ICS 35.020
CCS L70

DB21

辽 宁 省 地 方 标 准

DB XX/T XXXX—XXXX

数据管理能力 数据治理实施规范

Data management capability - Data management specification

（征求意见稿）

（本草案完成时间：2021-8-21）

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

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　总则 3
4.1　概述 3
4.2　基本原则 3
5　数据安全风险评估 3
5.1　数据场景分析 4
5.2　敏感数据分析 4
5.3　数据安全风险分析 4
6　数据安全策略制定 5
6.1　建立数据安全管理体系目标 5
6.2　识别数据安全管理及需求 5
6.3　建立数据安全组织体系 6
6.4　建立数据安全管理体系 6
6.5　建立数据安全技术体系 7
6.6　形成技术解决方案 13
6.7　建立数据安全运营体系 19
7　数据安全运营 20
7.1　数据合规及风险评估和监测 20
7.2　数据安全事故响应和处置 21
7.3　数据安全平台运营 22
7.4　数据安全事件分析与处理 22
7.5　安全体系监督、优化和持续改进 23
8　数据安全审计 23
8.1　规范审计 24
8.2　过程审计 24
8.3　合规审计 25
8.4　供应商审计 25
8.5　审计报告 26
8.6　数据安全建议 26
9　结语 27
参考文献 28

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：辽宁省工业和信息化发展研究院、鞍钢数智科技（辽宁）有限公司、国网辽宁省电力有限公司信息通信分公司、辽宁职业学院、沈阳化工大学、本溪钢铁（集团）信息自动化有限责任公司、中国工商银行股份有限公司辽宁省分行。

本文件主要起草人：姜胜海、张帅、李博文、王姝、高洋、吴庆、高强、徐鑫、黄健、关庆伟、张雪、刘洋等。

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。

本文件归口单位通讯地址：沈阳市北陵大街45-2号，联系电话：024-86913384

本文件起草单位通讯地址：沈阳市和平区太原北街2号综合楼A座10层，联系电话：024-88785218

数据管理能力 数据治理实施规范

1 范围

本文件提供了大数据环境下开展数据治理中数据安全管理实施指南，包括数据安全风险评估，数据安全策略制定，数据安全运营，数据安全审计。

本文件适用于指导组织和机构开展数据治理中数据安全管理工作。

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。

GT/T 35274—2023 数据安全技术 大数据服务安全能力要求

GB/T 44109—2024 信息技术 大数据 数据治理实施指南

GB/T 43679—2024 数据安全技术 数据分类分级规则

GB/T 34960.1—2017 信息技术服务 治理 第1部分：通用要求

GB/T 35295—2017 信息技术 大数据 术语

GB/T 36073—2018 数据管理能力成熟度评估模型

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态能力。

注：这些措施包括但不限于技术手段（如加密、访问控制、数据备份与恢复等）、管理措施（如制定安全策略、建立安全制度、明确人员职责等）以及物理措施（如数据中心的物理安全防护、存储设备的安全存放等）。

[来源：GT/T 35274 - 2023，3.17]

3.2

数据治理 data governance

对数据资源管理行使权力和控制的活动集合（计划、监督和执行）。这一过程涉及到多个层面和环节，包括数据战略规划（确定数据管理的目标和方向）、数据架构设计（构建合理的数据架构以支持业务需求）、数据质量管理（确保数据的准确性、完整性、一致性等）、数据安全管理（如本文件所重点阐述的内容）以及数据生命周期管理（对数据从产生到销毁的全过程进行管理）。

[来源：GB/T 44109-2024，3.1]

3.3

数据分类 data classification

按照数据的来源、内容、用途、格式、时效性等属性将数据分为不同的类别；例如，从来源角度可分为内部数据和外部数据；从内容角度可分为客户数据、业务数据、财务数据等；从用途角度可分为操

作数据、分析数据等；从格式角度可分为结构化数据、非结构化数据等；从时效性角度可分为实时数据、历史数据等。分类的目的是为了更好地组织和管理数据，便于后续的处理和分析。

3.4

数据分级 data grading

根据数据的敏感程度、重要性以及对组织的影响程度等因素，将数据划分为不同的级别。

注：分级过程需要综合考虑多方面因素，如数据泄露或损坏后对组织的财务状况、声誉、法律责任、业务运营等方面的影响。例如，高度敏感数据可能包括核心商业机密、客户隐私信息等；中度敏感数据可能包括一般性业务数据但对特定业务流程较为关键；一般敏感数据可能包括对业务影响较小的数据，但仍需适当保护。不同级别的数据应采取不同的安全措施进行保护，以确保数据的安全性和合规性。

3.5

数据加密 data encryption

采用特定算法对数据进行变换，使得只有授权用户能够通过相应的密钥还原数据。数据加密算法通常分为对称加密算法（如AES、DES等）和非对称加密算法（如RSA等）。对称加密算法使用相同的密钥进行加密和解密，速度较快但密钥管理相对复杂；非对称加密算法使用公钥和私钥进行加密和解密，密钥管理相对简单但速度较慢。在实际应用中，常常会结合使用这两种算法以达到更好的加密效果。同时，加密还涉及到密钥的生成、存储、分发和更新等环节，这些环节都需要严格的安全措施来保障，以防止密钥泄露导致数据安全问题。

3.6

数据脱敏 data masking

通过特定的算法和技术，对敏感数据进行处理，在保留数据原始特征和格式的前提下，隐藏或替换敏感信息，使得处理后的数据在不泄露隐私的情况下可用于测试、开发、分析等非生产环境的操作。

注：数据脱敏技术包括替换、随机化、加密等多种方法。例如，将客户姓名替换为虚拟姓名，将身份证号码部分数字替换为星号等。其目的是在满足业务需求的同时保护数据的隐私和安全性。

3.7

数据水印 data watermarking

一种将特定的标识信息嵌入到数据中的技术，这些标识信息可以是不可见的或对数据的正常使用影响极小。数据水印可用于数据的版权保护、溯源追踪以及验证数据的真实性和完整性。

注：如在图片数据中嵌入水印信息，当图片被非法传播时，可以通过提取水印来确定数据的来源和版权归属；在文本数据中嵌入水印，可以在数据被篡改时通过检测水印的变化来发现问题。

3.8

双因素认证 two-factor authentication

一种身份验证方法，要求用户在提供用户名和密码等常规凭证之外，还需提供另一种验证因素，以增加身份验证的安全性。第二种验证因素可以是基于用户拥有的物品（如动态口令牌、手机验证码等）或用户的生物特征（如指纹、面部识别等）。

注：双因素认证通过结合两种不同类型的验证因素，大大降低了身份被冒用的风险，提高了系统的安全性。

3.9

数据防泄漏 data leakage prevention

通过一系列技术手段和管理措施，防止敏感数据在未经授权的情况下从组织内部流出到外部环境，或者在组织内部的不同系统、部门之间被不当传播。数据防泄漏技术包括数据监控（实时监测数据的流动情况）、数据过滤（根据设定的规则过滤敏感数据）、数据屏蔽（对敏感数据进行屏蔽处理，使其在特定环境下不可见）等。同时，还需要建立相应的管理制度，如明确数据的访问权限、规范数据的传输流程等。

3.10

数据访问控制 data access control

通过设定规则和权限，对用户访问数据的行为进行限制和管理，确保只有经过授权的用户能够在授权范围内访问和使用相应的数据。

注：访问控制可以基于角色（如管理员、普通用户等）、基于属性（如数据的类别、级别等）或基于时间、地点等多种因素进行设定。例如，只有具有管理员角色的用户才能访问系统配置数据，普通用户只能在工作时间访问与自身业务相关的数据。

3.11

数据备份与恢复 data backup and recovery

将数据从原始存储位置复制到其他存储介质或位置，以防止数据因意外事件（如硬件故障、软件错误、人为失误、自然灾害等）而丢失或损坏。数据恢复则是指在数据丢失或损坏的情况下，利用备份数据将数据还原到原始状态或可使用状态的过程。

注：数据备份策略包括全量备份（备份所有数据）、增量备份（只备份自上次备份以来发生变化的数据）等。备份的存储位置可以是本地存储（如硬盘、磁带等）或异地存储（如远程数据中心、云存储等），以确保数据的安全性和可恢复性。

4 总则

4.1 概述

参考GB/T 44109-2024中数据安全管理要求对组织和机构其进行数据治理。数据安全管理活动包括数据安全风险评估、数据安全策略制定、数据安全运营、数据安全审计。

a) 数据安全风险评估:包括数据处理活动识别,数据安全风险源识别,数据安全风险分析等;
b) 数据安全策略制定:依据国家、行业等监管需求,结合自身的数据安全业务需要,制定适合的数据安全管理目标、原则和策略;
c) 数据安全运营:围绕数据应用过程中识别的风险,开展数据合规及数据安全风险与事件监测数据安全事件分析、数据安全事件响应和应急处置等,并进行数据安全平台运营、数据安全基线检查等;
d) 数据安全审计:包括过程审计、规范审计、合规审计、供应商审计、审计报告发布、数据安全建议。

4.2 基本原则

基本原则包括：

a) 合法合规原则。严格遵守国家和地方相关法律法规，以及行业标准和规范。组织和机构在进行数据处理活动时，必须获得必要的授权和许可，确保数据来源合法，使用目的正当，处理过程符合法律规定；
b) 最小必要原则。只收集、使用和存储为实现业务目的所必需的数据，避免过度收集和滥用数据；
c) 全程可控原则。对数据的全生命周期进行严格控制，从数据的产生到销毁，确保每一个环节都在可控范围内。建立数据访问控制机制，对数据的访问、修改、传输等操作进行严格授权和审计。

5 数据安全风险评估

5.1 数据场景分析

要求包括：

a) 业务系统梳理。组织和机构应对所持有业务系统进行全面梳理，详细记录每个业务系统的名称、功能、所涉及的数据类型和存储方式等信息。业务系统可包括：经营决策系统；运营管理系；智能制造系统；基础装备系统；

b) 数据处理活动。组织和机构应分析数据在不同业务系统中的处理活动，如数据的输入、输出、修改、删除等操作。针对每个业务系统，绘制数据处理流程图，清晰展示数据在系统内的流动路径和处理过程；

c) 数据流转整理。组织和机构应对内部以及与外部合作伙伴之间的数据流转情况进行全面整理。包括数据从哪个部门或系统流出，流向哪个部门或系统，以及在流转过程中所经过的中间环节（如数据传输通道、数据转换平台等）；

d) 数据流转地图绘制。根据数据流转整理的结果，绘制详细的数据流转地图。数据流转地图应直观展示数据的流转路径、涉及的部门和系统以及关键的控制节点（如数据审批环节、数据加密环节等）；

e) 数据分级分类规范建立。组织和机构应根据业务特点和数据敏感程度，制定详细的数据安全标准。数据分类应从业务的视角定义数据的分类体系，明确数据分类。可参考行业通用分类方法，并结合企业自身业务进行细化。例如，可分为客户类、财务类、技术类、运营类等。数据安全分级应在数据分级过程中根据数据遭到泄露或者损坏后对组织和机构、个人、公共利益和国家安全等方面的影响，明确组织及机构数据安全等级的划分。例如：可分为公开数据、一般数据、敏感数据、机密数据、绝密数据。

