UDC

MH

中华人民共和国行业标准

P

MH/T xxxx—xxxx

智慧民航数据治理
数据安全规范

Smart Civil Aviation Data Governance

Data Security Specification

（征求意见稿）

2021-xx-xx 发布

202x-xx-xx 施行

中国民用航空局　　发布

中华人民共和国行业标准

智慧民航数据治理
数据安全规范

Smart Civil Aviation Data Governance
Data Security Specification

MH/T××××—202×

（征求意见稿）

主编单位：中国民用航空局发展计划司

中国民航管理干部学院

批准部门：中国民用航空局

施行日期：202x 年 xx 月 xx 日

中国民航出版社有限公司

2021　北京

前 言

随着智慧民航的推进，民航各单位的数据将逐步实现从信息化资产到生产要素的转变，数据安全的重要性日益凸显。为指导行业单位建立科学的数据安全分级与防护机制，强化数据安全保护能力，促进民航数据的安全共享与应用，制定本规范。

本规范以《推动新型基础设施建设促进民航高质量发展实施意见》、《推动民航新型基础设施建设五年行动方案》为指导，深入调研和总结民航行业的数据安全现状，认真吸收总结民航各单位的数据安全治理经验，借鉴行业内外数据安全分级与防护的有关标准和技术要求，经广泛征求意见和多次专家审查，最终形成本规范。

本规范共 6 章。主要内容包括：总则、术语、民航数据安全治理框架、民航数据安全分级、民航数据全生命周期安全防护、民航数据安全组织保障。

本规范的日常维护工作由中国民航管理干部学院大数据与信息管理研究中心负责，执行过程中如有意见或建议，请函告本规范日常维护组（联系人：XX；地址：北京市朝阳区花家地东路 3 号；电话：XXXX，邮箱：XXXX），以便修订时参考。

主编单位：中国民用航空局发展计划司

中国民航管理干部学院

主　　编：****

参编人员：****

主　　审：****

参审人员：****

目　次

1 总 则

1.0.1 为提升民航数据安全，指导行业数据安全治理工作，建立科学的数据安全分级与防护机制，制定本规范。

1.0.2 本规范适用于航空公司、机场、空管、运行保障单位、行业监管单位等民航行业单位的数据安全治理工作。

1.0.3 民航业单位应在本规范内容的框架与指导下，结合自身发展现状及目标，进一步细化研究具体实施方案与细则，确保符合实际、具备可操作性。

1.0.4 民航行业数据安全治理工作，除应满足本规范的规定外，尚应符合国家、行业现行有关标准的规定。

2 术 语

下列术语适用于本规范。

2.0.1 数据安全 data security

数据安全是指通过采取必要措施，保障数据得到有效保护和合法利用，并持续处于安全状态的能力。

2.0.2 敏感数据 sensitive data

敏感数据指泄露后可能会给国家安全、公众权益、个人隐私、企业合法权益等造成不同程度损害的数据。

2.0.3 数据脱敏 data masking

数据脱敏指对某些敏感数据通过脱敏规则进行变形，实现敏感数据的可靠保护。

2.0.4 数据采集 data collection

数据采集指获取数据的过程。

2.0.5 数据传输 data transmission

数据传输指数据从一个控制主体发送到另一个控制主体的过程。

2.0.6 数据存储 data storage

数据存储指将数据进行持久化保存的过程。

2.0.7 数据使用 data usage

数据使用指对数据的访问、加工、展示等一系列处理过程。

2.0.8 数据共享 data sharing

数据共享指本单位不同部门之间或与其他单位、行业主管单位的数据共享，各方承担相关权利和义务的过程。

2.0.9 数据销毁 data destruction

数据销毁指采用数据擦除或者物理销毁的方式确保数据无法复原的过程。

3　民航数据安全治理框架

3.0.1　民航数据安全治理应基于数据安全原则，以数据安全分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并建立健全数据安全组织支撑，全面加强民航业单位数据安全保护能力。民航数据安全治理框架如图 3.0.1 所示。

