.3.4.2 等级描述

6.3.4.2.1 基础建设级——一般增强要求

该等级的数据安全能力要求描述如下:

制度流程:

1) 核心业务应明确数据分析安全的原则或要求，如对个人明细数据、生产监测数据、工艺参数、库存数据等业务明细数据（涉及L0至L4各层）进行聚合分析过程中应考虑的关键安全风险等（BP.09.01）；

2) 核心业务团队应对涉及个人信息的数据分析需求进行了人工审核，针对具体的工业数据分析场景制定了相应的隐私保护方案（BP.09.02）；

6.3.4.2.2 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

组织建设:应由业务团队相关人员负责数据分析过程中的生产监测数据、工业控制数据、库存数据等工业（涉及L0至L4各层）数据的安全风险控制（BP.09.03）。

6.3.4.2.3 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设:组织应设立负责数据分析安全的岗位和人员，负责整体的工业数据分析安全原则制定、提供相应技术支持（BP.09.04）。

b) 制度流程:

1) 应明确数据处理与分析过程的安全规范，覆盖构建生产监测数据、工业控制数据、工业现场监控音视频流媒体数据、库存数据等工业数据（涉及L0至L4各层）的数据仓库、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（BP.09.05）；

2) 在对生产监测数据、工业控制数据、工业现场监控音视频流媒体数据、库存数据等工业数据（涉及L0至L4各层）进行数据分析时，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、分析操作等方面的正当性（BP.09.06）；

3) 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，整体保证针对生产监测数据、工业控制数据、工艺参数等工业数据（涉及L0至L4各层）的数据分析预期不会超过相关分析团队对数据的权

限范围（BP.09.07）；

4) 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，防止针对生产监测数据、工业控制数据、工艺参数等工业数据（涉及L0至L4各层）的数据分析结果输出造成安全风险（BP.09.08）；

c) 技术工具：

1) 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露风险，如差分隐私保护、K匿名等（BP.09.09）；

2) 应记录并保存针对生产监测数据、工艺参数和工业现场监控音视频流媒体等工业数据（涉及L0至L4各层）进行数据处理与分析的过程中对个人信息、重要数据等敏感数据的操作行为（BP.09.10）；

3) 应提供组织统一的工业数据处理与分析系统，并能够呈现生产监测数据、工艺参数和库存数据等工业数据（涉及L0至L4各层）在数据处理前后数据间的映射关系（BP.09.11）。

d) 人员能力：应能够基于合规性要求、相关标准对生产监测数据、工艺参数和工业现场监控音视频流媒体等工业数据（涉及L0至L4各层）的数据安全分析过程中可能引发的数据聚合的安全风险进行有效的评估，并能够针对分析场景提出有效的解决方案（BP.09.12）。

6.3.4.2.4 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1) 应结合技术手段降低工业数据分析过程中的安全风险，比如基于机器学习的工业领域重要数据自动识别、数据安全分析算法设计等（BP.09.13）；

2) 应采取必要的技术手段（如对分析结果数据进行扫描并采取必要的控制措施）和管理措施，避免输出的数据分析结果包含可恢复的个人信息、重要数据（如工业现场监控音视频流媒体数据、工艺参数、库存数据等（涉及L0至L4各层））等数据和结构标识（如用户鉴别信息的重要标识和数据结构），以防止数据分析结果危害个人隐私、公司商业价值、社会公共利益和国家安全（BP.09.14）；

3) 应建立数据分析过程的安全风险监控系统，针对生产监测数据、工业控制数据、工艺参数和库存数据等工业数据（涉及L0至L4各层）的数据分析过程中可能涉及的安全风险进行批量的分析和跟进（BP.09.15）；

4) 应具备基于机器学习的工业现场监控音视频流媒体数据、工艺参数、排产计划和库存数据等（涉及L0至L4各层）敏感数据自动识别、数据分析算法安全设计等数据分析安全能力（BP.09.16）；

5) 应在个人信息、重要数据（如关键工艺参数、库存数据等（涉及L0至L4各层））等数据有恢复需求时，采取必要的技术手段恢复数据（BP.09.17）。

6.3.4.2.5 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应跟踪新业务需求、国内外法律法规变化和技术发展变化，使用人工智能等前沿技术动态调整和改进数据分析安全管理方案（如改进数据分析的个人隐私保护方案）（BP.09.18）；

b) 人员能力：负责该项工作的人员应具备对针对生产监测数据、工业控制数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）开展数据分析的安全技术，能够及时跟进先进的最佳实践以保证对相关技术的合理应用（BP.09.19）。

c) 技术工具：
应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.09.20）。

6.3.5 PA10 数据合规性使用

6.3.5.1 PA 描述

基于国家相关法律法规对数据分析和利用的要求，建立数据使用过程的责任机制、评估机制，保护国家秘密、商业秘密和个人隐私，防止数据资源被用于不正当目的。

6.3.5.2 等级描述

6.3.5.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：
制度流程：
利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理（BP.10.01）。

6.3.5.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：
核心业务应明确生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）使用合规性的制度，保证数据使用在声明的目的和范围内（BP.10.02）；

6.3.5.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：
1) 应加强访问控制，对数据的使用加工进行授权和验证，并遵循最小化访问原则（BP.10.03）；
2) 应明确原始数据使用加工过程中的数据获取方式、安全措施，并周期性地检查数据操作行为的情况（BP.10.04）；
3) 应对测试过程中产生的过程性数据进行防护（BP.10.05）。

6.3.5.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
组织建设：应由业务团队相关人员负责生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及L0至L4各层）使用的合规性评估（BP.10.06）。

6.3.5.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
技术工具：

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，并采用技术手段实现所有数据挖掘、使用、加工、分析行为可溯源（BP.10.07）。

6.3.5.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应设立相关岗位或人员，负责对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据合规使用管理、评估和风险控制（BP.10.08）。

b) 制度流程：

1) 应明确数据使用的评估制度，所有个人信息和重要数据（如关键工艺参数、工业现场监控音视频流媒体数据、库存数据等（涉及 L0 至 L4 各层））的使用应先进行安全影响评估，满足国家合规要求后，允许使用。数据的使用应避免精确定位到特定个人，避免评价信用、资产和健康等敏感数据，不得超出与收集数据时所声明的目的和范围（BP.10.09）；

2) 应明确生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）使用合规性的制度，保证相关数据的使用在声明的目的和范围内（BP.10.10）；

c) 技术工具：

1) 应依据合规要求建立相应强度或粒度的访问控制机制，限定用户可访问数据范围（BP.10.11）；

2) 应完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责（BP.10.12）。

d) 人员能力：负责该项工作的人员应能够按最小够用等原则管理权限，并具备对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）合规使用的相关风险的分析和跟进能力（BP.10.13）。

6.3.5.2.7 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应具备违约责任、缔约过失责任、侵权责任等数据使用风险分析和处理能力（BP.10.14）。

b) 技术工具：应具备技术手段或机制，针对关键工艺参数、工业现场监控音视频流媒体数据、库存数据等工业数据（涉及 L0 至 L4 各层）滥用行为进行有效的识别、监控和预警（BP.10.15）。

c) 人员能力：负责该项工作的人员应具备发现关键工艺参数、工业现场监控音视频流媒体数据、库存数据等工业数据（涉及 L0 至 L4 各层）不合规使用安全风险的能力（BP.10.16）。

6.3.5.2.8 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1) 应研究并利用新的技术提升对用户的身份及访问管理能力，并通过人工智能等前沿技术和风险监控与审计实现对工艺参数、工业现场监控音视频流媒体数据、库存数据等工业数据（涉及 L0 至 L4 各层）使用的安全风险进行自动化

分析和处理（BP.10.17）；

2) 应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.10.18）。

6.3.6 PA11 数据处理环境安全

6.3.6.1 PA 描述

为组织内部的数据处理环境建立安全保护机制，提供统一的数据计算、开发平台，确保数据处理的过程中有完整的安全控制管理和技术支持。

6.3.6.2 等级描述

6.3.6.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

技术工具:

1) 原则上禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet、RDP 等高风险通用网络服务，对必要开通的网络服务采取安全接入代理等技术进行用户身份认证和应用鉴权（BP.11.01）；

2) 如果的确需要远程访问工业控制系统相关数据的，则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（BP.11.02）。

6.3.6.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程: 应明确生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据处理环境的安全管理要求（BP.11.03）。

6.3.6.2.3 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 应由业务团队相关人员负责生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据处理环境安全管理（BP.11.04）。

b) 技术工具: 核心业务的数据处理环境（如针对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的处理环境），应实现了身份鉴别、访问控制、安全配置等（BP.11.05）。

6.3.6.2.4 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 应由业务团队相关人员负责生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据处理环境安全管控（BP.11.06）。

b) 制度流程:

1) 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（BP.11.07）；

2) 组织应基于生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数

据（涉及 L0 至 L4 各层）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、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄露等方面进行安全要求和控制（BP.11.08）；

3) 组织应明确适合生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）处理环境的数据加解密处理要求和密钥管理要求（BP.11.09）。

c) 技术工具：

1) 针对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据处理系统与数据权限管理系统应实现了联动，用户在使用数据系统前已获得了授权（BP.11.10）；

2) 基于数据处理系统的多租户的特性，应对不同的租户保证其在该系统中的数据、系统功能、会话、调度和运营环境等资源实现隔离控制（BP.11.11）；

3) 应建立针对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的数据处理日志管理工具，记录用户在数据处理系统上的加工操作，提供数据在系统上加工计算的关联关系（BP.11.12）；

d) 人员能力：负责该项工作的人员应了解在生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）环境下的数据处理系统的主要安全风险，并能够在相关的系统设计、开发阶段通过合理的设计以及运维阶段的有效配置规避相关风险（BP.11.13）。

