ICS 35.020
L 70

# 团　　体　　标　　准

T/GDCSA 008—2021

# 信息技术应用创新项目数据安全保护指南

Guide for data security protection of information technology application innovation project

2021-12-28 发布　　2021-12-28 实施

广东省网络空间安全协会　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。

本文件由广东省网络空间安全协会提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：北京网御星云信息技术有限公司、杭州安恒信息技术股份有限公司、北京启明星辰信息安全技术有限公司、广东省电信规划设计院有限公司、杭州美创科技有限公司、广州绿盟网络安全技术有限公司、联通（广东）产业互联网有限公司、韶关学院、赛评信息技术有限公司、网安联认证中心有限公司、广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院、广州华南信息安全测评中心、网安联信息技术有限公司。

本文件主要起草人：程昌明、肖兴罗、邢静、杨钧安、黄根华、林龙、胡小立、颜燕、林业辉、黄东宁、招祥吉、胡贞华、李若飞、谭伟基、肖衍林、黄其森、黄学武、梁晓冰、林勇忠、胡文涛、杨佳能、赵仕嘉、黄珊珊、毛翠芳、李洪铭。

# 信息技术应用创新项目数据安全保护指南

## 1 范围

本文件规定了信息技术应用创新项目中数据保护对象的分类分级和数据安全等主要内容。

本文件适用于指导信息技术应用创新项目中数据保护对象的安全建设和监督管理工作。

## 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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB 50174-2008 电子信息系统机房设计规范

T/ISEAA 002-2021 信息安全技术 网络安全等级保护大数据基本要求

## 3 术语和定义

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

**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。

3.3

**数据全生命周期 data full life cycle**

数据的收集阶段、存储阶段、使用阶段、传输阶段、交换阶段和销毁阶段。

3.4

**国产密码 national code**

国家密码局认定的国产密码算法。

3.5

**线分类法 line classification method**

按选定的若干属性（或特征）将分类对象逐次地分为若干层级，每个层级又分为若干类目。统一分支的同层级类目之间构成并列关系，不同层级类目之间构成隶属关系。同层级类目互不重复，互不交叉。

# 4 数据分类分级

a) 应明确数据分类分级原则、标准和方法，并建立数据分类分级模型；
b) 应基于数据资产本身的行业属性特征，采用多维度和线分类法相结合实现分类；
c) 应基于数据资产的重要性和敏感程序对数据进行安全级别的划分；
d) 应根据所属行业的数据资源属性或特征，将其按照一定的原则和方法进行区分和归类，具体数据分类分级以行业规范为准。

# 5 数据安全

## 5.1 产生阶段

### 5.1.1 技术部分

#### 5.1.1.1 敏感数据定位

应进行数据资产管理，形成数据资产地图。

#### 5.1.1.2 安全审计

a) 应对用户进行安全审计，审计记录应包含事件的时间、事件类型、主体标识、客体标识和结果等内容；
b) 审计记录应禁止被修改，定期进行备份；
c) 审计进程应确保未被挂起或中断；
d) 应具备异常行为分析手段。

#### 5.1.1.3 数据源鉴别

a) 应明确数据采集的目的、用户、方式、范围、采集源等，对外部采集的数据须确认其合法性和完整性；
b) 应确保数据采集源可追溯。

#### 5.1.1.4 数据质量保障

a) 应建立有效的数据纠错机制；
b) 应定期检查数据的质量。

### 5.1.2 管理部分

数据生产/录入岗位权限，应对数据产生、录入、修改等相关岗位的帐号配置最小权限。删除数据时，应进行二次审批。

## 5.2 存储阶段

### 5.2.1 技术部分

#### 5.2.1.1 物理管控

参照 GB/T 22239-2019 中 8.1.1 或 GB 50174-2008 的 B 级进行设计。

#### 5.2.1.2 数据完整性

参照 T/ISEAA 002-2021 中 7.4.7c。

#### 5.2.1.3 数据库高可用性

a) 应具备抗攻击能力， 防止主数据宕机；
b) 应具备数据冗余能力，如日志异步、日志同步、存储同步等；
c) 应保证冗余数据的一致性；
d) 应明确启用冗余资源的方法，如故障的感知与应对方法；
e) 应建立数据库读写分离机制。

#### 5.2.1.4 数据库可靠性

a) 应具备用户登录验证机制，对登录用户进行校验；
b) 应具备配置最小权限功能，可精确分配用户权限；
c) 应采取措施，防止数据库内容被非法修改；
d) 应采取措施，防止非授权用户对数据库的恶意存取和破坏，防止数据库数据泄露；
e) 应及时发现系统漏洞并修补，无法修补的应采取其他安全防护措施防止外部攻击；
f) 应对数据库的访问行为进行细粒度审计，对可疑行为、危险操作进行告警及阻断。

