ICS 35.110
CCS L 70

DB12

天 津 市 地 方 标 准

DB12/T 1198—2023

网络数据安全监督检查规范

Specification for supervision and inspection of network data security

2023－04－07 发布　　2023－05－07 实施

天津市市场监督管理委员会　　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》的规定起草。

本文件由天津市互联网信息办公室提出并归口。

本文件起草单位：天津市互联网信息办公室、天津市大数据协会、天津市标准化研究院、天津市大数据管理中心、中科锐眼（天津）科技有限公司、中国电子技术标准化研究院、北京启明星辰信息安全技术有限公司、国家计算机网络与信息安全管理中心天津分中心、南开大学、天津市滨海新区互联网信息办公室、天津泰达智慧城市科技有限公司、北京市盈科律师事务所。

本文件主要起草人：王芸、徐滨彦、赵洪宇、贾文娟、赵玉玲、于卓、郝津蕾、由方岚、陆浩、丁钊、刘琳、高朗、张渊、曹洪星、尹太泽、苗兴宗、宋一萍、梁哲龙、黄格、徐聪、李凯悦、袁青霞、尚高峰、张尼、张健、蔡迎秋、徐羽佳、高晨涛、郭玉泉、曹静、张云乐、赵明、袁小梅、宋午阳、张良、王煜。

引　言

为维护国家安全、社会公共利益，保护公民、法人和其他组织在网络数据方面的合法权益，加强网络数据安全管理，强化网络数据安全监督检查，建立健全网络数据安全监管体系，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》《网络安全审查办法》《数据出境安全评估办法》《天津市数据安全管理办法（暂行）》《天津市网信部门网络数据安全监督检查工作规范》等法律法规和相关规范，结合本市实际，制定本规范。

网络数据安全监督检查规范

1 范围

本文件规定了网络数据安全监督检查的流程、 内容和要求。

本文件适用于网络数据安全监管部门、行业主管部门、第三方评估机构等组织，对网络数据处理者网络数据的收集、存储、使用、加工、传输、提供、公开和销毁等活动进行监督、检查、管理和评估，也适用于各类网络数据处理者开展建设、 自查、整改工作。

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。

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37988 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 35273和GB/T 37988界定的以及下列术语和定义适用于本文件。

3.1

网络数据 network data

通过网络处理和产生的各类电子数据。

3.2

重要数据 key data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的网络数据。

3.3

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识别的自然人有关的各种信息，不包括匿名化处理后的信息。

3.4

敏感个人信息 personal sensitive information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3.5

网络数据处理者 network data processor

在网络数据处理活动中自主决定处理目的和处理方式的个人和组织。

3.6

数据安全　data security

是指通过采取必要措施，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。

4　监督检查流程

4.1　准备阶段

4.1.1　监督检查发起部门负责编制检查工作方案，工作方案内容包括组织领导、网络数据处理者、检查内容、检查方式、工作安排、工作保障等内容。

4.1.2　实施监督检查前，应根据检查工作方案组建检查组、确定网络数据处理者、确认检查内容、选择检查方式，按照附录 A 执行。

4.1.3　检查组应不少于 2 人，至少有 1 人具备网络数据安全专业知识、培训经历或者从业经验。

4.1.4　检查组事先应向网络数据处理者告知相关检查事项，包括但不限于检查时间、检查内容等。

4.1.5　检查组在实施检查过程中，应如实记录检查时间、地点、内容、发现的问题及其处理情况等。

4.1.6　检查组在实施检查过程中，应严格遵守法律法规、工作纪律要求，对涉及国家秘密、商业秘密、个人隐私的信息，应当保密。

4.2　实施阶段

检查组可采用人员访谈、文档审核、工具测试、配置检查、流量核验等方式，开展检查工作，输出检查记录单，按照附录B执行。实施过程中，应不干扰、破坏网络数据处理者的业务连续性。

4.3　整改阶段

4.3.1　检查组应根据监督检查结果，出具书面检查记录单，针对检查中发现的安全问题，提出整改要求及整改时限。

4.3.2　网络数据处理者应按照整改要求，在规定的时间内，完成整改工作，并形成整改报告，提交检查组。

4.3.3　检查组应跟踪整改情况，并记录整改结果。

4.4　总结阶段

检查组应在检查结束后，总结检查情况，编写总结报告。对检查过程中收集的资料、检查记录单、相关过程文书及整改反馈资料等相关数据，按规定立卷存档，存档时间应不少于三年。