6.3.6.2.5 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应针对用户在数据处理系统上对生产监测数据、物料出库入库数据、工艺参数和库存数据等工业数据（涉及 L0 至 L4 各层）的操作开展定期审计，确定用户对数据的加工未超出前期申请数据时的目的（BP.11.14）。

b) 技术工具：

1) 应对分布式处理过程中不同数据副本节点数据的完整性和一致性进行定期检测（BP.11.15）；

2) 应建立分布式处理节点和用户安全属性的周期性确认机制（BP.11.16）；

3) 应建立数据分布式处理节点的服务组件自动维护和管控措施，包括虚假节点监测、故障用户节点确认和自动修复的技术机制（BP.11.17）；

4) 应建立分布式处理外部服务组件注册与使用审核机制（BP.11.18）；

5) 应具备对密文数据进行搜索、排序、计算等透明处理的技术能力（BP.11.19）；

6) 应建立分布式处理过程中的数据泄露控制机制，防止数据处理过程中的调试信息、日志记录等不受控制输出导致受保护个人信息、重要数据（如关键工艺参数、工业现场监控音视频流媒体数据、库存数据（涉及 L0 至 L4 各层））等敏感数据的泄露（BP.11.20）。

6.3.6.2.6 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应能使用人工智能等前沿技术对用户在生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及 L0 至 L4 各层）处理

系统上的操作执行实时监控，能够及时跟进风险并采取有效的风险控制措施（BP.11.21）。

b) 技术工具：应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.11.22）。

6.4 数据传输安全

6.4.1 PA12 数据传输安全管理

6.4.1.1 PA 描述

根据组织内部和外部的数据传输要求，采用适当的安全管理保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄露、篡改等。

6.4.1.2 等级描述

6.4.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

1）应根据工业应用场景、数据类型、数据级别和安全域等因素，制定数据传输安全策略（BP.12.01）；

2）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（BP.12.02）；

6.4.1.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a）制度流程：

涉及跨组织机构或者使用公共信息网络进行数据传输的，应进行内部登记、审批（BP.12.03）。

b）技术工具：

1）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（BP.12.04）；

2）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（BP.12.05）；

3）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（例如在设定时间内，某 IP 地址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（BP.12.06）。

4）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。（BP.12.07）

6.4.1.2.3 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

1）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（BP.12.08）；

2）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（BP.12.09）；

3)应具备数据溯源能力,使所有数据传输路径可恢复,数据传输行为可溯源(BP.12.10)。

6.4.2 PA13 数据传输加密

6.4.2.1 PA 描述

根据组织内部和外部的数据传输要求，采用适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄露、篡改等。

6.4.2.2 等级描述

6.4.2.2.1 基础建设级——般增强要求

该等级的数据安全能力要求描述如下:

a）制度流程:

应根据合规要求，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务实时性响应需求，在有关制度文件中针对性提出生产监测、工业控制等数据（主要涉及 L0、L1、L2 层）的传输防护要求（BP.13.01）。

b）人员能力:

应在有关人员培训内容中包含工业控制数据和生产监测数据（主要涉及 L0、L1、L2 层）传输防护相关针对性数据安全内容，提升人员数据传输防护安全意识（BP.13.02）。

6.4.2.2.2 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a）组织建设:

1）信息化部门相关人员应负责生产监测、工业控制等数据（主要涉及 L0、L1、L2 层）传输的安全防护措施部署（BP.13.03）;

2）生产现场相关人员应负责生产监测、工业控制等数据（主要涉及 L0、L1、L2 层）传输的安全防护措施执行（BP.13.04）。

b）制度流程:

应根据合规要求，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务实时性响应需求，在有关制度文件中针对性提出工业控制数据和排产计划、工艺参数、工单指令、库存等管理运营数据（主要涉及 L2、L3、L4 层）的加密传输要求（BP.13.05）。

c）技术工具:

应针对工业控制数据及相关文件（主要涉及 L1、L2 层）的通信进行加密（BP.13.06）。

d）人员能力:

负责数据传输加密工作的人员应了解工业控制数据和排产计划、工艺参数、工单指令、库存等管理运营数据（主要涉及 L2、L3、L4 层）常用的安全通道方案、身份鉴别和认证技术、主流加密算法，基于应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务选择合适的数据传输安全管理方式（BP.13.07）。

6.4.2.2.3 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a）组织建设:

应设置专人负责开展生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及 L0 至 L4 各层）的传输加密工作（BP.13.08）。

b）技术工具：

1）应能够对工业生产监测数据（主要涉及 L1、L2、L3、L4 层）及相关文件的通信进行针对性加密（BP. 13. 09）；

2）组织针对生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（主要涉及 L1、L2、L3、L4 层）使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求（BP. 13. 10）；

3）应采取相应技术手段实现针对生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（主要涉及 L2、L3、L4 层）的加密有效性持续监测（BP. 13. 11）。

6. 4. 2. 2. 4 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a）组织建设：

应设置专业团队负责开展生产监测、工业控制等生产数据（主要涉及 L0、L1、L2、L3 层）的传输加密工作（BP. 13. 12）。

b）制度流程：

应根据合规要求，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务实时性响应需求，在有关制度文件中针对性提出工业生产监测数据（主要涉及 L0、L1、L2、L3 层）加密传输要求（BP. 13. 13）。

c）人员能力：

负责生产监测、工业控制等生产数据传输加密工作的人员应熟悉生产业务数据，能够识别和审核被加密的生产监测、工业控制等生产数据（涉及 L0 至 L4 各层）是否完整（BP. 13. 14）。

6. 4. 2. 2. 5 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a）组织建设：

应设置专业团队负责开展生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及 L0 至 L4 各层）的传输加密工作（BP. 13. 15）。

b）制度流程：

应根据合规要求，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务实时性响应需求，在有关制度文件中对工业控制、生产监测、排产计划、工艺参数、工单指令、库存等各类数据（涉及 L0 至 L4 各层）的加密传输，以及分别使用的加密算法、加密隧道提出针对性要求（BP. 13. 16）。

c）技术工具：

1）应通过人工智能和大数据等相关技术手段，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务实时性响应需求，针对生产管理、企业管理等各类数据（主要涉及 L3、L4 层）提供加密方案用于辅助决策（BP. 13. 17）；

2）如使用远程加密（涉及 L0 至 L4 各层），建议使用协议不低于 TLS 1.3 版本（BP. 13. 18）。

6.5 数据提供安全

6.5.1 PA14 数据对外提供安全

6. 5. 1. 1 PA 描述

通过业务系统、产品对外部组织提供数据时，以及通过合作的方式与合作伙伴交换数据时执行共享数据的安全风险控制，以降低数据共享场景下的安全风险。

6.5.1.2 等级描述

6.5.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程:

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（BP.14.01）。

6.5.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程:

应明确工业生产和管理运营等核心业务数据共享安全评估机制，可从共享目的合理性、共享数据的范围和合规性、共享方式的安全性、共享后管理责任和约束措施等方面进行评估（BP.14.02）；

6.5.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 制度流程:

1) 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保护能力进行核查，例如核实历史数据安全事件发生情况（BP.14.03）；

2) 应对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（BP.14.04）。

b) 技术工具:

1) 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、数据脱敏等（BP.14.05）；

2) 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（BP.14.06）；

3) 应采用数据标注、水印等溯源技术，对数据流经节点及流转过程中的篡改、泄露、滥用等行为进行溯源（BP.14.07）。

6.5.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 应由业务团队相关人员负责对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的共享方案进行安全风险管控（BP.14.08）。

b) 人员能力: 负责数据共享安全的人员应具备对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的共享业务的理解能力，能够结合合规性要求给出适当的安全解决方案（BP.14.09）。

6.5.1.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

跨不同法人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（BP.14.10）。

6.5.1.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应针对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）设立了统一的数据共享交换安全管理的岗位和人员，负责相关原则和技术能力的提供，并推广相关要求在相关业务的落地执行（BP.14.11）。

b) 制度流程：

1) 应明确生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）共享的原则和安全规范，明确数据共享内容范围和数据共享的管控措施，及数据共享涉及机构或部门相关用户职责和权限（BP.14.12）；

2) 应明确生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的数据提供者与共享数据使用者的数据安全责任和安全能力（BP.14.13）；

3) 应明确生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的共享审计规程和审计日志管理要求，明确审计记录要求，为数据共享安全事件的处置、应急响应和事后调查提供帮助（BP.14.14）；

4) 在企业办公网及工业生产网中使用外部的软件开发包/组件/源码前应进行安全评估，获取的数据应符合组织的数据安全要求（BP.14.15）；

c) 技术工具：

1) 应采取措施确保个人信息在委托处理、共享、转让等对外提供场景的安全合规，如数据脱敏、数据加密、安全通道、共享交换区域等（BP.14.16）；

2) 应对共享数据及数据共享过程进行监控审计，共享的数据应符合工业生产及管理运营中的共享业务需求且没有超出数据共享使用授权范围（BP.14.17）；

3) 应明确生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的数据共享格式规范，如提供机器可读的格式规范（BP.14.18）；

d) 人员能力：负责该项工作的人员应能够充分理解组织的数据共享规程，并根据工业生产及管理运行等业务的特点及数据共享需求执行相应的风险评估，从而提出实际的解决方案（BP.14.19）。

6.5.1.2.7 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

1) 应在组织统一的数据共享原则基础上，针对主要的数据共享场景（如通过企业管理系统进行数据共享等）明确了安全细则或审批流程，如对境外机构的数据共享安全细则，对政府机构的数据共享安全细则等（BP.14.20）；

