ICS
CCS 点击此处添加 CCS 号

DB6101

西　　安　　市　　地　　方　　标　　准

DB 6101/T XXXX—XXXX

检验检测数据管理规范
第 3 部分：数据安全

Management Specification for Inspection and Detection Data
Part 3: Data Security

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

西安市市场监督管理局　　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。

本文是《检验检测数据管理规范》的第3部分。《检验检测数据管理规范》包括以下部分：

——第1部分：信息分类与编码；

——第2部分：数据接口；

——第3部分：数据安全。

本文件由西安市市场监督管理局提出并归口。

本文件起草单位：瑞特认证检测集团有限公司、陕西瑞智信息技术有限公司、陕西汉通建设工程质量检测有限公司、陕西省建筑科学研究院有限公司、西安尚易安华信息科技有限责任公司、陕西省产品质量监督研究院、国网陕西省电力公司西安供电公司、湖北铁建工程检测有限公司。

本文件主要起草人：曹原、祁喆、胡亚芹、畅亚文、张源、刘娟、孙晓广、田鹏辉、曹珺溥、李鹏、王雨润、王磊、马良.

检验检测数据管理规范
第3部分：数据安全

1 范围

本文件规定了检验检测数据管理通用安全、安全监管、数据传输安全、数据交换安全、数据退役安全等方面要求。

本文件适用于检验检测信息系统中基础信息的分类，检验检测机构信息系统的建设与应用及机构数据共享。

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 27000 合格评定 词汇和通用原则
GB/T 27020 合格评定 各类检验机构的运作要求
GB/T 11457 信息技术 软件工程术语
GB/T 37988 信息安全技术 数据安全能力成熟度模型
GB/T 39477 信息安全技术 证书信息共享 数据安全技术要求
RB/T 001 认证认可行业标准编写规范
RB/T 002 认证认可行业标准分类规范
RB/T 214 检验检测机构资质认定能力评价 检验检测机构通用要求
RB/T 028 实验室信息管理系统管理规范

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

采用技术和管理措施来保护数据的保密性、完整性和可用性等。

3.2

大数据 big data

在活动过程中产生的具有体量巨大、来源多样、生成极快、多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

3.3

敏感数据 sensitive data

由权威机构确定的受保护的信息数据。

注:敏感信息数据的泄露、修改、破坏或丢失会对人或事产生可预知的损害。

3.4

重要数据 important data

不涉及国家秘密，但如果泄露、毁损、丢失或被窃取、篡改和非法使用可能危害国家安全、国计民生、公共利益的未公开数据。

3.5

个人信息 personal Information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

3.6

数据脱敏 data masking

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。

3.7

数据擦除 data erase

使用预先定义的无意义、无规律的信息覆盖存储介质上原数据，达到对存储介质内电子数据进行销毁的目的，存储介质可继续使用。

3.8

数据销毁 data destruction

通过物理手段破坏存储介质的实体，让数据无法被读出。数据销毁分为- -级销毁和二级销毁。

4 概述

4.1 数据生命周期的各个阶段

本标准定义了数据生命周期的六个阶段，并针对公共数据特点和场景进行了描述。

--数据采集:组织机构内部系统中新产生数据，以及从外部系统收集数据的阶段；

--数据传输:数据从一个实体通过网络流动到另一个实体的阶段。在数据方面，通常是检验检测机构将数据传输归集到云平台、数据资源共享交换平台、大数据中心等；

--数据存储:数据以任何数字格式进行物理存储或云存储的阶段。在检验检测数据方面，数据存储可能涉及采集数据存储、归集汇聚后的数据存储、数据共享交换后的数据存储等；

--数据使用:组织机构针对数据进行计算、分析、可视化等操作的阶段。在检验检测数据方面，通常是对数据进行整合，形成基础数据库和主题数据库，并进行大数据分析利用转化成公共大数据产品或服务；