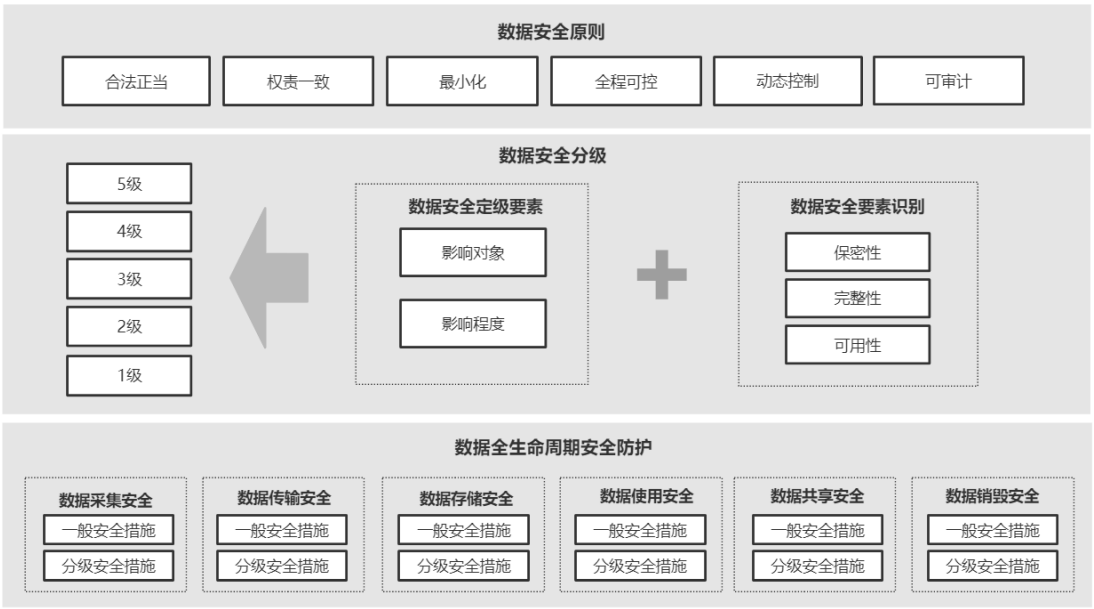

图 3.0.1　民航数据安全治理框架

3.0.2　数据安全基本原则

1　合法正当原则：对数据的收集、使用应基于法律依据，理解和履行数据相关的法律义务，确保数据全生命周期各环节数据活动的合法性和正当性。

2　权责一致原则：应明确本单位数据安全治理工作相关部门及其职责，相关部门及人员应积极落实相关措施，履行数据安全职责。因不履行或不当行使其职权等造成不良影响或损害的，应承担相应的安全责任。

3　最小化原则：在保证业务功能实现的基础上应赋予数据活动中各角色最小的操作权限和最小数据集，制定数据访问授权审批流程。

4　全程可控原则：对数据进行安全分级，通过实施与数据安全级别相匹配的安全管控机制和技术措施，确保数据在全生命周期各阶段的安全性，避免被未授权访问、破坏、篡改、泄漏或丢失等。

5　动态控制原则：数据的安全控制策略和防护措施应基于业务需求、安全环境属性、

系统用户行为等因素进行实时和动态调整。

6　可审计原则：应实现对业务各环节的数据安全审计，记录数据活动中各项操作的相关信息，保障记录可追溯。

3.0.3　数据安全分级

民航业单位应采用规范、明确的方法区分数据的重要性和敏感程度差异，确定数据安全级别，并根据数据不同安全级别，确定数据在其生命周期的各个环节应采取的数据安全防护策略和管控措施。

3.0.4　数据全生命周期安全防护

民航业单位应依据本规范安全措施要求，在采集、传输、存储、使用、共享以及销毁等各个环节采取符合数据安全级别要求的安全防护措施，建立覆盖数据全生命周期的安全防护机制。