2) 应定期评估数据共享机制，相关组件和共享通道的安全性（BP.14.21）；
3) 应在共享生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）时，对数据接收方的数据安全能力进行评估（BP.14.22）。

b) 技术工具：
1) 应建立组织统一的数据共享交换系统，结合工业数据的重要及敏感程度及时提示数据共享交换的安全风险并进行在线审核（BP.14.23）；
2) 应配置数据共享机制或服务组件，明确生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）共享的最低安全防护要求（BP.14.24）。

6.5.1.2.8 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
组织应及时跟进业务相关法律法规的更新和产业内的优秀做法，使用人工智能等前沿技术定期评估针对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的数据共享机制、服务组件和共享通道的安全性，对数据共享的风险控制方案进行持续的优化调整（BP.14.25）；

b) 技术工具：应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.14.26）。

6.5.2 PA15 数据接口安全

6.5.2.1 PA 描述

通过建立组织的对外数据接口的安全管理机制，防范组织数据在接口调用过程中的安全风险。

6.5.2.2 等级描述

6.5.2.2.1 基础建设级——般增强要求

该等级的数据安全能力要求描述如下：

制度流程：工业生产和管理运营中的核心业务或系统应定义数据接口安全策略（BP.15.01）。

6.5.2.2.2 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由业务团队相关人员负责企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全管理工作（BP.15.02）。

b) 技术工具：应采用技术工具实现对企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口调用的身份鉴别和访问控制（BP.15.03）。

c) 人员能力：负责企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的

数据接口安全工作的人员应具备基本的数据接口调用的安全意识和安全知识（BP.15.04）。

6.5.2.2.3 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 组织应设立统一负责企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全管理的岗位和人员，由该岗位人员负责制定整体的规则并推广相关流程的推行（BP.15.05）。

b) 制度流程:

1) 应明确企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全控制策略，明确规定使用数据接口的安全限制和安全控制措施，如身份鉴别、访问控制、授权策略、签名、时间戳、安全协议等（BP.15.06）;

2) 应明确企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全要求，包括接口名称、接口参数等（BP.15.07）;

3) 应与企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口调用方签署了合作协议，明确数据的使用目的、供应方式、保密约定、数据安全责任等（BP.15.08）。

c) 技术工具:

1) 应具备对企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的接口不安全输入参数进行限制或过滤能力，为接口提供异常处理能力（BP.15.09）;

2) 应具备企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口访问的审计能力，并能为数据安全审计提供可配置的数据服务接口（BP.15.10）;

3) 应对跨安全域间的数据接口调用采用安全通道、加密传输、时间戳等安全措施（BP.15.11）。

d) 人员能力: 负责企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全工作的人员应充分理解数据接口调用业务的使用场景,具备充分的数据接口调用的安全意识、技术能力和风险控制能力（BP.15.12）。

6.5.2.2.4 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

技术工具: 应建立企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口安全监控措施，以对接口调用进行必要的自动监控和处理（BP.15.13）。

6.5.2.2.5 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

a) 应在对企业管理系统、仓储管理系统、生产执行系统、生产现场监控平台等系统及上位机、服务器、工业控制器等设备（主要涉及L1、L2、L3、L4层）的数据接口调用进行必要的自动化监控和处理基础上，及时跟进最近技术及相关制度，使用人工智能等前沿技术进行安全管理和工程过程的持续改进工作（BP.15.14）；

b) 应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为行业标杆（BP.15.15）。

6.6 数据公开安全

6.6.1 PA16 数据公开安全

6.6.1.1 PA 描述

在对外部组织进行数据发布的过程中，通过对发布数据的格式、适用范围、发布者与使用者权利和义务执行的必要控制，以实现数据发布过程中数据的安全可控与合规。

6.6.1.2 等级描述

6.6.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

1) 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（BP.16.01）；

2) 应在数据公开前，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（BP.16.02）。

6.6.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

应明确工业生产和管理运营中的核心业务数据公开发布的安全制度和审核流程（BP.16.03）；

6.6.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：宜采取数据脱敏、数据水印等必要措施，保证数据公开安全（BP.16.04）。

6.6.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由业务团队相关人员负责数据发布的安全风险控制（BP.16.05）。

b) 人员能力：负责数据发布安全工作的人员应基本理解数据发布安全的制度要求（BP.16.06）。

6.6.1.2.5 集成管控级—核心预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：核心数据原则上不允许公开（BP.16.07）。

6.6.1.2.6 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应设立相关岗位人员，负责组织的数据公开发布信息，并且对数据发布人员进行安全培训（BP.16.08）。
b) 制度流程：
   1) 应明确数据公开发布的审核制度，严格审核数据发布合规要求（BP.16.09）；
   2) 应明确数据公开内容、适用范围及规范，发布者与使用者权利和义务（BP.16.10）；
   3) 应定期审查公开发布的数据中是否含有非公开信息（如关键工艺参数、包含国家关键信息基础设施位置坐标的工业现场监控视频流媒体数据等（主要涉及L0至L3级）），并采取相关措施满足数据发布的合规性（BP.16.11）；
   4) 应采取必要措施建立数据公开事件应急处理流程（BP.16.12）。
c) 技术工具：
   1) 应建立数据发布系统，实现公开数据登记、用户注册等发布数据和发布组件的验证机制（BP.16.13）；
d) 人员能力：负责数据发布安全管理工作的人员应充分理解数据安全发布的制度和流程，通过了岗位能力评估，并能够根据实际发布要求建立相应的应急方案（BP.16.14）。

6.6.1.2.7 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
   1) 组织应针对关键的数据资源发布（如工艺参数、计划数据、工业现场监控音视频流媒体数据等（涉及L0至L4级））明确了安全发布细则和审核流程（BP.16.15）；
   2) 组织应细化明确各类数据发布场景的审核流程，从审核的有效性和审核的效率层面充分考虑流程节点的制定（BP.16.16）。
b) 技术工具：组织应针对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）建立统一的数据发布系统，提示数据发布安全风险并进行在线审核（BP.16.17）。

6.6.1.2.8 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 技术工具：
   1) 应使用人工智能等前沿技术对发布的数据，建立持续的追踪能力，优化生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及L0至L4各层）的发布规程（BP.16.18）；
   2) 应参与国际、国家或行业数据安全相关标准制定。在业界分享最佳实践，成为

行业标杆（BP.16.19）。

6.7 数据销毁安全

6.7.1 PA17 数据销毁处置

6.7.1.1 PA 描述

通过建立针对数据的删除、净化机制，实现对数据的有效销毁，防止因对存储媒体中的数据进行恢复而导致的数据泄露风险。

6.7.1.2 等级描述

6.7.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程:

1) 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(BP.17.01);
2) 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（BP.17.02）。

6.7.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程:

应明确工业生产及管理运营中核心业务数据销毁方案和存储媒体销毁方案（BP.17.03）;

6.7.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程:

1) 不得对销毁数据进行恢复（BP.17.04）;
2) 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或核心数据目录（BP.17.05）。

6.7.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 应由业务团队相关人员负责生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的销毁工作（BP.17.06）。
b) 技术工具:应采用技术工具对工业生产及管理运营中核心业务存储媒体的数据内容进行擦除销毁（BP.17.07）。
c) 人员能力:负责数据销毁处置的人员应具备针对数据销毁的需求制定对应的数据销毁方案的能力（BP.17.08）。

6.7.1.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设：组织应设立统一负责生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的数据销毁管理的岗位和人员，负责制定数据销毁处置规范，并推动相关要求在业务部门落地实施（BP.17.09）。

b) 制度流程：

1) 应依照数据分类分级建立生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的数据销毁策略和管理制度，明确数据销毁的场景销毁对象、销毁方式和销毁要求（BP.17.10）；

2) 应建立规范的生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）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（BP.17.11）；

3) 应按国家相关法律和标准销毁个人信息、重要数据（如关键工艺参数、工业现场监控音视频流媒体数据、库存数据（涉及 L0 至 L4 各层））等敏感数据（BP.17.12）；

c) 技术工具：

1) 应针对网络存储数据，建立硬销毁和软销毁的数据销毁方法和技术，如基于安全策略、基于分布式杂凑算法等网络数据分布式存储的销毁策略与机制（BP.17.13）；

2) 应配置必要的数据销毁技术手段与管控措施，确保以不可逆方式销毁敏感数据及其副本内容（BP.17.14）。

d) 人员能力：负责数据销毁安全工作的人员应熟悉生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的数据销毁的相关合规要求，能够主动根据政策变化和技术发展更新相关知识和技能（BP.17.15）。

6.7.1.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

1) 应明确数据销毁效果评估机制，定期对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的数据销毁效果进行抽样认定（BP.17.16）；

2) 应明确已共享或者已被其他用户使用的生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的销毁管控措施（BP.17.17）。

b) 技术工具：

1) 组织的数据资产管理系统应能够对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的销毁需求进行明确的标识，并可通过该系统提醒数据管理者及时发起对数据的销毁（BP.17.18）；

2) 应通过技术手段避免对生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的误销毁（BP.17.19）。

6.7.1.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 制度流程: 应定期审核生产监测、工业现场监控音视频等生产数据和排产计划、工艺参数、库存等管理运营数据（涉及 L0 至 L4 各层）的存储时长的情况，考虑数据存储成本的需求、法律法规和更新合同的需求，以及相关数据销毁技术的发展现状，使用人工智能等前沿技术对数据销毁的整体方案进行及时更新（BP.17.20）。

b) 技术工具: 应参与国际、国家或行业相关数据安全标准制定。在业界分享最佳实践，成为行业标杆（BP.17.21）。

6.7.2 PA18 存储媒体销毁处置

6.7.2.1 PA 描述

通过建立对存储媒体安全销毁的规程和技术手段，防止因存储媒体丢失、被窃或未授权的访问而导致存储媒体中的数据泄露的安全风险。

6.7.2.2 等级描述

6.7.2.2.1 基础建设级——一般增强要求

该等级的数据安全能力要求描述如下:

