

附件 1

内蒙古自治区电信领域数据安全管理工作实施细则 (征求意见稿)

第一章 总则

第一条 为加强内蒙古自治区电信领域数据安全管理工作，进一步提高数据安全保护水平，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《工业和信息化领域数据安全管理办法(试行)》等法律法规和有关规定，结合我区实际，制定本细则。

第二条 内蒙古自治区的电信领域数据处理者开展数据处理活动及其安全监管，应当遵守相关法律、行政法规和本细则的要求。

第三条 本细则所称电信领域数据是指在电信业务经营过程中产生和收集的数据，包括各类基础电信业务和增值电信业务数据。

电信领域数据处理者是指数据处理活动中自主决定处理目的、处理方式的取得电信业务经营许可证的电信业务经营者。

数据处理活动包括但不限于数据收集、存储、使用、加工、传输、提供、公开等活动。

第四条 在工业和信息化部统筹指导下，内蒙古自治区通信

管理局负责内蒙古自治区电信领域数据安全的组织协调、统筹规划和监督管理工作。

第五条 数据安全应当坚持总体国家安全观，统筹数据发展与安全，鼓励数据开发利用，加强数据治理，保证数据供给、流通、使用全过程安全合规。

第二章 基础性数据安全保护要求

第六条 电信领域数据处理者应当每年至少开展一次数据梳理工作，按照电信领域重要数据和核心数据识别标准识别重要数据和核心数据，相关工作开展情况按年度形成报告并报送内蒙古自治区通信管理局，报告内容包括数据梳理工作开展情况、数据分类分级情况、数据分级防护措施等。

第七条 电信领域数据处理者应当按要求将识别出的重要数据和核心数据进行目录填报，并报内蒙古自治区通信管理局备案。备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况，不包括数据内容本身。

备案内容发生重大变化的，电信领域数据处理者应当在发生变化的三个月内履行备案变更手续。重大变化是指某类重要数据和核心数据规模(数据条目数量或者存储总量等)变化 30%以上，重要数据或核心数据类别新增或减少，数据安全情况、责任主体信息发生变动，或者其他备案内容发生变化。

内蒙古自治区通信管理局对备案信息完整性、重要数据和核

心数据类别、级别、数据量等填报内容准确完备性进行审核，在电信领域数据处理者提交备案申请的二十个工作日内完成并反馈审核结果。备案未通过的申请人应当在收到反馈情况后的十五个工作日内再次提交备案申请。

内蒙古自治区通信管理局对重要数据和核心数据目录备案落实情况进行监督检查，电信领域数据处理者应当予以配合。

第八条 电信领域数据处理者应当根据实际工作需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理。

电信领域重要和核心数据处理者还应当建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，负责牵头内部数据安全管理工作，明确数据处理关键岗位和岗位职责，要并配备具备相应技能水平的专职人员，定期参与行业认可的数据安全考核与培训。

第九条 电信领域数据处理者应加强权限审批管理，合理配置数据处理活动的权限，明确各部门和相关人员权限管理要求，包含但不限于数据处理活动平台系统账号权限分配原则、流程等，建立并定期更新权限分配表。

第十条 电信领域数据处理者应对数据处理、系统运行、权限管理、人员操作等日志进行留存管理，日志留存时间不少于六个月。日志记录信息应包括执行时间、操作账号、处理方式等，针对数据使用加工、关联分析、批量访问、批量复制等数据处理行为还应记录授权情况、登录信息等，记录完整、准确、不可修

改。

第十一条 电信领域数据处理者应定期开展数据安全审计，审计对象完整覆盖全部数据处理活动，审计发现问题需及时整改，并对审计及处置记录进行留存管理。

重要数据处理活动应至少每半年开展一次审计，核心数据处理活动应至少每季度开展一次审计。

第十二条 电信领域数据处理者应当开展数据安全风险监测，对数据安全风险隐患进行预警，并及时开展处置。对于可能造成较大及以上安全事件的风险，应及时向内蒙古自治区通信管理局报告，报告内容包括但不限于风险类别和级别、涉及数据情况、产生时间、影响范围等信息。

第十三条 电信领域数据处理者应制定数据安全事件应急预案并开展应急演练。应急预案应充分结合数据泄露、数据滥用、数据篡改、数据损毁、数据违规使用等数据安全事件场景和等级明确应急响应工作责任分工、实施流程、保障措施等。

在数据安全事件发生后，电信领域数据处理者应当按照应急预案，及时开展应急处置。涉及重要数据和核心数据的安全事件，第一时间向内蒙古自治区通信管理局报告，事件处置完成后立即开展事件调查、问题整改、责任追究，在处置完成七个工作日内形成总结报告并报送内蒙古自治区通信管理局。对于发生过数据安全事件的电信领域数据处理者还应每年向内蒙古自治区通信管理局报告数据安全事件处置情况。

第十四条 电信领域重要数据和核心数据处理者应当自行或委托第三方评估机构,每年对其数据处理活动至少开展一次风险评估,及时整改风险问题,并向内蒙古自治区通信管理局报送风险评估报告。

重要数据和核心数据目录备案内容发生重大变化的,电信领域数据处理者应当在履行备案变更手续后及时启动风险评估,备案变更后三个月内向内蒙古自治区通信管理局重新提交风险评估报告。

电信领域一般数据处理者应当自行或委托第三方评估机构,每年至少开展一次数据安全合规性评估,及时整改问题,并向内蒙古自治区通信管理局报送评估报告。评估内容包括但不限于数据合规使用情况、数据安全保障措施配备情况与完善程度、合作方数据安全保护水平等。

