合同编号：x2026-166

内蒙古自治区大数据中心

项目采购合同

项目名称：信息技术服务九处、数据资源服务处符合性评估项目

项目编号：NMGZCS-G-F-260692

包段名称：符合性评估服务(数据资源服务处)-密码应用安全性评估、网络安全等级保护测评服务项目（采购包3）

签订地点：内蒙古呼和浩特

签订日期：2026 年 10 月 17 日

甲方：内蒙古自治区大数据中心

法定代表人：张树礼

地址：内蒙古自治区呼和浩特赛罕区敕勒川大街 6 号

邮编：010010

联系电话：0471-4827807

乙方：天津联信达软件技术有限公司

法定代表人：王海金

地址：天津市河西区内江路与崇江道交口东南角陈塘科创园(观塘大厦)1 号楼 1802-2 室

邮编：300000

联系电话：022-59565208

甲方通过 公开招标 采购方式确定乙方为 符合性评估服务(数据资源服务处)-密码应用安全性评估、网络安全等级保护测评服务 项目的服务供应商。为了保护甲乙各方合法权益，根据《中华人民共和国民法典》《中华人民共和国政府采购法》《政府采购货物和服务招标投标管理办法》等相关法律法规的规定，并严格遵循 信息技术服务九处、数据资源服务处符合性评估项目 NMGZCS-G-F-260692 招标文件中的相关规定，由采购人（内蒙古自治区大数据中心）与供应商（天津联信达软件技术有限公司）签订本合同，并共同遵守。

一、合同文件

本合同所附下列文件资料为本合同不可分割的部分:

（一）甲方授权发布的项目招标文件;

（二）乙方递交的全套投标文件（视作乙方对甲方明确的、已生效的承诺）;

（三）中标通知书;

（四）采购人、供应商的更正、澄清、说明、补充事项及承诺等。

如上述文件出现不一致的情况，按上述文件顺序解释。

二、项目概况

（一）项目名称：信息技术服务九处、数据资源服务处符合性评估项目采购包 3 符合性评估服务(数据资源服务处)-密码应用安全性评估、网络安全等级保护测评服务项目

（二）项目交付物及提供形式:

提供如下正式版报告:

1.《内蒙古自治区公共信息资源开放平台网络安全等级保护测评问题汇总及整改建议》、《内蒙古自治区公共信息资源开放平台网络安全等级保护测评证书》、《内蒙古自治区公共信息资源开放平台网络安全等级保护测评报告》

2.《内蒙古自治区“一表通”系统商用密码应用安全性评估问题汇总及整改建议》、《内蒙古自治区“一表通”系统商用密码应用安全性评估报告》

3.《内蒙古自治区公共信息资源开放平台商用密码应用安全性评估问题汇总及整改建议》、《内蒙古自治区公共信息资

源开放平台商用密码应用安全性评估报告》

（三）履行期限：2026年10月17日-2027年10月16日

三、服务内容和标准

序号	服务名称	系统名称	标准	备案等级	单价（元）
1	网络安全等级保护测评服务	内蒙古自治区公共信息资源开放平台	测评结论达到符合或基本符合	三级	25340
2	密码应用安全性评估服务	内蒙古自治区“一表通”系统	测评结论达到符合或基本符合	三级	30240
		内蒙古自治区公共信息资源开放平台	测评结论达到符合或基本符合	三级	30240

（一）密码应用安全性评估服务

1.服务内容

(1)服务质量保证:乙方应能根据质量体系要求建立科学的质量保证体系,从人员配备、工具保障以及科学的测评方法论、工作过程等多方面保证项目实施过程的质量。

(2)测评工具配备:要求测评过程使用专用测评设备,并配备国家权威机构认证的测评工具,工具应具有相关采购证明材料。

(3)乙方须按照甲方需求,协助做好被测系统的备案等工作。

(4) 根据甲方要求，以电子版和纸版形式按需求输出成果，并针对甲方的咨询进行及时反馈，方式不限于现场支撑、邮件、电话或报告。主要产出物包括但不限于：《商用密码应用安全性评估问题汇总及整改建议》、《商用密码应用安全性评估报告》。