4　民航数据安全分级

4.1　数据安全分级原则

4.1.1　数据安全分级应遵循以下原则：

1　合法合规原则：应满足国家法律法规及行业主管部门有关规定。

2　可执行原则：数据定级规则应避免过于复杂，以确保数据定级工作的可行性。

3　时效性原则：数据安全级别应具有一定的有效期限，宜按照级别变更策略对数据级别进行及时调整。

4　自主性原则：应结合本单位自身数据管理需要（如战略需要、业务需要、风险接受程度等），在本框架下自主确定数据安全级别，并采取与数据安全级别相应的防护措施。

5　差异性原则：应根据数据的重要性、敏感程度等差异，将数据划分至不同的数据安全层级，不宜将所有数据集中划分到其中若干个级别中。

4.2　数据安全分级要素

4.2.1　确定数据安全级别的判断依据是数据安全性遭到破坏后可能造成的影响，民航数据安全分级主要考虑要素为：影响对象与影响程度。

4.2.2　影响对象

影响对象指数据安全性遭受破坏后受到影响的对象，包括国家安全、公众权益、个人隐私、企业合法权益等。影响对象的确定主要考虑以下内容：

1　影响对象为国家安全的情况，一般指数据的安全性遭到破坏后，可能对国家政权稳固、领土主权、民族团结、社会和民航稳定等造成影响。

2　影响对象为公众权益的情况，一般指数据的安全性遭到破坏后，可能对社会秩序和公众的政治权利、人身自由、经济权益等造成影响。

3　影响对象为个人隐私的情况，一般指数据的安全性遭到破坏后，可能对个人信息、私人活动和私有领域等造成影响。

4　影响对象为企业合法权益的情况，一般指数据的安全性遭到破坏后，可能对某企业或其他组织（可能是民航业单位，也可能是其他行业单位）的生产运营、声誉形象、公信力等造成影响。

4.2.3 影响程度

影响程度指数据安全性遭到破坏后所产生影响的大小，从高到低划分为严重损害、一般损害、轻微损害和无损害。影响程度的确定宜综合考虑数据类型、数据特征与数据规模等因素，并结合民航业务属性确定影响程度。影响程度参考说明如表 4.2.1 所示。

表4.2.1 影响程度说明

影响程度	参考说明
严重损害	1.可能导致危机国家安全的重大事件，发生危害国家利益或造成重大损失的情况。 2.可能导致严重危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致民航业秩序遭到严重破坏等情况。 3.可能导致民航业单位遭到监管部门严重处罚，或者影响重要/关键业务无法正常开展的情况。 4.可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。
一般损害	1.可能导致危害社会秩序和公共利益的事件，引发区域性集体诉讼事件，或者导致民航业秩序遭到破坏等情况。 2.可能导致民航业单位遭到监管部门处罚，或者影响部分业务无法正常开展的情况。 3.可能导致一定规模的个人信息泄露、滥用等安全风险，或对个人权益可能造成一定影响的事件。
轻微损害	1.可能导致个别诉讼事件，使民航单位经济利益、声誉等轻微受损。 2.可能导致民航机构部分业务临时性中断等情况。 3.可能导致对个人权益造成部分或潜在影响。
无损害	对企业合法权益和个人隐私等不造成影响，或仅造成微弱影响但不会影响国家安全、公众权益、民航业秩序或者民航业机构各项业务的正常开展。

4.3 数据安全分级要素识别

4.3.1 数据安全分级要素识别应通过数据安全性影响评估，确定数据各项安全性遭到破坏后所影响的对象及影响程度，作为数据安全分级要素。

4.3.2 安全性影响评估

数据安全性包括数据保密性、完整性、可用性，数据安全性影响应分别从数据的保密性、

完整性、可用性遭到破坏后可能影响的对象和影响程度进行评估。

1 保密性影响评估：评价数据遭受未经授权的披露所造成的影响，以及民航业单位继续使用这些数据可能产生的影响。评估的内容包括但不限于：

1）数据未经授权的披露，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

2）数据被非授权对象获取或利用，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

3）数据被非授权对象利用进行窃密、篡改、销毁或拒绝服务等攻击，可能对国家安全、公众权益、个人隐私及企业合法权益等造成的损害，以及损害的严重程度。

4）数据的未经授权披露或传播是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。

2 完整性影响评估：评价数据遭受未经授权的修改或损毁所造成的影响，以及民航业单位继续使用这些数据可能产生的影响。评估的内容包括但不限于：

1）数据未经授权修改或损毁，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

2）数据未经授权修改或损毁，可能对其他组织或个人造成的损害，以及损害的严重程度。

3）数据未经授权修改或损毁，可能对机构职能、公信力造成的损害，以及损害的严重程度。

4）数据未经授权修改或损毁是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。

3 可用性影响评估：评价数据及其经组合/融合后形成的各类数据出现访问或使用中断所造成的影响，以及民航业单位无法正常使用这些数据可能产生的影响。评估的内容包括但不限于：

