

SZSD

数 字 山 东 工 程 标 准

SZSD07 0001—2024

公共数据脱敏管理规范

Specification for public data desensitization

2024-04-15 发布

2024-06-01 实施

目 次

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

 3.1 公共数据 1

 3.2 敏感数据 1

 3.3 数据脱敏 1

 3.4 动态脱敏 1

 3.5 静态脱敏 1

 3.6 脱敏算法 1

 3.7 脱敏系统 1

4 基本原则 2

 4.1 真实性 2

 4.2 有效性 2

 4.3 一致性 2

 4.4 稳定性 2

5 管理要求 2

 5.1 基本要求 2

 5.2 系统要求 3

 5.3 人员要求 4

 5.4 安全要求 5

 5.5 技术要求 5

参考文献 6

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。

本文件由潍坊市大数据局提出并归口。

本文件起草单位：昌乐县大数据中心、山东环球软件股份有限公司。

本文件主要起草人：吴巍、吴珂、程庆军、刘德永、孙兴善、张林、陈颜章、郝俊堂、张阳。

公共数据脱敏管理规范

1 范围

本文件规定了公共数据脱敏的基本原则和管理要求。
本文件适用于公共数据脱敏工作的规划、实施和管理。

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 20945—2013 信息安全技术信息系统安全审计产品技术要求和测试评价方法

3 术语和定义

3.1 公共数据 public data

国家机关、法律法规规章授权的具有管理公共事务职能的组织，在依法履行职责和提供公共服务过程中，所获取的数据资源以及法律、法规规定纳入公共数据管理范围的其他数据资源。

3.2 敏感数据 sensitive data

能具备一定的安全性要求，一旦泄露会对人、单位、企业、甚至国家产生某种风险的数据。

3.3 数据脱敏 data desensitization

对某些敏感信息按照一定规则进行数据变形，实现敏感信息隐私数据的可靠保护。

3.4 动态脱敏 dynamic desensitization

针对敏感数据进行数据抽取、数据漂白和动态掩码的专业数据脱敏技术，主要对查询生产库返回的数据进行实时脱敏处理，确保返回数据可用而安全。

3.5 静态脱敏 static desensitization

针对敏感数据从生产环境脱敏完毕之后，在非原生产环境使用，一般用于解决测试、开发、共享、数据分析等场景下需要生产库的数据量与数据间的关联，以排查问题或进行数据分析等，但又不能将敏感数据存储于非生产环境的问题。

3.6 脱敏算法 desensitization algorithm

对原始数据进行变形，去隐私化处理的算法。

3.7 脱敏系统 desensitization system

采用各种脱敏算法，通过自动化工具实现敏感数据发现、脱敏操作执行和脱敏全流程管理的应用系统。

4 基本原则

4.1 真实性

脱敏过程需保持用于后续分析的数据真实特征，以助于实现数据相关业务需求。真实性特征包括但不限于数据结构特征和数据统计特征。

4.2 有效性

经过数据脱敏处理后，原始信息中包含的敏感信息已被移除，无法通过处理后的数据得到敏感信息。

4.3 一致性

数据脱敏后，保留主外键关联一致性，保留业务数据关联业务一致性，保留原数据间隐含包含及关联关系。

4.4 稳定性

由于原始数据间存在关联性，为保障数据使用者可正常使用和分析数据，因此数据脱敏时需保证对相同的原始数据，在各输入条件一致的前提下，无论脱敏多少次，其最终结果数据是相同的。

5 管理要求

5.1 基本要求

5.1.1 流程管理

应制定数据脱敏流程规范，并符合下列要求：

- a) 明确敏感数据管理和使用部门，并明确参与数据脱敏工作各方的业务和安全责任边界；
- b) 根据安全合规要求，参照敏感数据分类分级规范，明确各类数据的安全管控方式；
- c) 建立完备的脱敏审批机制，确保数据脱敏工作安全合规；
- d) 建立数据脱敏全生命周期工作过程体系，确保数据脱敏执行工作合规；
- e) 建立数据脱敏系统操作和运维管理制度，并定期评审和修订；
- f) 数据脱敏流程规范建立后，定期对数据管理、数据使用、脱敏系统运维等相关各方开展培训，提升主体责任和规范化意识。

5.1.2 组织管理

应成立专门的数据脱敏管理小组，并设置专门的脱敏操作员、安全管理员和审计管理员，分工协作，实现“三权分离”。

5.1.3 评价管理

应按照系统、人员、安全、技术以及数据脱敏工作过程等多方面规范要求，每年开展至少1次及以上数据脱敏评价工作，评价其真实性、有效性、稳定性。评价工作宜在数据脱敏工作验收结束后1个月内完成。

5.2 系统要求

5.2.1 脱敏系统安全

脱敏系统应采用经国家有关部门认证的产品。系统上线前应进行源代码审查，并通过信息系统安全等级保护三级以上测评。系统运行过程中应定期进行安全扫描，接受网络信息安全和数据安全风险评估，确保安全可靠，无漏洞后门。

5.2.2 系统账号口令

脱敏系统账户的口令应为无意义的字符组，长度至少为十位，并包含大写字符、小写字符、数字和特殊符号，脱敏系统账户口令应定期修改，最长使用时间不超过3个月。

5.2.3 数据源

应适用数据库、文件、大数据平台、动态数据流等不同类型的数据库源。

5.2.4 数据脱敏任务

5.2.4.1 静态数据脱敏产品应制定数据脱敏任务。任务宜包括：

- a) 设置原始数据存储源；
- b) 设置抽取范围；
- c) 设置脱敏内容；
- d) 选择脱敏规则；
- e) 设置目标数据存储源。

5.2.4.2 动态数据脱敏产品应制定数据脱敏任务。任务宜包括：

- a) 根据动态数据源的范围，设置数据脱敏任务；
- b) 配置数据源的参数信息；
- c) 设置动态数据的脱敏范围；
- d) 设置脱敏内容；
- e) 设置数据脱敏的起止时间；
- f) 选择脱敏规则。