(5) 对本次测评系统不符合商用密码应用安全有关管理规范和技术标准的，乙方必须出具行之有效的整改方案，并协助甲方进行整改，直至系统通过密码测评。该项目过程中产生的文档，归甲方所有。

(6) 交付时限：乙方应在甲方规定的时间内完成相关工作。

2. 测评要求

从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对信息系统中应用的密码技术进行分析与评估。

(1) 物理和环境层面测评：分析评估信息系统是否合理、合规的利用商用密码完整性、真实性功能，对影响信息系统安全防护效能的物理和环境层面因素进行保护。包括但不限于下列典型因素：场所的物理访问控制，监控设备的物理访问控制，以及物理访问记录、监控信息等敏感信息数据完整性。

(2) 网络和通信层面测评：分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的网络和通信层面因素进行保护。包括但不限于下列典型因素：安全认证连接到内部网络的设备，通信双方的身份认证过程，通信数据完整性，敏感信息数据字段机密性，网络边界访问控制信息完整性，系统资源访问控制信息完整性，安全设备、安全组件的集中管理方式和信息传输通道。

(3) 设备和计算层面测评：分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的设备和计算层面因素进行保护。包括但不限于下列典型因素：登录信息系统设备和计算环境的用户身份鉴别过程，系统设备和计算环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要程序或文件完整性，信息系统设备和计算环境的日志记录完整性。

(4) 应用和数据层面测评：分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性以及不可否认性功能，对影响信息系统安全防护效能的应用和数据层面因素进行保护。包括但不限于下列典型因素：登录信息系统应用和数据操作环境的用户身份鉴别过程，系统应用和数据操作环境资源访问控制信息完整性，重要信息资源敏感标记完整性，重要数据传输过程的机密性、完整性，重要信息存储过程的机密性、完整性，重要程序的加载和卸载过程，信息系统应用相关实体行为不可否认性，信息系统应用和数据操作环境的日志记录完整性。

(5) 密钥管理测评：对影响商用密码防护效能的密钥生命周期相关环节，以及相关环节管理和策略制定的全过程进行分析与评估。密钥生命周期相关环节包括但不限于下列典型环节：密钥生成，密钥存储，密钥分发，密钥导入，密钥导出，密钥使用，密钥备份，密钥恢复，密钥归档，密钥销毁。

(6) 安全管理测评：对影响商用密码防护效能的管理制度与措施进行分析与评估。管理制度与措施包括但不限于下列典型维度：安全管理制度，人员管控，信息系统实施，应急预案。

① 安全管理制度维度，包括但不限于下列内容与措施：密码建设、运维、人员、设备、密钥管理内容，密码相关操作规范、安全操作规范，安全管理制度的合理性和适用性论证与审定，安全管理制度的改进和修订，安全管理制度的发布，安全管理制度的执行。

② 人员管控维度，包括但不限于下列内容与措施：了解并遵守密码相关法律法规密码产品使用，关键岗位划分，相关人员职责与权限划分，岗位责任制与人员制约、监督机制，管理和使用账号，人员培训、人员选拔，人员考核、奖惩与调离，人员保密措施。

③ 信息系统实施维度，包括但不限于下列内容与措施：信息系统规划，信息系统建设方案，信息系统密码产品、服务选用，信息系统运行前与定期评估，信息系统整改。

④ 应急预案维度，包括但不限于下列内容与措施：应急预案，应急资源准备，应急情况与处置，密码主管部门应急报告。

(7) 其他要求：通过现场测评，逐项找出系统现状与国家相关标准要求之间的差距，进行逐项分析、整体分析，发现各信息系统密码应用的薄弱环节和风险点，为密码应用安全提供科学评价，提出完善、可行的整改建议。客观、全面、准确地评价各系统密码应用的合规性、正确性和有效性，度量其与密码应用需求的符合性；找出系统密码应用现状与相应等级密码保护要求之间的差距，并分析其密码应用的薄弱环节及面临的安全风险，提供科学的评估报告。

（二）网络安全等级保护测评服务

1.服务内容

(1)提供定级信息系统的定级、备案变更咨询服务,并协助完成信息系统定级、备案变更工作。

(2)网络安全等级保护测评服务。信息系统网络安全等级保护测评报告已到期,应在测评授权后一个月内出具测评报告;服务期内,如有测评结论和综合得分变化的,应按照最新结论和得分出具新报告。