--数据交换:组织机构与组织机构及个人进行数据共享、开放、交换的阶段。检验检测数据共享通常是检验检测机构因履行职责需要使用其他数据；

--数据退役;不再进行处理的数据进入数据退役阶段，涉及对信息的归档、转移、丢弃、销毁以及对存储介质的销毁处理等。

4.2 数据安全体系

数据生命周期安全如图1所示。

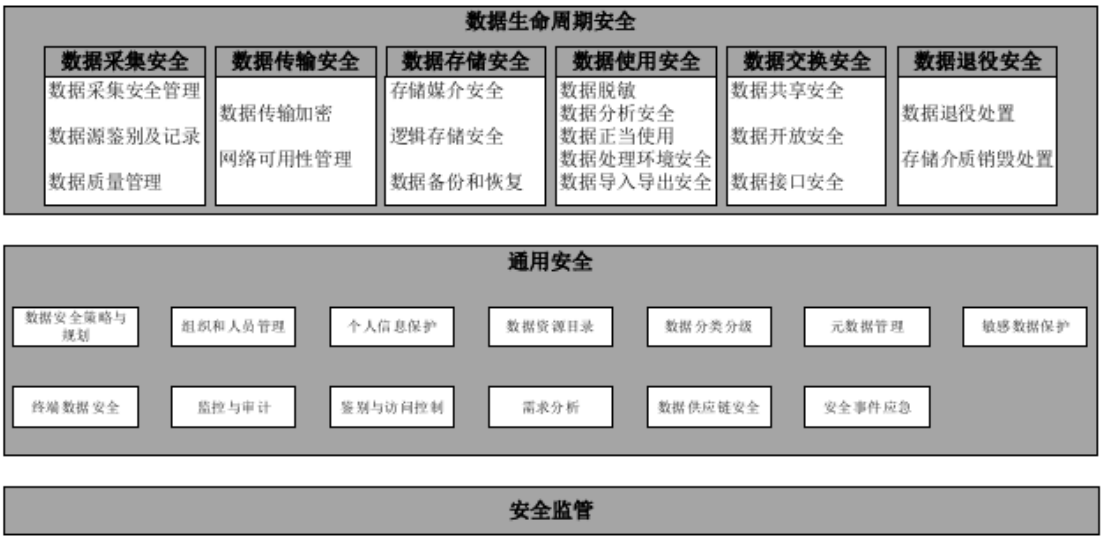

图1 数据生命安全周期

5 通用安全

5.1 数据安全策略规划

建立组织机构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。

检验检测机构应:

a) 设立负责组织机构数据安全制度流程和战略规划的建设的岗位和人员；

b) 明确符合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；

c) 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；

d) 明确并实施大数据系统和数据应用安全实施细则；

e) 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;

f) 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;

g) 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；

h) 确保负责制定数据安全总体策略和战略规划的人员了解组织的业务发展目标，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；

i) 确保负责制定数据安全制度和规程的人员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；

j) 确保负责推广数据安全策略规划的人员能够以员工和相关方易理解的方式，通过培训等形式对数据安全管理的方针、策略和制度进行有效传达。

5.2 数据分类编码

数据分级编码应满足DB6101/T XXXX.1《检验检测数据管理规范 第1部分：数据分类与编码》的要求。

6 数据采集安全

6.1 应设置数据采集安全团队，主要负责为公司整体的数据采集制定合理的管理制度，同时推动制度、要求和流程的落实和执行；另方面针对不同的业务和项目场景的数据安全提供评价服务，负责数据采集的风险评价服务。

