网络数据安全管理指南

1 范围

本文件给出了网络数据安全管理的基本要求，包括管理机制、通用安全、数据处理活动安全和个人信息保护。

本文件适用于指导数据处理者开展网络数据安全的建设和评估工作，也可为主管监管部门进行网络数据安全监管提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或者其他方式对信息的记录。

3.2

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

3.3

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的能力。

3.4

数据处理活动 data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等活动。

3.5

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注 1：重要数据不包括国家秘密。

注 2：重要数据一般不包括个人信息和企业内部管理信息，但达到一定规模的个人信息或者基于海量个人信息加工形成的衍生数据，如其一旦遭到篡改、破坏、泄露或者非法获取、非法利用可能危害国家安全、公共利益，也应满足重要数据保护要求。

注 3：处理 100 万人以上个人信息的数据处理者，按照重要数据处理者进行管理，应满足重要数据保护要求。各行业、各领域有规定的，从其规定。

3.6

核心数据 core data

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

[来源：GB/T 43697—2024，3.3]

3.7

一般数据 general data

核心数据、重要数据之外的其他数据。

[来源：GB/T 43697—2024，3.4]

3.8

个人信息 personal information

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

注 1：个人信息不包括匿名化处理后的信息。

注 2：个人信息包括姓名、出生日期、公民身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[来源：GB/T 41479—2022，3.6]

3.9

敏感个人信息 sensitive personal information

一旦泄露、非法提供或滥用有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注 1：敏感个人信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、健康生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

注 2：个人信息处理者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，也属于敏感个人信息。

[来源：GB/T 41479—2022，3.7]

3.10

个人信息主体 personal information subject

个人信息已识别或可识别（所标识或关联到）的自然人。

[来源：GB/T 41479—2022，3.8]

3.11

个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

[来源：GB/T 35273—2020，3.4]

3.12

数据合作方 data partner

通过业务合作、提供技术支撑和数据服务等，并可能接触到组织机构数据的外部机构。

3.13

第三方应用 third party application

由第三方提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务中的自动化工具。

注：本文件中的第三方应用包括但不限于软件开发工具包、第三方代码、组件、脚本、接口、算法模型、小程序等。

[来源：GB/T 41479—2022，3.12]

3.14

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

[来源：GB/T 41479—2022，3.13]

3.15

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

[来源：GB/T 35273—2020，3.15]

3.16

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

[来源：GB/T 37988—2019，3.12]

3.17

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。

根据发起者不同，分为自评估和检查评估。

自评估由数据处理者自身发起，组成机构内部评估小组或委托第三方评估机构，依据有关政策法规与标准，对评估对象的数据安全风险进行评估的活动。

检查评估由数据处理者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起的，依据有关政策法规与标准，对评估对象的数据安全风险进行的评估活动。

3.18

大型互联网平台 large internet platform

通过网络技术将个人与个人、商品、信息、服务、线下资源、数据、资金、软件等进行连接，并以此为基础提供业务的较大规模的网络平台。

注 1：较大规模是指在过去的一年期间，在我国累计活跃用户总数不低于 5000 万。

注 2：提供业务包括但不限即时通信、社交网络、电子商务、直播、短视频、信息资讯、应用商店、网络预约汽车、网络支付等。

4 网络数据安全建设框架

4.1 网络数据安全建设应包括管理机制、通用安全、数据处理活动安全和个人信息保护等内容，涵盖数据安全的基本保护要求（一般数据安全要求）、重要数据保护扩展要求和个人信息的一般个人信息保护要求和敏感个人信息保护要求等。重要数据保护应同时满足基本保护要求和重要数据扩展要求；核心数据应在重要数据保护的基础上依照有关规定从严保护；个人信息保护应同时满足数据安全的基本保护要求，达到重要数据管理条件的还应同时满足重要数据保护扩展要求。框架结构图见图 1。