5.2 敏感数据分析

要求包括：

a) 敏感数据系统调研。对包含敏感数据的系统进行全面调研，确定敏感数据所在的系统名称、位置、存储方式以及访问控制机制等。例如，对于存储客户隐私信息的客户关系管理系统，调研其数据库架构、用户认证方式、数据加密情况等，以便全面了解敏感数据的安全状况；

b) 数据应用场景分析。分析敏感数据在不同业务场景中的应用情况，包括内部业务流程中的使用以及与外部合作伙伴的交互使用。例如，客户隐私信息在营销活动中的使用（用于精准营销）以及在与第三方物流企业合作时的共享情况（用于发货通知），分析在这些场景中可能存在的安全风险；

c) 敏感数据识别。根据数据场景分析结果和制定的数据分类分级标准，识别并标记敏感数据。宜采用自动化工具和人工审核相结合的方式，确保敏感数据识别的准确性和完整性。例如，利用数据标签技术对敏感数据进行标记，以便在数据处理过程中进行有效的监控和管理。

5.3 数据安全风险分析

要求包括：

a) 数据安全风险评估。根据数据场景分析结果，通过系统化的方法对数据安全风险的进行评估及赋值。在评估的过程中可采用定性和定量相结合的方法：定性评估可根据风险的可能性和影响程度进行分类，如高风险、中风险、低风险；定量评估可采用风险矩阵方法，计算风险值。
如，对于数据泄露风险，如果泄露可能性高且影响程度大，则评估为高风险；如果泄露可能性低且影响程度小，则评估为低风险；

b) 敏感数据流转风险分析。根据敏感数据分析结果，对所识别的敏感数据在流转过程中的风险进行分析，可包括数据泄露风险、数据篡改风险、数据丢失风险等。针对每种风险，分析其产生的原因（如网络攻击、内部人员违规操作等）和可能造成的后果（如企业声誉受损、经济损失、法律责任等），同时形成数据安全风险评估表。例如，敏感数据在通过互联网传输给外部合作伙伴时，可能存在被网络攻击窃取的风险，一旦泄露，可能导致客户隐私泄露，企业面临法律诉讼和声誉受损的风险。

6 数据安全策略制定

6.1 建立数据安全管理体系目标

a) 短期目标

1) 确定重点问题：组织相关部门（如数据安全管理部门、业务部门等）进行数据安全现状评估会议。通过对近期数据安全事件的回顾、现有安全措施的有效性分析以及业务需求的梳理，确定如数据泄露风险较高等重点问题；

2) 明确具体指标：制定详细的数据加密和访问控制计划。对于数据加密比例提高的指标，明确计算加密比例的方法（如加密数据量占总数据量的百分比），以及如何通过技术手段（如加密软件的部署和配置）和管理措施（如对加密数据的定期检查和更新）来实现。对于降低未授权访问次数的指标，确定如何通过访问控制技术（如设置用户权限、IP 限制等）和监控机制（如实时监测访问日志）来达成。

b) 长期目标

1) 制定战略目标：由组织的高层管理人员（如 CEO、CTO 等）牵头，结合组织的战略发展规划，考虑数据安全在未来的重要性和影响，制定如建立完善的数据安全管理体系，使数据安全管理达到行业领先水平的长期目标；

2) 分解目标任务：组织数据安全专家和相关部门负责人召开目标分解会议。针对长期目标，如在未来一年内完成数据安全组织体系的建设，明确每个阶段的具体任务，包括人员招聘和培训计划、组织架构的设计和搭建等；对于未来两年内完成数据安全技术体系的建设，确定技术选型、研发计划和项目进度安排等，并设定相应的时间节点。

6.2 识别数据安全管理及需求

a) 关注法律法规

1) 了解国家法规更新：安排专人（如法务人员或数据安全管理人员）负责关注国家相关法律法规的动态，订阅相关的法规资讯服务，及时获取《中华人民共和国数据安全法》等法规的更新情况，并向组织内部相关人员传达；

2) 研究地方政策要求：针对地方政府出台的有关数据安全监管政策和指导意见，组织专题研究会议，分析政策对组织业务的影响，确保组织的行为符合当地政策要求，如确定需要满足的特定数据安全标准和报告义务等；

b) 结合自身业务；

1) 分析业务特点需求：由业务部门和数据安全管理部门共同开展业务分析工作。例如对于金融机构，详细分析客户资金信息的流转过程、存储方式和使用场景，确定其安全需求，如需要对客户资金信息采用高级加密技术和严格的访问控制措施；对于医疗行业，深入了解患者隐私信息在各个业务环节的处理情况，明确对其保护的重点和要求；

2) 确定重点保护数据：根据业务需求，制定重点保护数据清单。明确需要重点保护的数据类型（如金融机构的客户资金信息、医疗行业的患者隐私信息等）以及相应的安全措施（如加密技术、访问控制等），并确保清单随着业务发展和数据变化及时更新。

6.3 建立数据安全组织体系

a) 确定岗位角色

1) 设置岗位：根据组织和机构的数据安全管理需求，确定需要设置的数据安全管理员、数据安全审计员等岗位。明确各岗位的职责和权限，如数据安全管理员负责数据的日常安全管理，包括数据的加密、备份、访问控制等操作的实施和监督；数据安全审计员负责对数据安全管理进行审计，检查各项安全制度和措施的执行情况；

2) 明确职责：制定详细的岗位说明书，对每个岗位的职责进行详细描述。例如，数据安全管理员的岗位说明书应包括对数据加密算法的选择和应用、数据备份策略的制定和执行、访问控制规则的设置和维护等职责；数据安全审计员的岗位说明书应涵盖审计计划的制定、审计方法的选择、审计结果的报告和跟踪等职责。

b) 培养专业能力

1) 制定培训计划：由人力资源部门和数据安全管理部门共同制定员工培训计划。针对数据安全管理员，提供包括数据加密技术、访问控制技术、数据备份与恢复技术等在内的培训课程；对于数据安全审计员，提供审计方法、审计工具使用、数据安全法规等方面的培训课程。培训计划应明确培训的时间、地点、培训师以及培训方式（如内部培训、外部培训、在线培训等）；

2) 鼓励专业认证：鼓励员工参加相关的专业考试和认证，如 CISA（注册信息系统审计师）考试。制定相应的激励措施，如对通过认证的员工给予奖金、晋升机会等，提高员工的专业水平。

6.4 建立数据安全管理体系

a) 制定策略

1) 制定目标策略：明确数据安全管理的目标和方向，如确保数据的保密性、完整性和可用性。制定详细的目标实现计划，包括如何通过技术手段（如加密、访问控制等）和管理措施（如制定安全制度、加强人员培训等）来确保数据的保密性；如何通过数据冗余、校验和等技术以及数据备份制度来确保数据的完整性；如何通过建立高可用的系统架构和故障恢复机制来确保数据的可用性；

2) 制定风险策略：采用定性和定量相结合的方法评估风险。定性评估方面，制定风险评估标准，如根据风险发生的可能性（高、中、低）和影响程度（高、中、低）对风险进行分类；定量评估方面，介绍风险矩阵方法的具体应用，如确定风险值的计算方法（风险值 = 可能性×影响程度），并根据风险值对风险进行排序和管理。根据评估结果，制定相应的防范措施，如对于高风险的情况，采取强化安全措施（如增加加密强度、严格访问控制等）；对于中风险的情况，进行定期监测和优化措施；对于低风险的情况，保持关注并进行一般性的预防措施；

3) 制定技术策略：选择合适的技术手段来保障数据安全。例如，对于数据加密，根据数据的重要性和敏感性选择不同的加密算法（如 AES 加密算法用于重要数据）；对于访问控制，采用基于角色的访问控制（RBAC）模式，根据用户的角色和权限分配访问权限；对于数据传输安全，采用 SSL/TLS 协议等技术；

4) 制定运营策略：对数据安全运营进行规划和管理。建立数据安全风险与事件监测机制，明确监测的内容（如数据的完整性、保密性和可用性等方面的风险）、监测的方式（如通过自动化监测工具和人工巡检相结合）以及监测的频率（如实时监测关键数据和系统，定期监测一般数据和系统）。

b) 建立制度

1) 建立责任制度：明确各个岗位在数据安全管理中的责任。制定详细的责任制度文档，如规定数据安全管理员对数据的安全负责，包括对数据的加密、备份、访问控制等方面的安全负责；数据安全审计员对审计结果负责，包括对审计报告的准确性、完整性和及时性负责；

2) 建立审计制度：规范审计的流程和标准。明确审计的周期（如每月、每季度或每年进行一次审计），审计的内容（如对数据安全管理体系的各项制度和措施的执行情况进行审计），审计的方法（如采用内部审计、外部审计或二者相结合的方式，通过查阅文档、检查系统、访谈人员等方法进行审计）；

3) 建立备份制度：保障数据的安全备份。确定数据备份的频率（如每天、每周或每月进行一次备份），备份的方式（如全量备份、增量备份等），备份的存储地点（如本地存储、异地存储或二者相结合），并制定备份恢复测试计划，定期对备份数据进行恢复测试，确保备份数据的可用性；

4) 建立访问制度：规范数据的访问行为。明确谁可以访问哪些数据（如根据用户的角色和权限分配访问权限），在什么条件下可以访问（如通过身份验证、授权等方式），以及访问的记录和审计要求（如对所有的访问操作进行记录，并定期进行审计）。

6.5 建立数据安全技术体系

6.5.1 数据采集阶段

a) 技术要点

1) 数据源认证与授权

- 采用多种认证方式相结合，如数字证书、生物识别技术（如指纹识别、面部识别等）以及传统的用户名和密码组合，增强数据源身份认证的安全性和准确性；
- 建立动态授权机制，根据数据源的实时状态、数据类型和采集频率等因素，自动调整授权权限，确保数据采集的合法性和安全性，同时提高数据采集的效率；
- 实施访问令牌管理，为每个经过认证的数据源颁发唯一的访问令牌，令牌具有时效性和权限范围限制，数据源在进行数据采集操作时需携带令牌，以便系统进行验证和授权。