(3)服务质量保证:乙方应能根据质量体系要求建立科学的质量保证体系,从人员配备、工具保障以及科学的测评方法论、工作过程等多方面保证项目实施过程的质量。

(4)测评工具配备:要求测评过程使用专用测评设备,并配备国家权威机构认证的测评工具,工具应具有相关采购证明材料。

(5)乙方须按照采购方需求,协助做好系统备案,取得自治区公安厅认可的备案证书。

(6)根据甲方要求,以电子版和纸版形式按需求输出成果,并针对甲方的咨询进行及时反馈,方式不限于现场支撑、邮件、电话或报告。主要产出物包括但不限于:《网络安全等级保护测评问题汇总及整改建议》、《网络安全等级保护测评证书》、《网络安全等级保护测评报告》。

(7)对本次测评系统不符合网络安全等级保护有关管理规范和技术标准的,乙方必须出具行之有效的整改方案,并协助甲方进行整改,并完成整改项的再次测评服务。该项目过程中产生的文档,归甲方所有。

(8) 交付时限: 乙方应在甲方规定的时间内完成相关工作。

2. 测评要求

从“定级-备案-等级测评-安全建设整改-配合监督检查”5个环节配合采购单位做好等级保护工作。

(1) 从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等层面,所要求的基本安全控制在信息系统中的实施配置情况;整体测评应主要测评分析信息系统的整体安全性,内容上应包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评。

(2) 安全通信网络: 是针对通信网络提出的安全控制要求。主要对象为广域网、城域网和局域网;涉及的安全控制点包括网络架构、通信传输和可信验证等。

(3) 安全区域边界: 是针对网络边界提出的安全控制要求。主要对象为系统边界和区域边界等;涉及的安全控制点包括边界防护、访问控制、入侵防范、恶意代码防范、安全审计和可信验证等。

(4) 安全计算环境: 是针对边界内部提出的安全控制要求。主要对象为边界内部的所有对象,包括网络设备、安全设备、服务器设备、终端设备、应用系统、数据对象和其他设备等;涉及的安全控制点包括身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份与恢复、剩余信息保护和个人信息保护等。

(5) 安全管理中心: 是针对整个系统提出的安全管理方面的

技术控制要求，通过技术手段实现集中管理；涉及的安全控制点包括系统管理、审计管理、安全管理和集中管控。

(6) 安全管理制度：是针对整个管理制度体系提出的安全控制要求；涉及的安全控制点包括安全策略、管理制度、制定和发布以及评审和修订等。

(7) 安全管理机构：是针对整个管理组织架构提出的安全控制要求；涉及的安全控制点包括岗位设置、人员配备、授权和审批、沟通和合作以及审核和检查等。

(8) 安全管理人员：是针对人员管理模式提出的安全控制要求；涉及的安全控制点包括人员录用、人员离岗、安全意识教育和培训以及外部人员访问管理等。

(9) 安全建设管理：是针对安全建设过程提出的安全控制要求；涉及的安全控制点包括定级和备案、安全方案设计、安全产品采购和使用、自行软件开发、工程实施、测试验收、系统交付、等级测评和服务乙方管理等。

(10) 安全运维管理：是针对安全运维过程提出的安全控制要求；涉及的安全控制点包括环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理和外包运维管理等。

（三）整体服务要求

(1) 应急响应服务要求。针对本次项目，在项目期内，提供7*24 的应急响应服务。

(2) 技术支持服务。针对本次项目，在项目期内，提供 5*8 小

时即时服务响应,包括:电话、邮件、QQ、信函、上门等形式。

(3)咨询服务。针对本次项目,在项目期内,提供咨询服务,包括商用密码应用以及其他相关安全咨询服务。

(4)协助甲方制定商用安全密码相关制度,对甲方开展密码安全等方面的培训。

(5)保密服务要求。投标人应承诺遵守知识产权与安全保密有关规定,并与甲方签署安全保密协议。投标人必须承诺对本项目技术文件以及由甲方提供的所有内部资料、技术文档和信息予以保密;未经甲方书面许可,不得以任何形式向第三方透露本项目标书以及本项目的任何内容。