6.2 数据安全岗位的能力要求应满足但不限于以下要求：

a) 熟悉国家网络安全法，以及组织机构所属行业的政策和监管要求；

b) 熟悉中华人民共和国密码法，以及组织机构所属行业的政策和监管要求；

c) 熟悉中华人民共和国数据安全法，以及组织机构所属行业的政策和监管要求；

d) 严格按照网络安全法和个人信息安全防范等相关法律法规和行业规范执行；

e) 熟悉组织机构的业务特征，了解业务线的政策方向和战略调整，具备良好的数据采集安全风险意识；

f) 有针对性的风险评估报告和相应的解决方案，确保项目实施过程中数据采集能够顺利有序地进行。

6.3 在对数据采集的过程中应组织风险评估小组对采集过程进行风险评估，评估内容如下：

a）采集过程是否合规：是否有采集负责人对相关采集操作进行审核，采集的数据是否最小化，采集过程是否足够公开透明并接受了外部监督；

b）采集过程中的安全要求：是否采用了加密，完整性校验，匿名，日志和断网等保护措施，以保护被采集数据的安全；

c）数据采集相关的其他工作。

6.4 数据采集安全应能实现采集策略遵循最小够用原则，确保采集数据的一致性，且保证采集的数据不会被滥用，确保通信过程采取双向加密以及脱敏过程的安全。

7 数据传输安全

7.1 在数据采集传输过程中需进行数据防泄漏，目前可采用但不限于以下数据防泄漏技术对数据进行保护：

a） 采用数据加密技术包含磁盘加密，文件加密，透明文档加解密等技术路线，目前以透明文档加解密技术最为常见，透明文档的加解密技术通过过滤驱动对受保护的敏感数据内容设置相应的参数，从而有选择性的保护特定进程产生的特定文件，写入时进行加密存储，读取文件时进行自动解密，整个过程不会影响到其他受保护的内容；

b） 采用数字权限管理（DRM）安全策略，在敏感数据文件生成，存储和传输的同时实现自动化保护，以及通过条件访问控制策略防止对敏感数据进行非法复制，泄露和扩散等操作；

c） 采用基于内容的数据防泄漏DLP，数据防泄漏以深层内容识别为核心，基于敏感数据内容策略定义,监控数据的外传通道,对敏感数据的外传进行审计和控制,数据防泄漏不会改变正常的业务流程，具备丰富的审计功能，可用于对数据泄露事件进行时候定位和追责溯源。

7.2 数据的网络传输过程依赖于网络的可用性，应确保数据在网络中传输的稳定性，需将网络故障或网络瘫痪的可能性降到最低，同时要求网络和业务恢复时间处在可控范围之内。

