

协议编号：

重庆市产业大脑应用开发软测、密评与等保服务 委托协议书

项 目 名 称 ： 重庆市产业大脑应用开发软测、密评与等保服务项目

被 服 务 单 位 ： 重庆市经济和信息化委员会

委托单位(甲方)： 重庆巽诺科技有限公司

受托单位(乙方)： 重庆巽诺科技有限公司

签 订 地 点 ： 重庆市

签 订 日 期 ： 2025 年 12 月 22 日

依据《中华人民共和国民法典》的规定，乙方受甲方委托，就重庆市产业大脑应用开发软测、密评与等保服务工作协商一致，特签订本协议。

一、服务内容

1.1 服务范围：甲方委托乙方严格按照国家相关标准要求，提供定级备案咨询、网络安全等级保护测评、商用密码应用安全性评估、软件测试服务。

测评服务：

网络安全服务：

序号	被服务单位名称	被服务系统名称	安全保护等级	服务内容	服务频次	服务成果
1	重庆市经济和信息化委员会	重庆市产业大脑应用	三级	网络安全等级保护等级测评	1次/年	《网络安全等级保护等级测评报告》
2			三级	商用密码应用安全性评估	1次/年	《商用密码应用安全性评估报告》
4			-	软件测试	1次	《系统检测报告》
备注：本次测评的被服务单位名称、被服务系统名称及安全保护等级最终以属地公安机关颁发的《信息系统安全等级保护备案证明》为准。						

1.2 依据：乙方依据国家安全相关法律法规政策文件、相关标准规范以及指导文件开展工作。

依据法规政策文件包括但不限于：

- 《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》
- 《关键信息基础设施安全保护条例》
- 《网络安全审查办法》
- 《中华人民共和国计算机信息系统安全保护条例(国务院 147 号令)》
- 《信息安全等级保护管理办法（公通字[2007]43 号）》
- 《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见（公网安[2020]1960 号）》

- 《中华人民共和国密码法》
- 《中华人民共和国电子签名法》
- 《商用密码管理条例》
- 《商用密码应用安全性评估管理办法》
- 《“十四五”软件和信息技术服务业发展规划的通知（工信部规〔2021〕180 号）》

依据标准规范和指导文件包括但不限于：

- GB 17859-1999 《计算机信息系统 安全保护等级划分准则》
- GB/T 22240-2020 《信息安全技术 网络安全等级保护定级指南》
- GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》
- GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》
- GB/T 28449-2018 《信息安全技术 网络安全等级保护测评过程指南》
- GB/T 20984-2022 《信息安全技术 信息安全风险评估方法》
- GB/T 31509-2015 《信息安全技术 信息安全风险评估实施指南》
- GB/T 39204-2022 《信息安全技术 关键信息基础设施安全保护要求》
- ISEAA 001-2020 《网络安全等级保护测评高风险判定指引》
- GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
- GM/T 0116-2021 《信息系统密码应用测评过程指南》
- 《信息系统密码应用高风险判定指引（2021）》
- 《商用密码应用安全性评估量化评估规则（2023）》
- 《商用密码应用安全性评估 FAQ（第三版）》
- 《商用密码应用安全性评估测评实施指引》

● GB/T 25000.51-2016《系统与软件工程系统与软件质量要求和评价 (SQuaRE) 第 51 部分：就绪可用软件产品 (RUSP) 的质量要求和测试细则》

二、具体服务内容及要求

(一) 软件测评服务内容及要求

1. 服务内容

乙方应对“重庆市产业大脑应用开发项目”的软件系统实施第三方软件评测，验证其软件的功能、性能等指标是否符合相应技术规范要求，包括功能性、性能效率、安全性并出具第三方软件测试报告。测试方式覆盖黑盒测试、白盒测试等，测试流程包括伴随测试、模块测试、专项测试等。测试报告包括测试项目的详细信息、需求指标的符合性结论、验收测试的总体结论，测试报告应加盖乙方检验检测专用章、CMA 或 CNAS 签章。

2. 服务要求

2.1 技术标准

2.1.1 乙方的服务应符合 GB/T 25000.51-2016《系统与软件工程系统与软件质量要求和评价 (SQuaRE) 第 51 部分：就绪可用软件产品 (RUSP) 的质量要求和测试细则》的标准。

2.1.2 测试原则

(1) 客观性和公正性原则：乙方应按照评估双方相互认可的评估方案，基于明确定义的评估方式和解释，实施评估活动。

(2) 可再现性原则：不论谁执行评估，依照同样的要求，使用同样的评估方式，乙方应对每个评估实施过程的重复执行应该得到同样的结果。

(3) 结果完善性原则：乙方的测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应确保其满足了测评方案的要求。