(6)服务人员要求。

为保证本项目服务质量,项目组人员不少于5人,包含项目负责人、测评师等,应急团队配备负责、指挥、监测、研判、处置、保障等工作人员。

乙方参与本项目的所有工作人员必须通过甲方的审核并签订保密协议。乙方工作人员安全由乙方和工作人员本人负责,甲方不承担相应的安全责任。因用工引起的劳动纠纷等问题由成交乙方负责解决。

如在项目实际执行过程中发生项目负责人不能按采购文件要求胜任相关工作的,甲方有权要求更换项目负责人,乙方需在7日内调整为符合采购文件要求且能胜任相关工作的项目负责人并到位开展工作,否则甲方有权终止合同并报相关管理部门进行处理。

乙方指派固定的团队为本项目提供专业服务,如须调整服

务团队成员，须书面向甲方提出申请，说明申请理由，经甲方书面同意方可调整团队人员，调入人员的资历和从业经验不低于调出人员，否则视为违约行为，甲方有权终止服务合同。

须提供项目团队人员整体构成表，投标文件中所列出的项目团队人员必须与实际参加测试工作保持完全一致，如因特殊原因导致不一致，由投标方提出人员更换申请，经甲方同意后方可更换。

(7)服务交付的成果(或需要交付的材料)

《网络安全等级保护测评问题汇总及整改建议》、《网络安全等级保护测评证书》、《网络安全等级保护测评报告》、《商用密码应用安全性评估问题汇总及整改建议》、《商用密码应用安全性评估报告》。

网络安全等级保护测评报告已到期应在测评授权后 1 个月内出具正式测评报告。

服务期内，等级保护测评和密码测评如有测评结论和综合得分有变化时，应按照最新结论和得分出具新报告。

四、质量要求

（一）技术服务质量标准:

密码应用安全性评估依据包括但不限于以下：《中华人民共和国密码法》；《商用密码管理条例》；《商用密码应用安全性评估管理办法》;《信息安全技术信息系统密码应用基本要求》(GB/T 39786-2021)；《信息安全技术信息系统密码应用测评要求》(GB/T 43206-2023)；《信息系统密码应用测评过程指南》(GM/T 0116-2021)。

网络安全等级保护测评依据包括但不限于以下：《中华人民共和国网络安全法》、《中华人民共和国密码法》、《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》、《关键信息基础设施安全保护条例》、《网络安全等级保护管理办法》、《网络安全等级保护条例》；《计算机信息系统安全保护等级划分准则》（GB17859-1999）；《信息安全技术网络安全等级保护实施指南》（GB/T25058-2020）；《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）；《信息安全技术网络安全等级保护安全设计技术要求》（GB/T25070-2019）；《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）；《信息安全技术网络安全等级保护定级指南》（GB/T22240-2020）；《信息安全技术网络安全等级保护测试评估技术指南》（GB/T36627-2018）；《信息安全技术网络安全等级保护安全管理中心技术要求》（GB/T36958-2018）。

（二）技术服务质量期限要求:

公共信息资源开放平台网络安全等级保护测评报告已到期，应在测评授权后 1 个月内出具正式网络安全等级保护测评报告，测评结论达到符合或基本符合。 在合同约定时间内完成内蒙古自治区“一表通”系统、公共信息资源开放平台密码应用安全性评估，出具合规密评报告，评估结论达到符合或基本符合，满足密码管理部门监管核查要求。服务期内，网络安全等级保护测评和密码应用安全性评估如有测评结论和综合得分有变

化时，应按照最新结论和得分出具新报告。

五、合同金额及支付方式

（一）合同金额：根据中标（成交）通知书，本项目合同金额为：¥85820（大写：人民币捌万伍仟捌佰贰拾元整（元整）。

（二）分期付款：

本合同款项共分 2 期支付。

第一期：合同签订后，乙方完成人员备案，甲方收到等额发票后 20 日内，甲方向乙方支付合同总金额的 30 %，即人民币 25746 元，大写 贰万伍仟柒佰肆拾陆元整 。

第二期：项目执行完成后经甲方验收合格后，甲方收到等额发票后 20 日内，甲方向乙方支付合同总金额的 70 %，即人民币 60074 元，大写 陆万零柒拾肆元整 。如项目因合同解除、终止、政策调整、项目合并等原因提前终止服务，按已完成项目的工作量结算。