5　监督检查方式

5.1　管理检查

管理检查的检查方式包括但不限于：

a)　人员访谈：通过访谈的方式与网络数据处理者进行交流、讨论等活动,获取相关资料,了解有关信息，检查实际工作与管理制度、文档记录之间的一致程度；

b） 文档审核： 由网络数据处理者提供与数据安全相关的文档材料(如网络数据安全的方针政策、制度规范流程、培训教育材料、以及与产品技术相关的设计实施方案、配置说明、运行记录和其他配套表单),检查组审核相关的文档材料是否已涵盖检查内容。

5.2 技术检查

技术检查的检查方式包括但不限于：

a） 工具测试：利用技术工具和人工方式对系统进行测试,验证是否符合检查内容的技术保障能力要求；

b） 配置检查：根据网络数据处理者提供的技术材料,登录相关的系统工具平台,检查配置是否与材料保持一致,对文档审核内容进行核实；

c） 流量核验：采用旁路部署的方式，对网络数据处理者的系统进行全流量采集，核验是否符合检查内容的技术保障能力要求。

6 监督检查要求

6.1 总体要求

监督检查要求包含通用安全、数据收集安全、数据存储安全、数据使用安全、数据加工安全、数据传输安全、数据提供安全、数据公开安全和数据销毁安全九个部分。涉及重要数据的网络处理者原则上应在符合基本要求的基础上，满足增强要求。

6.2 通用安全

6.2.1 安全合规管理

6.2.1.1 基本要求

本项检查基本要求包括：

a） 是否定期开展数据安全评估工作；

b） 是否定期开展网络安全等级保护测评工作，是否按照测评报告要求，开展整改工作；

c） 是否填报数据安全备案信息，并及时更新相关数据；

d） 是否明确数据安全管理机构、管理岗位及相关职责，是否定期开展数据安全自查工作；

e） 是否明确数据安全事件应急预案，是否定期开展数据安全培训和应急演练活动；

f） 是否建立个人信息管理制度和操作规程，是否明确审批制度、流程、管理范围、安全策略和管控措施，是否明确指定个人信息保护负责人；

g） 涉及个人信息处理的，是否定期对其处理个人信息遵守法律、行政法规的情况进行合规审计；

h） 是否建立数据跨境管理制度，是否明确审批制度、流程、管理范围、安全策略和管控措施；

i） 涉及数据出境的，检查数据出境前是否开展数据出境风险自评估，是否通过网信部门数据出境安全评估。

6.2.1.2 增强要求

本项检查增强要求包括：

a） 涉及处理敏感个人信息，或利用个人信息进行自动化决策，或委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，或向境外提供个人信息的，是否事前开展个人信息保护影响评估；
b） 涉及收集使用儿童个人信息的，是否在符合个人信息保护的基础上，加强对儿童个人信息的保护；
c） 是否建立密码安全管理制度，是否定期开展密码应用安全性评估；
d） 相关信息系统是否采用商用密码检测认证机构核准的密码技术和产品。

6.2.2 数据分类分级

6.2.2.1 基本要求

本项检查基本要求包括：
a） 是否建立数据分类分级制度、规程、操作指南；
b） 是否开展数据分类分级标识和管理工作。

6.2.2.2 增强要求

是否按照数据分类分级的要求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。

6.2.3 终端数据安全

6.2.3.1 基本要求

本项检查基本要求包括：
a） 是否制定面向终端的数据安全管理规范和要求；
b） 是否设置数据安全管理岗位，并指定专人对终端数据安全进行统一管理；
c） 是否为在网络环境的终端设备，安装统一的防病毒软件。

6.2.3.2 增强要求

本项检查增强要求包括：
a） 是否为进入内部网络环境的终端设备，分配终端识别号，并实现计算机终端设备与用户账号的一对一绑定；
b） 是否部署终端数据防泄漏方案，通过技术手段对终端上传输的数据进行风险监测。

