附件

会计师事务所数据安全管理暂行办法

第一章　总则

第一条 为保障会计师事务所数据安全，规范会计师事务所数据处理活动，根据《中华人民共和国注册会计师法》、《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》等法律法规，制定本办法。

第二条 在中华人民共和国境内依法设立的会计师事务所开展下列审计业务相关数据处理活动的，适用本办法:

（一）为上市公司以及非上市的国有金融机构、中央企业等提供审计服务的;

（二）为关键信息基础设施运营者或者超过100万用户的网络平台运营者提供审计服务的;

（三）为境内企业境外上市提供审计服务的。

会计师事务所从事的审计业务不属于前款规定的范围，但涉及重要数据或者核心数据的，适用本办法。

第三条 本办法所称数据，是指会计师事务所执行审计业务过程中，从外部获取和内部生成的任何以电子或者其他方式对信息的记录。

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。

第四条 会计师事务所承担本所的数据安全主体责任，履行数据安全保护义务。

第五条 财政部负责全国会计师事务所数据安全监管工作，省级（含深圳市、新疆生产建设兵团）财政部门负责本行政区域内会计师事务所数据安全监管工作。

第六条 注册会计师协会应当加强行业自律，指导会计师事务所加强数据安全保护，提高数据安全管理水平。

第二章 数据管理

第七条 会计师事务所应当在下列方面履行本所数据安全管理责任：

（一）建立健全数据全生命周期安全管理制度，完善数据运营和管控机制；

（二）健全数据安全管理组织架构，明确数据安全管理权责机制；

（三）实施与业务特点相适应的数据分类分级管理；

（四）建立数据权限管理策略，按照最小授权原则设置数据访问和处理权限，定期复核并按有关规定保留数据访问记录；

（五）组织开展数据安全教育培训；

（六）法律法规规定的其他事项。

第八条 会计师事务所的首席合伙人（主任会计师）是本所数据安全负责人。

第九条 会计师事务所应当按照法律、行政法规的规定和被审计单位所处行业数据分类分级标准确定核心数据、重要数据和一般数据。

会计师事务所和被审计单位应当通过业务约定书、确认函等方式明确审计资料中核心数据和重要数据的性质、内容和范围等。

第十条 会计师事务所对核心数据、重要数据的存储处理，应当符合国家相关规定。

存储核心数据的信息系统要落实四级网络安全等级保护要求。存储重要数据的信息系统要落实三级及以上网络安全等级保护要求。

数据汇聚、关联后属于国家秘密事项的，应当依照有关保守国家秘密的法律、行政法规规定处理。

第十一条 会计师事务所应当对审计业务相关的信息系统、数据库、网络设备、网络安全设备等设置并启用访问日志记录功能。

涉及核心数据的，相关日志留存时间不少于三年。涉及重要数据的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的相关日志留存时间不少于三年。

第十二条 会计师事务所应当明确数据传输操作规程。核心数据、重要数据传输过程中应当采用加密技术，保护传

输安全。

第十三条 审计工作底稿应当按照法律、行政法规和国家有关规定存储在境内。相关加密设备应当设置在境内并由境内团队负责运行维护，密钥应当存储在境内。

第十四条 会计师事务所应当建立数据备份制度。会计师事务所应当确保在审计相关应用系统因外部技术原因被停止使用、被限制使用等情况下，仍能访问、调取、使用相关审计工作底稿。

第十五条 会计师事务所不得在业务约定书或者类似合同中包含会计师事务所向境外监管机构提供境内项目资料数据等类似条款。

第十六条 会计师事务所应当采用网络隔离、用户认证、访问控制、数据加密、病毒防范、非法入侵检测等技术手段，及时识别、阻断和溯源相关网络攻击和非法访问，保障数据安全。

第十七条 会计师事务所应当建立数据安全应急处置机制，加强数据安全风险监测。发现数据外泄、安全漏洞等风险的，应当立即采取补救、处置措施。发生重大数据安全事件，导致核心数据或者重要数据泄露、丢失或者被窃取、篡改的，应当及时向有关主管部门报告。

第十八条 会计师事务所向境外提供其在境内运营中收集和产生的个人信息和重要数据的，应当遵守国家数据出境

管理有关规定。

第十九条 会计师事务所对于审计工作底稿出境事项应当建立逐级复核机制，采取必要措施严格落实数据安全管控责任。对于需要出境的审计工作底稿，按照国家有关规定办理审批手续。

第三章 网络管理

第二十条 会计师事务所应当建立完善的网络安全管理治理架构，建立健全内部网络安全管理制度体系，建立内部决策、管理、执行和监督机制，确保网络安全管理能力与提供的专业服务相适应，为数据安全管理工作提供安全的网络环境。

第二十一条 会计师事务所应当按照业务活动规模及复杂程度配置具备相应职业技能水平的网络管理技术人员，确保合理的网络资源投入和资金投入。

第二十二条 会计师事务所应当做好信息系统安全管理和技术防护，根据存储、处理数据的级别采取相应的网络物理隔离或者逻辑隔离等措施，设置严格的访问控制策略，防范未经授权的访问行为。

第二十三条 会计师事务所应当拥有其审计业务系统中网络设备、网络安全设备的自主管理权限，统一设置、维护系统管理员账户和工作人员账户，不得设置不受限制、不受监控的超级账户，不得将管理员账号交由第三方运维机构管

理使用。

加入国际网络的会计师事务所使用所在国际网络的信息系统的，应当采取必要措施，使其符合国家数据安全法律、行政法规和本办法的规定，确保本所数据安全。

第四章 监督检查

第二十四条 财政部和省级财政部门（以下统称省级以上财政部门）与同级网信部门、公安机关、国家安全机关加强会计师事务所数据安全监管信息共享。

第二十五条 省级以上财政部门、省级以上网信部门对会计师事务所数据安全情况开展监督检查。公安机关、国家安全机关依法在职责范围内承担会计师事务所数据安全监管职责。

第二十六条 对于承接金融、能源、电信、交通、科技、国防科工等重要领域审计业务且符合本办法第二条规定范围的会计师事务所，省级以上财政部门在监督检查工作中予以重点关注，并持续加强日常监管。

第二十七条 会计师事务所对于依法实施的数据安全监督检查，应当予以配合，不得拒绝、拖延、阻挠。

第二十八条 会计师事务所开展数据处理活动，影响或者可能影响国家安全的，应当按照国家安全审查机制进行安全审查。

第二十九条 相关部门在履行数据安全监管职责中，发

现会计师事务所开展数据处理活动存在较大安全风险的，可以对会计师事务所及其责任人采取约谈、责令限期整改等监管措施，消除隐患。

第三十条 会计师事务所及相关人员违反本办法规定的，应当按照《中华人民共和国注册会计师法》、《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》等法律、行政法规的规定予以处理处罚；涉及其他部门职责权限的，依法移送有关主管部门处理；构成犯罪的，移送司法机关依法追究刑事责任。

第三十一条 相关部门工作人员在履行会计师事务所数据安全监管职责过程中，玩忽职守、滥用职权、徇私舞弊的，依法追究法律责任。

第五章 附则

第三十二条 会计师事务所及相关人员开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三十三条 会计师事务所及相关人员开展其他涉及个人信息的数据处理活动，应当遵守有关法律、行政法规的规定。

第三十四条 会计师事务所可以参照本办法加强对非审计业务数据的管理。

第三十五条 本办法由财政部、国家网信办负责解释。

第三十六条 本办法自 2024 年 10 月 1 日起施行。