#### 5.2.1.5 数据库访问权限

应基于用户身份标识与鉴别、数据访问控制等策略进行数据库访问权限控制，控制的策略至少包括黑白名单机制。

#### 5.2.1.6 数据库审计

应识别数据库越权使用、权限滥用等行为，管理数据库帐号权限。

#### 5.2.1.7 存储方式选择

应根据关键业务数据、热数据、温数据和冷数据等数据类型，自动分层存储，实现当数据冷却时自动往下移动。

#### 5.2.1.8 数据备份恢复

a) 应提供数据的本地备份与恢复功能；
b) 应提供重要数据的异地实时备份功能；
c) 宜定期对备份数据的有效性进行测试。

#### 5.2.1.9 远程运维安全

a) 宜对运维过程中访问的敏感数据进行实时脱敏；
b) 应定期对脱敏后的数据进行去标识化的评估。

#### 5.2.1.10 数据加密

a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

#### 5.2.1.11 恶意代码防范

a) 应及时识别包括勒索病毒在内的恶意代码，并将其有效阻断；
b) 宜采用主动免疫机制加强恶意代码检测、清除能力。

#### 5.2.2 管理部分

##### 5.2.2.1 数据库高可用性

应建立数据库读写分离机制。

##### 5.2.2.2 介质管理

a) 应当基于组织机构的数据分类分级要求以及介质使用的要求，制定存储介质访问、使用的安全策略及管理规范，制定介质使用的审批流程并记录；
b) 应建立对存储介质使用的常规和随机检查机制。

##### 5.2.2.3 存储方式选择

a) 应结合数据类型、重要性、敏感程度等选择数据存储介质以及数据存储方式；
b) 应注意数据存储介质的存放期限。

##### 5.2.2.4 数据备份恢复

a) 应明确数据备份和恢复管理工作的岗位和人员；
b) 应建立数据备份与恢复的操作规程，明确定义备份和恢复的范围、频率、工具、过程、日志、时长等；
c) 重要的数据应具备跨地域的容灾能力。

##### 5.2.2.5 数据加密

a) 应采取国密加密算法进行数据加密；
b) 应对加密密钥进行定期备份，防止密钥丢失；
c) 应明确密文数据申请访问流程，申请内容包括但不限于需要访问的数据目标、数据类别（精细到表或字段级）、访问时间、合理性及必要性等。

### 5.3 使用阶段

#### 5.3.1 技术部分

##### 5.3.1.1 端口使用管控

应对终端端口进行实时管控，管控范围包含蓝牙、光驱、串口/并口、USB 接口、WIFI 接口、调制解调器、红外设备等。

##### 5.3.1.2 无线网络管理

应采取必要措施发现网络中的钓鱼 SSID、第三方非法 SSID，且能够通过有效措施进行屏蔽。

##### 5.3.1.3 恶意代码防范

a) 应及时识别入侵和病毒行为，并将其有效阻断；
b) 应具备防病毒客户端统一管理能力，并定时更新病毒库；
c) 宜采用主动免疫机制加强恶意代码检测、清除能力。

#### 5.3.1.4 用户身份鉴别

a) 应满足 GB/T22239-2019 中 9.1.4.1 要求；
b) 应具备动态鉴权能力，通过周期性地校验终端用户的合法性和安全状态，隔离非法用户。

#### 5.3.1.5 终端实体和用户行为分析

a) 应具备终端实体和用户行为分析能力，包括终端操作系统层面和用户流量层面，及时阻断高危应用服务和高风险操作行为；
b) 应采取技术手段监控和分析用户实体行为，实现从网络系统中采集日志、流量以及行为数据并创建实体的动态行为基线，通过利用行为基线进行对比分析；
c) 应具备安全审计能力，安全审计主要涉及的方面包括:用户登录情况、管理用户的操作行为，关键的业务操作行为、系统功能执行以及系统资源使用情况等。

#### 5.3.1.6 数据防泄露

应通过文件水印、数据加密、防截屏等技术，实现多种数据泄露途径的封堵和数据泄露行为的审计。

#### 5.3.1.7 打印刻录审计

a) 应针对本地或网络打印行为进行审计及控制；
b) 应对终端光盘刻录行为进行审计及控制，审计内容包括刻录时间、刻录的文件名称等信息；
c) 应对刻录文档设置只读、打印、修改、再次授权、阅读次数等权限；
d) 应对内容复制/粘贴、拖拽、副本另存为、截屏/录屏、打印等方式对文档内容进行移植及转存的行为进行审计。

#### 5.3.1.8 访问控制

a) 数据访问控制的颗粒度应达到主体为用户级或工具级，客体为数据库表级及字段级、数据库对象级（敏感对象、系统对象、表空间）、数据库代码级（过程、函数、触发器、视图）；
b) 应采取一定的技术手段对于接入数据库的行为提供多维度的监控及防护措施，包括身份管理、应用防假冒、防撞库、直连控制和免密登陆等；
c) 应基于应用程序名、IP 地址、操作系统账户、数据库实例名、时间等对数据资源访问行为进行授权，实现权限进行集中管理，形成统一权限库。

