附件2-2

《隐私计算安全可信要求和测试方法》团体标准编制说明

一、工作简况

（一）任务来源

随着数字经济时代的全面来临，数据安全已成为保障国家安全与公民隐私的核心基石。2024 年新颁布的《网络数据安全管理条例》第十条，正是在此背景下对网络数据处理者提出的刚性要求，明确其需在等级保护框架下，综合运用加密、备份、访问控制等技术手段，确保数据免受侵害并承担主体责任。为将法规精神转化为可执行的行业实践，加速我国数据安全技术的创新发展，北京理工大学主动担当，携手济南超级计算技术研究院与重庆市科学技术研究院，于 2025 年率先开启了团体标准的制修订工作。此项合作致力于通过标准化引领，凝聚产业共识，护航数据安全，为构建一个健康、统一、公平的市场环境贡献关键力量。

（二）主要工作过程

2025 年 2 月—3 月，北京理工大学组织召开了标准化工作启动会，明确了《隐私计算安全可信要求和测试方法》标准化对象与标准化需求，成立团体标准编制小组，小组成员对隐私计算系统的可信评估手段进行调研分析，参考相关标准和规范文件，起草了标准草案。

2025 年 4 月，北京理工大学牵头，邀请济南超级计算技术

研究院、重庆市科学技术研究院对标准进行讨论，修改完善形成征求意见稿。

2025 年 5 月—7 月，标准编制小组对标准初稿进行了进一步的修改完善，并提交山东科技咨询协会（以下简称协会）。

2025 年 11 月 6 日，协会标准化建设专业委员会组织召开团体标准立项评审会。会议邀请山东师范大学、山东省计算中心（国家超级计算济南中心）等单位的 3 位专家，对北京理工大学起草的《联邦学习场景的安全可信技术指南》《隐私计算密码融合机制技术指南》两项团体标准进行立项评审。会上，评审专家听取了标准起草组对两项团体标准立项的目的意义、适用范围、主要技术内容等方面的汇报，审阅了立项申请材料，逐项对标准草案及编制说明内容进行质询和研讨，并出具了立项评审意见。评审专家一致认为《联邦学习场景的安全可信技术指南》《隐私计算密码融合机制技术指南》两项团体标准符合立项条件，同意立项。

二、标准编制原则、主要内容及其确定依据

（一）标准编制原则

本标准的编制，严格遵循统一性、协调性、适用性、一致性、规范性五大原则，依据 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》进行起草。旨在保证标准具有规范性；规定明确且无歧义的条款；清楚和准确；能被未参加标准编制的专业人员所理解；标准内容便于实施。

（二）主要内容

本标准主要涵盖范围、规范性引用文件、术语和定义、系统架构与关键要素、技术分类与融合路径、应用场景与解决方案等内容。

（1）范围:

本文件围绕隐私计算系统全生命周期，系统化提出数据采集、处理、训练、推理、监控及跨周期协同的安全与可信要求，并给出相应的测试方法，构成隐私计算安全治理与验证的完整技术框架。

（2）术语和定义:

本文件界定了与隐私计算可信要求和测试相关的核心概念和专业术语，包括多方安全计算、联邦学习、参与方、安全模型等。

（3）概述:

本文件从隐私计算系统全生命周期出发，提出数据采集、处理、训练、推理、监控及跨周期协同的安全与可信要求，并配套给出相应测试方法，为隐私计算产品的研发、评估与合规提供统一技术规范支撑。

（4）安全要求:

本标准围绕隐私计算系统“数据采集—数据处理—模型训练—推理部署—监控评估—跨生命周期安全管理”六大阶段，提出分层分级的安全可信技术要求。针对隐私计算“数据可用不可见”

的协作特性,从数据来源合法性、隐私边界划定与管理、加密与匿名化机制、模型训练与聚合过程安全、推理服务的机密性与可验证性、模型效果与公平性监控以及密钥与数据全生命周期管理等方面进行系统规范。标准在上述六个阶段分别给出一级“基础安全保障”、二级“恶意行为防护”和三级“可证明语义安全”三类要求:一级面向一般性数据协作场景,通过身份认证、通信加密和操作审计等手段,确保各参与方原始数据在计算过程中不被非授权方获取,并满足基本的可追溯性要求;二级面向需防范内部威胁的数据协作场景,基于可证明安全的密码学基础,引入差分隐私、同态加密等技术,确保恶意参与方无法在偏离协议时窃取数据或破坏计算正确性,实现全流程安全可审计与隐私保护效果可量化;三级面向高价值或强监管数据协作场景,要求通过形式化验证方法证明达到可证明的隐私安全理论上限,强调对多方合谋攻击的防御能力、深度防御机制的引入,以及对机器遗忘、密钥生命周期等关键问题的可验证安全保障,从根本上杜绝非约定信息泄露。通过分阶段、分等级的技术要求体系,为不同业务场景和监管强度下的隐私计算系统建设提供可选、安全、可落地的标准化配置路径。

（5）测试方法:

为验证隐私计算系统是否满足上述分阶段、分等级的安全可信要求，本标准构建了覆盖全生命周期的测试与评估方法体系。测试方法按照数据采集、数据处理、计算建模、推理部署、监控

评估以及跨生命周期安全管理六个阶段分别设计具体测试用例，给出测试编号、对应条款、测试项目、前置条件、测试步骤及分级预期结果等要素，形成可直接操作和复现的评估方案。

