Q/BJKB

北京坤标检验认证有限公司企业标准

Q/BJKB 011-2026

网络数据安全管理体系 基本要求

Basic Requirements for Network Data Security Management System

2026-4-1 发布　　2026-4-1 实施

北京坤标检验认证有限公司　　发　布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》起草，以 GB/T 41479-2022《信息安全技术 网络数据处理安全要求》 为核心依据，融合管理体系高阶结构（HLS），形成可用于第三方认证的网络数据安全管理体系企业标准。

本文件规定组织建立、实施、保持和持续改进网络数据安全管理体系的认证要求，适用于各类网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等全生命周期安全管理，可用于第三方认证、自我评价、内部审核与监管评估。

本文件由北京坤标检验认证有限公司提出并归口。

本文件主要起草人：陈刚辉、杨英者、吕晚香、李英华。

企业标准信息公共服务平台
公开 2026年05月07日 09点36分

网络数据安全管理体系 基本要求

1 范围

1.1 本文件规定**网络数据安全管理体系**的组织环境、领导作用、策划、支持、运行、绩效评价、改进等要求。
1.2 适用于网络运营者建立、实施、认证与改进网络数据安全管理体系，覆盖个人信息、重要数据及其他网络数据的全生命周期处理活动。
1.3 本文件可作为数据安全合规、监管检查、第三方评估与认证的依据，不替代国家法律法规、行业标准与强制性要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 信息安全技术 术语
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 41479-2022 信息安全技术 网络数据处理安全要求
GB/T 19011 管理体系审核指南

3 术语和定义

下列术语和定义适用于本文件。
GB/T 25069 信息安全技术 术语
GB/T 35273 信息安全技术 个人信息安全规范
GB/T 41479-2022 信息安全技术 网络数据处理安全要求
GB/T 19011 管理体系审核指南
界定的术语和定义适用于本文件。

4 组织的背景

4.1 了解组织和其背景

组织应确定与数据安全相关的内外部问题：
外部：法律法规、监管要求、行业标准、第三方合作、数据出境、公共安全要求等；
内部：组织战略、业务模式、数据类型、数据量级、系统架构、第三方应用、外包服务等。

4.2 理解相关方的需求和期望

组织应识别并确定相关方要求：
a）监管部门对数据安全、个人信息保护、重要数据管理的要求；
b）数据主体对个人信息查阅、更正、删除、账号注销等权利要求；
c）客户、合作方、第三方应用接入方的数据安全责任与义务；
d） 社会公众、行业协会对数据安全与隐私保护的期望。