制度流程: 应明确工业生产和管理运营中的核心业务媒体销毁的流程和管理要求（BP.18.01）。

6.7.2.2.2 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 应由业务团队相关人员负责存储媒体销毁管理（BP.18.02）。

b) 技术工具: 核心业务的存储媒体，应仅采用物理销毁的形式进行销毁（BP.18.03）。

c) 人员能力: 相关人员应具备针对数据销毁需求能够明确判断媒体销毁的必要性（BP.18.04）。

6.7.2.2.3 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 组织应设立统一负责媒体销毁管理的岗位和人员，结合组织机构、工业应用场景等因素，整体制定组织媒体销毁管理的制度，并推动相关内容在业务团队实施落地（BP.18.05）。

b) 制度流程:

1) 应明确存储媒体销毁处理策略、管理制度和机制，明确销毁对象和流程（BP.18.06）;

2) 应依据存储媒体存储内容的重要性，明确磁媒体、光媒体和半导体媒体等不同类存储媒体的销毁方法（BP.18.07）;

3) 应明确对存储媒体销毁的监控机制，确保对销毁存储媒体的登记、审批、交接等存储媒体销毁过程进行监控（BP.18.08）。

c) 技术工具:

1) 组织应提供统一的存储媒体销毁工具，包括但不限于物理销毁、消磁设备等工

具，能够实现对各类媒体的有效销毁（BP.18.09）；

2) 应针对闪存盘、硬盘、磁带、光盘等存储媒体数据，建立硬销毁和软销毁的数据销毁方法和技术（BP.18.10）。

d) 人员能力：负责该项工作的人员应能够结合工业应用场景等因素，依据数据销毁的整体需求明确应使用的媒体销毁工具（BP.18.11）。

6.7.2.2.4 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

1) 应明确存储媒体销毁效果评估机制，定期对存储媒体销毁效果进行抽样认定（BP.18.12）；

2) 应定期进行存储媒体销毁记录的检查（BP.18.13）。

b) 技术工具：应由经过认证的机构或设备对存储媒体进行物理销毁，或联系经认证的销毁服务商进行存储媒体销毁工作（BP.18.14）。

6.7.2.2.5 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应使用人工智能等前沿技术持续根据组织在工业生产和管理运营等场景下的存储媒体销毁需求优化存储媒体销毁的流程以及方案（BP.18.15）。

b) 技术工具：

1) 应持续更新组织的存储媒体销毁工具，以保证存储媒体销毁的效果（BP.18.16）；

2) 应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.18.17）。

7 通用安全能力成熟度评估

7.1 PA19 安全管理制度

7.1.1 PA 描述

建立适用于组织数据安全风险状况的组织整体的数据安全策略规划，数据安全策略规划的内容应覆盖数据全生命周期的安全风险。

7.1.2 等级描述

7.1.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

应结合所属行业领域的数据特征、数据处理场景等，建立数据安全管理制度，明确组织机构、责任落实、安全防护、风险评估、应急处置、培训教育等管理要求（BP.19.01）。

7.1.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：组织工业生产及管理运营的核心业务应基于主要的数据安全风险，建立以数据安全生命周期为核心思想的数据安全制度体系（BP.19.02）；

7.1.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：宜建立监督考核机制，定期对数据安全工作相关部门进行安全责任评估（BP.19.03）；

7.1.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由业务团队具体人员负责制定工业生产及管理运营等业务的数据安全策略（BP.19.04）。

b) 人员能力：组织负责工业生产及管理运营核心业务工作的人员应具备对组织执行数据安全风险评估，以及将数据安全要求提炼形成制度的能力（BP.19.05）。

7.1.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应设立专职的岗位和人员，负责组织涵盖生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及L0至L4各层）的数据安全制度流程和战略规划的建设（BP.19.06）。

b) 制度流程：

1) 应结合组织工业生产及管理运营业务特点提炼数据安全需求，明确组织数据战略规划的数据安全总体策略，明确安全方针、安全目标和安全原则（BP.19.07）；

2) 应基于组织的数据安全总体策略，在组织层面明确以数据为核心的数据安全制度和规程覆盖数据全生命周期相关的业务、系统和应用，内容包含目的、范围、岗位、责任、管理层承诺、内外部协调机制及合规目标等（BP.19.08）；

3) 应结合组织生产运行等业务需求及信息化系统应用现状，明确并实施大数据系统和数据应用安全实施细则（BP.19.09）；

4) 应结合组织机构特点和工业应用场景需求，明确数据安全制度规程分发机制，将数据安全策略、制度和规程分发至组织相关部门、岗位和人员（BP.19.10）；

5) 应结合组织机构特点和工业应用场景需求，明确数据安全制度及规程的评审、发布流程，并确定适当的频率和时机对制度和规程进行审核和更新（BP.19.11）；

6) 应结合组织机构特点和工业应用场景需求，明确组织层面的数据安全战略规划，包括各阶段目标、任务、工作重点，并保障其与业务规划相适应（BP.19.12）。

c) 技术工具：应结合组织机构特点和工业应用场景需求，建立数据安全策略规划的系统，通过该系统向组织全体员工发布策略规划的解读材料，以便于策略规划的落地推进（BP.19.13）。

d) 人员能力：

1) 负责制定数据安全总体策略和战略规划的人员应了解组织的工业生产及管理

运营业务发展目标，能够将数据安全工作的目标和业务发展的目标进行有机结合（BP.19.14）；

2) 负责制定数据安全制度和规程的人员应具备信息安全管理体系建设的知识，并具备良好的规范撰写能力（BP.19.15）；

3) 负责推广数据安全策略规划的人员应能够以员工和相关方易理解的方式，通过培训等宣导形式对数据安全管理的方针、策略和制度进行有效传达（BP.19.16）。

7.1.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

1) 在组织架构发生重大调整或数据服务业务发生重大变化时，应及时结合更新后的组织架构及生产运营业务特点评估数据安全制度与规程的实施效果，并将效果反映到安全制度和规程文件的修订过程中（BP.19.17）；

2) 应结合组织架构及生产运营业务特点，定期对数据安全制度和规程进行体系化的评估，制定数据安全能力提升计划（BP.19.18）；

3) 应结合组织架构及生产运营业务特点，定期对数据安全战略规划进行评估，确保数据安全总体策略、安全目标和战略规划内容的合规性（BP.19.19）。

b) 人员能力：负责该工作的人员能够及时评估策略规划的实施效果，并根据实施效果修订数据安全策略规划文件（BP.19.20）。

7.1.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应持续跟进国内外在数据安全领域的管理标准和技术发展，并关注组织所在行业的发展动态及组织自身的业务发展方向，及时对数据安全策略规划进行调整和改进（BP.19.21）。

b) 技术工具：

1) 应建立数据安全规划动态调整机制，通过使用人工智能等前沿技术和信息化系统执行对数据安全规划的动态管理（BP.19.22）；

2) 应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.19.23）。

c) 人员能力：负责该工作的人员应能够持续跟踪国内外数据安全政策、标准、产业趋势、新技术，并能够对组织的数据安全策略规划实现持续优化（BP.19.24）。

7.2 PA20 组织机构

7.2.1 PA 描述

通过建立组织内部负责数据安全工作的职能部门及岗位，防范组织管理过程中存在的数据安全风险。

7.2.2 等级描述

7.2.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：应明确数据安全管理的责任部门，统筹负责数据处理活动的安全监督管理（BP.20.01）。

7.2.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

1) 工业生产等相关核心业务应明确针对数据安全违规的纪律处理制度（BP.20.02）；
2) 工业生产等相关核心业务应对重要岗位候选者从法律法规、行业道德准则等层面执行背景调查（BP.20.03）；
3) 工业生产等相关核心业务应明确数据安全职能部门或岗位的制度，明确数据安全相关岗位和职责（BP.20.04）；

7.2.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

1) 应设置专门的数据安全管理责任部门，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，并建立常态化沟通与协作机制（BP.20.05）；
2) 应建立数据安全工作体系，覆盖数据安全责任部门，以及研发设计、生产制造、经营管理、运行维护、外部服务、采购、审计、法务等相关部门（BP.20.06）；

7.2.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：工业生产等相关核心业务应具有数据安全职能部门或岗位，以实现对关键业务环节数据安全风险的有效管理（BP.20.07）。

7.2.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：
   1) 人力资源部门与数据安全部门的人员应能够进行有效配合（BP.20.08）；
   2) 工业企业应建立组织层面专职的数据安全职能部门和岗位并在职能岗位设计时考虑了职责分离的原则（BP.20.09）；
   3) 应建立组织层面的数据安全领导小组，指定机构最高管理者或授权代表担任小组组长，并明确了组长的责任与权力，指导开展工业数据（涉及L0至L4各层）治理工作（BP.20.10）；
   4) 应建立组织内部的监督管理职能部门，负责对组织内部的生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及L0至L4各层）的数据操作行为进行安全监督（BP.20.11）；
   5) 应指定工业大数据系统的安全规划、安全建设、安全运营和系统维护工作的责任部门（BP.20.12）；
b) 制度流程：
   1) 应明确数据安全追责机制，定期对责任部门、安全岗位、生产系统组织安全检