1）数据的访问或使用中断，可能对国家安全、公众权益、个人隐私及企业合法权益造成的损害，以及损害的严重程度。

2）数据的访问或使用中断，可能对机构职能、公信力造成的损害，以及损害的严重程度。

3）数据的访问或使用中断，可能对其他组织或个人造成的损害，以及损害的严重程度。

4）数据的访问或使用中断是否违反国家法律法规、行业主管部门有关规定或机构内部管理规定。

4.3.3 分级要素确定

通过综合考虑保密性、完整性和可用性的影响评估结果，确定数据安全定级关键要素，应满足：

1 因不同数据在安全性（保密性、完整性、可用性）方面有不同侧重，以实际业务中所侧重的安全性评估结果，作为相应数据安全定级的主要依据。

2 数据的保密性、完整性和可用性要求基本一致的，重点以保密性评估所确定的定级要素为主要定级依据。

4.4 数据安全分级规则

4.4.1 根据数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别从高到低划分为 5 级、4 级、3 级、2 级、1 级，重要数据的安全等级不可低于 5 级。数据安全级别划定规则及各级数据一般特征如表 4.4.1 所示。

表4.4.1 数据安全分级规则参考表

最低安全级别参考	数据定级要素		数据一般特征
	影响对象	影响程度	
5	国家安全	严重损害/一般损害/轻微损害	• 重要数据，通常主要用于民航运行核心关键业务，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对国家安全造成影响，或对公众权益造成严重影响。 • 例如：影响航空器飞行或运行安全的重要保障数据。
5	公众权益	严重损害	
4	公众权益	一般损害	• 数据用于民航业单位关键或重要业务，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但不影响国家安全。 • 例如：涉及到旅客敏感隐私信息的航空出行数据，如旅客身份证信息、手机号信息等。
4	个人隐私	严重损害	
4	企业合法权益	严重损害	
3	公众权益	轻微损害	• 数据用于民航业单位关键或重要业务，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。 • 数据的安全性遭到破坏后，对公众权益造
3	个人隐私	一般损害	

3	企业合法权益	一般损害	成轻微影响，或对个人隐私或企业合法权益造成一般影响，但不影响国家安全。 • 例如：航空运输企业的经营类数据。
2	个人隐私	轻微损害	• 数据用于民航业单位一般业务，一般针对受限对象公开，通常为内部管理且不宜广泛公开的数据。 • 数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响，但不影响国家安全、公众权益。 • 例如：涉及到旅客一般隐私信息的航空出行数据，如值机时间、过安检时间、登机时间等。
2	企业合法权益	轻微损害	
1	国家安全	无损害	• 数据一般可被公开或可被公众获知、使用。 • 数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不造成影响，或仅造成微弱影响但不影响国家安全、公众权益。 • 例如：航班基本信息数据。
1	公众权益	无损害	
1	个人隐私	无损害	
1	企业合法权益	无损害	