（三）乙方收款信息

户　　名： 天津联信达软件技术有限公司

开户银行： 中国银行股份有限公司天津荣业大街支行

账　　号： 2778 6005 2631

（四）甲方开票信息

户　　名： 内蒙古自治区大数据中心

开户银行： 中国建设银行股份有限公司呼和浩特锡林南路电力支行

账　　号： 15050170667800000176

（五）甲方向乙方履行付款义务前，乙方应当向甲方开具

相应金额的普通发票，发票信息应与合同约定的账户信息一致，甲方凭票付款。若因乙方开票原因导致迟延付款，甲方对此不负责任。

（六）甲方向合同约定的账户汇入资金即为甲方履行了本合同约定的付款义务。乙方账户信息发生变更的，应在甲方付款前至少5日内以书面方式（签章）通知甲方，并说明更改收款账户信息的合理原因。乙方书面通知到达甲方前，甲方已向上述账户付款的，视为甲方已履行本合同约定的付款义务，由此造成的损失由乙方承担。

六、保密责任

（一）乙方对在合作过程中知悉的甲方的业务数据、业务实务及相关信息及文档等具有商业价值的一切内容负有保密义务，应尽合理的注意义务为甲方的前述秘密信息采取保密措施，仅可在乙方从事该业务的负责人和工作人员范围内知悉，不得以任何方式向任何第三方泄露，并不得自行使用在与本合同项目无关的地方。

（二）本合同履行期间以及终止后，乙方应按照甲方要求，将从甲方收到的含有上述项目信息的所有文件或资料归还给甲方，或者以甲方认可的方式予以销毁，不得私自留存。

（三）保密期限：在本合同有效期内以及在履行完毕后，甲乙双方均不得将合同及项目相关的所有技术资料、技术秘密、业务数据等资料在成为公共信息之前披露给任何第三方。

七、甲方的权利义务

（一）为乙方开展工作提供便利，承担对甲方各部门的协

调工作；向乙方提供与服务事项相关的资料，并保证其真实、有效。

（二）按照采购文件、响应文件的内容要求对乙方的服务质量及行为进行监督和检查，提出意见建议。对乙方技术人员的工作态度、完成情况进行监督、签收，提出意见，以提高服务质量。

（三）甲方应按时支付合同款。

八、乙方的权利义务

（一）乙方应按照招标文件、响应文件的要求及本合同的约定，按期、保质保量地完成项目成果。

（二）必须遵守职业道德和执业纪律。

（三）未经甲方书面同意，乙方不得将本合同项目的全部或部分工作转委托给第三方承担。

乙方项目小组成员信息：

组长：周[redacted]联系方式：136[redacted]。

成员：栗[redacted]联系方式：182.[redacted]。

成员：赵[redacted]联系方式：137[redacted]。

成员：郭[redacted]联系方式：182[redacted]。

成员：刘[redacted]联系方式：176[redacted]。

九、验收方法及标准

完成内蒙古自治区“一表通”系统、公共信息资源开放平台密码应用安全性评估，出具合规密评报告，评估结论达到符合或基本符合，满足密码管理部门监管核查要求。

完成公共信息资源开放平台三级网络络安全等级保护测

评，出具合规测评报告，测评结论达到符合或基本符合。

经验收，达不到质量和技术要求的，甲方可以拒收，并解除合同且不承担任何法律责任。

十、违约责任

（一）甲乙双方应正当行使权利、合理履行义务，保证本合同的正确履行。双方无法定或约定理由单方解除本合同的，需向对方支付合同金额 10 %的违约金。造成对方损失且违约金不足以弥补对方损失的，违约方还应进行相应赔偿。

（二）乙方应按照合同约定的期限向甲方交付本项目成果，若因乙方原因导致未按照约定时间完成本项目，每逾期 1 日，乙方应向甲方支付本合同总金额 1 %的违约金；逾期天数超过 30 日，甲方有权单方解除合同，乙方应赔偿由此给甲方造成的所有损失。

（三）乙方交付的项目成果不符合国家规定标准或采购文件要求及本合同约定的，甲方有权拒收成果并要求乙方限期整改完善，乙方应按照甲方要求及时交付符合质量要求的项目成果。由此而发生的一切费用由乙方承担，并且应赔偿由此给甲方造成的所有损失。