8 数据存储安全

8.1 存储媒介安全

针对组织内需要对检验检测数据存储媒介进行访问和使用的场景，提供有效的技术和管理手段，防止不当使用而可能引发的数据泄漏风险。存储媒介包括终端设备及网络存储。

检验检测机构应：

a) 设立统一负责检验检测数据存储媒介安全管理的岗位和人员；

b) 明确检验检测数据存储媒介访问和使用的安全管理规范，建立存储媒介使用的审批和记录流程；

c) 明确购买或获取检验检测数据存储媒介的流程，要求通过可信渠道购买或获取存储媒介，并针对各类存储媒体建立格式化规程；

d) 建立检验检测数据存储媒介资产标识，明确存储媒介存储的数据；

e) 对检验检测数据存储媒介进行常规和随机检查，确保存储媒介的使用符合机构公布的关于存储媒介使用的制度；

f) 使用技术工具对检验检测数据存储媒介性能进行监控，包括存储媒介的使用历史、性能指标、错误或损坏情况，对超过安全阈值的存储媒介进行预警；

g) 对检验检测数据存储媒介访问和使用行为进行记录和审计；

h) 确保负责该项工作的人员熟悉检验检测数据存储媒介安全管理的相关合规要求，熟悉不同存储媒介访问和使用的差异性；

i) 确保云服务客户数据、用户个人信息、重要数据等存储于中国境内，如需出境应遵循国家相关规定。

8.2 逻辑存储安全

基于检验检测数据业务特性和数据存储安全要求，建立针对检验检测数据库和逻辑存储架构的有效安全控制。

检验检测机构应：

a) 设立组织内统一负责检验检测数据数据逻辑存储安全管理的岗位和人员，由该岗位和人员明确整体的数据逻辑存储系统安全管理要求，并推进相关要求的实施；

b) 设立各数据逻辑存储系统的安全管理员，负责执行数据逻辑存储系统、存储设备的安全管理和运维工作；

c) 明确检验检测数据逻辑存储管理安全规范和配置规则，各类数据存储系统的账号权限管理、访问控制、日志管理、加密管理、版本升级等方面的要求；

d) 确保内部的检验检测数据存储系统在上线前应遵循统一的配置要求进行有效的安全配置，对使用的外部数据存储系统也进行有效的安全配置；

e) 明确数据逻辑存储隔离授权与操作要求，确保具备多用户数据存储安全隔离能力；

f）提供检验检测数据存储系统配置扫描工具，定期对主要数据存储系统的安全配置进行扫描，保证符合安全基线要求；

g）利用技术工具监测逻辑存储系统的检验检测数据使用规范性，确保数据存储符合组织的相关安全要求；

h）具备对个人信息、重要数据等敏感数据的加密存储能力；

i）对敏感检验检测数据采用符合国家相关规定的数据加密方式与密码算法进行加密存储保护；

j）确保负责该项工作的人员应熟悉数据存储系统架构，并能够分析出数据存储面临的安全风险，从而能够保证对各类存储系统的有效安全防护。

8.3 数据备份和恢复

通过对检验检测数据定期的备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。检验检测机构应：

a）明确负责检验检测数据备份和恢复管理工作的岗位和人员，由该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；

b）明确检验检测数据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；

c）明确检验检测数据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；

d）明确检验检测数据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；

e）依据检验检测数据生存周期和业务规范，建立数据生命周期各阶段数据归档的操作流程；

f）明确归档检验检测数据的压缩或加密要求；

g）明确对归档检验检测数据的安全管控措施，非授权用户不能访问归档数据；

h）识别组织适用的合规要求，按监管部门的要求对相关检验检测数据予以记录和保存；

i）明确检验检测数据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；

j）明确过期检验检测数据存储的安全保护机制，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；

k）建立检验检测数据备份与恢复的统一技术工具，保证相关工作的自动执行；

l） 建立备份和归档检验检测数据安全的技术手段，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；

m） 定期采取必要的技术措施查验备份和归档检验检测数据的完整性和可用性；

n） 建立对过期存储检验检测数据及其备份数据彻底删除或匿名化处理的方法和机制，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；

o） 通过风险提示和技术手段避免非过期检验检测数据的误删除，确保在一定的时间窗口内的误删除数据可以手动恢复；

p） 确保存储架构具备跨机柜或跨机房容错部署的能力；

q） 确保负责该项工作的人员了解检验检测数据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；

r） 确保负责该项工作的人员了解检验检测数据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。

9 数据使用安全

9.1 数据脱敏

根据检验检测数据相关法律法规、标准的要求以及业务需求，对敏感检验检测数据进行脱敏处理，保证数据可用性和安全性的平衡。

检验检测机构应：

a） 设立负责检验检测数据脱敏的岗位和人员，由该岗位和人员制定数据脱敏的原则和方法，并提供相关技 术支持；

b） 在检验检测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数据脱敏规则及方法；

c） 明确检验检测数据脱敏规范，明确数据脱敏的规则、脱敏方法和使用限制等；

d） 明确需要对检验检测数据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分工；

e） 如果涉及检验检测数据可视化场景，对可视化数据进行脱敏处理，明确组织内须脱敏的可视化数据范围；

f） 供统一的检验检测数据脱敏工具，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；

g）提供面向不同检验检测数据类型的脱敏方案，可基于场景需求自定义脱敏规则；

h）确保检验检测数据脱敏后保留原始数据格式和特定属性，满足开发与测试需求；

i）对检验检测数据脱敏处理过程相应的操作进行记录，以满足数据脱敏处理安全审计要求；

j）明确针对可视化检验检测数据的脱敏方案，确保数据的保密性；

k）确保负责该项工作的人员熟悉常规的检验检测数据脱敏技术，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；

l）确保负责该项工作的人员具备对检验检测数据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。

9.2 数据分析安全

通过对检验检测数据整合分析利用过程采取适当的安全措施，防止检验检测数据挖掘、分析过程中有价值信 息和个人隐私泄露的安全风险。

检验检测机构应：

a）设立负责检验检测数据分析安全的岗位和人员，由该岗位和人员负责制定数据分析安全原则、提供相应技术支持；

b）明确检验检测数据处理与分析过程的安全规范，覆盖构建数据仓库、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；

c）明确检验检测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、分析操作等的正当性；

d）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，整体保证检验检测数据分析的预期不会超过相关分析团队对数据的权限范围；