4.5 数据安全级别变更

4.5.1 数据安全定级完成后，出现下列情形之一时，宜对相关数据的安全级别进行变更。

1 数据内容发生变化，导致原有数据的安全级别不适用变化后的数据，如数据脱敏、删除关键字段等。

2 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据安全级别不再适用。

3 因数据汇聚融合（对数据进行集中、清洗、转换、重组、关联分析、多方计算等处理），导致原有数据安全级别不再适用汇聚融合后的数据。

4 因国家或行业主管部门要求，导致原定的数据安全级别不再适用。

5 需要对数据安全级别进行变更的其他情形。

5　民航数据全生命周期安全防护

5.1　数据采集安全

5.1.1　数据采集阶段的主要数据安全目标是：通过对采集过程的合法合规管理、采集设备和数据源的安全性验证，实现对数据采集过程的有效安全防护。

5.1.2　数据采集一般安全措施

1　定义采集数据的目的和用途，明确数据源和采集数据范围。

2　遵循合法正当原则，确保数据采集的合法性、正当性和必要性。

3　对采集的数据进行分类分级标识，并对不同级别的数据实施相应的安全管理策略和保障措施。

4　制定采集数据的清洗、转换、加载等操作规范，明确操作方法、手段，并做好备份工作，避免操作过程中出现数据遗漏、丢失等问题。

5.1.3　数据采集分级安全措施

1　跟踪和记录 2 级及以上数据的采集过程，并采取技术措施确保所收集信息来源的可追溯性。具备条件的单位宜记录 1 级及以上数据的信息来源。

2　从单位外部系统采集 3 级及以上数据时，应结合口令密码、设备物理位置、网络接入方式、设备风险情况等多种因素对数据采集设备或系统的安全性进行增强验证；APP、WEB 等客户端完成采集后不应留存 3 级及以上数据，并及时对缓存进行清理。

3　从单位外部系统采集 4 级及以上数据时，应对采集的数据进行加密，对采集全过程进行持续动态认证，确保数据采集设备或系统的真实性，必要时可实施阻断、二次认证等操作。

5.2　数据传输安全

5.2.1　数据传输阶段的主要数据安全目标是：通过对传输的数据以及传输数据的网络通道的安全机制建立，实现对传输过程中数据的保密性和完整性保护。

5.2.2　数据传输一般安全措施

1　敏感数据传输至目标系统前，确保目标系统具备与当前系统相当的安全防护能力；对敏感数据传输信道进行加密；不应通过互联网、外部系统等方式传输敏感数据。

2　采用设备冗余、线路冗余等措施，确保数据传输的可用性；采用负载均衡、防入侵攻击等安全技术或设备来降低数据传输网络的可用性风险。

3　传输通道建立前，应对通信双方进行身份鉴别和认证，确保数据传输双方可信任。

4　对数据传输过程实施数据完整性校验。

5.2.3　数据传输分级安全措施

1　2 级及以上数据传输，应事先经过审批授权，并留存数据传输日志；2 级及以上数据对单位外的传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。

2　3 级及以上的数据传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。

3　通过物理介质批量传递 3 级及以上数据时应对数据进行加密或脱敏，传递过程中物理介质不应离开相关责任人、监控设备等的监视及控制范围，且不应在无人监管情况下通过第三方进行传递。

4　4 级及以上数据传输，应对数据进行字段级加密，并采用安全的传输协议进行传输。

5.3　数据存储安全

5.3.1　数据存储阶段的主要数据安全目标是：防止存储数据的泄露和未授权的修改、删除和销毁。

5.3.2　数据存储一般安全措施

1　对数据存储设备和系统进行必要的安全管控，包括设备操作终端的鉴权机制、系统的访问控制、系统配置的安全基线等，并定期进行安全风险评估。

2　数据存储不应因存储形式或存储时效的改变而降低安全保护强度。

3　应对数据存储区域进行规划，将不同级别的数据分开存储，并采取物理或逻辑隔离机制，对不同区域之间的数据流动进行安全管控。

4　建立数据容灾备份和恢复机制，做好数据容灾应急预案，一旦发生数据丢失或破坏，可及时检测和恢复数据，保障数据资产安全、用户权益及业务连续性。

5.3.3　数据存储分级安全措施

1　存储 2 级及以上数据时，应采取技术措施保证存储数据的保密性，必要时可采取多因素认证、固定处理终端、固定处理程序或工具等安全策略。

2　存储 3 级及以上数据时，应采用密码技术、权限控制等技术措施保证数据完整性；

采取加密等技术措施保证数据保密性。

3　保存 4 级及以上数据的信息系统，其网络安全建设及监督管理宜满足网络安全等级保护 3 级要求。

5.4　数据使用安全

5.4.1　数据使用阶段的主要数据安全目标是：采用预防和探测的手段，防止数据的未授权操作，降低数据窃取、泄漏、篡改、损毁等安全风险。

5.4.2　数据使用一般安全措施

1　依据数据保护的法律法规要求，明确数据使用的目的和范围；建立内部责任制度，保证使用数据不超出声明的数据使用目的和范围；

2　遵循最小化原则，提供数据细粒度访问控制机制；

3　遵循可审计原则，记录和管理数据处理活动中的操作；

4　对数据处理结果进行风险评估，避免处理结果中包含可恢复的敏感数据。

【条文说明】数据的使用范围应控制在合理的用途之内，例如：旅客隐私数据应限定在旅客出行服务、安全防控场景等范围使用；航班运行数据应限定在航班运行保障等范围使用。

5.4.3　数据使用分级安全措施

1　访问 2 级及以上的数据时应对访问者实名身份认证，将数据访问权限与实际访问者的身份或角色进行关联，防止数据的非授权访问；2 级及以上的数据访问过程应留存相关操作日志，操作日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等。