（四）乙方以任何形式擅自将项目部分或全部转包给第三方实施的，乙方构成单方违约，应向甲方承担合同金额 5% 的违约金。造成甲方损失且违约金不足以弥补损失的，还应进行相应赔偿。

（五）乙方如将甲方商业秘密泄露给第三人或使用商业秘密使甲方遭受损失的，乙方应对甲方进行赔偿，其赔偿数额不

少于由于其违反义务所给甲方带来的损失。

十一、项目联系人

双方确认：在本合同有效期内，甲方指定 何[redacted] 为甲方的项目联系人（联系方式：139[redacted]）。乙方指定 多[redacted] 为乙方的项目联系人（联系方式：135[redacted]）。

在本合同履行过程中，若甲方或乙方要求变更联系人，应书面通知对方。

十二、解决合同纠纷的方式

因履行本合同发生纠纷，双方应协商解决。协商不成可以采用下列第 （二） 种方式解决：

（一）提交呼和浩特仲裁委员会仲裁；

（二）向甲方住所地有管辖权的人民法院提起诉讼。

十三、不可抗力

（一）如果发生不可抗力事件（地震、台风、水灾、火灾、战争、国际或国内运输中断、流行病、罢工，以及根据中国法律或一般国际商业惯例认作不可抗力的其他事件），影响一方履行其在本合同项下的义务，则在不可抗力造成的延误期内中止履行，而不视为违约。

（二）发生不可抗力的一方应迅速书面通知另一方，并在其后的十五天内提供证明不可抗力发生及其持续时间的足够证据。

（三）如果发生不可抗力事件，双方应立即互相协商，以找到公平的解决办法，并且应尽一切合理努力将不可抗力的影响减少到最低限度。如不可抗力的发生或后果对一方造成重大

妨碍，时间超过六个月，并且各方没有找到公平的解决办法，则任何一方可开始终止本合同的程序。

十四、通知与送达

（一）双方约定在合作过程中重要的来往文件包括：双方盖章的书面文件、双方以电子邮件形式确认的文件均可作为合作执行的依据。一方向另一方发出的通知、函件，以电子邮件形式发送的，自电子邮件进入收件方指定之电子邮件系统的时间即视为已送达；以快递形式发送的，以对方签收之日视为对方收到该通知。

（二）如任一方所列的联系人或联系方式发生变更的，变更方应当在发生变更前 3 个工作日向另一方发出书面通知。否则，其送达地址仍以先前的通讯地址或邮箱地址为准。

（三）双方可通过以下任一方式变更己方联系人或联系方式：

1. 变更方以书面通知（应签章）的方式告知对方的；

2. 变更方以指定之电子邮箱发出变更联系人或联系方式的电子邮件进入对方指定之电子邮件系统告知的。

十五、其它条款

未尽事宜可由双方协商一致签订补充合同，与本合同具有同等效力。二者有不一致的地方，以补充合同为准。

十六、合同生效

本合同经双方法定代表人或授权代表签字盖章后生效，本合同一式陆份，甲乙双方各执叁份，具有同等法律效力。

----------（以下无正文）----------

甲方：

法定代表人或授权代表：

经办人：

签订日期：2026.10.17

乙方：

法定代表人或授权代表：

签订日期：2026.10.17

保 密 协 议

甲方： 内蒙古自治区大数据中心

法定代表人： 张树礼

住所地： 呼和浩特市赛罕区敕勒川大街 6 号

乙方： 天津联信达软件技术有限公司

法定代表人： 王海金

住所地： 天津市河西区内江路与崇江道交口东南角陈塘科创园(观塘大厦)1 号楼 1802-2 室

甲方与乙方因 信息技术服务九处、数据资源服务处符合性评估项目符合性评估服务第三包 建立合作关系，于 2026 年 10 月 签订了 信息技术服务九处、数据资源服务处符合性评估项目 符合性评估服务(数据资源服务处)-密码应用安全性评估、网络安全等级保护测评服务项目（采购包 3）。为履行合同义务，一方需向另一方披露本协议定义的保密信息，为保证保密信息不被未经授权地披露、使用，经友好协商，双方约定如下条款:

第一条：词汇定义

（一）保密信息： 本协议所指保密信息是指为本协议一方已合法拥有的或在合作过程中产生的，未在公共范围内知悉的所有项目相关信息，包括但不限于文件、资料、数据、技术需求、改善需求或技术信息、商业信

息等。但以下信息不属于保密信息：

1. 披露方已经合法向公众公开的信息；

2. 已由披露方事先未附加任何条件书面同意公开的信息；

3. 在未使用本协议约定的保密信息的全部或任何部分的情形下，接受方单独所掌握的信息；

4. 接受方从第三方合法、正当地取得，且该第三方就该等保密信息对该披露方不承担保密义务的信息；

5. 非因违反本协议约定的行为导致已经公开的保密信息，但因第三方违反对该披露方的相关保密义务导致公开的除外。

（二）知识产权：指对发明专利、实用新型、外观设计、著作、商标及集成电路布图、软件、核心技术、资料、数据及其他受法律保护的所有知识创造物所拥有的权利。

（三）披露方：本协议的“披露方”是指披露、透漏保密信息的一方，本协议中的任何一方都可能是披露方。

（四）接受方：本协议的“接受方”是指接收保密信息的一方。本协议中的任何一方都可能是接受方。

第二条：知识产权

（一）披露方向接受方披露本协议所列信息不构成披露方授予接受方享有披露方对其商标、专利或保密信息拥有的权益，也不构成向接受方转让或授予第三方许可给披露方的商标、专利或保密信息等有关权益。接受方获悉披露方保密信息时，不得被认为或被解释为取得披露方对保密信息所享有的权利。

（二）双方各自持有的知识产权由各方所有，不因本协议的签订而以任何形态（包括明示，暗示或自然形态）导致知识产权的转让或使用许可。

双方在欲对知识产权的所有权或使用权进行转让或许可时，需另行签订协议来约定相关知识产权事项。

（三）接受方不得以披露方提供的产品、服务、商业方法等相关信息或保密信息及其变型为基础申请或登记有关知识产权。违反本条规定的，接受方应立即、无条件地将申请或登记的有关知识产权归还给披露方；披露方自该权利产生或登记之日起具有独自使用权以及独立向第三方授予使用许可的权利。本条款在本协议的效力中止或终止后仍有效。

（四）如果本协议所述合作项目是关于接受方基于披露方所提出的技术需求完成相应技术成果，则无论所述技术成果是由接受方单独做出的或者由披露方与接受方双方共同做出的，技术成果及其相应知识产权均归披露方所有；接受方不得独自申请或登记有关知识产权；违反本条规定的，接受方应立即、无条件地将申请或登记的有关知识产权归还给披露方；披露方自该权利产生或登记之日起具有独自使用权以及独立向第三方授予使用许可的权利；本条款在本协议的效力中止或终止后仍有效，接受方无权就此向披露方主张任何权利。

（五）除前述所约定的各种情形外，对于披露方与接受方共同作出的技术成果，双方需另行协商知识产权归属，任何一方不得在双方达成一致意见之前独自申请或登记有关知识产权；如一方违反本条款规定，则上述所申请或登记的有关知识产权的所有权由另一方单独拥有，另一方自该权利产生或登记之日起具有独自使用权以及独立向第三方授予使用许可的权利；本条款在本协议的效力中止或终止后仍有效。

第三条：保密义务

（一）保密信息归披露方所有。接受方对保密信息只有为实现合作项目的目的而进行使用的权利，绝不为与该项目无关的目的使用保密信息，

且没有所有权、知识产权和其他权益。不得通过任何途径获取与本职工作或本项目无关的任何信息。

（二）接受方应严格保管保密信息。接受方承诺采取与接受方对自己的保密信息所采取的措施相当的措施以保证保密信息不被泄露，此种措施至少应该是合乎常理的。项目实施及服务过程中所涉及的载体不得私自转让，须确保所存储信息的安全。

（三）未经披露方的事先书面批准，接受方不得直接或间接以任何形式或任何方式把保密信息和/或其中的任何部分，披露、透露给任何第三方或者公开。接受方亦不得依据披露方提供的任何保密信息，就任何问题，向任何第三方作出任何建议。