查，形成检查报告（BP.20.13）；

c) 技术工具：

1) 应以公开信息且可查询的形式，面向组织全员公布数据安全职能部门的组织架构（BP.20.14）。

7.2.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：

1) 应建立覆盖工业生产、信息化等各业务部门的体系化的数据安全管理部门，且配备必要的管理人员和技术人员（BP.20.15）；

2) 应将数据安全职能的运行效果纳入工业绩效指标体系，以量化指标为基准进行定期评估，并依据评估结果对数据职能岗位进行动态配置与持续优化。（BP.20.16）；

3) 应定期评估在当前组织职能架构下，数据安全职能岗位与各工业生产业务和职能岗位之间的关系是否平衡，是否能够保证安全需求在业务中的推广（BP.20.17）。

7.2.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应结合具体工业生产业务需求，能够持续优化组织的数据安全职能设置，以实现整体业务目标的优化（BP.20.18）。

b) 制度流程：应能够持续优化组织管理的相关流程，以保证符合工业生产等业务发展的实际情况（BP.20.19）。

c) 技术工具：应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.20.20）。

7.3 PA21 人员保障

7.3.1 PA 描述

通过对人力资源管理过程中各环节进行安全管理，防范人员管理过程中存在的数据安全风险。

7.3.2 等级描述

7.3.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

人员能力：

1) 宜根据企业和岗位性质，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（BP.21.01）；

2) 应定期开展数据安全教育与技能培训，强化从业人员数据安全意识和专业技能（BP.21.02）。

7.3.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

1) 工业生产等相关核心业务应明确数据安全培训计划，并按计划对相关人员开展数据安全培训（BP.21.03）；
2) 应与所有涉及生产监测数据、工业控制数据、货位数据、工艺参数、计划数据、工单指令（涉及 L0 至 L4 各层）等数据服务的人员签订安全责任协议和保密协议（BP.21.04）；

7.3.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

人员能力：

1) 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（BP.21.05）；
2) 应强化关键岗位人员管理，将处理重要数据和核心数据的人员确定为关键岗位人员（BP.21.06）；
3) 应明确数据处理关键岗位人员职责，并要求关键岗位人员签署数据安全责任书，责任书内容包括数据安全岗位职责、义务、处罚措施、注意事项等内容（BP.21.07）；
4) 宜制定数据处理关键岗位人员上岗、在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（BP.21.08）；
5) 宜对离岗关键岗位人员签订保密承诺书，要求继续履行不泄露企业重要数据和核心数据的责任义务（BP.21.09）。

7.3.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：应由信息化、工业生产等部门相关人员负责人力资源管理中安全要求（BP.21.10）；

7.3.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：
   1) 工业企业应明确在组织层面人力资源管理中承担数据安全要求制定和执行的人员或岗位，并与数据安全人员进行有效配合（BP.21.11）；
   2) 应明确组织层面承担人员数据安全培训管理职责的岗位和人员，负责对工业生产部门、管理部门等不同部门的数据安全培训需求的分析及落地方案的制定和推进（BP.21.12）。
b) 制度流程：
   1) 应明确数据服务人力资源安全策略，明确工业生产人员、管理人员等不同岗位人员在数据全生命周期各阶段相关的工作范畴和安全管控措施（BP.21.13）；
   2) 应明确组织层面的数据服务人员招聘、录用、上岗、调岗、离岗、考核、选拔等人员安全管理制度，将生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及 L0 至 L4 各层）的数据安全相关的要求固化到人力资源管理流程中（BP.21.14）；
   3) 在录用重要岗位人员前应对其进行背景调查，符合相关的法律、法规、合同要

求，对数据安全员工候选者的背景调查中也包含了对候选者的安全专业能力的调查，应熟悉工业生产等业务数据（涉及 L0 至 L4 各层）安全相关保障措施。（BP. 21. 15）；

4) 应明确生产监测数据、工业控制数据、经营管理数据（涉及 L0 至 L4 各层）等数据服务重要岗位的兼职和轮岗、权限分离、多人共管等安全管理要求；（BP. 21. 16）；

5) 应明确针对合作方的安全管理制度，对接触个人信息、生产监测、工业控制等生产数据和排产计划、工艺参数、工单指令、库存等管理数据（涉及 L0 至 L4 各层）等重要数据的人员进行审批和登记，并要求签署保密协议，定期对这些人员行为进行安全审查（BP. 21. 17）；

6) 在重要岗位人员调离或终止劳动合同前，应与其签订保密协议或竞业协议（BP. 21. 18）；

7) 应明确组织内部员工的数据安全培训计划，针对工业生产、信息化、行政等不同部门员工定制相关数据安全培训计划，按计划定期对员工开展数据安全培训（BP. 21. 19）；

8) 应明确重要岗位人员的数据安全培训计划，针对工业生产、信息化、行政等不同部门重点岗位员工定制相关数据安全培训计划，并在重要岗位转岗、岗位升级等环节对相关人员开展培训（BP. 21. 20）。

c) 技术工具：

2) 应通过技术工具自动化实现了数据安全相关的人力资源管理流程（BP. 21. 21）；

3) 应及时终止或变更离岗和转岗员工对生产监测、工业控制等生产数据和管理数据的操作权限，并及时将人员的变更通知到相关方（BP. 21. 22）；

4) 员工入职时应针对工业生产、信息化等不同部门按最少够用原则分配初始权限（BP. 21. 23）；

7. 3. 2. 6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：

1) 应明确重要岗位人员安全能力要求，并确定其培训工业技能、考核内容与考核指标，人员培训内容中包含工业控制数据和生产监测数据（主要涉及 L0、L1、L2 层）相关数据安全要求，定期对重要岗位人员进行审查和能力考核（BP. 21. 24）；

2) 应定期对数据安全培训计划审核更新（BP. 21. 25）。

b) 技术工具：应建立人员数据安全意识或能力的客观评价机制，通过在线的人力资源管理系统，量化管理人力资源安全中存在的风险点和改进点（BP. 21. 26）。

7. 3. 2. 7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应能够持续优化人员管理的相关流程，以保证符合工业生产等业务发展的实际情况（BP. 21. 27）。

b) 技术工具：应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP. 21. 28）。

7.4 PA22 权限管理

7.4.1 PA 描述

通过基于组织的数据安全需求和合规性要求建立身份鉴别和数据访问控制机制，防止对数据的未授权访问风险。

7.4.2 等级描述

7.4.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

1) 应合理确定数据处理活动的操作权限，严格实施人员权限管理（BP.22.01）；
2) 应按照最小授权原则分配账号权限（BP.22.02）。

7.4.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：工业生产等相关核心业务应明确工业控制系统、生产执行系统、企业管理系统等（涉及L0至L4各层）重要系统和数据库的身份鉴别、访问控制和权限管理的安全要求（BP.22.03）；

7.4.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：

1) 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（BP.22.04）；
2) 应定期对权限分配情况进行复核，严禁未授权访问数据（BP.22.05）；
3) 应在人员变更、调离或终止劳动合同时，及时变更或终止其数据处理权限（BP.22.06）；

7.4.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：应由工业生产、信息化等业务团队相关人员负责管理核心业务系统的用户身份及数据权限管理（BP.22.07）。
b) 技术工具：
   1) 工业控制系统、生产执行系统、企业管理系统等（涉及L0至L4各层）核心业务系统应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换（BP.22.08）；
   2) 工业控制系统、生产执行系统、企业管理系统等（涉及L0至L4各层）核心业务系统应提供访问控制功能，对登录的用户分配账户和权限（BP.22.09）；
   3) 工业控制系统、生产执行系统、企业管理系统等（涉及L0至L4各层）核心业务系统应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施（BP.22.10）。

7.4.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 组织建设：组织应设立统一的岗位和人员，负责制定组织内用户身份鉴别、工业控制系统、生产执行系统、企业管理系统等（涉及 L0 至 L4 各层）访问控制和权限管理的策略，提供相关技术能力或进行统一管理（BP. 22. 11）。

b) 制度流程：

1) 应定期审核工业控制、生产监测、排产计划、工艺参数、工单指令、库存等各类数据（涉及 L0 至 L4 各层）访问权限，及时删除或停用多余的、过期的账户和角色，避免共享账户和角色权限冲突的存在（BP. 22. 12）；

2) 应对外包人员和实习生的数据访问权限进行严格控制（BP. 22. 13）。

c) 技术工具：

1) 应建立组织统一的身份鉴别管理系统，支持组织工业控制系统、生产执行系统、企业管理系统等（涉及 L0 至 L4 各层）主要应用接入，实现对人员访问数据资源的统一身份鉴别（BP. 22. 14）；

2) 应建立组织统一的权限管理系统，支持组织工业控制系统、生产执行系统、企业管理系统等（涉及 L0 至 L4 各层）主要应用接入，对人员访问数据资源进行访问控制和权限管理（BP. 22. 15）；

3) 应采用技术手段实现身份鉴别和权限管理的联动控制（BP. 22. 16）；

4) 应采用口令、密码技术、生物技术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使用密码技术来实现（BP. 22. 17）；

5) 访问控制的粒度应达到主体为用户级，客体为工业控制系统、生产执行系统、企业管理系统等（涉及 L0 至 L4 各层）、文件、数据库表级或字段（BP. 22. 18）。

d) 人员能力：负责该项工作的人员应熟悉相关的数据访问控制的技术知识，熟悉工业控制数据、生产监测数据、生产管理数据和企业管理数据（主要涉及 L0、L1、L2、L4 层）的相关数据安全要求，并能够根据组织数据安全管理制度对数据权限进行审批管理（BP. 22. 19）。

7. 4. 2. 6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：组织应建立数据安全角色清单，明确数据安全角色的安全要求、分配策略、授权机制和权限范围（BP. 22. 20）。

b) 技术工具：

1) 应建立面向工业控制系统、生产执行系统、企业管理系统等（涉及 L0 至 L4 各层）数据应用的访问控制机制，包括访问控制时效的管理和验证，以及数据应用接入的合法性和安全性取证机制（BP. 22. 21）；

2) 应建立人力资源管理与身份鉴别管理、权限管理的联动控制，及时删除离岗、转岗人员的权限（BP. 22. 22）；

3) 应采用技术手段对系统或应用访问工业控制、生产监测、排产计划、工艺参数、工单指令、库存等各类敏感数据（涉及 L0 至 L4 各层）进行访问控制（BP. 22. 23）。