2) 数据质量评估与清洗技术

- 运用数据质量评估工具对采集到的数据进行多维度检测，除了准确性、完整性、一致性外，还包括数据的时效性、可靠性等指标。例如，对于实时数据采集，要重点关注数据的时效性，确保采集到的数据是最新的；
- 采用智能数据清洗算法，能够自动识别和处理数据中的异常值、缺失值和重复值。例如，通过机器学习算法对数据模式进行学习，从而更准确地判断异常值并进行合理的处理，如采用数据插值法或基于模型的预测值来填充缺失值；
- 建立数据质量反馈机制，将数据质量评估结果及时反馈给数据源，促使数据源改进数据质量，形成数据质量提升的闭环管理。

3) 隐私保护技术

- 在数据采集过程中，应用差分隐私技术，对数据添加适量的噪声，使得在不泄露个体数据隐私的前提下，仍能进行有效的数据分析。例如，在统计数据采集时，通过差分隐私算法对数据进行处理，保证统计结果的可用性，同时保护个体数据的隐私；
- 采用同态加密技术，在数据加密的状态下进行某些特定的运算，如求和、平均值计算等，无需解密数据即可得到正确的结果，最大限度地保护数据在采集和传输过程中的隐私安全。

b) 实施策略

1) 制定全面的数据源认证规范

- 详细规定不同类型数据源的认证方式选择标准，例如对于高风险数据源应优先采用生物识别技术和数字证书相结合的认证方式；
- 明确认证流程中的各个环节，包括申请、审核、颁发证书或令牌等步骤的具体操作流程和时间限制，确保认证过程的高效性和规范性；
- 建立认证责任追究制度，对于因认证不当导致的数据安全问题，明确相关责任人的处罚措施，提高认证工作的严谨性。

2) 建立高效的数据质量监控与清洗体系

- 搭建实时数据质量监控平台，利用大数据技术对海量采集数据进行实时监测和分析，及时发现数据质量问题；
- 制定数据清洗计划，根据数据质量问题的严重程度和类型，自动选择合适的清洗算法进行处理，并记录清洗过程和结果，以便后续追溯和分析；
- 定期对数据质量监控和清洗工作进行评估和优化，根据业务需求和数据特点调整评估指标和清洗算法，提高数据质量保障能力。

3) 加强隐私保护技术培训与宣传

- 组织数据采集人员参加隐私保护技术培训课程，邀请专家进行授课，详细讲解差分隐私、同态加密等先进技术的原理和应用场景，提高人员的技术水平；
- 开展内部宣传活动，通过海报、邮件、内部培训等方式，向全体员工普及隐私保护的重要性和相关法律法规要求，增强员工的隐私保护意识；
- 在与数据源合作时，明确隐私保护要求和责任，签订隐私保护协议，确保数据源在数据采集过程中也遵循相关隐私保护规定。

6.5.2 数据存储阶段

a) 技术要点

1) 访问控制技术

- 引入基于风险的访问控制（RBAC）模型，除了考虑用户角色和职责外，还结合用户行为风险评估结果动态调整访问权限。例如，当系统检测到用户的操作行为异常时，自动降低其访问权限或进行二次认证；
- 实施基于属性的访问控制（ABAC）时，利用人工智能技术对数据属性和用户属性进行智能分析和匹配，提高授权的准确性和灵活性。例如，通过机器学习算法自动学习数据的敏感属性和用户的安全需求，实现更加精细化的访问控制；
- 采用零信任访问控制策略，默认不信任任何访问请求，对每次数据访问都进行严格的身份验证和授权检查，即使是在内部网络环境中也不例外，有效防止内部威胁。

2) 数据加密技术

- 采用分层加密技术，对不同敏感度级别的数据进行不同层次的加密。例如，对于核心机密数据采用高强度的加密算法进行深层次加密，而对于一般敏感数据则采用相对较弱但效率较高的加密算法进行加密，以平衡数据安全性和存储性能；
- 应用加密密钥分层管理，将主密钥和工作密钥分开管理，主密钥用于加密和解密工作密钥，工作密钥用于实际的数据加密和解密操作，提高密钥管理的安全性和效率；
- 实现加密与存储系统的无缝集成，确保数据在存储过程中自动进行加密，减少人工干预带来的安全风险，同时提高数据存储的效率和安全性。

3) 数据备份与恢复技术

- 建立多云备份策略，将数据备份到多个不同的云服务提供商平台，以降低单一云平台故障导致数据丢失的风险。同时，利用云平台的弹性扩展能力，根据数据量的变化动态调整备份资源；
- 采用增量备份与差异备份相结合的方式，在减少备份数据量的同时，提高备份效率和恢复速度。例如，每周进行一次全量备份，每天进行增量备份或差异备份，根据数据变化情况灵活选择；
- 测试备份数据的完整性和可用性，定期进行恢复演练，模拟各种灾难场景，确保在实际发生数据丢失或损坏时能够快速、准确地恢复数据，满足业务连续性要求。

b) 实施策略

1) 构建先进的访问控制体系

- 对组织内的用户行为数据进行收集和分析，建立用户行为风险评估模型，为基于风险的访问控制提供数据支持；
- 完善ABAC的属性管理系统，确保数据属性和用户属性的准确采集和及时更新，为智能授权提供基础；
- 制定零信任访问控制策略的实施细则，包括网络架构调整、身份验证机制强化等方面的具体措施，逐步推进零信任架构的应用。

2) 实施完善的数据加密方案

- 评估数据的敏感度级别，制定相应的加密策略和算法选择标准，确保加密强度与数据安全需求相匹配；
- 建立加密密钥管理系统，采用硬件安全模块（HSM）等安全设备来存储和管理主密钥，提高密钥的安全性；
- 与存储系统供应商合作，推动加密技术与存储系统的深度集成，确保数据存储过程中的加密自动化和无缝化。

3) 优化数据备份与恢复体系

- 筛选可靠的云服务提供商，签订详细的服务协议，明确数据备份和恢复的责任和义务，确保多云备份策略的顺利实施；
- 制定增量备份和差异备份的计划和操作规程，根据数据变化规律合理安排备份时间和频率，优化备份资源的使用；
- 建立恢复演练制度，定期组织相关人员进行恢复演练，记录演练过程和结果，对发现的问题及时进行整改和优化。

6.5.3 数据传输阶段

a) 技术要点

1) 加密传输技术

- 采用量子加密技术，利用量子力学的基本原理实现密钥的安全分发和数据的加密传输，确保传输过程的绝对安全性，抵御未来可能出现的量子计算攻击；
- 应用自适应加密算法，根据网络状况、数据类型和传输要求等因素自动调整加密强度和方式，在保证数据安全的前提下提高传输效率；
- 建立加密传输隧道的实时监测和维护机制，及时发现和解决隧道中断、密钥泄露等问题，确保加密传输的稳定性和可靠性。

2) 网络隔离技术

- 实施微隔离技术，将网络进一步细分为更小的安全区域，对每个区域内的数据流进行精细化控制和隔离，有效防止横向移动攻击。例如，在企业内部网络中，将不同部门的服务器和终端设备划分到不同的微隔离区域，限制区域之间的不必要访问；
- 利用软件定义网络（SDN）技术实现动态网络隔离，根据业务需求和安全策略实时调整网络拓扑和访问控制规则，提高网络隔离的灵活性和适应性；
- 建立网络隔离的安全审计机制，对网络隔离设备的配置变更、访问日志等进行审计，及时发现和防范潜在的安全风险。

3) 传输监控与审计技术

- 利用大数据分析技术对传输监控数据进行深度分析，挖掘潜在的安全威胁和异常行为模式。例如，通过对大量传输数据的流量分析、协议分析等，发现异常的网络连接和数据传输行为；
- 实现传输监控与审计系统的智能化告警，当检测到异常情况时，能够自动根据预设的规则和风险级别进行分类告警，并及时通知相关人员进行处理；
- 建立传输监控与审计数据的长期存储和分析机制，以便对历史数据进行回溯和分析，为安全事件调查和防范提供有力支持。

b) 实施策略

1) 推动加密传输技术创新应用

- 研究和探索量子加密技术在实际数据传输中的应用场景和可行性，与相关科研机构和企业合作，开展试点项目，逐步推广量子加密技术的应用；
- 选择支持自适应加密算法的传输协议和工具，对网络环境和数据传输情况进行实时监测，根据监测结果自动调整加密参数，优化传输性能；
- 建立加密传输隧道的运维团队，负责隧道的日常监测、维护和故障排除，制定应急预案，确保在出现问题时能够快速响应和解决。

2) 加强网络隔离技术部署与管理

- 对网络架构进行全面评估，根据业务需求和安全要求规划微隔离区域，制定详细的微隔离策略和实施计划；
- 部署SDN控制器和相关设备，实现网络的软件定义和动态管理，与安全策略管理系统集成，确保网络隔离策略的及时更新和有效执行；
- 定期对网络隔离设备和策略进行审计，检查配置的合规性和有效性，及时发现和纠正存在的问题，加强网络隔离的安全性。

3) 完善传输监控与审计体系建设

- 搭建基于大数据平台的传输监控与审计系统，整合和分析来自多个数据源的监控数据，提高安全威胁检测的准确性和全面性；
- 制定智能化告警规则和流程，根据安全事件的严重程度和影响范围，确定不同级别的告警方式和响应时间要求，确保相关人员能够及时收到告警信息并采取相应措施；

- 投资建设数据存储设施，用于长期存储传输监控与审计数据，建立数据分析模型和工具，定期对历史数据进行分析和总结，为网络安全优化提供依据。

6.5.4 数据使用阶段

a) 技术要点

1) 身份认证与授权管理

- 引入多模态身份认证技术，结合多种认证因素，如密码、生物特征、行为特征等，进行用户身份认证。例如，通过分析用户的打字速度、鼠标操作习惯等行为特征，作为身份认证的辅助因素，增强认证的安全性和准确性；
- 实施基于区块链的授权管理，利用区块链的不可篡改和分布式特性，实现授权信息的安全存储和透明管理。用户的授权记录被记录在区块链上，任何授权变更都可追溯且不可篡改，确保授权管理的公正性和安全性；
- 建立实时权限监控系统，对用户的数据使用权限进行实时监测和分析，当发现用户的操作超出其权限范围时，及时进行预警和阻止，防止权限滥用。

