# 数据安全管理体系技术规范

编　号：　RY-GF-001-2025

版　本：　A/1

编制人：　技术研发部

审核人：　王敏捷

批准人：　王敏捷

瑞岳认证（江西）有限公司

2025-09-1发布　　2025-09-1实施

2025-11-25修订

修订说明

| 序号 | 修订内容说明 | 版本号 | 修订人 | 审批人 | 修订日期 |
| --- | --- | --- | --- | --- | --- |
| 1 | 数据安全管理能力描述变更为数据安全管理体系 | A/1 | 技术研发部 | 王敏捷 | 2025-11-25 |
| | | | | | |
| | | | | | |

## 1　适用范围

本文件规定了对组织的数据安全管理体系要求。本文件适用于数据安全管理体系认证。（简称 DSMC）

## 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，标注日期的引用文件，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 25069 信息安全技术术语

GB/T 37988 信息安全技术数据安全能力成熟度模型

GB/T 36073 数据管理能力成熟度评估模型

GB/T 41479 信息安全技术网络数据处理安全要求

GB/T 37973 信息安全技术大数据安全管理指南

GB/T 35273 信息安全技术个人信息安全规范

GB/T 39477 信息安全技术政务信息共享数据安全技术要求

GB/T 29246 信息技术安全技术信息安全管理体系

GB/T 39335 信息技术个人信息安全评估指南

GB/T 19000 质量管理体系基础和术语

## 3　术语及定义

GB/T 41479、GB/T 37988、GB/T 36073、GB/T 25069、GB/T 35273、GB/T 39335、

GB/T19000、GB/T 37973、GB/T 29246 等国家标准最新有效版本界定的以及下列术语和定义适用于本文件

**3.1 数据**

任何以电子或者其他方式对信息的记录。

**3.2 数据处理**

数据的收集、存储、使用、加工、传输、提供、公开等。

**3.3 数据安全**

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。

**3.4 个人信息**

个人信息是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。

注 1:个人信息包括姓名、出生日期、公民身份证号、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注 2：不包括匿名化处理后的信息。