7. 4. 2. 7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

a) 应使用人工智能等前沿技术辅助建立针对数据全生命周期各阶段的数据安全主动防御机制或措施，如基于用户行为或设备行为安全控制机制（BP.22.24）；
b) 应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.22.25）。

7.5 PA23 系统与设备安全

7.5.1 PA 描述

基于组织对终端设备层面的数据保护要求，针对组织内部的工作终端采取相应的技术和管理方案。

7.5.2 等级描述

7.5.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：
技术工具：

1) 应对数据库、研发终端、生产设备、开发代码库等数据载体及数据采集系统进行安全配置，建立安全配置清单，定期进行配置审计（BP.23.01）；
2) 应密切关注数据载体的重大安全漏洞及其补丁发布，及时采取升级措施，短期内无法升级的，应开展针对性安全加固（BP.23.02）。
3) 应强化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（BP.23.03）；
4) 在服务器、工程师站等主机上部署防病毒软件或采用应用软件白名单技术，防范勒索病毒等造成的数据破坏攻击行为（BP.23.04）；
5) 原则上禁止工业控制系统面向互联网开通 HTTP、FTP、Telnet、RDP 等高风险通用网络服务，对必要开通的网络服务采取安全接入代理等技术进行用户身份认证和应用鉴权（BP.23.05）。

7.5.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：工业生产等相关核心业务部门应制订面向办公终端设备和工业终端设备的数据安全管理要求（BP.23.06）。

7.5.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
技术工具：

1) 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双因子身份鉴别（BP.23.07）；
2) 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（BP.23.08）；
3) 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（BP.23.09）；
4) 应对处理重要数据和核心数据的系统提供不低于 GB/T22239-2019 第三级要求的防护（BP.23.10）；

5) 处理重要数据和核心数据的系统与设备应符合国家密码应用的有关要求（BP.23.11）。

7.5.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

技术工具:

1) 应为进入内部网络环境的终端设备分配了终端识别号，并实现计算机终端设备与用户账号的一对一绑定，保障相关数据操作可溯源，应为进入内部生产网络环境的工业终端设备分配了终端识别号，记录登录的操作员或工程师账号，实现数据操作账号与终端识别号绑定，保障相关数据操作可溯源（BP.23.12）;

2) 工业生产等相关核心业务员工的终端设备均应实现员工和终端设备的绑定，并为终端设备安装了统一的防病毒软件，保护终端设备数据安全（BP.23.13）。

7.5.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设: 组织内应设立统一的终端设备、办公数据、工业生产数据安全管理岗位和人员（BP.23.14）。

b) 制度流程: 组织应明确面向办公终端设备和工业终端设备的数据安全管理规范，明确办公终端设备和工业终端设备的安全配置管理、使用终端数据的注意事项和数据防泄露管理要求等（BP.23.15）。

c) 技术工具:

1) 打印输出设备应采用身份鉴别、访问控制等手段进行安全管控，并对用户账户在此终端设备上的数据操作进行日志记录（BP.23.16）;

2) 组织内入网的办公终端设备和工业终端设备均应按统一的要求部署防护工具，如防病毒、硬盘加密、终端入侵检测等软件，并定期进行软件的更新，并将终端设备纳入组织整体的访问控制体系中（BP.23.17）;

3) 组织应部署终端数据防泄露方案，通过技术工具对办公终端设备和工业终端设备上数据以及生产监测、工业控制、工艺参数、计划数据等（涉及L0至L4各层）数据的操作进行风险监控（BP.23.18）;

4) 应提供整体的终端安全解决方案，实现终端设备与组织内部员工的有效绑定，按统一的部署标准在办公终端设备和工业终端设备系统上安装各类防控软件（如防病毒、硬盘加密、终端入侵检测等软件）（BP.23.19）;

5) 组织在工业控制设备上线前对其进行安全性检测，工业控制设备固件中不存在恶意代码程序（BP.23.20）;

d) 人员能力: 负责该项工作的人员应充分了解办公终端设备和工业终端设备的数据出入口以及相应的数据安全风险，能利用相应的工具实现整体的安全控制方案（BP.23.21）。

7.5.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 制度流程: 组织应定期对办公终端数据和工业终端数据防泄露解决方案的成效进行量化评估，评估新风险和需要调整的控制措施，量化提升组织整体的终端数据防泄露方案（BP.23.22）。

b) 技术工具：终端数据安全自动化工具应能够量化统计数据安全泄露风险，并将相关风险展示，为后续办公终端数据和工业终端数据安全管控能力提升提供技术支持（BP.23.23）。

7.5.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
技术工具：
a) 应基于组织内部终端环境的变化，利用人工智能等前沿技术实现对多终端环境的动态数据防泄露保护配置策略调整（BP.23.24）；
b) 应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.23.25）。

7.6 PA24 数据供应链安全

7.6.1 PA 描述

通过建立组织的数据供应链管理机制，防范组织上下游的数据供应过程中的安全风险。

7.6.2 等级描述

7.6.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：
a) 制度流程：宜明确供应链数据安全风险控制措施，以合同、协议等方式明确供应商、生产商、服务商等供应链主体的数据安全防护要求和责任落实要求（BP.24.01）。
b) 技术工具：对供应链管理系统的接入接口做好授权认证等保护措施（BP.24.02）。

7.6.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：在核心业务中，应与工业生产数据、经营管理数据等（涉及 L0 至 L4 各层）数据上下游的供应方针对具体的数据工业供应场景签署了合作协议，在合作协议中明确了数据的使用目的、供应方式、保密约定等（BP.24.03）。

7.6.2.3 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
a) 组织建设：应由实际存在工业生产数据、经营管理数据等（涉及 L0 至 L4 各层）数据上下游供应的业务团队相关人员负责数据供应链的管理工作（BP.24.04）。
b) 人员能力：负责该项过程的人员应具备对具体数据工业供应场景的风险评估能力（BP.24.05）。

7.6.2.4 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
a) 组织建设：应设置了组织整体的数据供应链安全管理岗位和人员，结合应用的 Modbus、Profinet、EtherNet 等协议情况和具体工业生产业务需要，负责制定整体的数据供应链管理要求和解决方案（BP.24.06）。
b) 制度流程：

1) 应明确数据供应链安全管理规范，定义工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链安全目标、原则和范围，明确数据供应链的责任部门和人员、数据供应链上下游的责任和义务以及组织内部的审核原则（BP.24.07）；
2) 组织应通过合作协议方式明确数据链中工业生产数据、经营管理数据等（涉及L0至L4各层）数据的使用目的、供应方式、保密约定、安全责任义务等（BP.24.08）；
3) 应明确针对工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应商的数据安全能力评估规范，根据该规范对数据供应商的数据安全能力进行评估，并将评估结果应用于供应商选择、供应商审核等供应商管理过程中（BP.24.09）。

c) 技术工具：应建立组织整体的数据供应链库，用于管理数据供应链目录和相关数据源数据字典，便于及时查看并更新组织上下游数据链路的整体情况，并用于事后追踪分析工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链上下游合规情况（BP.24.10）。
d) 人员能力：负责该项过程的人员应了解组织上下游工业生产数据、经营管理数据等（涉及L0至L4各层)数据供应链的整体情况，熟悉供应链安全方面的法规和标准，并具备推进供应链管理方案执行的能力（BP.24.11）。

7.6.2.5 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应定期对工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链上下游数据活动的安全风险和数据供应方的数据安全管理能力进行评估（BP.24.12）。
b) 技术工具：
1) 应通过技术工具量化组织整体的工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链情况，对组织上下游的数据供应需求、工业场景、对象和方式进行分类整理，能够及时发现并跟进数据供应链管理过程中的潜在风险（BP.24.13）；
2) 应对工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链上下游的数据服务提供者和数据使用者的行为进行合规性审核和分析（BP.24.14）；
3) 应基于工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链的相关记录，利用技术工具对数据供应链上下游的相关方开展安全审核和分析（BP.24.15）。

7.6.2.6 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：组织整体的工业生产数据、经营管理数据等（涉及L0至L4各层）数据供应链管理方案应能够使用人工智能等前沿技术根据国内外数据供应链管理领域的监管动态和行业实践对组织整体的数据供应链管理方案进行及时调整（BP.24.16）。
b) 技术工具：应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.24.17）。

7.7 PA25 数据分类分级

7.7.1 PA 描述

基于法律法规以及业务需求确定组织内部的数据分类分级方法，对生成或收集的数据进行分类分级标识。

7.7.2 等级描述

7.7.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：应定期梳理本企业数据，形成数据资产清单并定期更新（BP.25.01）。

7.7.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应根据工业企业业务特性和外部合规要求，对工业企业核心生产业务涉及的工艺参数、工业控制数据、生产监测数据、计划数据等工业生产数据和管理运营数据（涉及L0至L4各层）等进行分类分级管理（BP.25.02）。

7.7.2.3 精准防护级—重要预备要求

制度流程：

1) 应按照有关要求和标准规范识别重要数据和核心数据，形成本单位的具体目录，并进行重要数据和核心数据目录备案（BP.25.03）；
2) 备案内容发生重大变化的，应当在发生变化的三个月内履行备案变更手续。重大变化是指某类重要数据和核心数据规模（数据条目数量或者存储总量等）变化30%以上，或者其它备案内容发生变化（BP.25.04）。

7.7.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：应由工业生产和管理运营业务团队相关人员，根据工业企业数据分类分级工作要求（涉及L0至L4各层），负责开展对应工业生产和管理运营业务的数据分类分级工作（BP.25.05）。