适当时保留成文信息，包括需求清单、合规清单、相关方沟通记录。

4.3 确定网络数据安全管理体系范围

组织应明确体系边界和适用性：

a）覆盖的业务、场所、系统、网络、第三方应用、外包环节；

b）覆盖的数据类型：个人信息、敏感个人信息、重要数据、其他数据；

c） 覆盖的数据处理活动：收集、存储、使用、加工、传输、提供、公开、删除、匿名化。

范围应形成成文信息，不适用条款应说明理由并保留记录。

4.4 网络数据安全管理体系

组织应按本文件建立、实施、保持并持续改进网络数据安全管理体系：

a) 确定体系所需过程及其在组织中的应用；

b) 确定过程顺序与相互作用；

c) 确定过程准则与方法，确保有效运行与控制；

d) 确保资源与信息可获取，支持过程运行与监视；

e) 监视、测量、分析过程绩效；

f) 实施措施，实现过程改进与体系预期结果。

外包过程应被识别、控制并保留责任追溯。

5 领导作用

5.1 领导作用和承诺

最高管理者应证实对体系的领导与承诺：

a）确保制定数据安全方针与目标，与战略方向一致；

b）确保将体系要求融入业务过程；

c）确保体系资源可获得；

d）沟通数据安全与合规的重要性；

e）确保体系实现预期结果；

f）指导、支持员工为体系有效性贡献；

g）推动持续改进；

h） 支持其他管理者在职责范围内发挥领导作用。

5.2 方针

数据安全方针应：

a）适应组织目的与数据安全风险；

b）为建立数据安全目标提供框架；

c）包含合规、保护个人信息、保护重要数据、持续改进的承诺；

d） 形成成文信息，沟通、传达，并可为相关方获取。

5.3 岗位、职责和权限

最高管理者应确保分配与沟通：

a）明确数据安全责任人及其职责权限；

b）数据安全管理部门、业务部门、IT 部门、法务、人事、审计的职责；

c）确保体系符合本文件要求；

d） 向最高管理者报告体系绩效、风险与改进机会。

6 策划

6.1 应对风险和机遇的措施

组织应确定与数据安全相关的风险与机遇：

—风险：未授权访问、泄露、篡改、损毁、丢失、非法提供、违规公开、第三方违规、数据出境风险等；

—机遇：合规提升、信任增强、数据价值释放、安全能力成熟、业务可持续。

组织应策划：

a) 应对风险和机遇的措施；

b) 如何将措施整合并实施到体系过程中；

c) 如何评价措施有效性。

措施应包括：数据识别、分类分级、风险评估、安全控制、应急处置、审计追溯、合规检查。

6.2 网络数据安全目标及实现策划

组织应在相关职能、层次建立可测量的数据安全目标：

a) 数据识别与分类分级覆盖率；

b) 个人信息合规处理率、授权合规率；

c) 重要数据保护措施落实率；

d) 安全事件发生率、整改闭环率；

e) 第三方数据安全合规率；

f) 应急演练覆盖率、响应时效达标率。

目标应：与方针一致、可测量、可监视、可沟通、适时更新、形成成文信息。

策划实现目标时应确定：做什么、资源、责任人、时限、评价方法。

6.3 变更的策划

当体系发生变更时，应按计划实施，确保变更过程安全、可控、不降低安全水平，保留变更记录。

7 支持

7.1 资源

组织应提供并保障：

a) 人力、技术、资金、设备、场所资源；

b) 数据安全责任人、安全管理员、审计员、应急人员配置；

c) 安全工具：加密、脱敏、访问控制、审计、备份、检测等；

d) 内部审核、管理评审、应急演练资源。

7.2 能力

组织应：

a) 确定从事数据安全活动人员的能力要求；

b) 基于教育、培训、经验确保人员胜任；

c) 提供数据安全、个人信息保护、合规、应急等培训；

d) 评价培训与能力有效性；

e) 保留能力、培训、考核记录。

7.3 意识

组织应确保人员知晓：

a) 数据安全方针；

b) 个人对体系有效性的贡献；

c) 违规、泄露、事件的后果与责任；

d) 个人信息保护、重要数据保护要求。

7.4 沟通

组织应建立内外部数据安全沟通机制：沟通内容、时机、对象、方式、记录，包括：

- 内部：安全要求、事件、整改、培训；
- 外部：监管、用户、合作方、第三方应用、数据接收方。

7.5 成文信息

7.5.1 组织应控制以下成文信息：

a) 方针、目标、范围；

b) 数据清单、分类分级清单；

c) 风险评估与处置记录；

d) 制度、流程、操作规程；

