人民法院数据安全管理办法

第一章总则

第一条为指导并规范人民法院数据处理活动，建立健全数据安全治理体系，提高人民法院数据安全保障能力，促进司法数据安全开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《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》《信息系统安全等级保护基本要求》《人民法院数据管理办法（2020）》等有关规定，结合人民法院工作实际，制定本办法。

第二条各级人民法院利用各类信息系统开展司法数据处理活动、数据的全生命周期管理，以及数据安全事件的监督、问责，适用本办法。

第三条本办法所称数据是指以电子或其他方式对信息记录的，各级人民法院产生和积累的审判执行、司法人事、司法政务、司法研究、信息化管理、外部协同等各类数据资源。

第四条各级人民法院开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第五条各级人民法院对本单位的数据及数据安全负责，并应

当明确本单位数据安全管理机构。最高人民法院数据安全管理机构负责全国法院数据安全管理的规划指导、组织协调、标准制定、审批决策、审查监督等工作，各高级人民法院数据安全管理机构负责辖区法院数据安全管理的规划指导、组织协调、评估考核、审批决策、审查监督工作。各级人民法院应根据本办法，制定适应于本法院的数据安全管理办法，并组织落实。

第二章数据分类分级管理

第六条人民法院数据分类分级按照数据分类管理、分级保护的思路，依据合法合规、分类多维、分级明确、就高从严、动态调整的原则进行划分。

第七条人民法院数据从多视角和维度对数据进行分类，包括但不限于：

1. 业务领域维度：审判执行数据、司法管理数据、系统运行数据；

2. 所属范围维度：局部数据、全局数据；

3. 数据来源维度：原生数据、外部数据；

4. 信息公开维度：可公开数据、非公开数据、秘密数据、机密数据；

5. 数据结构维度：结构化数据、非结构化数据。

第八条人民法院数据应根据数据遭到篡改、破坏、泄露或非

法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，将数据从低到高分成一般数据、重要数据、核心数据三个级别。

第九条各级人民法院应根据数据分类分级框架和原则开展数据分类分级工作，建立本单位数据目录，指导辖区法院建立数据目录，汇总形成辖区法院数据目录。数据目录应定期进行审查更新，并向上级人民法院备案。核心、重要数据应当明确数据安全负责人和管理机构。

第三章数据全生命周期安全管理

第十条人民法院数据收集遵循合法、合规、正当和最小范围的原则，应当在法律、法规规定的目的和范围内收集数据，不得窃取或者以其他方式非法获取数据。

应按照数据目录对收集的数据及时进行分类分级并标识；收集数据的来源应具有可追溯性，并使用技术手段实现对数据的监控；信息系统收集其他系统数据时应获得许可。

第十一条人民法院收集的数据应进行严格的存储管控，有效防止数据损坏、丢失、泄露。数据应存储在中华人民共和国境内，涉及国家秘密的数据应当存储在涉密单机或涉密网络，工作秘密、敏感信息及其他核心数据应存储在法院专网内，委托他人存储数据时应履行审批程序，明确数据安全管理要求并履行监督义务。

数据存储应采取符合国家密码管理规定的密码保护措施，根据各级人民法院实际业务情况，可采用异地或同地不同数据中心方式进行数据备份，定期开展数据恢复测试及演练，保障数据备份有效性。

第十二条人民法院应在履行法定职责的范围内使用和加工数据，使用、加工数据应当在确保数据安全的条件下进行。应建立数据使用台账及配套的审核制度，遵循“最小授权”原则，确定数据使用者可访问的数据范围，定期审计数据使用情况。经数据加工产生的新数据应根据数据目录及时进行分级分类工作。

第十三条人民法院进行数据传输时，应根据安全级别及数据规模，制定数据传输安全策略，并采用密码技术保障数据传输的安全，密码技术及产品使用应符合国家密码管理部门要求。

第十四条各级人民法院应明确可对外提供数据的范围、条件、程序等。向外部提供数据应符合“安全、必要和最小范围”原则，非必要不提供原始数据。数据提供应由本单位数据安全管理机构审批（必要时应提交上级人民法院审批），并监督受提供方履行数据安全保护义务。