2　访问 3 级及以上数据应建立访问权限申请和审核批准机制，并对实际操作和申请操作进行验证；3 级及以上的数据访问应实现多因素认证或二次授权，并应结合业务需要对数据采取脱敏和控制访问数据行数的技术措施。

3　业务系统对 2 级及以上数据明文查询应留存相关查询日志；2 级及以上数据的展示应事先通过审批授权后方可展示。

4　3 级数据的展示应在审批的基础上采用屏蔽等技术措施防止信息泄露。

5　3 级及以上数据加工之前应进行数据安全评估，并采用加密、脱敏等技术措施，保证数据加工过程的数据安全性。

6　3 级及以上数据原则上不应公开披露，4 级及以上数据原则上避免明文展示。

7　开发测试原则上不应涉及 4 级及以上数据。

5.5　数据共享安全

5.5.1　数据共享阶段的主要数据安全目标是：对数据的共享方式及用途等进行安全影响评估，通过技术手段确保数据共享时的数据安全。

5.5.2　数据共享一般安全措施

1　对共享数据的使用目的、内容、传输方式、使用时间、技术防护措施、数据使用后的处置方式等进行安全影响评估，并留存相关记录。

2　数据对单位外共享时，应与数据接收方通过合同协议等方式，明确双方在数据安全方面的责任及义务，并约定共享数据的内容和用途、使用范围等。

3　应定期对共享的数据进行安全审计。

4　应配套建立应急响应机制，必要时应及时切断数据共享。

5.5.3　数据共享分级安全措施

1　应对共享 2 级及以上的数据共享过程留存日志记录，记录内容包括但不限于共享内容、共享时间、防护技术措施等。

2　共享 3 级及以上的数据时，原则上应对含敏感字段的数据进行脱敏；若因业务确需，无法对数据进行脱敏的，对数据进行加密、选用安全可靠的传输协议或在安全可控的环境中进行共享。

5.6　数据销毁安全

5.6.1　数据销毁阶段的主要数据安全目标是：建立有效的数据销毁的规范和流程，辅助以技术工具，保证数据得到了有效销毁。

5.6.2　数据销毁一般安全措施

1　应制定数据存储介质销毁操作规程，明确数据存储介质销毁场景、销毁技术措施，以及销毁过程的安全管理要求，并对已共享或者已被机构内部部门使用的数据提出有针对性的数据存储介质销毁管控规程。

2　应明确数据销毁效果评估机制，定期对数据销毁效果进行抽样认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除结果。