2) 数据脱敏技术

- 采用动态数据脱敏技术，根据用户的角色、权限和数据使用场景，实时对敏感数据进行脱敏处理。例如，在数据分析场景中，不同级别的分析师可以看到不同程度脱敏后的数据，高级分析师可以看到更详细的数据，而普通分析师只能看到经过高度脱敏的数据；
- 应用数据脱敏算法的组合策略，针对不同类型的敏感数据选择合适的脱敏算法进行组合处理，提高脱敏效果和数据的可用性。例如，对于姓名、地址等文本型敏感数据，可以采用替换和模糊化相结合的算法；对于身份证号码、银行卡号等数字型敏感数据，可以采用部分掩码和加密相结合的算法；
- 建立脱敏数据的质量评估机制，定期对脱敏后的数据进行质量检查，确保脱敏后的数据满足业务需求和数据质量标准，避免因脱敏导致数据失真或不可用。

3) 数据防泄漏技术

- 利用人工智能技术进行数据防泄漏，通过机器学习算法对大量的正常数据使用行为和异常泄漏行为进行学习和建模，实时监测用户的数据操作行为，及时发现潜在的数据泄漏风险。例如，当用户的操作行为与已建立的正常行为模型不符时，系统自动发出警报；
- 部署数据水印技术，在数据中嵌入不可见的水印信息，当发生数据泄漏事件时，可以通过提取水印信息追溯数据的来源和泄漏路径，为数据泄漏事件的调查和取证提供有力支持；
- 建立数据防泄漏的应急响应机制，制定详细的应急预案，当检测到数据泄漏风险或事件时，能够迅速启动应急响应流程，采取措施阻止数据泄漏的进一步扩大，同时进行事件调查和处理。

b) 实施策略

1) 强化身份认证与授权管理体系

- 选择可靠的多模态身份认证技术供应商，集成多种认证方式到应用系统中，制定统一的认证接口和流程，提高用户体验；
- 搭建区块链授权管理平台，与现有业务系统进行对接，将授权管理流程迁移到区块链上，确保授权信息的安全和可信；
- 开发实时权限监控系统，与业务系统紧密集成，实时获取用户的操作行为数据，进行权限比对和分析，及时发现异常情况并进行处理。

2) 优化数据脱敏技术应用与管理

- 评估业务系统的数据使用场景和用户需求，制定动态数据脱敏的策略和规则，确保脱敏效果符合不同场景的要求；
- 对不同类型的敏感数据进行分类研究，选择最佳的脱敏算法组合，并进行测试和优化，提高脱敏数据的质量和可用性；
- 建立定期的数据质量评估机制，对脱敏后的数据进行抽样检查和质量评估，根据评估结果调整脱敏策略和算法，保证数据质量。

3) 提升数据防泄漏能力建设

- 引进先进的人工智能数据防泄漏解决方案，进行定制化开发和训练，使其适应企业的业务环境和数据特点；
- 选择合适的数据水印技术产品，按照数据安全要求和业务流程，将水印嵌入到关键数据中，并建立水印检测和提取机制；
- 制定数据防泄漏应急预案，明确应急响应团队的职责和分工，定期进行应急演练，提高应急响应能力和处理效率。

6.5.5 数据销毁阶段

a) 技术要点

1) 数据彻底删除技术

- 采用物理删除与逻辑删除相结合的方式，先进行逻辑删除标记，在经过一定的保留期后，再进行物理删除，确保数据无法恢复。例如，对于一些需要留存一定时间以备审计的数据，先进行逻辑删除，在审计期结束后再进行物理删除；
- 应用数据销毁验证技术，在数据删除后，通过数据恢复工具或技术对存储介质进行扫描，验证数据是否已被彻底删除，确保数据销毁的可靠性；
- 建立数据销毁记录的加密存储和备份机制，对数据销毁的时间、方式、操作人员等信息进行详细记录，并进行加密存储和备份，以便日后审计和追溯。

2) 介质销毁技术

- 采用专业的介质销毁设备，如硬盘粉碎机、消磁机等，对存储介质进行物理销毁，确保介质上的数据无法被恢复。对于不同类型的介质，选择合适的销毁设备和方法，确保销毁效果；
- 在介质销毁前，进行数据备份和清理，确保介质上的数据已不再需要且已进行了妥善备份。同时，对介质进行标识和登记，记录介质的基本信息、使用历史和销毁情况；
- 建立介质销毁的监督和审计制度，对介质销毁过程进行全程监督，确保销毁操作符合规定和标准。销毁后，对销毁结果进行审计和验证，出具销毁报告，并存档备查。

b) 实施策略

1) 制定严谨的数据销毁流程和规范

- 明确数据销毁的触发条件和审批流程，例如根据数据的存储期限、法律法规要求或业务需求确定是否销毁数据，销毁数据需经过相关部门和负责人的审批；
- 制定详细的数据销毁操作指南，包括物理删除和逻辑删除的具体步骤、工具使用方法、销毁验证流程等，确保操作人员能够按照规范进行操作；
- 规定数据销毁记录的管理要求，包括记录的格式、内容、存储期限、加密方式等，确保记录的安全性和可追溯性。

2) 加强介质销毁管理与监督

- 投资购买专业的介质销毁设备，并定期进行维护和检测，确保设备的正常运行和销毁效果；

- 建立介质管理制度，对介质的采购、使用、存储、销毁等环节进行全程管理，确保介质的安全和可追溯；
- 培训介质销毁操作人员，使其熟悉介质销毁设备的操作方法和安全注意事项，严格按照规定进行介质销毁操作。同时，加强对介质销毁过程的监督和审计，定期检查销毁记录和报告，确保介质销毁工作的合规性和有效性。

6.6 形成技术解决方案

6.6.1 数据标识

a) 方案概述

构建全面且规范的数据标识体系，为每一个数据实体赋予独一无二的标识符，确保其在复杂的数据环境中具有明确的身份识别。该标识符不仅要在数据的全生命周期内保持稳定，还需具备足够的灵活性，以适应数据的动态变化和不断增长的规模。通过数据标识，能够实现高效的数据管理、精准的追踪以及快速的定位，为数据治理和安全保障提供基础支撑。

b) 技术实现

1) 选用先进的标识符生成算法，如符合国际标准的通用唯一识别码（UUID）。UUID 具有高度的唯一性和随机性，能够有效避免标识符冲突。同时，利用分布式标识符生成技术，确保在大规模分布式系统中也能生成唯一且连续的标识符；
2) 在数据存储层面，无论是关系型数据库还是非关系型数据库，都应在相应的数据表结构中设立专门的标识字段。对于文件系统中的数据文件，可将标识符嵌入到文件的元数据部分，确保在文件操作过程中标识符始终与数据紧密关联。在数据传输过程中，通过在数据包头或协议字段中携带标识符，实现数据传输的可追踪性和准确性。

c) 应用场景

1) 在数据治理平台中，数据标识作为核心元素，用于整合和管理各类数据资产。通过标识符，能够快速检索和查询数据资产信息，实现数据的分类、统计和分析。例如，在数据目录编制过程中，依据数据标识对数据进行分类梳理，方便用户快速定位所需数据；
2) 在数据共享和交换场景中，数据标识发挥着关键作用。发送方在发送数据时，将标识符与数据一同传输，接收方可以根据标识符准确识别和接收数据，避免数据混淆和错误处理。同时，标识符还可用于数据传输的验证和审计，确保数据传输的完整性和准确性。

6.6.2 数据分类分级

a) 方案概述

依据数据的内在属性、价值含量、敏感程度以及对业务的影响程度等多维度因素，制定科学合理的数据分类分级标准和规范。通过对数据进行准确分类和分级，能够有针对性地为不同类型和级别的数据制定差异化的安全保护策略和管理措施，实现数据的精细化管理和安全保障。

b) 技术实现

1) 借助机器学习和自然语言处理技术，实现数据的自动分类。首先，收集大量已标注类别的数据样本，构建分类模型训练数据集。然后，运用深度学习算法，如卷积神经网络（CNN）或循环神经网络（RNN），对文本、图像、音频等不同类型的数据进行特征提取和学习。通过不断训练和优化模型，使其能够自动识别数据中的关键信息和特征模式，从而将数据准确划分到相应的类别中；
2) 对于数据分级，采用定性与定量相结合的综合评估方法。定性方面，考虑数据的保密性要求，如涉及国家秘密、商业机密、个人隐私等不同级别的保密程度；评估数据的完整性需

求，即数据的准确性、一致性和可靠性要求；分析数据的可用性影响，如数据不可用对业务运营造成的损失程度。定量方面，通过建立数据价值评估模型，综合考虑数据的产生成本、使用频率、对业务收入的贡献等因素，为数据赋予量化的价值指标。再结合数据泄露可能引发的经济损失、社会影响等风险因素，最终确定数据的级别。

c） 应用场景

1） 在数据存储环节，根据数据的分类分级结果，选择适配的存储设备和存储方式。对于高级别敏感数据，采用具有更高安全性的加密存储设备，并实施更为严格的访问控制和备份策略。例如，将核心业务数据存储在具备硬件加密功能的存储阵列中，并定期进行异地备份。对于低级别数据，可以选择成本较低的存储介质，但仍需确保基本的数据安全防护；

2） 在数据访问控制方面，依据数据级别精细设置访问权限。对高级别数据，仅授权给具有特定安全级别和业务需求的关键人员访问，并实施多因素身份认证和严格的审计机制。对于中级别数据，根据用户的角色和职责分配相应的访问权限，确保数据的合理使用。对于低级别数据，可适当放宽访问限制，但仍需进行基本的身份验证和操作记录。

6.6.3 数据加密

a） 方案概述

运用加密算法对数据进行转换处理，将明文数据变为密文形式，从而有效保护数据在存储、传输和使用过程中的机密性，防止数据被非法窃取、篡改或泄露。加密技术应覆盖数据的整个生命周期，确保数据在任何环节都处于安全状态。

b） 技术实现

1） 精心挑选合适的加密算法，以满足不同场景的安全需求。对于大量数据的快速加密处理，可采用对称加密算法，如高级加密标准（AES）。AES 算法具有加密速度快、安全性高的优点，适用于对数据存储和批量数据传输的加密。在密钥交换和数字签名等场景，非对称加密算法如 RSA 更为适用。RSA 算法基于公钥和私钥的配对机制，能够实现安全的密钥分发和身份认证。此外，对于一些特殊场景，如对实时性要求较高的视频流加密，可考虑采用轻量级加密算法。

