附件1

会计师事务所数据安全管理暂行办法

（征求意见稿）

第一章 总则

1. 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》、《中华人民共和国数据安全法》、《中华人民共和国网络安全法》等法律法规，制定本办法。
2. 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：
3. 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；
4. 开展跨境审计业务的。
5. 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，确保数据持续得到有效保护和合法利用。

1. 会计师事务所承担本机构的数据安全主体责任，履行数据安全保护义务。
2. 国务院财政部门会同国家网信部门负责全国会计师事务所数据安全监管工作，省、自治区、直辖市人民政府财政部门会同省级网信部门负责本行政区域内会计师事务所数据安全监管工作。
3. 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

1. 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。

1. 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。
2. 会计师事务所应当按照相关法律法规的规定和被审计单位所处行业数据分级分类标准确定核心数据、重要数据和一般数据。

会计师事务所应当通过业务约定书等方式与被审计单位明确审计资料分级分类要求，审计资料分级分类的要求应当与被审计单位相关资料分级分类的要求保持一致。

1. 针对核心数据，会计师事务所应当建立核心数据保护机制，通过专用服务器或者会计师事务所私有云平台设置内部专门空间存储，使用加密虚拟专用网络等技术手段传输，对核心数据的存储、读取、转移应当建立授权与记录机制并保证有效运行。

针对重要数据，会计师事务所应当制定和执行规范的处理流程，将其存放于和互联网逻辑隔离的信息系统中，并严格控制接触人员范围。

针对一般数据，会计师事务所应当采取基于用户角色的授权访问控制，并且按照最小权限原则授权。

1. 会计师事务所的审计工作底稿及相关数据应当存储在境内，不得在境外备份。

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。日志应当存放境内，其中，日志中的用户登录及访问日志保存期限不得少于十年，其他日志保存期限不得少于六个月。

1. 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。
2. 审计工作底稿和相关数据的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。
3. 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。
4. 会计师事务所不得在业务约定书或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。
5. 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。
6. 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的，应当及时向省级以上财政部门报告。
7. 会计师事务所在境内形成的审计工作底稿应当存放在境内。需要出境的，按照国家有关规定办理审批手续。
8. 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审计工作底稿涉密敏感信息管控责任。

第三章 网络管理

1. 会计师事务所应当建立完善的网络管理治理架构，建立健全内部网络管理制度体系，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。
2. 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关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。
3. 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。
4. 会计师事务所应当拥有其使用的审计业务系统中网络设备、网络安全设备的配置和管理的最高权限，统一管理、维护系统管理员账户和工作人员账户，不得设置不受限制的超级账户。

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，应当采取用户隔离和数据隔离等措施。

第四章 监督检查

1. 省级以上财政部门与同级网信部门加强会计师事务所数据安全监管信息共享。
2. 省级以上财政部门、省级以上网信部门（以下简称相关部门）对会计师事务所数据安全情况开展监督检查。

在监督检查过程中，相关部门可以委托国家、行业有关专业机构采用渗透测试、漏洞扫描及信息技术风险评估等方式，协助对会计师事务所开展监督检查。

相关部门和机构工作人员对监督检查中知悉的核心数据、重要数据、个人隐私等数据应当依法严格保护，不得泄露或者非法向他人提供。

1. 对于承接金融、能源、通信、交通、科技、国防科工等重要领域审计业务的会计师事务所，相关部门应当开展全覆盖监督检查，并持续加强日常监管。
2. 会计师事务所对于相关部门依法实施的数据安全检查，应当予以配合，提供符合要求的相关数据资料和工作便利，不得拒绝、拖延、阻挠。
3. 承接关系国计民生、重要领域审计业务的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，按照网络安全审查相关机制进行网络安全审查。
4. 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。
5. 会计师事务所及其从业人员违反本办法规定的，由相关部门依照《中华人民共和国数据安全法》、《中华人民共和国网络安全法》、《中华人民共和国注册会计师法》等法律、行政法规的规定进行处理处罚。
6. 对会计师事务所及其从业人员违反本办法规定，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。

第五章 附则

1. 会计师事务所及其从业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。
2. 会计师事务所开展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。
3. 会计师事务所的非审计业务数据管理可参照本办法执行。
4. 本办法由财政部、国家网信办负责解释。
5. 本办法自 年 月 日起施行。