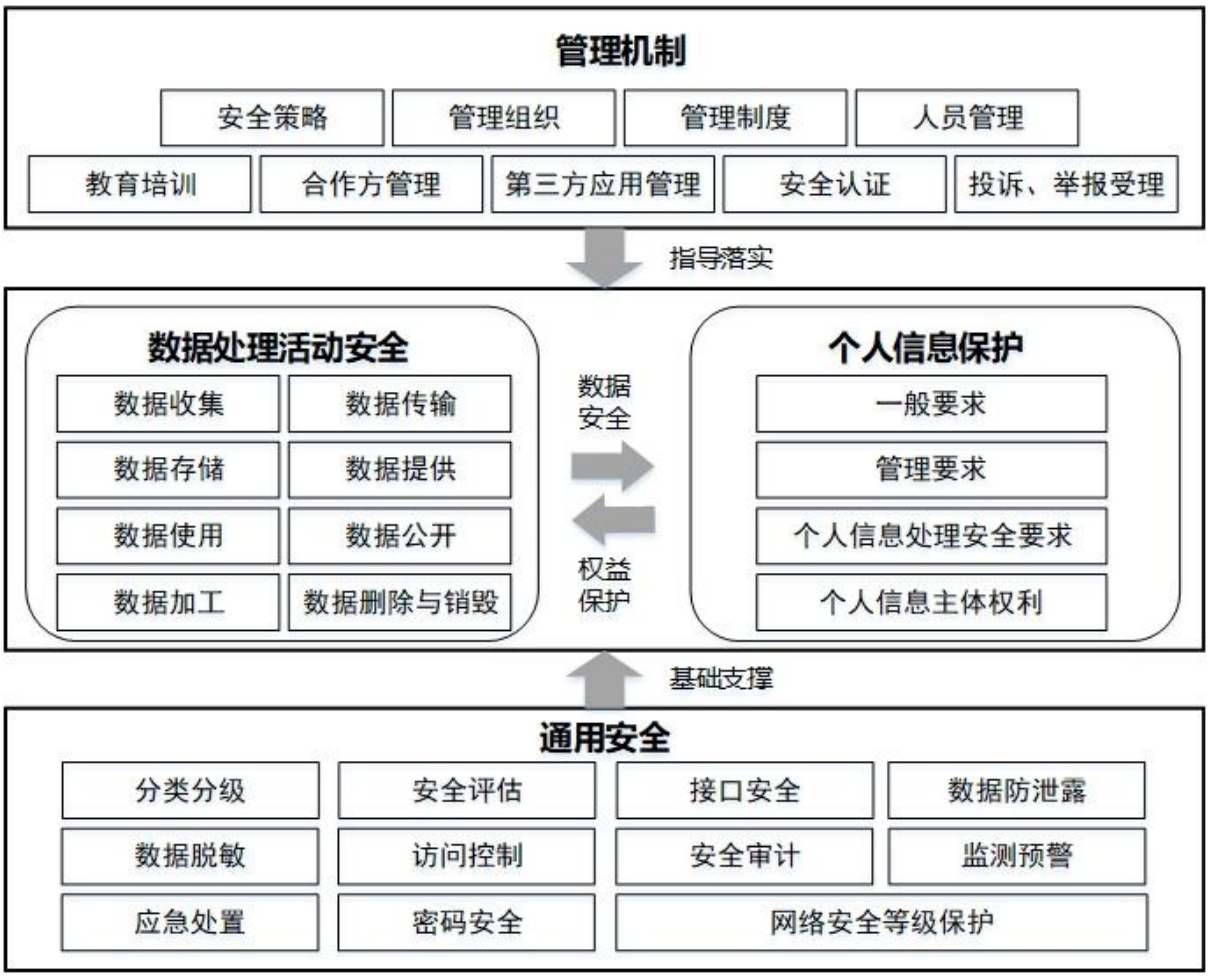

图 1 框架结构图

4.2 管理机制：围绕数据安全策略、数据安全管理组织、数据安全管理制度体系、数据安全人员管理、教育培训、数据合作方管理、第三方应用管理、数据安全管理认证和举报、投诉受理处置等方面，建立完善符合法律法规、相关标准规范的安全管理机制。
4.3 通用安全：围绕数据分类分级、数据安全评估、数据访问控制、数据接口安全、数据防泄露管理、数据脱敏、数据安全审计、数据安全风险监测预警、数据安全应急处置、密码安全管理、网络安全等级保护等方面落实基础安全管理措施。
4.4 数据处理活动安全：围绕数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等数据处理活动，开展数据安全管理，落实技术保护措施。
4.5 个人信息保护：围绕个人信息保护管理机制、个人信息处理要求、个人信息主体权利等方面规范保护要求，落实个人信息保护措施。

5 管理机制

5.1 数据安全总体策略

5.1.1 基本保护要求

5.1.1.1 应制定总体安全管理框架，明确数据安全管理总体策略，包括管理目标、原则、要求等内容。
5.1.1.2 制定数据安全管理总体策略应以重要数据、个人信息为重点。