e) 个人信息保护政策、授权记录、用户权利响应记录；

f) 安全控制、审计日志、备份与恢复记录；

g) 第三方管理、合同、评估记录；

h) 事件、应急、整改记录；

i) 内审、管理评审、改进记录。

7.5.2 成文信息应：标识、清晰、批准、发放、更改、存储、保护、检索、处置。

8 运行

8.1 运行策划和控制

组织应策划、实施、控制数据全生命周期处理过程，满足 GB/T 41479-2022 要求：

a) 数据识别：识别个人信息、敏感个人信息、重要数据，形成数据目录；

b) 分类分级：按标准实施分类分级，实施差异化保护；

c) 风险防控：开展风险评估，落实加密、脱敏、访问控制、备份、审计等措施；

d) 审计追溯：对全生命周期操作留痕，确保可审计、可追溯。

8.2 数据收集

应遵循合法、正当、必要、最小化：

a) 公开个人信息保护政策；

b) 取得明示同意，敏感个人信息取得单独同意；

c) 未成年人信息取得监护人同意；

d) 不超范围收集、不强制、不误导授权。

8.3 数据存储

a) 个人信息与重要数据加密、访问控制、安全存储；

b) 不超期存储，到期删除或匿名化；

c) 生物特征信息按规范严格保护。

8.4 数据使用

a) 定向推送应提供非定向选项；
b) 算法合成信息应明确告知；
c) 第三方应用接入应合同约束、监督、整改、停止接入。

8.5 数据加工

不得开展危害国家安全、公共安全、经济安全、社会稳定的数据加工活动。

8.6 数据传输

重要数据与敏感个人信息传输应加密、脱敏，向境外传输按国家规定执行。

8.7 数据提供

a) 提供个人信息应告知并取得同意；
b) 重要数据共享、转让应合同约束、安全防护；
c) 委托处理应明确目的、范围、安全责任、返还删除要求；
d) 并购、重组、破产应延续保护或删除。

8.8 数据公开

不得危害国家安全、公共安全、经济安全、社会稳定。

8.9 个人信息主体权利响应

建立渠道，及时响应：查阅、复制、更正、删除、账号注销等请求，不设置不合理障碍。

8.10 投诉举报处置

建立受理处置机制，在规定时限内响应、核查、处置、反馈。

8.11 访问控制与审计

基于分类分级授权，重要操作审批、留痕、审计，防止非授权访问、拷贝、删除、下载。

8.12 数据删除与匿名化

满足条件时及时删除或匿名化，存储介质报废应安全销毁。

8.13 第三方与外包管理

对第三方应用、供应商、合作方实施准入、评估、合同、监督、退出全流程管理。

8.14 数据安全事件应急处置

建立应急机制：分级、启动、资源、流程、预案、演练；事件发生时立即处置、补救、告知主体、报告监管、复盘改进。

9 绩效评价

9.1 监视、测量、分析和评价

组织应监视测量：

a) 目标完成情况；
b) 数据安全控制有效性；
c) 合规性、个人信息保护、重要数据保护情况；
d) 事件、隐患、整改闭环；
e) 第三方合规、审计结果；
f) 相关方反馈、投诉举报处理。

9.2 内部审核

组织应按年度实施内审，验证：
a) 符合本文件、法律法规、自身要求；
b) 有效实施与保持。
应制定审核方案，确保客观公正，出具报告，对不符合项整改验证。

9.3 管理评审

最高管理者应定期评审，确保体系适宜、充分、有效。输入包括：
a) 以往评审跟踪措施；
b) 内外部问题与相关方需求变化；
c) 目标绩效、监视测量结果；
d) 内审结果、不符合与纠正措施；
e) 风险评估、事件、应急、第三方情况；
f) 资源充分性、改进机会。
输出包括：改进、目标调整、资源、风险措施更新。

10 改进

10.1 持续改进

组织应持续改进体系的适宜性、充分性、有效性。

10.2 不合格与纠正措施

发生不合格、事件、隐患、内审 / 评审发现问题时：
a) 处置不合格；
b) 评审原因；
c) 采取纠正措施；
d) 验证有效性；
e) 更新成文信息。

参 考 文 献

[1] GB/T19011 管理体系审核指南
[2] GB/T27011 合格评定认可机构要求
[3] GB/T27021.1 合格评定管理体系审核认证机构要求第 1 部分：要求
[4] GB/T25069 信息安全技术 术语
[5] GB/T35273 信息安全技术个人信息安全规范
[6] 国家认证认可监督管理委员会 20 年第 3 号公告认证技术规范管理办