e）明确检验检测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，防止数据分析结果输出造成安全风险；

f）在针对个人信息的数据分析中，采用多种技术手段以降低数据分析过程中的隐私泄漏风险，如差分隐私保护、k匿名、常态加密法等；

g）记录并保存检验检测数据处理与分析过程中对个人信息、重要数据等敏感数据的操作行为；

h）提供组织统一的检验检测数据处理与分析系统，并能够呈现数据处理前后数据间的映射关系；

i）确保负责该项工作的人员能够基于合规性要求、相关标准，对检验检测数据安全分析中所可能引发的数 据聚合的安全风险进行有效评估，并针对分析场景提出有效的解决方案。

9.3 数据正当使用

基于国家相关法律法规对检验检测数据使用的要求，建立检验检测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，防止检验检测数据资源被用于不正当目的。

检验检测机构应：

a）设立负责对检验检测数据正当使用管理、评估和风险控制的岗位或人员；

b）明确检验检测数据使用的评估制度，使用个人信息和重要数据前，先进行安全影响评估，保证满足国家 合规要求后，才允许使用；

c）避免检验检测数据使用时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；

d）明确检验检测数据使用正当性的制度，保证数据使用在声明的目的和范围内；

e）依据检验检测数据国家合规要求，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；

f）完整记录检验检测数据使用过程的操作日志，以备识别潜在违约使用者；

g）确保负责该项工作的人员能够按照最小够用等原则管理权限，并具备对检验检测数据正当使用相关风险的分析和跟进能力。

9.4 数据处理环境安全

为组织内部的检验检测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，确保检验检测数据处理的过程中有完整的安全控制管理和技术支持。

检验检测机构应：

a）明确业务团队负责检验检测数据处理环境安全管理的岗位和人员；

b）确保在检验检测数据处理环境的系统设计、开发和运维阶段制定相应的安全控制措施，实现对安全风险的管理；

c）明确对检验检测数据处理环境的安全管理要求；

d）基于检验检测数据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漏等方面进行安全要求和控制；

e）明确适合检验检测数据处理环境的数据加解密处理策略和密钥管理要求；

f）确保检验检测信息管理平台具备分布式处理过程中数据文件鉴别和访问用户身份认证的策略，保障分布式处理检验检测数据文件的可访问性；

g）实现检验检测数据处理系统与数据权限管理系统的联动机制，确保用户在使用数据系统前已获得授权；

h）确保基于检验检测数据处理系统的多用户的特性，对不同的用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；

i）建立检验检测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；

j）确保检验检测信息管理平台具备分布式处理节点间可信连接策略和规范，采用节点认证等机制确保节点接入的真实性；

k）确保负责该项工作的人员了解在检验检测数据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。

9.5 数据导入导出安全

通过对检验检测数据数据导入、导出过程中对数据的安全性进行管理，防止检验检测数据导入导出过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的检验检测数据泄漏风险。