5.1.2 重要数据保护扩展要求

无重要数据保护扩展要求。

5.2 数据安全管理组织

5.2.1 基本保护要求

5.2.1.1 应通过正式文件或制度明确数据安全管理各级组织及相应职责。
5.2.1.2 应明确数据安全负责人。职责包括但不限于负责牵头制定数据安全管理制度、指导数据安全管理工作、协调各相关部门开展数据保护工作、组织内部数据安全教育培训工作、提出数据安全保护的对策建议、监督管理制度和措施的执行落实情况等。
5.2.1.3 应明确数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

a) 研究提出数据安全相关重大决策建议；
b) 制定实施数据安全保护计划和数据安全事件应急预案；
c) 开展数据安全风险监测，及时处置数据安全风险和事件；
d) 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；
e) 受理、处置数据安全投诉、举报；
f) 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

5.2.1.4 应明确数据安全管理部门，牵头承担单位整体数据安全管理工作，落实数据安全保护责任。包括但不限于组织制定数据安全管理制度并执行，落实数据安全技术防护措施，开展数据安全教育培训、数据安全评估、数据安全监测、数据安全事件应急处置等工作。
5.2.1.5 应明确岗位职责和能力要求，足额配备具备相应岗位能力的数据安全人员，负责具体落实数据安全管理工作。包括但不限于数据梳理、分类分级、安全评估、合规性检查、权限管理、安全审计、监测预警、应急处置和信息报送、教育培训等工作。数据管理员、数据安全管理员、数据安全审计员应专人专岗。

5.2.1.6　宜建立独立的数据安全审计机构，负责开展数据安全和个人信息保护监督审计工作，并向管理层直接汇报。

5.2.2　重要数据保护扩展要求

5.2.2.1　重要数据处理者的数据安全负责人应由数据处理者决策层成员承担，并具备数据安全专业知识和相关管理工作经历。
5.2.2.2　具有国家网信部门或有关主管部门规定的特定种类、规模的重要数据的，应设置独立的数据安全管理机构。

5.3　数据安全管理制度

5.3.1　基本保护要求

5.3.1.1　应建立健全数据安全管理制度体系，并通过正式、有效的方式发布数据安全管理制度和版本控制，严格执行。
5.3.1.2　应形成由总体策略、管理规范、操作规程、记录表单等构成的数据安全管理制度体系。
5.3.1.3　制度体系内容应包括但不限于数据安全总体策略、组织机构与人员管理、数据分类分级、数据处理活动安全管理要求、数据访问控制、数据安全评估、数据安全审计、数据安全风险监测预警、数数据安全应急与处置、数据安全教育培训、合作方管理、数据出境、投诉举报受理处置等制度。
5.3.1.4　应建立数据安全制度文件管理控制流程，规范制度文件的建立、审批、发布、修订和废止，实施文件版本控制，确保制度文件的及时更新和有效访问。
5.3.1.5　应定期对数据安全管理制度的合理性、充分性和适用性进行论证和评价，对存在不足或需要改进的安全管理制度进行修订。

5.3.2　重要数据保护扩展要求

重要数据处理者应确保重要数据安全管理制度覆盖全部重要数据处理活动，并在安全环境、法规政策、组织架构或业务发生重大变化时及时评估和修订数据安全管理制度和安全策略。

5.4　人员管理

5.4.1　基本保护要求

5.4.1.1　应明确规定人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的数据安全管理要求并予以落实。
5.4.1.2　应明确人员岗位职责、数据访问和操作权限管理要求、人员调离保密要求、保密期限、违约责任等，定期审查其行为，对其数据操作行为进行有效约束。
5.4.1.3　在开展与关键信息基础设施网络安全和信息化有关的决策时，应有专门数据安全管理机构人员参与。
5.4.1.4　数据安全岗位人员履职情况应留存相关工作记录，如数据安全管理监督检查记录、数据安全事件信息报送记录等。

5.4.2　重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据等人员落实资格审查、签署保密协议、审批和登记，明确岗位职责、数据访问范围、操作权限、人员调离保密要求、保密期限、违约责任等措施，定期审查其行为，对其数据操作行为进行有效约束。

5.5 教育培训

5.5.1 基本保护要求

5.5.1.1 应建立数据安全教育培训制度，明确培训周期、培训对象、培训内容、次数、课时和考核评价等。

5.5.1.2 应制定数据安全培训计划，定期（至少每年一次）或者政策发生变化时组织数据安全专业化培训工作，并对培训结果进行考核评价，留存相关记录（如培训计划、培训通知、培训课件、签到表、培训考核情况等相关记录文件）。

