深圳市大数据平台

政务数据安全管理办法

二〇二三年六月

# 第一章 总则

**第一条 【目的】**为加强深圳市大数据平台（以下简称“大数据平台”）政务数据安全管理，建立健全政务数据安全保障体系，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《深圳经济特区数据条例》《信息安全技术 大数据服务安全能力要求》等相关法律法规规定，结合大数据平台实际，制定本办法。

**第二条 【适用范围】**本办法适用于本市行政机关和事业单位使用大数据平台开展政务数据处理活动的数据安全管理工作。涉及国家秘密、商业秘密、个人隐私的，按照国家相关法律、法规、规章的规定执行。

**第三条 【管理原则】**政务数据安全管理应遵循：

1. **职责明确。**根据“谁提供、谁负责，谁流转、谁负责，谁使用、谁负责”的原则，明确各方数据安全保障职责。
2. **合法合规。**在法律法规规定的范围内，依照法律法规规定的条件和程序，开展数据汇聚、数据存储、数据使用、数据加工等数据处理活动。
3. **最小授权。**在保证业务功能完整实现的前提下，应赋予数据活动中用户角色最小的操作权限，避免用户非法或异常操作所造成的损失。
4. **安全分级。**根据政务数据安全分类分级要求对数据进行分类分级管理，对不同级别的数据采取分级管控措施。
5. **监管可追溯。**对数据的修改、查询、删除、导出等操作进行监管，记录操作行为并进行监管审查，保障数据安全问题可审查可追溯。

# 第二章 职责分工

**第四条 【工作体系】**政务数据安全管理工作体系包括大数据平台管理部门、大数据平台运营单位、大数据平台运维单位、大数据平台使用部门（以下统称“各部门”）。

**第五条 【工作职责】**大数据平台管理部门负责统筹、协调、指导和监督大数据平台的数据安全管理工作，建立并完善大数据平台相关管理办法、规范和制度。

大数据平台运营单位负责大数据平台运营及数据安全保障工作，协同调查政务数据安全事件、处理数据安全问题，并监督问题整改。

大数据平台运维单位负责大数据平台运行运维工作和对大数据平台及其使用资源的运行监控和管理。

大数据平台使用部门作为本部门政务数据安全管理的责任主体，负责履行下列职责：

1. 贯彻落实国家、省、市政务数据安全法律、法规、规章和标准，制定本部门政务数据安全管理制度；
2. 明确政务数据安全负责人和管理机构，履行数据安全保护义务；
3. 负责本部门政务数据生命周期安全管理工作，覆盖数据汇聚、使用、共享、销毁等环节；
4. 定期开展政务数据处理活动风险评估，配合有关部门进行政务数据安全检查，发现问题及时整改。

# 第三章 平台安全管理

**第六条 【平台传输安全】**数据传输应采用校验技术、密码技术、加密通道、身份鉴别等措施保障平台数据传输过程可信、可控，并对传输过程进行记录。

**第七条 【平台存储安全】****大**数据平台运营单位应采用数据加密存储工具，对大数据平台数据湖内数据进行整体加密保护。

**第八条 【平台安全审计】**大数据平台运营单位应采取日志监测措施，实现平台数据处理日志统一监测管理，通过日志常态监控和日志定期安全审查等方式保障数据操作过程安全；对审计日志进行备份，审计日志保存期限至少6个月，避免受到非预期的删除、修改或覆盖等。

# 第四章 数据生命周期安全管理

**第九条 【数据汇聚安全】**通过大数据平台开展政务数据汇聚活动时，应明确汇聚政务数据的目的、依据和用途，确保政务数据汇聚的合法性、正当性和必要性，应当采取必要的安全管控措施，确保环境、设施、人员等安全可控。

**第十条 【数据分类分级】**大数据平台内的政务数据在编目前原则上需先进行分类分级。大数据平台使用部门应参照政务数据安全分类分级指南，完成本部门政务数据的分类分级工作，并根据数据安全等级、场景数据使用风险等级确定数据的安全管控措施。

**第十一条 【数据传输安全】**大数据平台使用部门应遵守平台传输要求进行政务数据传输。

**第十二条【数据存储安全】**使用大数据平台存储的数据，由大数据平台运营单位统一开展政务数据备份工作，并建立备份及恢复的制度流程和应急措施，确保发生政务数据安全事件时可进行政务数据恢复。

**第十三条 【数据处理安全】**使用大数据平台开展政务数据使用与加工活动时，必须遵循国家有关法律法规以及标准规范要求，应采取管控措施确保数据使用与加工合规，过程安全可控、可溯源。不得超出合理范围使用政务数据，不得滥用政务数据侵犯公共利益与个人合法权益。

**第十四条 【数据共享安全】**使用大数据平台开展政务数据共享活动时，应参照政务数据共享安全指引，按要求做好数据共享需求的提出与审核，保障数据共享实施安全。

**第十五条 【数据销毁安全】**大数据平台使用部门应建立本部门政务数据销毁制度，规范数据销毁的审批和记录流程，明确销毁方式和销毁要求，并妥善保存销毁记录。

# 第五章 供应链安全管理

**第十六条 【全流程管理】**各部门应当监督受委托建设、维护政务信息系统的供应商依照法律法规的规定和合同约定履行政务数据安全保护义务，防止供应商发生擅自留存、使用、泄露或者向他人提供政务数据，擅自将数据用于其他用途等违法违规和违反合同约定的行为；在供应商参与政务信息化建设和运维过程中涉及敏感个人信息的，各部门应当监督供应商按照有关法律法规要求采取备份、加密、访问控制等必要措施。

**第十七条 【权限管理】**各部门应当加强大数据平台的权限管理，建立最小授权的访问控制策略，对数据库、操作系统等的最高管理员权限必须由各部门指定专人负责，不得擅自转交供应商人员管理使用，防范越权访问带来的数据泄露、篡改、删除等风险。

# 第六章 安全监督审计

**第十八条 【数据安全监督检查】**各部门应在各自职责范围内监督检查本部门人员的平台操作行为安全和数据处理活动安全，对检查中发现的问题及时整改。

**第十九条　【数据安全审计】**各部门应对本部门职责范围内的工作定期开展数据安全审计，对于发现的数据安全问题，应会同大数据平台管理部门及时整改。

# 第七章 风险与应急处置

**第二十条 【数据安全风险评估】**各部门应定期开展数据安全风险评估，确保数据安全工作机制有效，对于发现的安全隐患及时整改。

各部门可采取自评估、第三方评估等方式，对本部门管理的重要数据和敏感数据安全状态以及数据处理活动情况进行数据安全风险评估，完善数据安全保障措施，确保数据安全。

**第二十一条　【应急处置】**各部门应定期组织开展数据安全意识教育和政务数据安全培训，制定本部门政务数据安全事件应急处置预案，定期组织应急演练，掌握岗位职责和应急处置策略，并对演练情况进行评估，针对演练中发现的问题，补充修订应急预案。

# 第八章 附则

**第二十二条 【术语解释】**本办法下列用语的含义：

**（一）数据安全**，是指通过采取必要措施，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。

**（二）政务数据**，是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。本办法中特指大数据平台中的政务数据。

**（三）政务数据分类**，是指根据政务数据的属性或特征，将其按一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序的过程。

**（四）政务数据分级**，是指根据政务数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会稳定、经济运行、公共健康和安全造成的危害程度，对数据进行定级。

**第二十三条**本办法由深圳市大数据资源管理中心负责解释。

**第二十四条**　本办法自发布之日起开始实施。