7.7.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：
   1) 应对不同类别和级别的工业生产和管理运营等工业企业数据（涉及L0至L4各层）建立相应的访问控制、数据加解密、数据脱敏等安全管理和控制措施（BP.25.06）；
   2) 应明确工业企业数据分类分级变更审批流程和机制，通过该流程保证对数据分类分级的变更操作及其结果符合组织的工业生产和管理运营（涉及L0至L4各层）要求（BP.25.07）。
b) 技术工具：应建立工业企业数据分类分级打标或数据资产管理工具，实现对工业生产数据和管理运营数据等工业企业数据的分类分级自动标识、标识结果发布、审核

等功能（BP.25.08）。

7.7.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
技术工具：

a) 应记录自动分类分级结果与人工审核后的分类分级结果之间的差异（涉及 L0 至 L4 各层），定期分析改进分类分级标识工具，提升工具处理的准确度（BP.25.09）；
b) 应对工业企业数据分类分级的操作、变更过程进行日志记录和分析，定期通过日志分析等技术手段进行变更操作审计（主要涉及 L3、L4 层），实现工业企业数据分类分级可追溯（BP.25.10）。

7.7.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应定期评审工业企业数据分类分级的规范和细则（涉及 L0 至 L4 各层），考虑其内容是否完全覆盖了当前的工业生产等相关业务，并执行持续的改进优化工作（BP.25.11）；
b) 技术工具：应跟踪工业企业数据分类分级标识效果，应用人工智能等前沿技术持续改进（主要涉及 L3、L4 层）工业企业数据分类分级的技术工具（BP.25.12）。

7.8 PA26 安全风险评估

7.8.1 PA 描述

根据组织需符合的法律法规要求，保证组织业务的发展不会面临个人信息保护、重要数据保护等方面的安全治理风险。

7.8.2 等级描述

7.8.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：
制度流程：宜自行或委托第三方评估机构开展数据安全风险评估（BP.26.01）。

7.8.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：
制度流程：

1) 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（BP.26.02）。
2) 应在跨主体提供、转移、委托处理核心数据时开展安全风险评估（BP.26.03）。

7.9 PA27 日志留存

7.9.1 PA 描述

通过对日志留存提出相应要求，提升数据安全事件可追溯性。

7.9.2 等级描述

7.9.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程:

1) 应对数据处理日志、权限管理日志、人员操作日志等进行记录（BP.27.01）;
2) 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（BP.27.02）。

7.9.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程:

1) 应加强日志访问和处理管理（BP.27.03）;
2) 应对高风险操作（例如批量复制、批量传输、批量销毁等操作）日志进行备份（BP.27.04）。

7.10 PA28 监控与安全审计

7.10.1 PA 描述

针对数据全生命周期各阶段开展安全监控和审计，以保证对数据的访问和操作均得到有效的监控和审计，实现对数据未授权访问、数据滥用、数据泄露、数据篡改等安全风险的防控。

7.10.2 等级描述

7.10.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程: 宜对数据处理活动进行定期审计（BP.28.01）。

7.10.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程: 工业生产等核心业务应建立数据安全风控或审计监控相关规则，如对生产监测、工业控制、工艺参数、排产计划等（涉及L0至L4各层）数据访问和操作进行监控的方案（实时监控或定期批量监控等），并纳入定期审计范围（BP.28.02）。

7.10.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

技术工具: 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（BP.28.03）。

7.10.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设:应由业务团队相关人员负责对工业生产等业务数据的交换进行安全监控（BP.28.04）。
b) 制度流程:
   1) 应明确组织内部相关数据（工业控制、生产监测、排产计划、工艺参数、工单

指令、库存等数据）访问和操作日志的记录要求、安全监控要求和审计要求（涉及L0至L4各层），并遵照实施（BP.28.05）；

2) 应记录数据操作事件，制定数据安全风险行为识别和评估规则，并纳入审计依据（BP.28.06）。

c) 技术工具：

1) 应配备针对数据访问和操作的日志监控技术工具，实现数据异常访问和操作告警，特权账户对工业控制、工艺参数、生产计划等数据的访问和操作（主要涉及L2、L3、L4各层）应纳入重点监控范围（BP.28.07）；

2) 应部署必要的数据防泄露实时监控技术手段，监控并报告工业生产和管理运营等数据（涉及L0至L4各层）的跨域传输行为（BP.28.08）。

d) 人员能力：负责该项工作的人员应充分理解数据监控和审计的要求（BP.28.09）。

7.10.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

组织建设：组织应设立负责工业生产和管理运营数据监控审计的安全管理岗位，岗位人员负责明确各类数据监控和审计要求（涉及L0至L4各层），并推进相关要求的实施（BP.28.10）。

7.10.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 技术工具：

1) 应配备统一的数据访问和操作的日志监控技术工具，该工具应能够对相关数据（工业控制、生产监测、排产计划、工艺参数、工单指令、库存等数据）访问和操作日志进行统一处理和分析（涉及L0至L4各层），并量化数据访问和操作引发的数据安全风险，实现对数据安全风险的整体感知（BP.28.11）；

2) 应具备对相关数据（工业控制、生产监测、排产计划、工艺参数、工单指令、库存等数据）异常或高风险操作进行自动识别和实时预警的能力（涉及L0至L4各层）（BP.28.12）。

b) 人员能力：负责该项工作的人员应具备识别数据泄露风险的专业能力，并能够自行采取有效措施（BP.28.13）。

7.10.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：

a) 应利用数据分析技术改进日志监控技术工具，提升对安全风险事件发现的精确度和效率（BP.28.14）。

b) 应使用人工智能等前沿技术不断改进完善数据安全风险识别规则和模型，持续提升数据安全风险控制能力（BP.28.15）。

7.11 PA29 监测预警、信息共享与应急处置

7.11.1 PA 描述

建立针对数据的安全事件应急响应体系，对各类安全事件进行及时响应和处置。

7.11.2 等级描述

7.11.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下:

制度流程:

1) 应开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险，接到数据安全风险通报信息后，应及时处置风险并按要求反馈处置情况（BP.29.01）；
2) 应及时将可能造成较大及以上安全事件的风险向本地区行业监管部门报告（BP.29.02）；
3) 宜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（BP.29.03）；
4) 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（BP.29.04）；
5) 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（BP.29.05）；
6) 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（BP.29.06）；
7) 宜建立用户投诉处理机制（BP.29.07）。

7.11.2.2 基础建设级——一般增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

制度流程:工业生产等相关核心业务应明确数据安全事件管理和应急响应的策略和具体方案（BP.29.08）。

7.11.2.3 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 制度流程：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（BP.29.09）；
b) 技术工具：宜采用技术手段进行数据安全风险监测（BP.29.10）；

7.11.2.4 精准防护级—重要增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

组织建设:工业生产等相关核心业务应设立负责数据安全事件管理和应急响应的岗位和人员（BP.29.11）。

7.11.2.5 集成管控级—核心增强要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下:

a) 组织建设：组织应设立专职负责数据安全事件管理和应急响应的岗位和人员（BP.29.12）。
b) 制度流程:
   1) 应明确数据安全事件管理和应急响应工作指南，根据工业应用场景、数据类型、

数据级别和安全域等因素定义数据安全事件类型，明确不同类别事件的处置流程和方法（BP.29.13）；

2) 应明确数据安全事件应急预案，定期开展工业数据（涉及L0至L4各层）泄露应急演练活动（BP.29.14）；

3) 组织的数据安全事件应急响应机制，应符合国家有关主管部门的政策文件要求（BP.29.15）。

c) 技术工具：应建立统一的安全事件管理系统，对生产监测、工业控制、排产计划数据等（涉及L0、L1、L2、L3各层）日志、流量等内容进行关联分析（BP.29.16）。

d) 人员能力：负责该项工作的人员应具备安全事件的判断能力，熟悉工业场景安全事件应急响应措施（BP.29.17）。

7.11.2.6 综合协同级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

技术工具：安全事件管理系统应能够基于各工业层级（涉及L0至L4各层）发生安全事件分析的内容实现预警及自动化响应决策（BP.29.18）。

7.11.2.7 智能优化级

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

a) 制度流程：应使用人工智能等前沿技术辅助安全事件管理和应急响应机制动态调整、更新和完善，组织应定期对组织员工开展流程培训和宣贯（BP.29.19）。

b) 技术工具：应参与国际、国家或行业相关标准制定。在业界分享最佳实践，成为行业标杆（BP.29.20）。

7.12 PA30 数据出境

7.12.1 PA 描述

根据组织需符合的法律法规要求，保证组织跨境相关业务的发展不会面临个人信息保护、重要数据保护等方面的数据安全风险。

7.12.2 等级描述

7.12.2.1 基础建设级——一般预备要求

该等级的数据安全能力要求描述如下：

制度流程：

1) 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（BP.30.01）；

2) 应明确出境数据的名称、类型、数据接收方、安全保护措施等(BP.30.02)。

7.12.2.2 精准防护级—重要预备要求

在满足前序级别要求的基础上，该等级还应满足的数据安全能力要求描述如下：

制度流程：应根据法律法规要求，对需申报数据出境安全评估的情形按要求开展数据出境风险评估，向国家网信部门申报数据出境安全评估并获得批准（BP.30.03）。

附录 A

（规范性附录）

工业企业主要数据流向及数据安全风险框架

面向工业企业，提出了典型工业企业数据安全风险参考框架，分为 L0 现场设备层、L1 现场控制层、L2 过程监控层、L3 生产管理层和 L4 企业管理层 5 个层级，列举了 20 余类常见工业企业数据和 10 余类常见数据安全风险问题，如图 A.1 所示。