6.2.4 监控与审计

6.2.4.1 基本要求

是否明确对内部各类数据访问和操作的日志记录要求、安全监控要求和审计要求。

6.2.4.2 增强要求

是否采用自动和人工审计相结合的方式对网络传输数据的高风险操作进行监测。

6.3 数据收集安全

6.3.1 基本要求

本项检查基本要求包括：

a） 是否制定符合业务的数据收集原则、收集流程和方法；

b） 是否明确收集数据的目的和用途，检查数据收集和获取的合法性和正当性；

c） 涉及个人信息收集的，是否明确个人信息收集的目的、方式和范围，并经被收集者同意或符合其他合法方式。收集儿童个人信息的，应当取得儿童监护人的同意。

6.3.2 增强要求

本项检查增强要求包括：

a） 是否采取技术手段或管控措施，对收集和获取到的数据进行完整性和一致性校验；

b） 是否采取技术手段或管控措施，防止个人信息和重要数据在收集过程中泄露。

6.4 数据存储安全

6.4.1 基本要求

本项检查基本要求包括：

a） 是否建立数据存储管理制度，规范存储媒体使用、购买和标记流程；

b） 是否具备数据备份与恢复技术，建立数据存储冗余策略和存储安全管理制度；

c） 是否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。

6.4.2 增强要求

本项检查增强要求包括：

a） 是否具备对存储媒体性能监控措施，包括使用历史、性能指标、错误或损坏情况，对超过安全阈值的存储媒体进行预警；

b） 是否具备存储媒体访问和使用的安全管理规范，并对存储媒体使用行为进行记录和审计；

c） 是否具备对个人敏感数据、重要数据存储加密的能力。

6.5 数据使用安全

6.5.1 数据正当使用

6.5.1.1 基本要求

是否建立数据使用正当性的管理制度，在数据使用声明的目的和范围内对受保护的个人信息、重要数据进行使用和分析处理。

6.5.1.2 增强要求

是否采用技术手段记录和管理数据使用操作行为。

6.5.2 数据导入导出安全

6.5.2.1 基本要求

本项检查基本要求包括：

a） 是否建立数据导入导出安全制度或审批流程；

b） 是否用存储媒体进行数据导出时，应建立存储媒体的标识规范；

c） 是否对导入导出的终端、用户或服务组件等执行身份鉴别，验证其身份的真实性和合法性。

6.5.2.2 增强要求

是否定期验证导出数据的完整性和可用性。

6.5.3 鉴别与访问控制

6.5.3.1 基本要求

本项检查基本要求包括：

a） 是否指定专人负责管理核心业务系统的用户身份及数据权限管理；

b） 是否制定核心业务系统和数据库的身份鉴别、访问控制和权限管理制度及要求；

c） 是否对业务系统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。

6.5.3.2 增强要求

是否采用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。

6.5.4 数据展示安全

6.5.4.1 基本要求

本项检查基本要求包括：

a） 是否建立数据展示操作规范，明确数据的展示范围、内容、方式；

b） 是否依据用户角色，展示相应数据；

c） 是否在对外部组织展示重要数据和敏感个人信息时，采用数据脱敏等技术。

6.5.4.2 增强要求

是否在展示重要数据和敏感个人信息时，采用防截屏或屏幕水印等技术。

6.6 数据加工安全

6.6.1 数据分析安全

6.6.1.1 基本要求

是否建立数据分析相关数据源获取规范和使用机制，明确数据获取方式、访问接口、授权机制、数据使用等。

6.6.1.2 增强要求

本项检查增强要求包括：

a） 是否建立多源数据聚合、关联分析等数据分析过程中的数据资源操作规范和实施指南；

b） 是否建立数据分析结果输出的安全审查机制和授权控制机制，并采取必要的技术手段和管控措施。

6.6.2 数据脱敏安全

6.6.2.1 基本要求

本项检查基本要求包括：

a） 是否建立数据脱敏制度、流程和方法，指导数据脱敏操作；

b） 是否具备数据脱敏软件或工具，对敏感数据传输、共享、发布等环节敏感信息进行隐藏、模糊化处理。

6.6.2.2 增强要求

是否对脱敏处理过程进行记录，并满足安全审计的要求。

6.7 数据传输安全

6.7.1 基本要求

本项检查基本要求包括：

a） 是否制定数据安全传输管理规范，明确数据传输安全要求；

b） 是否具备对传输通道两端进行主体身份鉴别和认证的技术方案和工具。

6.7.2 增强要求

是否明确业务中需要加密传输的数据范围和加密算法。

6.8 数据提供安全

6.8.1 数据共享安全

6.8.1.1 基本要求

本项检查基本要求包括：

a） 是否制定数据共享内容、范围、安全管理制度；

b） 是否明确数据保护责任，规范第三方网络数据处理者行为；

c） 是否明确数据共享最低安全防护要求或技术保护措施；

d） 是否在数据共享过程中采取数据脱敏、数据加密、安全通道等措施。

6.8.1.2 增强要求

是否对共享数据、数据共享范围及数据共享过程进行监控审计。

6.8.2 数据供应链安全

6.8.2.1 基本要求

本项检查基本要求包括：

a） 是否制定数据供应链安全管理规范，定义数据供应链安全目标、原则和范围；

b） 是否明确数据供应链上下游保护的义务和责任、保护范围、使用目的、供应方式、保密约定等。

6.8.2.2 增强要求

本项检查增强要求包括：