5.5.1.3 教育培训应覆盖单位全员，培训内容覆盖数据安全法律法规、单位制度要求和实操规范等内容。针对单位全员的培训内容包括但不限于普及数据安全意识、法律法规等，针对数据安全岗位人员的培训内容包括但不限于标准规范、技能培训、安全评估、应急响应、应急演练等。

5.5.1.4 数据安全人员宜考取资质证书，持证上岗。

5.5.2 重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据的相关人员每年开展数据安全培训考核，依据考核结果确定任职资格。

5.6 数据合作方管理

5.6.1 基本保护要求

5.6.1.1 应明确管理相关数据合作方（含数据供应链、外包服务机构、外包服务人员）的数据安全监督管理部门和执行配合部门，并设置专岗负责相关工作，明确工作职责。

5.6.1.2 应梳理形成数据合作方清单并定期更新，合作方清单包含合作方名称、合作业务或系统、合作形式、合作期限、合作方联系人、合作涉及数据类型与数量等信息。

5.6.1.3 应建立数据合作方安全管理机制，如对合作方或外包服务机构的选择、评价、管理、监督机制等。明确合作方的数据安全保护方式和责任落实要求，包括但不限于服务合同、合作方资质审核、接入管理、权限管理、主体授权、多个合作方管理、安全技术要求、数据脱敏、行为监测、数据销毁、数据安全应急响应及处置等管理要求。

5.6.1.4 应审核数据合作方的资质背景、网络和数据安全保障能力、业务连续性保障能力、数据安全事件发生等情况，并开展安全评估。

5.6.1.5 应通过服务合同或安全保密协议等形式明确数据合作方的数据安全保护责任和义务。明确具体条款，包含但不限于下述内容：合作方及参与人员可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围、期限及用途（应符合最小化原则），合作方及参与人员的数据安全责任，合作方的保障措施配备情况（保障措施不低于本方的安全要求），合作结束后数据删除要求，合作方违约责任和处罚等。

5.6.1.6 应在合作结束后停用或下线向数据合作方提供的系统权限和接口，并回收数据及要求合作方对数据进行删除。

5.6.2 重要数据保护扩展要求

5.6.2.1 对处理重要数据的数据合作方，应重点排查数据传输安全、数据存储安全、数据访问安全、数据提供、数据删除与销毁等方面的风险并加强管控。

5.6.2.2 对处理重要数据的数据合作方，应每年组织开展合作方安全检查或评估工作，对发现的问题及时督促整改，必要时停止合作，并留存相关检查和安全评估记录不少于三年。

5.7 第三方应用管理

5.7.1 基本保护要求

5.7.1.1 应严格监督第三方应用运营者加强数据安全管理，通过签订合同等方式明确数据安全责任和义务。

5.7.1.2 应对接入或嵌入的第三方应用开展技术检测，确保其数据处理行为符合双方约定要求，对技术检测时发现超出双方约定的行为应及时停止接入。

5.7.1.3 应定期开展安全检查，发现第三方应用没有落实安全管理责任的，应及时督促整改，必要时停止接入。

5.7.1.4 服务结束后，应停用或下线相关系统权限和接口。

5.7.2 重要数据保护扩展要求

5.7.2.1 重要数据处理者对第三方应用应至少每年开展一次安全检查或评估工作，对发现的问题及时督促整改，必要时停止合作，并留存相关检查和安全评估记录不少于三年。

5.7.2.2 第三方应用发生重大变更或更新时，应在变更和更新前进行安全评估。

5.8 数据安全认证

5.8.1 基本保护要求

宜开展数据安全管理认证工作，通过认证方式规范网络数据处理活动，加强网络数据安全保护。

5.8.2 重要数据保护扩展要求

无重要数据保护扩展要求。

5.9 投诉、举报受理处置

5.9.1 基本保护要求

应建立投诉、举报受理处置制度，包括建立数据安全事件投诉、举报渠道及受理处置流程以及公布接受投诉、举报的联系方式、责任人等受理处置信息。收到通过其服务或业务平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报的，自接受投诉举报起，受理时间不超过3天。受理后进行调查取证，对于查实的编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报，依法采取停止传输、消除等处置措施。