涉及向外国司法或执法机构提供数据，应当按照数据安全法要求，报中华人民共和国主管机关批准。

第十五条各级人民法院应参考国家政务数据开放目录，梳理本单位数据开放目录，在数据公开发布前应分析可能对国家安全、公共利益、个人隐私等方面产生的影响，履行审批程序，敏感数

据或者个人信息公开应采取脱敏处理。应采用技术手段对公开的数据进行审计和监督。

第十六条各级人民法院应定期对数据进行归档处理，归档数据应明确数据类型、级别、保存时间等要素信息，形成数据归档目录。已停用系统的数据应及时归档。

应及时对冗余数据进行归并。归档或归并后不再使用的数据及其他无保留必要的数据应当及时销毁。数据销毁应采取技术手段保障数据不可恢复，并对数据销毁活动进行记录。

第十七条各级人民法院开展数据处理活动，应当在网络安全等级保护制度的基础上，在数据全生命周期各个环节采取必要的仅限管控、加密保护、监控审计、防篡改、数据备份、数据脱敏、运维管控等技术措施，保障数据处理活动中数据和系统的安全。

第四章数据安全保障要求

第十八条各级人民法院应对管理使用的数据定期开展清点检查工作，建立并及时更新数据清单。数据清单应当明确数据量、数据类型、存储位置、对外提供情况、防护措施等要素信息。

第十九条各级人民法院应当建立数据安全事件应急响应预案，组织协调重要数据和核心数据安全事件应急处置工作。发生重要、核心数据泄露、受损、丢失等数据安全事件时，应及时采取补救措施，并按照规定及时向有关主管部门和上一级人民法院报告。最高人民法院及各高级人民法院应每年组织数据安全应急

演练。

第二十条各级人民法院应定期开展数据安全风险评估工作，并向上级人民法院报送风险评估报告。风险评估报告应包括处理的数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及应对措施等。对于发现的数据安全缺陷、漏洞等风险，应及时处置清零。

第二十一条最高人民法院应建立数据安全审查制度，对影响或者可能影响国家安全、公共利益、个人隐私的数据处理活动进行安全审查。

各级人民法院应对辖区法院的数据安全管理情况履行监督职责；各级人民法院应对本单位信息系统承建方、运营方的数据安全相关工作进行监督。

监督过程中发现数据安全管理责任落实不到位的，应督促整改；发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第二十二条各级人民法院应每年组织全员开展数据安全意识教育培训，并针对数据安全管理专员开展专业化数据安全技术技能培训与考核。

第二十三条最高人民法院和各高级人民法院应成立专业化**数据**安全保障团队，开展常态化数据安全管理工作，对辖区法院数据的分类分级、生产、传输、管理、应用等全过程进行安全监

管。各级人民法院应明确数据安全负责人，并设立数据安全岗位，明确岗位职责，并对数据安全工作提供配套的经费保障。

第二十四条各级人民法院及相关单位工作人员应当对履职过程中知悉的数据资源及相关信息承担保密责任，不得泄露或者擅自向其他单位、组织或人员提供。

第二十五条违反相关法律法规及本办法规定，发生重要、核心数据或个人信息泄露、受损、丢失或其他数据安全事件的，由所在法院或上级人民法院依据情节对责任主体予以通报、追责并责令整改。涉及行政处罚或构成犯罪的，转交相关部门处理。

第二十六条各级人民法院涉及国家秘密的数据处理活动，应当遵循《中华人民共和国保守国家秘密法》等法律和行政法规的规定。在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五章附则

第二十七条本管理办法由最高人民法院网络安全和信息化领导小组办公室负责解释。

第二十八条本管理办法自印发之日起实施