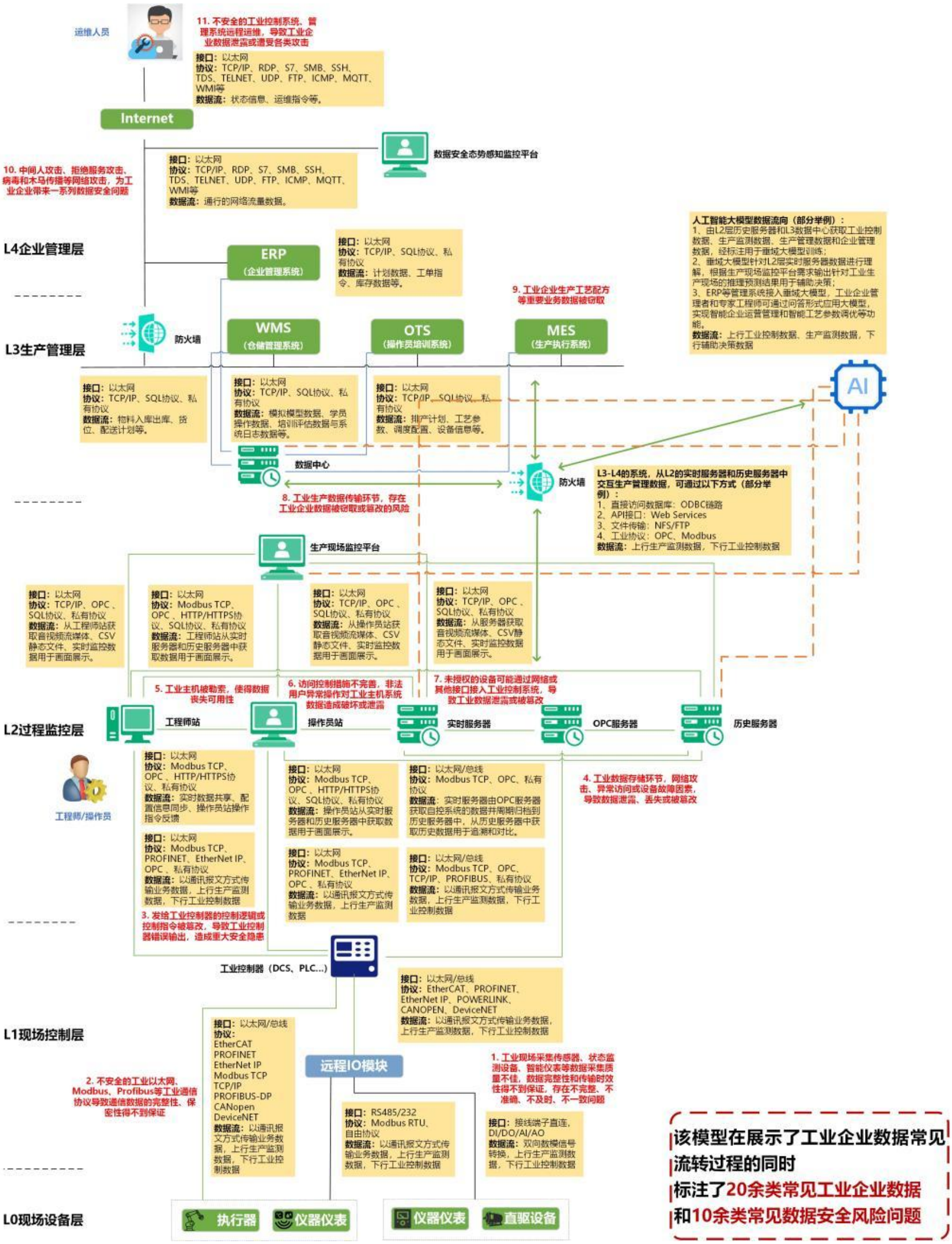

图 A.1 典型工业企业数据安全风险参考框架

各层级主要工业企业数据类型和常见数据安全风险问题如下表所示。

表 A.1 主要工业企业数据类型

序号	工业数据	主要涉及层级
1	生产监测数据	L0、L1、L2、L3
2	工业控制数据	L0、L1、L2、L3
3	工业现场监控音视频流媒体数据	L0、L1、L2
4	物料出库入库数据	L3
5	货位数据	L3
6	配送计划数据	L3
7	排产计划	L3
8	工艺参数	L1、L3
9	调度配置	L3
10	设备信息	L3
11	模拟模型数据	L3
12	学员操作数据	L3
13	培训评估数据	L3
14	系统日志数据	L3
15	计划数据	L4
16	工单指令	L4
17	库存数据	L4
18	系统状态信息	L4
19	运维指令	L4
20	辅助决策数据	L3、L4

表 A.2 常见数据安全风险问题

序号	数据安全风险	主要涉及层级
1	工业现场采集传感器、状态监测设备、智能仪表等数据采集质量不佳，数据完整性和传输时效性得不到保证，存在不完整、不准确、不及时、不一致问题	L0、L1
2	不安全的工业以太网、Modbus、Profibus 等工业通信协议导致通信数据的完整性、保密性得不到保证	L0、L1、L2
3	发给工业控制器的控制逻辑或控制指令被篡改，导致工业控制器错误输出，造成重大安全隐患	L1、L2
4	工业数据存储环节，网络攻击、异常访问或设备故障因素，导致数据泄露、丢失或被篡改	L2、L3、L4
5	工业主机被勒索，使得数据丧失可用性	L2
6	访问控制措施不完善，非法用户异常操作对工业主机系统数据造成破坏或泄露	L2
7	未授权的设备可能通过网络或其他接口接入工业控制系统，导致工业数据泄露或被篡改	L2
8	工业生产数据传输环节，存在工业企业数据被窃取或篡改的风险	L2、L3、L4

9	工业企业生产工艺配方等重要业务数据被窃取	L1、L3
10	中间人攻击、拒绝服务攻击、病毒和木马传播等网络攻击，为工业企业带来一系列数据安全问题	L1、L2、L3、L4
11	不安全的工业控制系统、管理系统远程运维，导致工业企业数据泄露或遭受各类攻击	L3、L4

附录 B

（规范性附录）

能力成熟度等级评估

工业企业数据安全能力成熟度等级评估方法采用“总体达标，单项合格”的思想开展，具体内容如下。

a) 为保证效果评估结果的公正和客观，采用基于证据的方式，须有证据支持每条细则的评估结果，证据包括：负责人谈话记录、制度文件、设备运行记录、现场核查结果和测试结果等。

b) 工业企业数据安全能力提升通过渐进的方式实现，即组织在达到低能力成熟度要求基础上，开展高能力成熟度等级的评估。

c) 一般预备要求、重要预备要求、核心预备要求中各适用 BP 总体通过率需为 100%。

d) 工业企业数据安全能力成熟度模型中除一般预备要求、重要预备要求、核心预备要求以外的各 BP 的权重相同，总体通过率需高于 80%。即，若假设某工业企业数据安全能力成熟度等级中，第 1 个~第 19 个过程类中组织适用的 BP（不包含一般预备要求、重要预备要求、核心预备要求中各 BP）数量为 N_1，N_2，…，N_{18}，各过程类中组织符合的 BP（不包含一般预备要求、重要预备要求、核心预备要求中各 BP）数量为 M_1，M_2，…，M_{18}，则当以下 2 个条件同时满足时，组织工业企业数据安全能力达到相应的成熟度等级：

1）（M1+M2+…+M18）/（N1+N2+…+N18）> 0.8；

2） Mi/Ni > 0.4 （0<i<20）。

附录 C

（规范性附录）

工业企业数据安全基线要求

为落实《中华人民共和国数据安全法》和《工业和信息化领域数据安全管理办法（试行）》中针对工业领域数据处理者提出的数据安全基线要求，**本《实践指南》对照 YD/T 4982-2024《工业企业数据安全防护要求》中针对一般数据、重要数据、核心数据提出的安全防护要求，分别在基础建设级、精准防护级、集成管控级中设置一般预备要求、重要预备要求和核心预备要求进行映射**（一般增强要求、重要增强要求和核心增强要求，是在对应预备要求基础上，提出的进一步拓展要求，不是基线要求的组成部分）。

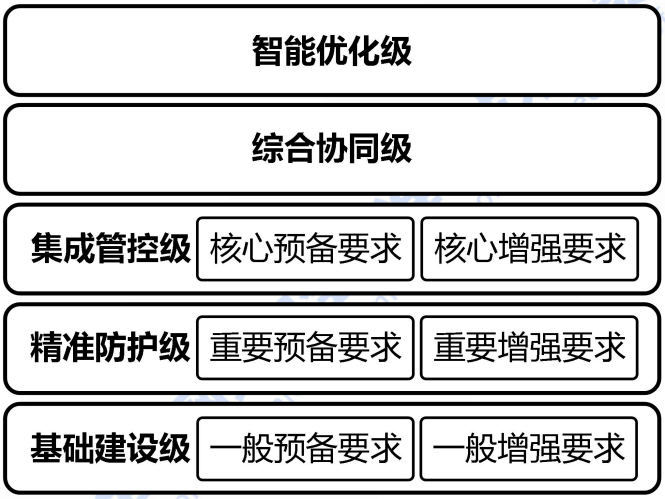

图 C.1 工业企业数据安全基线要求映射图

其中，基础建设级由一般预备要求和一般增强要求组成，结合工业领域数据分类分级防护需求，建议一般数据处理者以该级别及以上为目标开展数据安全能力建设工作。

精准防护级由重要预备要求和重要增强要求组成，结合工业领域数据分类分级防护需求，建议重要数据处理者以该级别及以上为目标开展数据安全能力建设工作。

集成管控级由核心预备要求和核心增强要求组成，结合工业领域数据分类分级防护需求，建议核心数据处理者以该级别及以上为目标开展数据安全能力建设工作。

参 考 文 献

[1] 中华人民共和国数据安全法
[2] 国令第 790 号　网络数据安全管理条例
[3] 工信部网安〔2022〕166 号　工业和信息化领域数据安全管理办法（试行）
[4] 工信部网安〔2024〕82 号　工业和信息化领域数据安全风险评估实施细则（试行）