5.9.2 重要数据保护扩展要求

无重要数据保护扩展要求。

6 通用安全

6.1 数据分类分级保护

6.1.1 基本保护要求

6.1.1.1 应结合数据识别技术手段，梳理数据，形成数据清单。清单内容包括所属部门、数据类型、数据项名称、数据数量、数据来源、存储位置（如系统名称、数据库、表名等）、数据处理情况（访问、导出、共享、出境等）、数据关联系统等，并定期对已形成的数据清单进行更新。

6.1.1.2 应明确数据分类分级标准，确定数据类别和对应的安全等级。依据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用时对国家安全、社会秩序和公共利益或者个人、组织合法权益造成危害程度确定安全等级。

6.1.1.3 应依据数据分类分级制度和方法，在数据清单的基础上标记类别和级别，形成数据分类分级清单。清单内容包括所属部门、数据类别、数据项名称、数据数量、数据级别、数据来源、存储位置（如系统名称、数据库、表名等）、数据处理情况（如访问、导出、共享、出境等）、数据关联系统、是否为重要数据、是否为个人信息数据、是否为敏感个人信息数据等。

6.1.1.4 应根据政策要求和业务变化等对数据分类分级情况进行动态调整和评审，留存调整和评审记录。

6.1.1.5 应在数据分类分级的基础上，落实不同数据安全等级差异化防护措施要求。明确在数据处理活动中针对不同类别、级别的数据采取相应的安全保障措施，包括不限于数据分类分级标识、数据加密、数据脱敏、去标识化、匿名化、数据访问权限控制、数据流动记录、操作行为记录、数据备份与恢复、数据销毁删除等管理和技术措施。

6.1.1.6 宜建立数据分类分级标识技术措施，管理数据分类分级清单并实现对各类数据的分类分级标识。

6.1.1.7 宜使用数据管理技术工具定期对相关平台系统数据进行定期扫描，能够发现识别重要数据和个人信息、敏感个人信息，定期对数据加密、脱敏、去标识化等技术措施效果进行验证，确保各类数据处理场景中数据保护的持续有效性和合规性。

6.1.2 重要数据保护扩展要求

6.1.2.1 应对重要数据采取加密等安全防护措施重点保护，核心数据应在重要数据保护的基础上依照有关规定从严保护。

6.1.2.2 宜对重要数据的流转进行跟踪溯源。

6.1.2.3 处理重要数据的数据处理者，应在识别重要数据后的十五个工作日内向市级网信部门备案。备案内容包括：

a) 数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；
b) 处理数据的目的、规模、方式、范围、类型、数据来源、存储期限、存储地点、数据处理情况、数据安全措施等，不包括数据内容本身；
c) 国家网信部门和主管、监管部门规定的其他备案内容；
d) 处理数据的目的、范围、类型及数据安全措施有着重大变化的，应当重新备案。

6.2 数据安全评估

6.2.1 基本保护要求

6.2.1.1 应制定数据安全评估制度，明确评估目的、范围、依据、流程、方法、内容、频率等内容。

6.2.1.2 应定期开展数据安全合规性检查或风险评估，包括但不限于数据安全管理、数据处理活动合规、数据安全防护措施落实、个人信息保护等情况，并根据评估结果进行处置。

6.2.1.3 开展数据共享、交易、委托处理等活动前，出现法律法规重大更改或增删，业务活动发生重大变化，数据发生重大变化，发生重大数据安全事件，数据安全管理方针发生变化等重大情况时，应进行局部或全面数据安全风险评估，形成数据安全风险评估报告。

6.2.2 重要数据保护扩展要求

涉及处理重要数据的机构，应按照有关规定每年开展一次数据安全风险评估，评估报告保留不少于三年，并向市级网信部门和有关主管部门报送风险评估报告。风险评估报告应包括处理的重要数据种类、数量，存储期限、存储地点、开展数据处理活动的情况、安全措施的有效性， 以及面临的数据安全风险和应对措施等。

6.3 数据访问控制

6.3.1 基本保护要求

6.3.1.1 根据不同数据安全级别，应明确数据管理、审计账号权限、处理活动平台系统账号权限的分配、开通、使用、变更、注销等安全管理要求和审批流程要求。

6.3.1.2 数据处理活动使用的账号权限分配应遵循“职责明确、权限分离、最小特权”原则，并分配最小化数据访问权限。

6.3.1.3 应对数据处理全流程使用的各类账号及对应权限进行记录。账号关联对象包括内部、外部和数据合作方人员，重点关注离职人员账号回收、管理权限变更、沉默账号、复活账号等，并在账号或权限发生变更时及时更新记录。