检验检测机构应：

a）设立负责检验检测数据导入导出安全管理岗位和人员，由岗位和人员负责制定规则和提供技术能力，推动在组织机构内业务场景落地执行；

b）依据检验检测数据分类分级要求，建立数据导入导出安全策略，如授权和访问控制策略、脱敏策略、加密策略等；

c）按照检验检测数据提供方对共享数据的分级分类要求，建立相应的授权和访问控制机制，标记数据资产的责任主体；

d）建立检验检测数据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；

e）按照检验检测数据导入导出安全策略，将敏感数据脱敏后再导出；

f）具有对检验检测数据导入过程的保护和回退机制，保证获取过程中产生问题时能有效还原和恢复数据；

g）具有检验检测数据自动加载的故障恢复能力；

h) 在数据导入时检验数据的质量，包括对数据格式和接口提出统一要求，并对获取数据是否满足要求做出认定；

i) 建立针对导出介质的标识规范，明确介质的命名规则、标识属性等重要信息，定期验证导出检验检测数据的完整性和可用性；

j) 制定导入导出审计策略和日志管理规范,并保存导入导出过程中的异常检验检测数据处理记录；

k) 记录并定期审计组织内部的检验检测数据导入导出行为，确保未超出数据授权使用范围；

l) 对检验检测数据导入导出终端、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；

m) 采取数据加密、访问控制等技术手段，保障数据在传输中的保密性、完整性和可用性；

n) 在导入导出完成后，清除数据导入导出通道缓存的检验检测数据，保证导入导出过程中涉及的数据不被恶意恢复；

o) 确保负责检验检测数据导入导出安全工作的人员充分理解组织机构的数据导入导出策略，并根据数据导入导出的业务场景执行相应的风险评估，提出实际的解决方案。

10 检验检测数据交换安全

10.1 检验检测数据交换和共享安全

10.1.1 总体要求

如下：

a) 应按照 GB/T 22239 进行网络安全等级保护设计和实施；

b) 应按照 GB/T 22240 确定网络安全防护等级。

c) 应按照 GB/T 39786-2021 进行系统加密。

10.1.2 安全策略

10.1.2.1 安全管理

应根据实际环境满足安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理相关要求。

10.1.2.2 安全技术

应根据实际环境满足安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心相关要求。

10.1.3 认证与授权

10.1.3.1 身份确认

认证与授权在数据和目录传输之前应核实对方身份真实性。

10.1.3.2 访问控制

认证与授权应根据数据敏感等级及用户身份，制定相应的访问控制策略，确保只有合法用户才能操作并访问资源。

10.1.3.3 加密管理

认证预授权应施以密码为基础的安全机制分级管理，可根据不同外在、内在环境选择不同等级密码算法和秘钥分发技术

10.2 检验检测数据接口安全

10.2.1 安全认证

检验检测数据接口采用数字证书或数字令牌的方式实现安全认证。

10.2.2 数字证书

使用检验检测数据接口的生产经营者，可以申请具有相应资质的CA中心签发的数字证书。使用数字证书对接口的传输内容进行数字签名，实现身份识别和数据传输安全。

10.2.3 数字令牌

使用检验检测数据接口的生产经营者，可以申请追溯平台签发的唯一的数字令牌。使用接口传输数据时附加数字令牌，实现身份识别和数据传输安全。数字令牌的有效期为2个月，在数字令牌过期前，生产经营者需要重新申请新的令牌;生产经营者的新令牌一经颁发，原有令牌即刻失效。

10.2.4 密码算法

数字证书和数字令牌采用的密码算法，应按GB/T 20518和ISO 24165中的要求，采用符合国家规定的密码算法。

11 数据退役安全

11.1 数据退役处置

通过建立针对公共数据的归档、转移、删除、净化机制，实现数据退役，防止因对存储媒介中的数据进行恢复而导致的公共数据泄漏风险。

检验检测机构应:

d) 设立统一负责公共数据退役管理的岗位和人员，由该岗位和人员制定公共数据退役处置规范，明确公共数据转移和归档要求，推动相关要求在业务部门落地实施;

e) 建立组织的数据归档流程，明确归档安全要求，对归档数据进行审批、记录，确保所有归档过程可控、可溯源、可审计:

f) 建立明确的数据转移流程，明确数据转移安全要求，数据在组织内部或组织间转移时，应进行数据转移的安全风险评估;

g) 明确数据保存年限要求，数据在组织内部退役时，应进行数据保存年限评估，符合相应监管要求;

h) 记录转移过程和转移的数据情况，保证数据转移过程的安全可靠和可用性，确保转移数据的一致性、完整性;

i) 可单独采用电子归档形式，按国家和自治区有关规定对公共数据资源进行归档和登记备份

j) 建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问:

k) 建立归档数据的安全策略和管控措施，确保非授权用户不能访问归档数据;

l) 依照数据分类分级建立数据退役策略和管理制度，明确数据的退役场景、退役对象、退役方式和退役要求;

m) 建立规范的数据退役流程和审批机制，设置退得过程的相关收督角色，监督操作过程，并对审批和退役过程进行记录控制:

n) 按国家相关法律和标准销毁个人信息、重要数据等敏感数据;

o) 针对网络存储数据，建立硬销毁和软销毁的数据退役方法和技术，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退役策略与机制:

p) 配置必要的数据退役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。

q) 确保负责数据退役安全工作的人员应熟悉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。