### 3.5 敏感个人信息

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。

### 3.6 个人信息处理者

在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

### 3.7 去标识化

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

### 3.8 匿名化

个人信息经过处理无法识别特定自然人且不能复原的过程。

注：匿名化处理后的信息不属于个人信息

## 4　组织环境

### 4.1 理解组织及其环境

组织应确定与其宗旨和战略方向相关并影响其实现数据安全管理预期结果能力的各种外部和内部因素

组织应对这些外部和内部因素的相关信息进行监视和评审

## 4.2 理解相关方的需求和期望

组织应确定

a) 与数据安全管理体系有关的相关方；

b) 与数据安全管理体系有关的相关方的要求。

组织应监视和评审这些相关方的信息及其相关要求。

## 4.3 确定数据安全管理体系的范围

组织应确定数据安全管理体系的边界和适用性，已确定其范围。

在确定范围时，组织应考虑：

a) 4.1 中提及的各种外部和内部因素；

b) 4.2 中提及的相关方要求；

c) 组织的产品和服务。

组织的数据安全管理体系的范围应作为成文信息，可获得并得到保持，该范围应描述所覆盖的产品和服务类型。

## 4.4 数据安全管理体系及其过程

组织应按照本技术规范的要求，建立、实施、保持和持续改进数据安全管理体系，包括所需的过程及其相互作用。组织应确定数据安全管理体系所需的过程及其在整个组织中的应用。

在必要的范围和程度上，组织应：

a) 保持成文信息以支持过程运行；

b） 保留成文信息以确信其过程按照策划进行。

## 5 领导作用

### 5.1 领导作用和承诺

最高管理者应通过以下方面，证实其对数据安全管理体系的领导作用和承诺：

a) 对数据安全管理体系的有效性负责；

b) 确保制定数据安全管理体系方针和目标，并与组织环境相适应，与战略方向相一致；

c) 确保数据安全管理要求融入组织的业务过程；

d) 促进使用过程方法和基于风险的思维；

e) 确保数据安全管理所需的资源是可获得的；

f) 沟通有效的数据安全管理要求的重要性；

g) 确保数据安全管理实现其预期结果；

h) 促使人员积极参与，指导和支持他们为数据安全管理的有效性做出贡献；

i) 推动改进；

j) 支持其他相关管理者在其职责范围内发挥领导作用。

### 5.2 方针

最高管理者应制定、实施和保持数据安全管理方针，方针应

a) 适应组织的宗旨和环境并支持其战略方向；

b) 为建立数据安全管理目标提供框架；

c) 包括适用的要求承诺；

d) 包括持续改进数据安全管理的承诺；

e) 可获取并保持成文信息；

f) 组织内应得到沟通、理解和应用；

### 5.3 组织的岗位、职责和权限

最高管理者应确保组织相关岗位的职责、权限得到分配、沟通和理解。最高管理者应分配职责和权限，以：

a）确保数据安全管理体系符合本技术规范的要求；

b）确保各过程获得其预期输出；

c）报告数据安全管理体系的绩效以及改进机会，特别是向最高管理者报告；

d）确保在策划和实施数据安全管理体系变更时保持其完整性。

注：相关职责划分至少应包括数据安全第一责任人、监督层、分类分级及敏感数据保护、权限管理、内审应急、教育培训、投诉举报、合作方管理等。

组织应依据国家相关要求，建立数据安全管理机构，明确数据安全负责人。数据安全责任人履行职责包括但不限于：

a）组织制定数据保护计划并督促落实；

b）组织开展数据安全风险评估；

c）督促整改安全隐患；

d）按要求向有关部门报告数据安全保护和事件处置情况；

e）受理并处理用户投诉和举报。

# 6　策划

## 6.1 应对风险和机遇的措施

在策划数据安全管理体系时，组织应考虑到 4.1 所提及的因素和 4.2 所提及的要求，并确定需要应对的风险和机遇，以：

a）确保数据安全管理体系能够实现预期结果；

b）增强有力影响；

c）预防和减少不利影响；

d）实现改进。

组织应策划应对这些风险和机遇的措施；如何在数据安全管理体系过程中整合并实施这些措施，如何评价这些措施的有效性，应对措施应与风险和机遇对数据安全的潜在影响相适应。

## 6.2 数据安全目标及其实现的策划

组织应针对相关职能、层次和数据安全管理体系所需的过程建立数据安全目标。

目标应：

a）与数据安全方针保持一致；

b）可测量；

c）考虑适用的要求；

d）予以监视；

e）予以沟通；

f）适时更新。

组织应保持有关数据安全目标的成文信息。

策划如何实现质量目标时，组织应确定：

a）要做什么；

b）需要什么资源；

c）由谁负责；

d）何时完成；

e）如何评价结果。

## 7　支持

### 7.1 资源

组织应确定并提供所需的资源，以建立、实施、保持和持续改进数据安全管理体系。

组织应考虑：

a）现有内部资源的能力和局限；

b）需要从外部供方获得的资源。

人员：组织应确定并配备所需的人员，以实现数据安全管理体系。

基础设施：组织应确定、提供并维护所需的基础设施，以实现数据安全管理体系。

过程运行环境：组织应确定提供并维护所需的环境，以实现数据安全管理体系。

### 7.2 能力

组织应

a） 确定在其控制下工作人员所需具备的能力，这些人员从事的工作影响实现数据安全管理体系有效性；

b） 基于适当的教育、培训或经验，确保这些人员是胜任的；组织应针对数据安全管理相关岗位的人员制定培训计划，定期组织数据安全培训工作。确定参与数据安全培训的人员角色范围；制定数据安全培训考核体系。数据安全培训内容包括但不限于：数据安全法律法规、数据安全管理方法、数据安全技能能力等