第十五条 电信领域数据处理者应加强数据安全教育培训,鼓励企业通过积极参与本地区、本行业数据安全人才培养计划等方式,提升相关岗位人员数据安全保护意识和技能水平。

电信领域数据处理者应定期组织开展内部数据安全教育培训,培训内容涵盖数据安全法律法规、标准规范、管理制度和工作要求、知识技能、保护意识等,培训对象覆盖数据安全岗位人员,年度培训时长不小于30学时。

电信领域重要数据和核心数据处理者还应针对处理重要数据和核心数据的重点岗位人员定期开展教育培训,培训内容包括

但不限于重要数据和核心数据安全要求、安全操作规程、风险评估规范等，年度培训时长不少于 45 学时。

第十六条 电信领域数据处理者应当加强对合作方管理，通过签订合同协议等方式，明确数据委托处理、数据处理系统开发运维等合作方数据安全责任和义务。涉及重要数据和核心数据的，应当对合作方的数据安全保护能力、资质进行核验。

第三章 数据全生命周期安全保护要求

第十七条 电信领域数据处理者应当对数据处理活动负安全主体责任，建立健全全流程数据安全管理制度，针对不同级别数据，制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

第十八条 电信领域数据处理者收集数据应当遵循合法、正当的原则，不得窃取或者以其他非法方式获取数据。

数据收集过程中，采取规范化采集流程、方式、渠道和数据格式，根据数据安全级别采取相应的安全措施，加强重要数据和核心数据收集人员、设备的管理，并对收集来源、时间、类型、数量、频度、流向等进行记录。

对直接采集或者通过间接渠道获得的数据负有同等的保护责任和义务。通过间接途径获取重要数据和核心数据的，电信领域数据处理者应当与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

通过移动应用程序或其他方式面向用户直接收集个人信息

类数据的，应在业务用户协议或隐私政策文件中明确个人信息收集的目的、用途和范围，按照公开透明原则将收集规则以通俗易懂、简单明了的文字向用户明示，在获得授权或有其他合法性基础的前提下开展。

第十九条 电信领域数据处理者应当按照法律、行政法规规定和用户约定的方式、期限进行数据存储，应结合数据分类分级策略明确差异化数据存储安全策略和操作规程。

存储重要数据和核心数据的，应当采用校验技术、密码技术等措施进行安全存储，并实施数据容灾备份和存储介质安全管理，定期开展数据恢复测试，对备份数据的有效性和可用性进行检查和恢复验证。

第二十条 电信领域数据处理者进行数据使用加工应遵循目的明确原则，制定不同目的下数据使用审批流程、数据脱敏处理使用规则，明确数据使用结果发布和使用的安全保护规则。

利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。

第二十一条 电信领域数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。针对不同网络安全域之间的数据传输采取访问控制、监控等安全防护技术措施。传输重要数据和核心数据的，应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

第二十二條 電信領域數據處理者對外提供數據，應當明確提供的範圍、類別、條件、程序等，對數據提供形式、期限、涉及的业务或系統、數據安全保護措施等實施管理。提供重要數據和核心數據的，應當與數據獲取方簽訂數據安全協議，對數據獲取方數據安全保護能力進行核驗，採取校驗技術、密碼技術、安全傳輸通道、安全傳輸協議等必要的安全保護措施。

第二十三條 電信領域數據處理者應當在數據公開前分析研判可能對國家安全、公共利益產生的影響，擬公開前十個工作日前向內蒙古自治區通信管理局提交重要數據和核心數據公開申請，審批通過後予以公開，存在重大影響的不得公開。對於法律、行政法規要求公開的數據場景，應採用靜態脫敏等措施防止數據洩露或濫用。

第二十四條 電信領域數據處理者在中華人民共和國境內收集和產生的重要數據和核心數據，法律、行政法規有境內存儲要求的，應當在境內存儲，確需向境外提供的，應當依法依規進行數據出境安全評估。

第二十五條 電信領域數據處理者應當建立數據銷毀制度，明確銷毀對象、規則、流程和技术等要求，對銷毀活動進行記錄和留存。個人、組織按照法律規定、合同約定等請求銷毀的，電信領域數據處理者應當銷毀相應數據。

銷毀重要數據和核心數據的，應當設置銷毀相關監督角色並採用多人操作模式，單人不得擁有完整操作權限。重要數據和核

心数据销毁后，不得以任何理由、任何方式进行恢复;引起重要数据和核心数据目录备案内容发生变化的，应当履行备案变更手续。

电信领域数据处理者发生重组、解散、宣告破产、业务撤销等情形的，应当在有关情形发生前向内蒙古自治区通信管理局报告，按照相关要求移交或销毁数据。

第二十六条 跨主体提供、转移、委托处理核心数据的，电信领域数据处理者应当评估安全风险，采取必要的安全保护措施，并报送内蒙古自治区通信管理局。内蒙古自治区通信管理局按照有关规定进行审查后报工业和信息化部。

第四章 支持与投诉举报

第二十七条 鼓励电信领域数据处理者开展数据安全知识宣传普及、教育培训，增强全区公共数据安全保护意识，提高数据安全风险管理能力。

第二十八条 加强投诉举报，内蒙古自治区通信管理局健全数据安全违法行为投诉举报机制，依法接收、处理投诉举报，根据工作需要开展执法检查。鼓励电信领域数据处理者建立用户投诉处理机制。

第五章 附则

第二十九条 本细则自印发之日起施行。