2） 构建完善的密钥管理系统，保障加密密钥的全生命周期安全。在密钥生成环节，采用随机数生成器生成高质量的密钥，确保密钥的随机性和不可预测性。密钥存储方面，利用硬件安全模块（HSM）或加密文件系统等安全存储设备，对密钥进行加密存储，防止密钥泄露。密钥分发过程中，采用安全的通信通道和密钥交换协议，确保密钥准确无误地传递到授权用户手中。同时，定期对密钥进行更新和轮换，降低密钥被破解的风险。

c） 应用场景

1） 在网络数据传输过程中，如通过互联网进行文件上传下载、在线视频播放、即时通讯等应用场景，对数据进行实时加密。在数据发送端，使用加密算法对数据进行加密处理后再进行传输，接收端接收到密文数据后，使用相应的解密密钥进行解密，还原为明文数据。通过加密传输，确保数据在网络中传输的安全性，防止数据被黑客窃取或篡改；

2） 在数据库存储中，对敏感数据字段进行加密存储。例如，用户的身份证号码、银行卡信息等敏感字段，在数据库中以密文形式保存。在数据查询和使用时，通过数据库的加密和解密接口，对数据进行实时解密处理，确保数据在存储介质中的安全性，同时不影响业务系统对数据的正常使用。

6.6.4 数据签名

a） 方案概述

通过数据签名技术，为数据提供完整性验证和来源认证，确保数据在传输和存储过程中未被篡改，并且能够明确数据的来源和责任。数据签名基于私钥对数据进行加密生成数字签名，接收方可以使用相应的公钥对签名进行验证，从而判断数据的真实性和完整性。

b) 技术实现

1) 运用可靠的数据签名算法，如椭圆曲线数字签名算法（ECDSA）。ECDSA 算法具有签名长度短、计算效率高、安全性强等优点，广泛应用于各类数据签名场景。在进行数据签名时，使用数据所有者的私钥对数据进行加密运算，生成数字签名。同时，将数据和数字签名一并传输或存储；

2) 在数据传输和存储过程中，确保数据和签名的完整性和一致性。可以采用数字信封技术，将数据和签名封装在一起，防止签名被分离或篡改。在接收方收到数据后，使用数据发送方的公钥对数字签名进行解密验证，如果验证通过，则说明数据未被篡改，且来源可信。

c) 应用场景

1) 在电子文档签署和合同管理领域，数据签名具有重要应用价值。例如，在电子合同签署过程中，合同各方使用自己的私钥对合同文档进行数字签名，确保合同的完整性和真实性。一旦合同发生纠纷，可通过验证数字签名来确定合同的签署方和签署时间，防止合同被伪造或篡改；

2) 在软件代码分发和更新过程中，为了确保软件的来源可靠和完整性，开发者对软件代码进行数字签名。用户在下载和安装软件时，系统会自动验证软件的数字签名，只有通过验证的软件才能被安装和运行。这有效地防止了恶意软件通过伪装成合法软件进行传播和安装，保障了用户设备的安全。

6.6.5 数据脱敏

a) 方案概述

针对敏感数据，在不影响数据可用性的前提下，通过特定的技术手段对数据进行处理，降低数据的敏感程度，使其能够在安全可控的环境中被使用。数据脱敏旨在满足数据在开发、测试、数据分析等非生产环境中的使用需求，同时保护用户隐私和数据安全。

b) 技术实现

1) 采用多样化的数据脱敏算法，以适应不同类型数据和应用场景的需求。常见的脱敏算法包括替换算法，如将身份证号码中的部分数字替换为特定字符；模糊化算法，对地址、姓名等信息进行部分模糊处理；截断算法，去除数据中的部分敏感内容。此外，还可根据具体情况采用随机化算法、加密算法等进行数据脱敏；

2) 建立完善的脱敏规则库，对不同类型的数据和不同的使用场景制定详细的脱敏规则。例如，对于医疗数据，在用于科研分析时，可能需要对患者的姓名、身份证号码等进行脱敏处理，但要保留疾病诊断信息和治疗数据的准确性；对于金融数据，在进行数据分析培训时，需要对客户的账户余额、交易记录等进行脱敏，同时保证数据的统计特征和业务逻辑的一致性。通过规则库的管理，确保脱敏过程的标准化和规范化。

c) 应用场景

1) 在数据分析和挖掘场景中，为了获取有价值的信息，往往需要使用大量的生产数据。但这些数据中可能包含大量的用户隐私和敏感信息。通过数据脱敏技术，对敏感数据进行处理后再用于数据分析，既能够保护用户隐私，又能够满足数据分析的需求。例如，在市场调研分析中，对客户的个人信息进行脱敏后，分析客户的消费行为和偏好，为企业的市场营销决策提供支持；

2) 在软件开发和测试过程中，为了保证测试的真实性和有效性，需要使用接近生产环境的数据。但直接使用生产数据存在数据泄露的风险。因此，使用脱敏后的数据代替真实敏感数据，能够在不影响测试效果的前提下，降低数据泄露的风险。例如，在软件功能测试中，使用脱敏后的用户数据进行测试，验证软件对数据的处理和显示功能是否正常。

6.6.6 访问控制

a) 方案概述

建立健全的访问控制机制，对用户访问数据的权限进行严格管理和限制，确保只有经过授权的合法用户能够访问相应的数据资源，防止数据被非法访问和滥用。访问控制应涵盖数据的存储、传输和使用等各个环节，实现对数据的全方位保护。

b) 技术实现

1) 综合运用多种先进的访问控制模型，根据组织的实际业务需求和安全策略进行灵活配置。基于角色的访问控制（RBAC）模型通过定义不同的角色，并为每个角色分配相应的权限，用户根据其所属角色获得访问数据的权限。基于属性的访问控制（ABAC）模型则根据数据的属性、用户的属性以及环境属性等多维度因素进行动态授权。基于风险的访问控制（RBAC）模型在考虑用户角色和权限的基础上，结合用户行为风险评估结果，实时调整访问权限，进一步增强访问控制的安全性；

2) 实现访问控制策略的集中管理和动态调整。通过建立统一的访问控制管理系统，对所有数据资源的访问策略进行集中配置和管理。该系统应与身份认证系统紧密集成，实时验证用户的身份和权限信息。当用户的身份、角色或数据的属性发生变化时，系统能够自动调整相应的访问权限，确保访问控制策略的及时性和有效性。

c) 应用场景

1) 在企业内部信息系统中，针对不同部门和岗位的员工，根据其工作职责和业务需求，设置不同的数据访问权限。例如，财务部门的员工可以访问财务相关的数据，如财务报表、账目明细等，但不能访问人力资源部门的员工薪资数据；销售部门的员工可以查看客户信息和销售数据，但不能修改财务数据。通过精细化的访问控制，确保企业数据的安全访问和合理使用，防止数据泄露和滥用；

2) 在云服务环境中，由于多租户和复杂的资源共享模式，访问控制尤为重要。云服务提供商应为每个租户和用户提供细粒度的访问控制服务。通过虚拟私有云（VPC）技术实现网络隔离，为每个租户创建独立的网络环境，并在租户内部根据用户的角色和需求设置相应的数据访问权限。例如，在一个云存储服务中，不同租户的用户只能访问自己租户内的数据，而租户管理员可以对租户内的数据进行更高级别的管理操作，如数据备份、恢复和权限分配等。

6.6.7 身份鉴别

a) 方案概述

通过一系列技术手段和流程，准确验证用户的身份真实性，确保只有合法的用户能够访问系统和数据资源，防止非法用户冒充合法用户获取数据访问权限，从而保障系统和数据的安全。

b) 技术实现

1) 采用多因素身份鉴别方法，结合多种不同类型的鉴别因素，显著提高身份鉴别的安全性和可靠性。常见的鉴别因素包括用户所知的信息，如密码；用户所拥有的物品，如硬件令牌；用户的生物特征，如指纹识别、面部识别、虹膜识别等。在实际应用中，可以根据安全需求和用户体验的平衡，选择合适的多因素组合方式。例如，在登录企业关键信息系统时，

用户首先输入密码，然后通过手机接收短信验证码进行二次验证，或者使用指纹识别设备进行生物特征验证；

2) 建立集中式的身份认证服务器，用于统一管理用户的身份信息和认证策略。该服务器存储用户的注册信息、密码哈希值、生物特征模板等关键数据，并提供身份认证服务接口。在用户进行身份鉴别时，系统将用户提交的身份信息发送到身份认证服务器进行验证。身份认证服务器根据预先设定的认证策略，对用户的身份信息进行比对和验证，并返回验证结果。同时，为了实现单点登录和跨系统的身份认证，身份认证服务器应支持多种标准的身份认证协议，如 SAML、OAuth 等。

c) 应用场景

1) 在用户登录企业信息系统、应用程序和网络服务时，进行严格的身份鉴别是保障数据安全的首要环节。无论是员工通过内部办公系统访问企业资源，还是外部客户通过网上银行、电子商务平台等进行业务操作，都需要进行准确的身份鉴别。系统通过要求用户输入用户名和密码，并结合其他鉴别因素进行验证，只有通过身份鉴别的用户才能获得系统的访问权限，从而防止非法用户入侵系统，保护数据的安全；

2) 在远程办公和移动设备访问企业资源的场景中，由于网络环境的复杂性和设备的多样性，身份鉴别面临更大的挑战。为了保障数据安全，需要加强身份鉴别措施。例如，员工通过虚拟专用网络（VPN）连接到企业内部网络时，除了输入常规的用户名和密码外，还可能需要进行硬件令牌验证或生物特征识别。同时，移动设备管理系统可以对移动设备进行身份注册和认证，确保只有经过授权的设备才能访问企业数据，防止因设备丢失或被盗导致的数据泄露风险。

6.6.8 双因素认证

a) 方案概述

在传统的用户名和密码身份认证基础上，增加第二种独立的认证因素，如短信验证码、动态令牌、生物特征识别等，进一步增强用户身份认证的安全性，有效防止账号被盗用和身份伪造等安全威胁。

b) 技术实现

1) 选择安全可靠的双因素认证服务提供商或技术平台，确保其提供的认证技术符合行业标准和安全要求。这些服务提供商通常提供多种认证方式的集成解决方案，能够与现有的身份认证系统进行无缝对接。例如，一些知名的云身份认证服务提供商提供基于短信验证码、硬件令牌和软件令牌（如基于时间的一次性密码，TOTP）的双因素认证服务，企业可以根据自身需求选择合适的认证方式；