（四）接受方仅能向有知悉必要的接受方人员（包括但不限于雇员或顾问）披露保密信息。一经发现对保密信息的任何未经授权的披露或接受方及其人员违反本协议时，接受方应立即书面通知披露方，并采取措施防止进一步未经授权而使用保密信息或进一步泄露保密信息。

（五）接受方应与其根据合作项目需要而接触、知悉或了解保密信息的人员签订相应的书面保密协议，保证其遵守本协议的规定，接受方人员向第三方披露保密信息，或依据该等保密信息向第三方作出任何建议，都被视为接受方违反本协议。该等人员无论因何种原因离职，离职后仍对其在任职期间接触、知悉的属于披露方且承诺有保密义务的技术秘密和其它商业秘密信息，承担如同任职期间同样的保密义务，不得以任何形式使用或向任何其他方传播、泄露甲方单位的有关秘密信息。

（六）接受方应促使接触到保密信息的关联公司履行本协议约定义务，接受方关联公司违反本协议的行为，均视为接受方的违约行为。

（七）如接受方因实现合作项目的目的需要而将保密信息披露给其合

作公司时，接受方应事先获得披露方的书面批准；接受方应促使接触到保密信息的合作公司履行本协议约定义务，接受方的合作公司违反本协议的行为，均视为接受方的违约行为。

（八）接受方不得对任何由披露方根据本协议提供的任何软件或硬件进行反编译、反汇编及逆向工程，但法律另有规定的除外。

（九）接受方应确保其制作的保密信息的全部副本或摘录，应载有表示披露方所有权和/或保密性的指示。

（十）如果接受方得知第三方获得任何保密信息，则应及时书面通知披露方，并向披露方提供掌握的所有相关情况。

（十一）接受方在本协议签订及履行过程中、项目的商谈及合作过程中所接触到的披露方关联公司的保密信息，接受方应依据本协议约定履行保密义务、承担责任。

（十二）如果接受方应法律、行政法规要求披露信息（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序披露保密信息），应至少于实际披露行为前__7__日书面通知披露方，说明其拟根据规定披露有关的保密信息，并就披露对象和披露范围、方式等作出说明。

第四条：保密信息的归还

在披露方要求时，接受方应在__7__日内返还保密信息的所有原件、复印件、复制品、摘录及所有其他载有保密信息的载体，或依披露方的要求，销毁上述保密资料，并提供相关有效证明。

第五条：保密期限

自披露方第一次向接受方披露任何保密信息之日后起直至该保密信息合法公开时止接受方不得向任何第三方披露该保密信息。

第六条：违约责任

（一）接受方未履行或未完全履行本协议项下的条款均构成违约，接受方应赔偿因此给披露方造成的一切损失；披露方的损失难以计算的，赔偿额为接受方因违约行为所获得的利润；并应当承担披露方因调查接受方的违约行为而支付的合理费用。

（二）如果披露方确认，对接受方违反本协议的行为仅采取赔偿的补救措施是不够的，则披露方还有权根据国家有关法律、法规采取其他合理的救济措施。

第七条：陈述和保证

双方陈述和保证，本协议的执行及其履行本协议项下的义务将不会：

（1）违反营业执照、章程或类似组织文件的任何规定；

（2）违反其在任何合同或协议项下所承担的责任和义务；

（3）违反法律、行政法规的相关规定。

第八条：管辖法律和争议解决

1、本协议适用中华人民共和国法律并依其解释。

2、本协议执行过程中产生的或与本合同本身有关的任何争议，包括任何与违约、协议终止、协议无效等有关的争议、纠纷及索赔等，双方应通过友好协商进行解决。协商无法解决的，则任何一方均可向甲方所在地有管辖权的人民法院起诉。

第九条：其他

（一）本协议自双方法定代表人或授权代表签字并加盖公章或合同专用章之日起生效。在本协议签署前，披露方已经向接受方提供或披露的本协议范围内的保密信息也受本协议约束，此时本协议于该等保密信息提供或披露时发生效力。

（二）本协议一式 陆 份，双方各执 叁 份，具有同等法律效力。

（三）本协议未尽事宜，双方另行协商解决。

----------（以下无正文）----------

甲方：

[盖章]

签署：

乙方：

[盖章]

签署：

签订日期：2026.10.17

签订地：呼和浩特市