6.3.1.4 应对业务系统之间的数据访问采取身份鉴别、访问控制、安全审计、资源控制等技术措施。

6.3.1.5 应对数据跨网络区域传输采取安全管控措施，包括但不限于网络及应用层的访问控制策略，控制粒度为端口级。

6.3.1.6 基于数据分类分级结果和业务场景配置主体对客体的访问控制策略，访问控制粒度应达到：主体为用户级或服务、接口级别，客体为接口、应用功能、文件、数据库表级或数据项级别等。

6.3.1.7 应集中管控账号权限，对账号进行统一身份认证和授权，可采用口令管理、生物识别、数字证书、多因子认证等技术措施。

6.3.2 重要数据保护扩展要求

对重要数据的数据访问接口、数据服务调用以及查询、修改、删除、导出、共享、交换、备份、恢复等应设置严格审批流程和访问控制。

6.4 数据接口安全

6.4.1 基本保护要求

6.4.1.1 应明确数据接口的安全要求、管控措施和控制策略，对数据接口实施调用审批流程。

6.4.1.2 应在数据接口调用前进行身份鉴别，通过技术手段限制非白名单接口接入，对接口不安全输入参数进行限制或过滤。身份标识应具有唯一性，身份鉴别信息具有复杂度要求并定期更换，并采取必要措施防止鉴别信息在网络传输过程中被窃听。

6.4.1.3 应与接口调用方明确数据的使用目的、供应方式、保密约定及数据安全责任等情况。

6.4.1.4 应对相关接口调用行为和数据交互行为进行监测，并进行日志记录。

6.4.1.5 应建立数据接口全生命周期管理机制。定期梳理数据接口，形成接口清单，明确不同接口的类型、数据内容、频次、上下游信息系统等信息，并动态更新接口活动状态（如新增、活跃、失活、复活、下线等接口状态）。

6.4.1.6 应对数据接口定期开展安全检测，及时发现并处置数据安全风险隐患，不符合要求的接口应落实整改或关停。

6.4.1.7 宜实现对异常数据接口调用行为自动预警、拦截功能。

6.4.2 重要数据保护扩展要求

对重要数据传输接口的调用应采取严格的层级审批程序，由数据安全负责人进行接口调用审批。

6.5 数据防泄露

6.5.1 基本保护要求

6.5.1.1 应对网络、终端等数据泄露、流转途径进行监控，及时对异常数据操作行为进行预警，实现对异常数据操作行为及时定位和阻断。

6.5.1.2 应定期验证数据防泄露技术措施的有效性。

6.5.2 重要数据保护扩展要求

无重要数据保护扩展要求。

6.6 数据脱敏

6.6.1 基本保护要求

6.6.1.1 应制定数据脱敏制度，明确数据脱敏处理的应用场景、处理流程、脱敏规则、脱敏方法、操作记录和脱敏数据的使用限制等要求。

6.6.1.2 应建立静态数据脱敏和动态数据脱敏的技术能力。

6.6.1.3 应定期对开发测试、人员信息公示等应用场景的数据脱敏开展有效性验证。

6.6.2 重要数据保护扩展要求

无重要数据保护扩展要求。

6.7 数据安全审计

6.7.1 基本保护要求

6.7.1.1 应制定数据安全审计制度，审计覆盖数据处理活动各环节，明确审计策略、审计对象、审计内容、审计流程、审计周期、审计结果、审计问题跟踪、审计材料留存时间以及日志记录访问权限控制等要求。

6.7.1.2 应对数据处理活动环节实施日志留存管理，日志记录至少包括时间、IP 地址、操作账号、操作内容、操作结果等，并对日志进行备份，防止数据安全事件导致的日志被删除。在发生安全事件时可提供溯源取证能力，日志保存时间不少于 180 天。

6.7.1.3 应定期对数据处理活动各环节的数据访问和操作进行安全审计，每年至少一次，形成数据安全审计报告。针对异常情况进行复核并处置，留存处置记录。

6.7.2 重要数据保护扩展要求

处理重要数据应对数据访问接口、数据服务调用以及查询、修改、更新、删除、导出、共享、交换、备份、恢复等关键操作进行安全审计，并采取技术措施保护审计记录的完整、准确、真实和有效应用。

6.8 数据安全风险监测预警

6.8.1 基本保护要求

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：https://d.book118.com/648127113115006061