c） 保留适当的成文信息，作为人员能力的证据。

注：培训课时不低于 20 课时/每人/每年。

# 8 运行

## 8.1 运行的策划

为满足数据安全管理体系的要求，实施第 6 章所确定的措施，组织应通过以下措施对数据安全所需过程（见 4.4）进行策划和实施：

a）数据分类分级管理；

b）数据访问权限管理；

c）数据安全审计管理；

d）数据合作方管理；

e）数据安全应急响应

f）数据安全举报投诉管理

g）数据资产与数据资源管理

## 8.2 数据分类分级

组织应建立数据分类分级管理过程，并保持成文信息。覆盖的范围应包括数据处理活动涉及的所有平台系统。

数据分类分级应满足国家法律法规及相关标准的要求，综合考虑数据的类别属性、使用目的等，明确数据分类策略。

在数据分类的基础上，对每一类数据类型制定数据分级标准。分级标准应考虑以下因素：

a）数据重要及敏感程度；

b）数据的安全保护需求；

c）数据泄露、丢失或破坏可能造成的危害程度。

在数据分类分级的基础上规定不同级别数据的管控规则，包括但不限于：数据使用审批、数据权限管理、数据脱敏、数据加密等。

## 8.3 数据访问权限管理

组织应明确关键系统的用户账号分配、开通、使用、变更、注销等安全保障要求，明确账号权限最小化可用原则，明确操作审批要求和操作流程，形成并定期更新系统权限分配表。组织应关注离职人员账号回收、账号权限变更、沉默账号安全等问题。明确敏感系统操作安全基线定义，涉及数据重大操作的（如数据批量复制、传输、处理、开放共享和销毁等），组织应采取多人审批授权或操作监督，并实施日志审计。需以操作审计技术能力对应。

## 8.4 数据安全审计管理

组织应建立内部数据安全管理审计机制，审计维度包含：数据分类分级及管控、数据安全教育培训、举报投诉处理、权限管理与操作规范、合作方管理、账号权限审计、日志审计、技术能力实现效果等数据安全工作进行安全审计管理

每项审计对应审计方法、审计目的、审计内容、审计步骤应保留成文信息

## 8.5 数据安全合作方管理

应加强第三方数据合作的管理，与合作方签订服务合同和安全保密协议。

应明确对外合作中数据安全保护方式和合作方责任落实要求，合作结束后数据删除要求，合作方违约责任和处罚等。

应建立合作方台账管理机制，形成并定期更新合作方清单。清单的内容应包含合作方名称、相关资质、合作业务或系统、合作形式、合作期限、合作方联系人等。根据合作方共享数据的不同级别来制定不同的资质以及数据保护能力要求；对于接收的数据，则需对数据来源进行判定。最终由内部评审后通过。

## 8.6 数据安全应急响应

应根据不同的数据安全事件，制定完善的数据安全应急预案，明确应急响应及应急处置方案，从数据安全进行应急处理与处置。

应根据数据安全事件类型，明确事件原由、事件带来的危害、整改补救措施、应急审计、结案留档。

## 8.7 数据安全举报投诉管理

应建立数据安全用户举报与受理的成文信息，明确用户数据安全举报投诉渠道；明确举报投诉处理流程；明确举报投诉处理完成时限（不得超过 15 日）。

注：适宜的举报投诉渠道，如电子邮件、电话、传真、网站等。

## 8.8 数据资产与数据资源管理

为满足数据安全管理体系的要求，实施所确定的措施，实现数据安全目标，组织应至少建立健全以下数据安全技术能力，对所需的数据安全技术实现过程进行实施和控制：

a）数据资产范围；

b）数据识别；

c）数据防泄漏；

d）接口安全管理；

e）敏感数据保护;

