工业和信息化领域数据安全风险评估实施细则（试行）

第一条 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》等法律，按照《工业和信息化领域数据安全管理办法（试行）》有关要求，为引导工业和信息化领域数据处理者规范开展数据安全风险评估工作，提升数据安全管理水平，维护国家安全和发展利益，制定本细则。

第二条 本细则适用于对中华人民共和国境内工业和信息化领域重要数据和核心数据处理者数据处理活动开展的数据安全风险评估。

第三条 工业和信息化部统一管理、监督和指导工业和信息化领域数据安全风险评估工作，组织开展相关评估标准制修订及推广应用。

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局和无线电管理机构（以下统称地方行业监管部门）依据职责分别负责监督管理本地区工业、电信、无线电重要数据和核心数据处理者开展数据安全风险评估工作。

工业和信息化部及地方行业监管部门统称为行业监管部门。

第四条 重要数据和核心数据处理者按照及时、客观、

有效的原则开展数据安全风险评估，形成真实、完整、准确的评估报告，并对评估结果负责。

第五条 重要数据和核心数据处理者按照国家法律法规、行业监管部门有关规定以及评估标准，对数据处理活动的目的和方式、业务场景、安全保障措施、风险影响等要素，开展数据安全风险评估，重点评估以下内容:

（一）数据处理目的、方式、范围是否合法、正当、必要;

（二）数据安全管理制度、流程策略的制定和落实情况;

（三）数据安全组织架构、岗位配备和职责履行情况;

（四）数据安全技术防护能力建设及应用情况;

（五）数据处理活动相关人员是否熟悉数据安全相关政策法规、是否具备数据安全知识技能、是否接受数据安全相关教育培训等情况;

（六）发生数据遭到篡改、破坏、泄露、丢失或者被非法获取、非法利用等安全事件，对国家安全、公共利益的影响范围、程度等风险;

（七）涉及数据提供、委托处理、转移的，数据获取方或受托方的安全保障能力、责任义务约束和履行情况;

（八）涉及国家法律法规中规定需要申报的数据出境安全评估情形，履行数据出境安全评估要求情况。

第六条 重要数据和核心数据处理者每年至少开展一次

数据安全风险评估，评估结果有效期为一年，以评估报告首次出具日期计算。评估报告应当包括数据处理者基本情况、评估团队基本情况、重要数据的种类和数量、开展数据处理活动的情况、数据安全风险评估环境，以及数据处理活动分析、合规性评估、安全风险分析、评估结论及应对措施等。

在有效期内出现以下情形之一的，重要数据和核心数据处理者应当及时对发生变化及其影响的部分开展风险评估:

（一）新增跨主体提供、委托处理、转移核心数据的;

（二）重要数据、核心数据安全状态发生变化对数据安全造成不利影响的，包括但不限于数据处理目的、方式、适用范围和安全制度策略等发生重大调整的;

（三）发生涉及重要数据、核心数据的安全事件的;

（四）重要数据和核心数据目录备案内容发生重大变化的;

（五）行业监管部门要求进行评估的其他情形。

第七条 重要数据和核心数据处理者可以自行或者委托具有工业和信息化数据安全工作能力的第三方评估机构开展评估。评估过程应当建立至少包括组织管理、业务运营、技术保障、安全合规等人员的专业化评估团队，制定完备的评估工作方案，配备有效的技术评测工具。

第八条 重要数据和核心数据处理者委托第三方评估机构开展数据安全风险评估的，可以通过订立合同或者其他具

有法律效力的文件，明确双方的权利和责任，向第三方评估机构提供必需的材料和条件，确保相关材料的真实性和完整性，并确认评估结果。

第九条 重要数据和核心数据处理者对评估中发现的数据安全风险隐患，应当及时采取适当措施消除或降低风险隐患。

第十条 重要数据和核心数据处理者应当在评估工作完成后的10个工作日内，向本地区行业监管部门报送评估报告。

中央企业督促指导所属企业履行属地数据安全风险评估及评估报告报送要求，并将梳理汇总的企业集团本部、所属公司的评估报告报送工业和信息化部。

地方行业监管部门将本地区本领域重要数据和核心数据处理者的评估结果报送工业和信息化部。

第十一条 地方行业监管部门发现不符合法律法规和有关规定的，应当及时通知重要数据和核心数据处理者依法予以改正。地方行业监管部门于12月25日前，将本地区本年度评估报告接收和审核情况报送工业和信息化部。工业和信息化部视情对评估报告组织抽查审核。

涉及跨主体提供、转移、委托处理核心数据的，地方行业监管部门应当在数据处理者提交评估报告的20个工作日内完成审查，并报工业和信息化部按照国家有关规定进行复

核。

第十二条 鼓励熟悉工业和信息化领域数据安全工作，满足资质要求的认证机构开展第三方评估机构的能力认证。

相关认证机构配备相应的人员和技术保障能力，建立第三方评估机构能力认证制度，明确第三方评估机构在管理体系、人员能力、工具设施、评估领域等方面的规范要求，跟踪管理第三方评估机构的服务质量，督促第三方评估机构独立、公正、客观、科学地开展数据安全风险评估工作。

第十三条 第三方评估机构应当履行下列义务:

（一）对评估工作中知悉的国家秘密、重要数据和核心数据的目录与内容、商业秘密、个人隐私，以及与数据处理者签署的保密协议中约定的保密信息等严格保密;

（二）严格按照国家法律法规、行业监管部门有关规定以及评估标准，公正、独立地开展评估并出具评估报告，全面、准确、客观地反映重要数据和核心数据处理者的数据安全风险状况，提供务实有效的风险整改建议措施;

（三）除重要数据和核心数据处理者书面同意或者法律、行政法规另有规定外，不得向其他组织或个人提供评估中收集掌握的相关信息。

第十四条 工业和信息化部根据技术能力、人员配备、信誉资质等情况，择优遴选通过能力认证的第三方评估机构，建立工业和信息化领域数据安全风险评估支撑机构库。

地方行业监管部门可以参照建立本地区数据安全风险评估支撑机构库。

行业监管部门根据工作需要，可以自行或组织数据安全风险评估支撑机构库中的机构，对重要数据和核心数据处理者的数据处理活动开展专项风险评估，或对重要数据和核心数据处理者的风险评估工作落实情况进行监督检查。

重要数据和核心数据处理者对行业监管部门发起的专项风险评估及监督检查应当予以配合，并对评估发现的相关问题及时进行改正。

第十五条 行业监管部门对于违反国家认证认可相关规定的认证机构，将相关线索移交市场监督管理部门处理。

行业监管部门对第三方评估机构的评估活动进行监督管理，对违反法律法规、未按行业规定和标准开展评估活动、未履行保密义务的第三方评估机构，视情按照规定权限和程序进行约谈、通报，认证机构应根据通报信息，对不符合认证要求的第三方评估机构依法暂停直至撤销其相应认证证书。

第十六条 有违反本实施细则行为的，由行业监管部门按照相关法律法规，根据情节严重程度给予行政处罚；构成犯罪的，依法追究刑事责任。

第十七条 行业监管部门及委托支撑机构的工作人员对在履行职责中知悉的国家秘密、商业秘密、个人信息、评估

工作信息等，负有保密义务。

第十八条 对一般数据处理者数据处理活动开展的数据安全风险评估可参照本细则实施。涉及军事、国家秘密信息等数据处理活动，按照国家有关规定执行。

第十九条 本细则自 2024 年 6 月 1 日起施行。