2) 在用户进行重要操作或登录关键系统时，系统自动触发双因素认证流程。用户在输入用户名和密码后，系统会向用户预先绑定的手机号码发送短信验证码，或者要求用户使用硬件令牌或软件令牌生成动态密码，并输入到系统中进行验证。只有在用户成功提供第二种认证因素并通过验证后，才能获得系统的访问权限。同时，为了提高用户体验，系统可以设置合理的超时时间和重试次数，避免因用户未及时收到验证码或操作失误导致认证失败。

c) 应用场景

1) 在网上银行、电子支付等涉及资金交易的系统中，双因素认证是保障用户资金安全的重要手段。用户在进行转账汇款、在线支付等操作时，除了输入银行卡密码外，还需要通过手机短信验证码或动态令牌进行二次认证。这样可以有效防止黑客通过窃取密码进行非法资金交易，保障用户的资金安全。例如，在手机银行应用中，用户在进行大额转账时，系统会自动发送短信验证码到用户绑定的手机上，用户输入正确的验证码后才能完成转账操作；

2) 在企业内部敏感信息系统和关键业务应用的访问中，启用双因素认证可以增强数据的安全性。例如，企业的财务系统、客户关系管理系统（CRM）等包含重要商业机密和敏感数据的应用，只有经过双因素认证的用户才能访问。这可以防止内部员工因账号密码泄露导致的数据泄露风险，以及外部攻击者通过窃取账号密码获取企业敏感信息的威胁。

6.6.9 数据防泄漏

a) 方案概述

通过综合运用技术手段和管理措施，构建全方位的数据防泄漏体系，实时监测和防范数据在存储、传输和使用过程中可能发生的泄漏风险，确保数据的安全性和完整性，保护企业的核心资产和用户隐私。

b) 技术实现

1) 部署专业的数据防泄漏（DLP）系统，该系统利用先进的内容识别技术和行为分析技术，对数据的流动和使用情况进行实时监控。内容识别技术可以通过关键字匹配、正则表达式、数据指纹等方式，准确识别出敏感数据。行为分析技术则通过监测用户的操作行为，如数据的复制、粘贴、下载、发送邮件等，分析其是否存在异常行为模式，及时发现潜在的数据泄漏风险。例如，当系统检测到用户在短时间内大量复制敏感数据并试图通过外部存储设备导出时，系统会自动发出警报并阻止该操作；

2) 对网络边界和终端设备进行全面的安全防护。在网络边界处设置防火墙、入侵检测系统（IDS）/入侵防御系统（IPS）等安全设备，对进出网络的流量进行深度检测和过滤，防止外部攻击者通过网络入侵窃取数据。同时，在终端设备上安装防病毒软件、数据加密软件和终端安全管理系统，对终端设备上的数据进行加密存储，防止数据在终端设备上被泄露。例如，终端安全管理系统可以限制用户对外部存储设备的使用权限，防止用户通过 U 盘等设备将敏感数据带出企业内部。

c) 应用场景

1) 在企业内部网络中，DLP 系统可以实时监控员工对数据的操作行为，防止员工有意或无意地将敏感数据通过邮件、即时通讯工具、云存储等渠道泄漏出去。例如，当员工试图将包含公司机密的文件发送到外部邮箱时，DLP 系统会自动拦截并提示员工该操作违反了企业的数据安全政策。同时，系统还可以对员工的网络访问行为进行审计和记录，为后续的安全事件调查提供依据；

2) 在数据共享和合作场景中，确保数据在合作伙伴之间的安全传输和使用。企业在与合作伙伴进行数据共享时，可以通过 DLP 系统对共享的数据进行加密和标记，跟踪数据的使用情况，防止合作伙伴滥用数据或数据在合作过程中被泄漏。例如，企业在向供应商提供产品销售数据时，可以对数据进行加密处理，并设置数据使用期限和权限，供应商只能在规定的时间和范围内使用数据，一旦发现数据被异常使用，企业可以及时采取措施终止数据共享并追究责任。

6.6.10 数据水印

a) 方案概述

在数据中嵌入不可见的水印信息，作为数据的隐形标识，用于数据的版权保护、溯源和追踪。数据水印具有鲁棒性和不可感知性，即在不影响数据正常使用的前提下，能够抵抗各种常见的数据处理操作和攻击，确保水印信息的完整性和可靠性。

b) 技术实现

1) 采用先进的数字水印技术，将水印信息通过特定的算法嵌入到数据中。对于不同类型的数据，如文本、图像、音频、视频等，需要采用相应的水印嵌入算法。例如，对于图像数据，

可以利用图像的空间域或频域特性，将水印信息嵌入到图像的像素值或变换系数中；对于音频数据，可以在音频信号的时域或频域中嵌入水印。在水印嵌入过程中，需要考虑水印的强度和不可感知性之间的平衡，确保水印既能在数据中稳定存在，又不会对数据的质量和可用性产生明显影响；

2) 建立完善的水印检测和提取机制。当需要对数据进行溯源或验证时，能够准确地提取出水印信息。水印检测和提取算法应具有较高的准确性和可靠性，能够在各种复杂的环境和数据处理操作后仍能成功提取水印。同时，为了防止水印被非法去除或篡改，还可以采用一些水印保护技术，如水印加密、水印冗余等。例如，对水印信息进行加密处理，只有拥有正确密钥的授权用户才能提取和解读水印，增加了水印的安全性。

c) 应用场景

1) 在数字媒体内容（如图像、音频、视频）的版权保护中，数据水印发挥着重要作用。内容创作者可以在其作品中嵌入独特的水印信息，包括版权所有者的标识、创作时间、版权声明等。当作品在网络上传播或被非法复制时，通过提取水印信息，可以确定作品的来源和版权归属，为版权维权提供有力证据。例如，在图片库网站中，摄影师可以在上传的图片中嵌入水印，一旦发现图片被未经授权使用，可通过水印追溯到侵权者，维护自己的合法权益；

2) 在企业内部敏感数据的管理中，数据水印可用于数据的溯源和追踪。企业可以在重要的商业数据、客户数据等敏感数据中嵌入水印，记录数据的来源、流转路径和使用情况。当发生数据泄露事件时，通过提取水印信息，可以快速确定数据的泄漏源头和传播路径，有助于企业及时采取措施进行应急处理和责任追究。例如，在金融机构中，客户的交易数据和账户信息等敏感数据可以添加水印，一旦发现数据泄露，能够迅速查明是哪个环节出现了问题，是内部员工操作不当还是外部攻击导致，从而有针对性地进行整改和防范。

6.7 建立数据安全运营体系

a) 建立数据安全风险与事件监测机制

1) 选择监测工具：由数据安全管理部门负责评估和选择适合组织的自动化监测工具。同时，结合人工巡检的方法，制定人工巡检的路线、频率和检查内容，如定期检查服务器机房的物理环境、设备运行状态等；

2) 确定监测重点：组织相关部门（如业务部门、数据安全管理部门等）共同确定监测的重点区域和重点对象。重点区域可能包括核心数据存储区域、关键业务系统所在的服务器群组等；重点对象可能包括涉及大量敏感数据的业务流程、具有高级权限的用户账户等；

3) 设定监测标准：根据数据的完整性、保密性和可用性等方面的风险，设定不同的监测标准和条件。例如，对于数据完整性，设定数据校验和的阈值，当校验和超出阈值时触发警报；对于保密性，监测是否存在未经授权的访问尝试，当发现异常访问行为时发出通知；对于可用性，监测系统的响应时间和故障率，当响应时间过长或故障率过高时采取相应措施。

b) 制定完善的数据安全事件应急处置预案

1) 确定事件分级标准：由数据安全管理部门牵头，组织相关业务部门和专家召开会议，根据事件的影响范围、危害程度等因素，将数据安全事件分为重大事件、较大事件、一般事件等。例如，重大事件可能是导致核心业务系统瘫痪且数据大量丢失的情况；较大事件可能是部分重要业务功能受影响且有一定量敏感数据泄露的情况；一般事件可能是个别业务流程出现短暂故障且少量数据受到影响的情况；

2) 明确应急响应流程：针对不同级别的事件，详细规划在事件发生时应采取的具体行动步骤。以重大事件为例，当发生重大事件时，立即启动应急响应机制，通知数据安全管理团队、

业务部门负责人、高层管理人员等相关人员；迅速开展初步调查，确定事件的性质和严重程度；采取临时措施，如隔离受影响的系统或数据，防止事件进一步恶化；组织专业人员进行深入调查和修复工作；

3) 划分责任分工：明确各个部门和人员在应急处置过程中的职责。例如，数据安全管理部门负责协调各方资源，组织应急处置工作；业务部门负责提供业务相关信息，协助确定事件对业务的影响；技术部门负责提供技术支持，修复受损的系统和数据；行政部门负责对外沟通和信息发布，确保组织内外信息的畅通；

4) 规划恢复措施：制定针对不同级别事件的系统和数据恢复方案。对于重大事件，可能需要从备份数据中恢复核心业务系统和数据，并进行全面测试和验证，确保业务的正常运行；对于较大事件，根据受损情况有针对性地恢复部分业务功能和相关数据；对于一般事件，采取简单的修复措施，如重启相关服务或恢复少量数据。

c) 建立有效的数据安全事件沟通协作机制

1) 内部沟通协作：在组织和机构内部，明确各部门在数据安全事件处理中的沟通渠道和协作方式。设立专门的应急指挥中心，配备专用的通讯设备和办公设施。通过电话、邮件、即时通讯工具等方式进行信息传递和沟通协调。制定内部沟通的规则和流程，如规定在事件发生时，各部门应首先向应急指挥中心报告，由应急指挥中心统一调度和分配任务；要求相关人员在规定时间内回复信息，确保信息传递的及时性和准确性；

2) 外部合作关系：与外部相关机构建立合作关系，如与监管部门、行业协会、技术支持单位等保持密切联系。确定与外部机构的沟通方式和频率，如定期向监管部门报告数据安全事件的处理情况；及时向行业协会咨询行业最新动态和标准；在遇到技术难题时，迅速向技术支持单位寻求帮助。签订合作协议，明确双方的权利和义务，如规定技术支持单位应在接到求助后多长时间内提供解决方案，监管部门有权对组织的数据安全管理进行监督和检查等。

d) 建立严格的数据安全事件责任追究制度

1) 制定责任认定标准：由数据安全管理部门会同法务部门制定明确的责任认定标准。根据事件的原因、造成的损失以及相关人员的行为等因素，确定责任主体。例如，如果是因为技术人员操作失误导致数据泄露，那么技术人员应承担主要责任；如果是因为业务部门管理不善，导致数据安全制度执行不力，那么业务部门负责人应承担相应责任；