在数据采集阶段，通过对数字签名算法强度验证、联盟链存证时效性等项目的测试，检验数据来源合法性声明、签名存证及隐私边界管理机制的有效性；在数据处理阶段，通过对隐私集合求交协议正确性、零知识证明验证效率、差分隐私噪声注入效果等测试，评估隐私计算框架中数据预处理、对齐与中间结果生成过程的隐私保护强度与鲁棒性；在计算建模阶段，通过对差分隐私噪声尺度合规性、隐私预算累计消耗追踪准确性、容错恢复后计算结果一致性等测试项目，验证隐私计算任务执行过程中的隐私参数配置、随机数发生器质量以及分布式计算环境下容错与恢复机制的可靠性；在推理部署阶段，通过 TEE 远程证明完整性测试、加密推理端到端延迟测试等，评估隐私计算推理服务的部署环境可信度以及加密推理的实时性保障水平；在监控评估阶段，通过 AUC 群体公平性、DI 指数计算等测试项目，检验隐私计算系统的持续监控体系在公平性与隐私泄露风险预警方面的有效性；在跨生命周期安全管理阶段，通过对密钥轮换周期强制执行、区块链存证不可篡改性等测试，验证密钥与数据全生命周期管理、机器遗忘与审计存证机制的可信度。

各测试方法均针对不同安全等级设置量化预期结果和合格判据，实现从功能性验证到性能与安全边界评估的统一，为标准

条款的落地实施提供可操作、可度量、可对比的评估依据。

（三）确定主要内容的依据

本团体标准主要内容的制定，立足于国家数据要素市场化战略部署、行业智能化转型需求及隐私计算技术融合趋势的综合研判。

本标准严格遵循《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》等法律法规框架，深度贯彻“原始数据不出域、数据可用不可见”的合规要求，旨在构建隐私计算场景下数据安全协同的技术基座，推动数据要素合规流通与价值转化。

当前，在跨机构联合建模、多方数据协作等场景中，存在模型安全可信机制不完善、全流程隐私保护链条断裂等突出问题。本标准针对隐私计算特有的生命周期风险，首次系统化建立覆盖数据采集存证、加密计算、模型训练、推理部署及跨周期协同的全维度安全规范，重点解决分布式环境中数据权属不清、中间结果泄露、恶意节点攻击等核心隐患，为金融风控、医疗研究等高敏感领域提供标准化实施路径。

本标准的技术要求深度融合了密码学前沿进展与产业实践。通过创新性整合同态加密、零知识证明、可信执行环境等技术，构建分层协同的安全防护体系。其核心价值在于确立隐私计算系统全生命周期的安全基线，强化技术落地的可审计性与可控性，为数据要素的安全流通生态提供关键技术标准支撑。

三、试验（或验证）的分析报告、技术经济论证以及预期效益

本团体标准在研制过程中，深度融合了隐私计算安全机制的理论创新与产业实践验证。通过对全生命周期防护框架的多次压力测试与攻防推演，系统评估了其在跨域数据协同、联合分析等高敏场景下的安全性与鲁棒性。验证数据表明，本标准提出的安全控制链能有效防御梯度窃取、恶意节点攻击等典型威胁，为复杂异构环境提供可靠保障。

从技术经济可行性角度审视，本标准构建的安全体系已在实验环境中验证其基础防护效能，初步实现“数据不动模型动”的核心目标。现阶段，部分安全组件（如零知识证明验证效率、恶意模型容错机制）仍需持续优化以应对规模化应用挑战。尽管初期需投入密码模块部署及审计体系建设成本，但随着技术迭代与生态协同的深化，其降低数据泄露损失、释放跨域数据价值的长期效益将显著显现，为金融、医疗等高监管行业提供合规发展动能。

在预期社会效益层面，本标准的实施将加速隐私计算技术安全落地，破解数据权属与隐私保护协同难题。通过统一安全基线，不仅可提升敏感数据全流程防护能力，更将促进隐私计算产业的规范化发展，为构建“可控可溯、安全高效”的数据要素流通生态提供核心支撑。

四、与现行相关法律、法规及相关标准的关系

本标准与现行法律、法规相统一，协调一致，并与现行有效的国家标准和行业标准有很好的协调性，形成协同效应，共同构建完善的数据安全和隐私保护标准体系。

五、采用国际标准和国外先进标准情况，与国际、国外同类标准水平的对比情况，国内外关键指标对比分析或与测试的国外样品、样机的相关数据对比情况

本标准在编制过程中参考或引用相关标准:

GB/T 25069-2022 信息安全技术术语

YD/T 4691-2024 隐私计算联邦学习产品安全要求和测试方法

YD/T 4581-2023 隐私保护场景下安全多方计算技术指南

YD/T AAAA-AAAA 术语和定义

T/CCSA 407-2022 术语和定义

GB/T 46284-2025 术语和定义

YD/T 4987-2024

六、标准中如果涉及专利，应有明确的知识产权说明

本标准中不涉及专利。

七、重大分歧意见的处理过程、处理意见及其依据

本标准的制定过程中未出现重大的分歧意见。

八、实施标准的要求以及相关措施建议

为了使标准得到更好、更有效的实施，应组织相关管理人员、

技术人员和操作人员进行标准宣贯培训，使所有的技术人员和操作人员都能熟练掌握本标准的详细条款和具体要求，并在实际工作中得到认真的贯彻和执行。

标准编写组后续也将及时收集各单位在标准实施中的意见及建议，并在适当的时候对标准进行修订。

九、其他应当说明的事项

无。

《隐私计算安全可信要求和测试方法》团体标准

标准起草组

2025 年 12 月