#### 5.3.1.9 数据脱敏处理

a) 应梳理使用阶段的数据使用场景,对不同场景下的数据使用执行静态脱敏或动态脱敏等不同的脱敏措施；
b) 应根据数据使用方的不同身份和不同数据访问目的，对访问的敏感数据进行脱敏处理；
c) 应根据不同类型的敏感字段采用不同的脱敏规则；
d) 应通过敏感数据识别字典和脱敏算法来处理数据表中的敏感信息；
e) 应通过脱敏规则进行数据变形，实现敏感信息的可靠保护；
f) 应当保证数据脱敏前后的一致性和业务的关联性；
g) 数据脱敏后应保留原始数据格式和特定属性；
h) 应对数据脱敏处理过程的操作进行记录。

#### 5.3.1.10 数据使用审计

a) 应完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责；

b) 审计记录应包含时间、用户名、IP 地址、客户端程序名、数据库以及数据操作指令等信息，应对查询，新增，修改，删除等行为进行审计。

#### 5.3.2 管理部分

安全信息和事件管理及责任认定：

a) 应设立负责数据安全事件管理和应急响应的责任部门和人员；
b) 应明确数据安全事件管理和应急响应的策略及流程；
c) 应对安全事件进行评估、追责、复盘，并定期开展安全培训及应急演练。

### 5.4 传输阶段

#### 5.4.1 技术部分

##### 5.4.1.1 接入管理

a) 应对重要数据传输通道进行国密加密，限制非法设备接入，保留日志记录；
b) 应跟进传输通道加密保护的技术发展，评估新技术对安全方案的影响，适当引入新技术以应对最新的安全风险。

##### 5.4.1.2 流量清洗

a) 应采用技术手段对数据进行统一清洗，在数据清洗环节，根据校验规则，对数据的字段空值约束、字段值类型约束、数据的结构约束（是否字段缺失或者错误）；
b) 应对传输的数据流量进行实时监控，发现并清洗异常流量。

##### 5.4.1.3 入侵防范

参照 T/ISEAA 002-2021 中 7.4.4。

##### 5.4.1.4 恶意代码防范

参照 T/ISEAA 002-2021 中 7.4.5。

##### 5.4.1.5 完整性保护

a) 参照 GB/T22239-2019 中 9.1.4.7；
b) 应对传输数据的完整性进行检测，并具备数据容错、恢复的技术措施。

#### 5.4.2 管理部分

接入管理。**应采用符合国家密码要求的加密方式。**

### 5.5 交换阶段

#### 5.5.1 技术部分

##### 5.5.1.1 数据脱敏

应在数据被共享前，按照分类分级的策略，对数据进行脱敏处理。

##### 5.5.1.2 数据溯源

应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的

抗抵赖。

#### 5.5.1.3 数据导入导出

应对数据导入导出过程中的安全性进行管理，包括身份认证、权限控制、传输加密等方式。

#### 5.5.1.4 数据共享

a) 应在共享前采取身份验证，身份验证方式至少包括用户名/口令、数字证书等；
b) 应采用加密、数字签名、水印等技术对共享的数据进行保护。

#### 5.5.1.5 数据交换监控

应实时监控共享交换过程中的行为和内容，实现对异常数据交换行为的自动化识别和实时预警。

#### 5.5.1.6 数据完整性

参照 T/ISEAA 002-2021 中 7.4.7b。

### 5.5.2 管理部分

#### 5.5.2.1 数据接口

a) 应建立组织对外数据接口的安全管理机制，防范组织数据在接口调用过程中的安全风险；
b) 应明确数据接口的安全控制策略，包括身份鉴别、访问控制、授权策略、安全协议等；
c) 应明确数据接口安全要求，包括接口参数、名称，对不安全输入参数进行限制或过滤；
d) 应对数据库接口的调用、配置的修改、用户及权限、网络连接、系统资源的变化等进行安全审计和防护。

#### 5.5.2.2 数据导入导出

a) 应建立数据导入导出的安全管理制度，基于组织机构的数据分类分级要求定义数据导入导出相关的安全策略；
b) 应对导入导出数据做安全审计与标识；
c) 应对数据导入导出的安全管理制度定期进行更新并审计。

#### 5.5.2.3 数据共享

a) 应明确数据共享内容的范围、形式和管控措施，明确相关人员的职责及权限；
b) 应明确数据共享审计流程、审计记录内容和审计日志管理要求。

#### 5.5.2.4 数据发布

a) 应制定数据发布的审核制度，并对发布数据进行安全标识与审计；
b) 应对发布数据的格式、适应范围、发布者与使用者权利进行限制；
c) 应建立数据资源公开事件应急处理流程。

#### 5.5.2.5 数据交换监控

a) 应对数据交换行为制定数据交换风险行为识别和评估规则，并定期对数据交换行为进行审计；
b) 应设定数据内容敏感性检查和安全检查机制；
c) 应实时监控共享交换过程中的所有行为和内容，实现对异常或高风险数据交换操作的自动化识别和实时预警。

### 5.6 销毁阶段

#### 5.6.1 技术部分

剩余信息保护，参照 T/ISEAA 002-2021 中 7.4.10。

#### 5.6.2 管理部分

数据销毁制度，参照 T/ISEAA 002-2021 中 7.10.3。