2) 规定处罚措施：针对不同的责任主体，规定相应的处罚措施。对于负有责任的部门和人员，可采取警告、罚款、降职、辞退等处罚措施。例如，对于轻微违规的人员，给予警告处分；对于造成较大损失的部门，处以罚款；对于严重失职的人员，予以降职或辞退处理，以起到警示作用。

7 数据安全运营

7.1 数据合规及风险评估和监测

a) 数据合规性评估

1) 收集活动信息：由数据安全管理部门负责定期收集数据相关活动信息，包括数据收集、使用、存储和共享等环节的详细情况。设计专门的数据活动信息收集表格，表格内容包括收集的数据类型、来源、使用目的、存储位置、共享对象等。要求各业务部门如实填写表格，并定期提交给数据安全管理部门；

2) 对照检查标准：将收集到的信息与国家法律法规以及行业标准进行逐一比对。组织相关人员（如法务人员、数据安全管理人员等）进行检查，明确检查的方法和步骤。例如，首先检查数据来源是否合法，是否符合相关法律法规的规定；然后检查数据使用目的是否正当，是否符合行业标准中关于数据使用的要求；最后检查数据存储位置和共享对象是否符合规定；
3) 记录评估结果：对符合和不符合规定的情况进行详细记录，形成评估报告。评估报告应包括评估的时间范围、评估的对象（如各个业务部门的数据活动）、符合规定的情况概述、不符合规定的情况详细描述以及针对不符合规定情况的改进建议等内容。

b) 数据安全风险监测
1) 选择监测工具和方法：根据组织和机构的实际情况，选择合适的安全监测工具和方法。如前所述，对于网络安全监测，可以选择网络安全监测软件；对于系统漏洞扫描，可以选择专业的系统漏洞扫描工具，如 Nessus 等。同时，结合人工巡检等方法，确定人工巡检的路线、频率和检查内容；
2) 确定监测内容和重点：明确监测数据的完整性、保密性和可用性等方面的风险。重点监测关键系统和设备以及重要数据的相关风险。例如，对于核心业务系统，监测其系统的完整性，包括文件系统的完整性、数据库的完整性等；对于重要数据，监测其保密性，如是否存在未经授权的访问尝试；对于关键设备，监测其可用性，如设备的运行状态是否正常；
3) 建立监测机制：制定监测的时间间隔、责任人等相关制度，确保监测工作的持续进行。例如，设定网络安全监测软件的运行频率为每小时一次，系统漏洞扫描工具的运行频率为每周一次，人工巡检的频率为每天一次。明确各监测工具和方法的责任人，如网络安全监测软件由数据安全管理部门的某工作人员负责，系统漏洞扫描工具由另一名工作人员负责，人工巡检由各业务部门的值班人员负责。

7.2 数据安全事故响应和处置

a) 建立快速的数据安全事故响应机制
1) 设立应急响应热线：由组织的客服部门或数据安全管理部门负责设立应急响应热线，确保在事故发生时能够及时接到报告。热线电话应向全体员工和相关外部人员公布，并保持 24 小时畅通；
2) 制定启动响应流程：明确在接到事故报告后，如何根据事故的严重程度启动相应的响应流程。例如，对于轻微事故，通知相关的数据安全管理人员进行初步调查；对于严重事故，立即通知数据安全管理团队、业务部门负责人、高层管理人员等相关人员，并启动全面的应急响应机制。

b) 制定详细的数据安全事故处置流程
1) 事故调查：由数据安全管理部门组织相关人员对事故发生的原因、涉及的数据范围、影响的业务范围等进行详细调查。制定事故调查的流程和方法，如首先收集事故现场的相关证据，包括系统日志、操作记录等；然后对证据进行分析，确定事故的性质和严重程度；最后形成事故调查结果报告；
2) 采取补救措施：根据调查结果，采取相应的补救措施。例如，如果是因为数据丢失导致事故，那么采取数据恢复措施，如从备份数据中恢复丢失的数据；如果是因为系统漏洞导致事故，那么采取系统修复措施，如更新系统补丁、加强访问控制等；
3) 恢复数据和业务：制定恢复数据和业务的方案，确保数据的完整性和业务的正常运行。例如，对于数据恢复，确定恢复的数据源（如从本地备份或异地备份中恢复），恢复的方法

（如使用数据恢复软件或人工恢复）；对于业务恢复，确定恢复的业务流程（如先恢复关键业务流程，再恢复次要业务流程），恢复的方式（如重启相关服务或重新配置系统）；

4) 总结经验教训：对事故处理过程进行总结，分析存在的问题和不足，为今后避免类似事故提供参考。例如，总结事故发生的原因是否是因为安全制度执行不力，是否是因为监测工具和方法不够完善等，针对这些问题提出改进措施。

7.3 数据安全平台运营

a) 构建适合的平台

1) 设计功能模块：根据组织和机构的业务特点和数据安全需求，设计数据安全运营管理平台的功能模块。例如，风险监测模块用于实时监测数据的风险状况；事故响应处置模块用于处理数据安全事故；数据分类分级管理模块用于对数据进行分类分级管理；数据审计模块用于对数据安全管理进行审计。组织相关人员（如业务部门、数据安全管理部门等）进行研讨，确定各功能模块的详细需求和设计思路；

2) 选择技术架构和工具：根据平台的设计要求，选择合适的技术架构和相关工具。例如，对于大数据分析，可以选择 Hadoop 或 Spark 等技术。组织相关人员（如技术部门、数据安全管理部门等）进行技术选型的研讨，确定最佳的技术架构和工具组合。

b) 平台维护

1) 软件更新：定期对平台软件进行更新，修复漏洞，提升性能，确保平台的稳定性和安全性。由平台维护人员负责制定软件更新计划，包括更新的时间间隔、更新的内容（如修复的漏洞列表、新增的功能等）。在更新前，对更新内容进行测试，确保更新不会对平台的正常运行造成影响；

2) 硬件维护：对平台所使用的硬件设备进行定期维护，如检查硬件状态、更换故障部件等。由硬件维护人员负责制定硬件维护计划，包括维护的时间间隔、维护的内容（如检查哪些硬件设备、更换哪些故障部件等）。在维护前，对维护内容进行测试，确保维护不会对平台的正常运行造成影响；

3) 数据备份：制定数据备份策略，定期对平台数据进行备份，确保数据的安全性和可恢复性。由数据安全管理部门负责制定数据备份计划，包括备份的时间间隔、备份的类型（如全量备份、增量备份等）、备份的存储地点（如本地存储、异地存储等）。在备份前，对备份内容进行测试，确保备份不会对平台的正常运行造成影响。

7.4 数据安全事件分析与处理

a) 深入分析事件

1) 分析事件原因：从技术、人员、管理等多个角度分析事件发生的原因。例如，从技术角度，检查是否存在系统漏洞、软件故障等；从人员角度，检查是否存在操作不当、违规操作等；从管理角度，检查是否存在制度执行不力、管理不善等。组织相关人员（如技术部门、业务部门、数据安全管理部门等）进行讨论，确定事件的原因；

2) 确定事件影响范围：明确事件对数据、业务、用户等方面的影响范围。例如，对于数据方面，确定受影响的数据类型、数量等；对于业务方面，确定受影响的业务流程、业务功能等；对于用户方面，确定受影响的用户群体、用户数量等。通过调查和分析，确定事件的影响范围；

3) 分析事件发生时间：了解事件发生的具体时间，判断是否存在规律性，为今后预防类似事件提供参考。例如，分析事件是否总是在某个特定时间发生，如每周一早上或者每月的某一天，以便采取相应的预防措施。

b) 采取有效措施处理事件

1) 修复受损数据：根据受损数据的类型和严重程度，采取相应的修复措施。例如，如果受损数据是文件系统数据，那么可以使用数据恢复软件进行修复；如果受损数据是数据库数据，那么可以采用人工修复或数据恢复软件结合的方式进行修复；

2) 加强系统安全防护：针对事件暴露出来的系统安全问题，采取加强系统安全防护的措施。例如，如果是因为系统漏洞导致事件发生，那么采取更新系统补丁、加强访问控制等措施；如果是因为人员操作不当导致事件发生，那么采取培训人员、规范操作流程等措施；

3) 追究相关人员的责任：根据事件的原因和影响范围，确定相关人员的责任，采取相应的处罚措施。例如，如果是因为技术人员操作失误导致事件发生，那么技术人员应承担主要责任，给予警告、罚款等处罚措施；如果是因为业务部门管理不善导致事件发生，那么业务部门负责人应承担相应责任，给予降职、辞退等处罚措施。

7.5 安全体系监督、优化和持续改进

a) 建立健全的数据安全监督机制

1) 内部监督

- 组织检查活动：由企业内部的数据安全管理部门或审计部门负责，定期对数据安全政策执行情况、制度和规程遵守情况等进行检查。制定检查计划，包括检查的时间间隔（如每月一次）、检查的内容（如各项数据安全制度是否执行到位，各项操作规程是否遵守等）、检查的方法（如查阅文档、检查系统、访谈人员等）；
- 反馈检查结果：将检查结果反馈给相关部门和人员，如数据安全管理部门将检查结果反馈给业务部门，要求业务部门对不符合规定的情况进行整改。同时，对检查结果进行记录，形成内部监督报告，报告中应包括检查的时间范围、检查的对象、符合规定的情况概述、不符合规定的情况详细描述以及针对不符合规定情况的改进建议等内容。

2) 外部监督

- 接受监管检查：由政府监管部门或第三方审计机构负责，定期对企业是否符合国家和地方相关法律法规以及行业标准进行检查。企业应积极配合监管部门或第三方审计机构的检查，提供所需的资料和信息；
- 反馈检查结果：政府监管部门或第三方审计机构将检查结果反馈给企业，企业根据检查结果进行整改。同时，对检查结果进行记录，形成外部监督报告，报告中应包括检查的时间范围、检查的对象、符合规定的情况概述、不符合规定的情况详细描述以及针对不符合规定情况的改进建议等内容。

b) 持续优化和改进数据安全体系

1) 根据监督结果优化：根据内部监督和外部监督的结果，对数据安全体系中存在的问题进行优化。例如，如果内部监督发现某项数据安全制度执行不力，那么对该制度进行调整，加强执行力度；如果外部监督发现企业不符合某项行业标准，那么对相关制度和规程进行调整，使其符合行业标准；