【条文说明】数据销毁的场景包括业务服务停止、数据存储空间释放再分配等等，处理对象涵盖数据库、服务器、终端和硬件存储介质。

5.6.3　数据销毁分级安全措施

1　存放 3 级及以上数据的存储介质不应移作他用，销毁时应采用物理销毁的方式对其进行处理，如消磁或磁介质、粉碎、融化等。

2　当涉及 3 级及以上数据的业务下线时，应对使用期结束后线下保存数据副本的存储介质进行数据销毁处理，确保数据不可还原。

3　4 级及以上数据存储介质的销毁应参照国家及行业涉密载体管理有关规定，由具备相应资质的服务机构或数据销毁部门进行专门处理。

6　民航数据安全组织保障

6.0.1　数据安全治理工作依托本单位数据治理组织架构开展，一般涉及单位数据管理组织、业务数据管理组织和数据安全工作组，如图 6.0.1 所示。

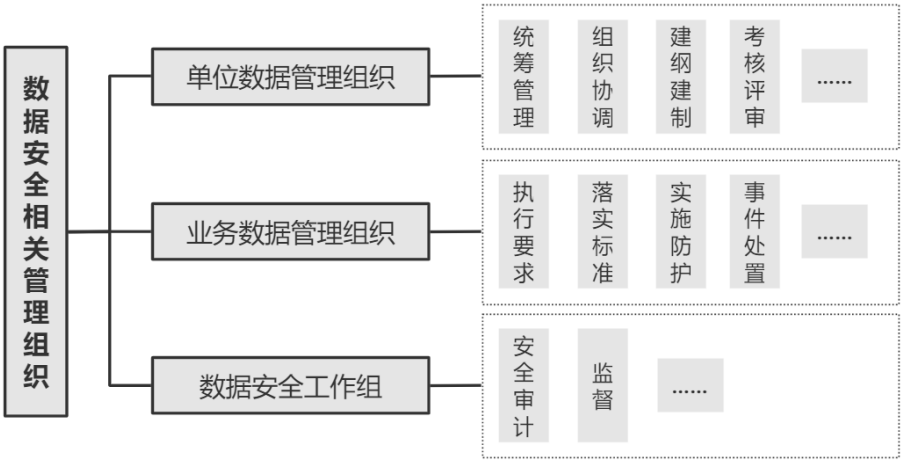

图 6.0.1　数据安全相关管理组织

6.0.2　单位数据管理组织总体负责本单位数据安全工作的统筹组织、指导推进和协调落实，确保单位内部数据安全自顶向下管理的一致性。负责以下工作：

1　制定、发布和维护本机构数据安全管理制度、规程和细则；

2　组织开展本单位数据安全分级工作；

3　制定、签发、实施、定期更新数据隐私政策和相关规程；

4　监督本单位内部，以及本单位与外部合作方数据安全管理情况；

5　在数据服务或相关信息系统上线发布前组织开展数据安全评估；

6　公布投诉、举报方式等信息，并及时受理数据安全相关投诉和举报。

6.0.3　各业务数据管理组织负责落实单位数据安全制度及措施，负责以下工作：

1　根据单位数据安全相关策略和规程，落实本业务数据安全控制措施；

2　负责本业务所辖数据的安全分级工作；

3　经授权审批程序后，为获得授权的各相关方分配数据权限；

4　对本业务数据脱敏、对外提供等关键活动的数据安全控制有效性进行确认；

5　配合执行数据相关安全评估及技术检测等工作；

6　处置本业务有关数据安全事件。

6.0.4　数据安全工作组负责监督和评价单位各业务领域的数据安全管理情况，负责以下工作：

1　根据本单位数据相关业务实际情况，确定相应审计策略，包括但不限于审计周期、审计方式、审计形式等内容；

2　监督数据安全政策、方针的执行；

3　开展数据安全内部审计和分析，发现并反馈问题和风险，并对后续相关整改工作进行监督。

标准用词说明

1　为了便于在执行本规范条文时区别对待，对要求严格程度不同的用词，说明如下：

1）表示很严格，非这样做不可的用词：

正面词采用“必须”，反面词采用“严禁”。

2）表示严格，在正常情况下均应这样做的用词：

正面词采用“应”；反面词采用“不应”或“不得”。

3）表示允许稍有选择，在条件许可时首先这样做的用词：

正面词采用“宜”；反面词采用“不宜”。

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2　本规范中指定应按其他有关标准、规范执行时，写法为“应符合……的规定”或“应按……的规定执行”。

引用标准名录

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，仅所注日期的版本适用。于本文件凡是不注日期的引用文件，其最新版本（包含所有修改单）适用于本文件。

[1] 中华人民共和国数据安全法

[2] 新时代民航强国建设行动纲要

[3] 推动新型基础设施建设促进民航高质量发展实施意见

[4] 推动民航新型基础设施建设五年行动方案

[5] 信息技术服务 治理 第 5 部分：数据治理规范（GB/T 34960.5）

[6] 信息安全技术 大数据服务安全能力要求（GB/T 35274）

[7] 信息安全技术 数据安全能力成熟度模型（GB/T 37988）

[8] 信息安全技术 大数据安全管理指南（GB/T 37973）

[9] 信息安全技术 政务信息共享 数据安全技术要求（GB/T 39477）