### 8.8.1 数据资产范围

组织应：

a）确定数据安全相关的资产；

b）梳理数据资源，明确数据资源内容、数据量、存放位置、保存期限、数据关联系统、数据共享情况等；

c）按照分类分级法，确定组织的数据资源安全等级；

d）根据安全等级，制定适宜的数据资产与资源的控制措施；

e）定期验证控制措施的有效性。

在数据资源识别时，应配备技术能力，定期对相关平台系统数据库数据资产、文件服务器以及终端数据资产、 API 数据资产进行扫描，发现识别敏感数据信息。

### 8.8.2 数据识别

在数据资源识别时，应配备技术能力，定期对相关平台系统数据库数据资产、终端数据资产进行扫描，发现识别敏感数据信息；

在验证控制措施的有效性时，应配备技术能力，对数据脱敏、数据分类分级效果进行验证，确保各类数据处理场景中数据脱敏的有效性和合规性。

### 8.8.3 数据防泄漏

涉及存储、处理、展示敏感数据的平台系统，应配备数据防泄露能力，优先从网络侧和终端侧等进行部署，逐步扩大能力覆盖范围。

组织应具备对网络、邮件、 FTP、USB、多种数据导入导出渠道进行实时监控的能力，可及时对异常数据操作行为进行预警拦截，以防范数据泄露风险。对于已经发生的数据泄露事件，应采取日志审计、水印溯源等方式追溯。

### 8.8.4 接口安全管理

具备针对内外部访问流量分析能力，对使用接口的风险行为进行记录并告警；

具备对接口自身的安全性，防外部攻击的发现能力

### 8.8.5 敏感数据保护

对授权收集到的敏感数据信息，应采取去标识化、关键字段加密安全存储措施。根据相关方要求，删除、销毁的个人信息可进行匿名化处理。

在跨安全域或通过互联网传输敏感数据信息时，采用加密传输措施。

注:适宜的加密传输措施，例如可确保安全的加密算法或传输通道。

在用户端显示敏感数据信息时，应采取措施防止未授权人员获取敏感数据信息。（动态脱敏：注意脱敏失效）

在用户端显示敏感数据信息时，应根据敏感数据级别，采取动态脱敏策略防止未授权人员获取敏感数据信息。对于权限较高人员，应采用可逆脱敏，支持查看脱敏数据的明文。

## 9 绩效评价

### 9.1 监视、测量、分析和评价

组织应评价数据安全绩效及数据安全能力的有效性。

组织应确定

a) 需要监视和测量什么；

b) 需要用什么方法进行监视、测量、分析和评价，以确保结果有效；

组织应保留适当的成文信息，以作为结果的证据。

## 9.2 内部审核

组织应按照策划的时间间隔进行内部审核，以确定数据安全管理体系：

a）是否符合：

1）组织自身的要求

2）本技术规范的要求

b）是否得到有效的实施和维护

## 9.3 管理评审

最高管理层应按计划的时间间隔评审组织的数据安全管理体系，以确保其持续的适宜性、充分性和有效性。

策划和实施管理评审应考虑:

a）以往管理评审所采取的措施情况:

b）与数据安全管理体系相关的内外部因素变化;

c）有关数据安全绩效的反馈，包括以下方面的趋势;

1）不符合和纠正措施;

2）监视和测量结果;

3）审核结果

4）数据安全目标完成情况。

5）有关相关方反馈;

6）数据安全管理体系目标的实现程

d）资源的充分性

e）应对风险和机遇所采取措施的有效性（见 6.1）

f）持续改进的机会

管理评审的输出，应包括与持续改进机会、数据安全管理体系的所需变更及需求相关的决定和措施。组织应保留成文信息，作为管理评审结果的证据

## 10 改进

### 10.1 不符合及纠正措施

当发生不符合时，组织应

a) 对不符合做出应对，并在适用时：

1）采取措施，以控制并予以纠正不符合

2）处理后果

b) 通过以下活动，评价是否需要采取措施，以消除产生不符合的原因，避免其再次发生或者在其他场合发生：

1）评审和分析不符合

2）确定不符合的原因

3）确定是否存在或可能发生类似的不符合

c) 实施所需的措施；

d) 评审所采取纠正措施的有效性；

e) 需要时，更新在策划期间确定的风险和机遇

f) 需要时，对数据安全管理体系进行变更。

纠正措施应与不符合产生的影响相适应。

不符合性质以及采取的措施及纠正措施的结果组织应保留成文信息作为证据。

## 10.2 持续改进

组织应持续改进数据安全管理体系的适宜性、充分性和有效性。

组织应考虑分析和评价的结果以及管理评审的输出，以确定是否存在需求和机遇，这些需求或机遇应作为持续改进的一部分加以应对。