5.2.5 敏感数据自动扫描和检测

产品应能够根据预定义的策略对敏感数据进行自动扫描和检测：

- a) 静态数据脱敏产品应能对整个数据库或文件中敏感数据进行自动扫描和检测；
- b) 动态数据脱敏产品应能对数据流中敏感数据进行自动扫描和检测。

5.2.6 数据脱敏子集抽取

静态数据脱敏的产品应能够创建子集抽取规则。产品宜包括下列功能：

- a) 根据用户的要求创建相比原始数据较小的子集；
- b) 应具有抽取多表间关联子集的功能，在数据脱敏后，保持数据表之间的关联关系。

5.2.7 任务监控

脱敏产品应能够对数据脱敏任务进行监控。产品宜包括下列功能：

- a) 数据脱敏任务应定时调度(静态脱敏)；
- b) 能够启动、暂停、继续和停止数据脱敏任务(静态脱敏)；
- c) 提供对数据脱敏任务的状态监测，以图形化方式展现每个任务的处理进度，以日志方式展现任务处理明细及任务告警(静态脱敏)；
- d) 实时展现脱敏情况(动态脱敏)；
- e) 展现历史记录，一定时间段的脱敏情况(静态脱敏、动态脱敏)

5.2.8 审计记录

5.2.8.1 审计记录生成，产品应对下列可审计事件生成记录：

- a) 数据脱敏操作日志，包括数据脱敏审批流程和数据脱敏任务的执行等；
- b) 鉴别机制的使用，包括系统用户的登录和注销日志；
- c) 管理操作日志，包括安全策略变更、对用户及角色进行增加、删除和修改等；
- d) 包括事件发生的日期和时间，事件类型，主体身份和成功或失败事件；
- e) 详细记录原始数据、脱敏范围、目标位置等信息。

5.2.8.2 审计记录查阅，产品应包含下列审计记录查询与访问功能：

- a) 只允许授权管理员访问审计记录；
- b) 满足按条件对审计记录进行组合查询。

5.2.8.3 审计记录存储，产品应根据GB/T 20945-2013 标准中说明的基本级、增强级等级划分，提供下列安全功能要求：

- a) 存储于掉电非易失性存储介质中(基本级)；
- b) 审计记录导出，并能够异地存储(增强级)；
- c) 审计记录应至少保存 6 个月及以上时间，其中涉及关键性日志建议保留 1 年以上或永久保存。

5.2.9 接口管理

开发者应提供一个接口规范。接口规范宜满足下列要求：

- a) 描述所有外部接口的用途与使用方法，适当提供效果、例外情况和错误消息的细节；
- b) 标识安全功能子系统的所有接口；
- c) 标识安全功能子系统的哪些接口是外部可见的；
- d) 完备地表示产品安全功能。

5.3 人员要求

5.3.1 保密管理

脱敏操作员、安全管理员、安全审计员应以个人名义与组织签署保密协议和安全承诺书。若涉及相关脱敏实施单位，该单位应同时与组织签署保密协议和数据安全承诺书。

5.3.2 审计管理员

负责对脱敏操作员、安全管理员的操作行为进行审计、跟踪、分析、和监督检查，及时发现违规行为和异常行为，进行数据库日志、脱敏系统日志、安全事件的分析和取证。

5.3.3 安全管理员

负责制定脱敏系统的安全策略，数据脱敏工作的范围和日程，并进行日常安全检查、权限管理和日常操作培训。

5.3.4 脱敏操作员

负责数据脱敏工作的具体执行，并向安全管理员和脱敏审计员定期汇报工作情况。

5.4 安全要求

5.4.1 安全角色

根据授权用户不同的安全角色，赋予授权用户不同的访问权限，并且安全角色之间应相互制约。重要功能(如用户/权限管理、审计记录管理、数据脱敏任务管理和敏感数据操作)应由不同用户执行。

5.4.2 审批流程

在对敏感数据进行操作时，应提供审批流程，通过审批后才能执行数据脱敏任务。

5.4.3 通信安全

在脱敏过程中，脱敏系统应确保各组件之间传输的数据非明文。

5.4.4 安全可控

原始数据经过数据脱敏处理后，仍保持部分统计特征和结构特征，存在泄露风险，应采取恰当的安全管理手段，防止数据外泄。

5.4.5 安全审计

应在数据脱敏的各个阶段加入安全审计机制，详细记录数据处理过程中的相关信息，形成完整数据处理记录。

5.4.6 安全评估

应制定数据脱敏评估体系，定期评估和维护数据脱敏内容，并定期对接触到脱敏数据的相关方进行脱敏安全培训。

5.5 技术要求

5.5.1 数据脱敏算法

按照数据使用场景及安全要求配置不同的脱敏算法。

5.5.2 脱敏处理要求

敏感数据进行适用的脱敏算法规则处理后，可通过数据打标，区分脱敏后数据与原始数据。经过脱敏处理后的数据在对外共享开放前，应满足脱敏结果核对需求：

- a) 脱敏数据标识随着敏感数据一起流动；
- b) 标识信息不易被恶意攻击者删除和篡改；
- c) 考虑便捷性和安全性，使标识后的数据容易被识别。

参 考 文 献

- [1] 《中华人民共和国网络安全法》
 - [2] 《中华人民共和国数据安全法》
 - [3] 《中华人民共和国个人信息保护法》
-