2) 根据业务发展和技术更新换代的需要改进：考虑到企业业务发展和技术更新换代的需要，对数据安全体系进行改进。例如，如果企业业务拓展到新的领域，那么对新领域的数据安全需求进行分析，调整组织架构和技术手段，以适应新的业务需求；如果技术更新换代，如出现新的加密技术或访问控制技术，那么将其引入到数据安全体系中，提高数据安全水平。

8 数据安全审计

8.1 规范审计

a) 检查制度建设情况
   1) 审查制度建立情况：由数据安全审计部门负责审查数据安全管理制度是否建立。检查组织和机构是否制定了数据安全管理制度，包括责任制度、审计制度、备份制度、访问制度等。查阅相关文档，确认制度是否存在，制度的内容是否完整；
   2) 检查标准制定情况：检查是否制定了数据安全管理标准，如数据分类分级标准、数据加密标准等。查看相关文档，确认标准是否存在，标准的内容是否合理；
   3) 检查组织建设情况：了解数据安全管理组织是否建立，包括是否设置了相关岗位，如数据安全管理员、数据组合起来不明确，是否为数据安全审计员等。确认岗位是否存在，岗位的职责是否明确。
b) 分析制度存在问题
   1) 制度完整性分析：检查现有制度是否涵盖了数据安全管理的各个方面，是否存在漏洞和不足。通过对制度内容的分析，找出制度未涉及的方面，如某些特殊数据类型的管理未在制度中明确规定；
   2) 制度合理性分析：分析制度的规定是否合理，是否符合实际情况和行业标准；
   3) 制度可行性分析：评估制度在实际执行过程中是否可行，是否存在操作上的困难。
c) 提出整改建议
   1) 补充缺失内容：针对制度完整性分析中发现的问题，提出补充制度缺失内容的建议。例如，对于特殊数据类型的管理，制定专门的管理制度，明确其分类分级标准、安全措施以及相关人员的职责等；
   2) 调整不合理规定：根据制度合理性分析的结果，调整不合理的规定。如根据业务实际情况合理调整备份频率，使其既能保证数据安全又不会对业务造成过大负担；按照最小必要原则重新设置访问权限，确保只有必要的人员能够访问相关数据；。
   3) 改进不可行操作：对于制度可行性分析中发现的问题，改进不可行的操作。例如，选择更合适的加密算法，在保证数据安全的同时提高系统性能；简化审计流程，通过采用自动化审计工具或优化审计步骤，提高审计效率。

8.2 过程审计

a) 分析制度落实执行情况
   1) 检查分类分级情况：由数据安全审计部门检查各业务系统中数据的分类分级情况。查看是否按照规定对数据进行了分类分级，分类分级是否准确。可以通过抽查数据样本，检查其分类分级标签是否正确，以及与相关制度规定是否相符；
   2) 检查管理人员设置情况：确认是否设置了相应的安全管理人员，其职责是否明确。查阅组织架构图和岗位说明书，查看是否有数据安全管理员、数据安全审计员等岗位，以及这些岗位的职责描述是否清晰准确；
   3) 检查管理工具建设情况：了解是否开发或采用了相应的管理工具，如数据分类分级工具、数据加密工具等。查看相关项目文档或软件系统，确认是否存在这些工具，以及它们的功能是否满足数据安全管理的要求；
   4) 检查风险监控和评估情况：查看是否建立了风险监控和评估机制，是否定期进行风险评估。检查风险监控系统的运行日志，查看是否有定期的风险评估报告生成，以及报告中的风险评估结果是否合理。
b) 掌握日常运行情况

1) 综合检查结果：通过上述各项检查，综合掌握数据安全的日常运行情况。包括数据的分类分级是否准确、安全管理人员是否到位、管理工具是否有效、风险监控和评估是否正常等方面的情况；
2) 对比目标策略：将掌握的日常运行情况与数据安全目标、策略、标准和预期结果进行对比。确保数据安全的实际运行情况符合设定的目标、策略和标准，以及能够达到预期的结果。

c) 对比结果进行分析
1) 分析差异原因：将实际执行情况与制度规定进行对比，分析存在的差异。找出哪些方面没有达到制度要求，例如数据分类分级不准确可能是因为业务人员对分类分级标准理解不到位，或者管理工具存在缺陷等原因；
2) 提出改进措施：根据分析的差异原因，提出针对性的改进措施。例如，如果是业务人员理解不到位，加强对业务人员的培训；如果是管理工具存在缺陷，对管理工具进行升级或更换。

8.3 合规审计

a) 检查合法处理情况
1) 检查个人数据处理：由数据安全审计部门检查个人数据的合法处理情况。查看是否按照法律法规和行业标准对个人数据进行处理，如是否取得了用户的同意、是否保护了用户的隐私等。可以通过检查用户协议、隐私政策等相关文档，以及查看相关业务流程中对个人数据的处理情况来进行判断；
2) 检查消费者隐私权保障：了解是否对消费者的隐私权进行了有效保障，如是否采取了相应的防护措施、是否存在侵犯消费者隐私权的行为。检查相关的安全措施是否到位，如数据加密、访问控制等措施是否应用于消费者数据，以及是否存在非法访问或泄露消费者数据的情况。

b) 记录审计结果

形成审计结果报告：对合法处理情况和消费者隐私权保障情况进行记录，形成审计结果报告。报告中应包括审计的时间范围、审计的对象（如个人数据处理情况和消费者隐私权保障情况）、符合规定的情况概述、不符合规定的情况详细描述以及针对不符合规定情况的改进建议等内容。

8.4 供应商审计

a) 检查合作内容
1) 检查数据来源合规性：由数据安全审计部门检查数据供应商提供的数据来源是否合法，是否符合法律法规和行业标准。要求供应商提供相关证明材料，如数据采集许可证、数据授权书等，以证明其数据来源合法；
2) 检查协议完整性：检查外部数据需求方与组织和机构签订的合作协议是否完整，是否涵盖了所有必要的内容。查看协议中是否包含数据使用范围、数据安全责任、保密条款等重要内容，以及这些内容是否符合法律法规和行业标准；
3) 检查使用范围合规性：检查外部数据需求方使用数据的范围是否符合法律法规和行业标准。查看合作协议中规定的使用范围是否与实际使用情况相符，以及是否存在超范围使用数据的情况。

b) 确保履行义务
1) 要求提供证明材料：根据检查结果，确保供应商切实履行数据安全义务。要求供应商提供相关证明材料，如数据安全保障方案、数据加密技术方案等，以证明其有能力保障数据安全；

2) 签订补充协议：如果发现合作协议存在缺陷或供应商未完全履行义务，签订补充协议。补充协议应明确双方的权利和义务，特别是关于数据安全的责任和义务，以确保供应商在后续的合作中能够更好地履行数据安全义务。

8.5 审计报告

a) 综合分析审计情况

1) 分析风险和建议：结合规范审计、过程审计、供应商审计等方面的审计情况，分析数据安全管理过程中的风险和应对建议。确定风险的类型、程度和影响范围，如数据泄露风险、数据篡改风险、合规风险等，并根据风险的优先级排序，如高风险、中风险、低风险。针对不同风险等级，提出相应的应对建议，如对于高风险，加强安全措施和监控；对于中风险，进行定期监测和优化；对于低风险，保持关注和预防；

2) 确定风险优先级：根据风险的类型、程度和影响范围，确定风险的优先级。可以采用风险矩阵方法，根据风险的可能性和影响程度计算风险值，然后根据风险值对风险进行排序。风险值越高，风险优先级越高，需要采取更加强有力的措施来应对。

b) 制定报告内容

1) 确定接收人：确定审计报告接收人，如组织和机构的管理层、监管部门等。明确报告是为了向这些接收人提供关于数据安全审计的结果和建议，以便他们能够采取相应的行动；

2) 明确审计目的范围责任：在报告中详细说明审计的目的、范围以及双方的责任。审计目的可能是评估数据安全管理状况，范围可能包括数据采集、存储、传输、使用和销毁等全生命周期过程，双方责任可能是审计部门负责审计工作，被审计部门负责配合审计工作并根据审计结果进行整改；

3) 记录问题风险建议：将审计过程中发现的问题、可能存在的风险以及整改建议记录在报告中。问题可能包括制度不完善、执行不到位、数据来源不合规等，风险可能包括数据泄露风险、数据篡改风险、合规风险等，整改建议可能包括补充制度、加强执行、规范数据来源等。

8.6 数据安全建议

a) 结合审计结果提出改进建议

1) 针对不符合项改进：根据审计结果中存在的不符合项以及企业数据安全管理的薄弱环节，提出针对性的改进建议。例如，如果审计结果显示制度不完善，建议加强制度建设，制定详细的管理制度，明确各岗位的职责和权限；如果执行不到位，建议加强对员工的培训，提高员工对制度的执行能力；如果数据来源不合规，建议规范数据来源，要求供应商提供合法合规的数据源；

2) 针对预防措施建议：针对预防数据安全问题的措施，提出具体的操作建议。例如，为了预防数据泄露，建议增加培训频次，使员工更加熟悉数据安全知识和操作规范；为了预防数据篡改，建议细化制度内容，明确对数据篡改行为的处罚措施；为了预防合规风险，建议及时了解法律法规和行业标准的更新情况，确保企业的行为符合规定。

b) 确定改进方向

确定管理改进方向：根据提出的改进建议，确定企业数据安全管理的改进方向。例如，如果建议加强制度建设，那么企业数据安全管理的改进方向是完善制度体系，确保制度涵盖数据安全管理的各个方面；如果建议提高员工素质，那么改进方向是加强员工培训，提高员工的专业水平和对数据安全知识的掌握程度；如果建议提升技术水平，那么改进方向是引入新的技术手段，如采用更先进的加密算法、访问控制技术等。

9 结语

本文件旨在为各类组织提供一套全面的数据安全管理规范，帮助组织有效识别和管理数据安全风险，确保数据的安全和合规使用。希望本文件能够为组织的数据安全管理工作提供有力支持。

参 考 文 献

[1]GT/T 35274—2023 数据安全技术 大数据服务安全能力要求
[2]GB/T 44109—2024 信息技术 大数据 数据治理实施指南
[3]GB/T 43679—2024 数据安全技术 数据分类分级规则
[4]GB/T 34960.1—2017 信息技术服务 治理 第1部分：通用要求
[5]GB/T 35295—2017 信息技术 大数据 术语
[6]GB/T 36073—2018 数据管理能力成熟度评估模型