2.1.3 测评内容

乙方提供的测评内容包括功能性、性能效率、安全性测试，并出具第三方软件测试报告。

(1) 功能性测试

1) 软件产品满足明确和隐含要求功能的能力。具体内容包括：功能完备性、功能正确性、功能适合性、功能性的依从性。功能测试的目的是在系统集成之后，通过设计测试用例、执行用例、获取结果，保证系统功能符合用户的业务需求；

2) 分析被测信息系统功能需求, 依据《软件需求规格说明书》《系统详细设计文档》等和软件产品质量要求验证系统实现了全部需求和设计, 测试覆盖所有功能点, 确保各项功能是可正确执行的;

3) 根据系统《软件需求规格说明书》和《系统详细设计文档》等文件, 分析各功能点测试的优先级别。用户经常使用、关系到系统核心功能、优先级别较高的功能点应予以重点关注, 尤其在回归测试时应优先执行。

(2) 性能效率测试

1) 软件产品所提供性能的能力。关注在多用户、大并发量的情况下系统是否满足客户的实际需要, 主要从吞吐量、点击率、平均事物响应时间、负载下的平均事物响应时间等来进行测试。

2) 使用性能测试工具, 对系统进行压力负载、疲劳强度、大数据量等测试, 验证系统的性能是否满足用户的业务需求。

3) 各信息系统的数据存储能力、存储周期、并发访问量、性能指标根据《软件需求规格说明书》和《系统详细设计文档》确定。

4) 时间特性和资源利用特性

5) 分析系统用户行为, 依据性能需求验证分级部署的信息系统支持高并发处理业务的能力;

6) 系统的关键业务, 诸如数据采集、数据同步、数据统计等, 具备快速响应能力;

7) 系统数据容量在设计值范围内, 响应时间满足用户性能需求;

8) 系统资源利用在合理的数值范围, 不超过资源指标的预警值;

9) 测试在大用户量、大并发量、大数据量和长时间连续运行等条件下, 系统的响应时间和稳定运行情况。

(3) 信息安全性测试

按照项目信息安全性测评要求, 测评对象和方式包括: 应用安全测试。具体内容包括: 身份鉴别、访问控制、日志审计、数据完整性、数据保密性等。

2.1.4 保密要求

在开展系统测评工作的过程中, 乙方及实施人员须严格遵守法律法规, 对相关敏感、系统风险信息、项目实施内容及成果信息进行严格保密。未经同意, 严

禁将上述内容与任何第三方透露或用于其他商业用途,并承担由此产生的一切损失(提供承诺函,格式自拟,加盖乙方公章)。

2.1.5 实施要求

(1) 乙方应根据项目实际情况制定项目实施计划,严格按照项目实施计划推动项目实施,确保项目进度。

(2) 为保障测评工作的顺利推进,乙方应指定一名专职服务人员,通过现场或远程支撑的方式为测评过程中的技术问题(包括但不限于需整改的问题)提供技术支撑服务。

(3) 乙方应加强本项目资料的保密管控,必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施,记录资料由生成到销毁整个生命周期内的使用日志,并根据实际工作情况及时对制度进行调整。乙方应加强本项目在用户工作场所使用设备,特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备,必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

(4) 乙方应组织应急技术支撑队伍,在服务期限内加强与业主单位的联防、联动,积极配合处理网络安全事件,提升业主单位应对网络安全事件的应急处理能力。

(二) 网络安全等级保护测评服务内容及要求

1. 项目背景

1.1 服务目标

为了提升信息系统的安全保护能力、加强信息安全管理,根据《中华人民共和国网络安全法》《信息安全等级保护管理办法》《GB/T 22239-2019 网络安全技术信息系统安全等级保护基本要求》等法规和标准的要求,对“重庆市产业大脑应用开发项目”的信息系统开展网络安全等级保护测评工作。

乙方通过测评,准确反映待测信息系统的安全防护能力现状,分析排查所涉及信息系统的信息安全隐患,提出安全整改建议;同时提升系统安全防护能力,优化、加强系统信息安全管理,确保本单位网络安全建设工作满足国家法律法规、标准规范的要求,信息系统达到相应安全等级的防护水平。

1.2 项目依据

乙方应依据国家《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)、《信息安全等级保护管理办法》(公通字〔2007〕43 号)、《中华人民共和国国家标准 GB/T 22239-2019 信息安全技术信息系统安全等级保护基本要求》《中华人民共和国国家标准信息安全技术信息系统安全等级保护测评要求》《中华人民共和国国家标准信息安全技术信息系统安全等级保护测评过程指南》《中华人民共和国国家标准 GB/T 20984-2022 信息安全风险评估规范》等法规要求进行网络安全等级保护测评。

2. 采购服务内容

乙方需要测评的系统包括被测系统运行密不可分的物理环境、网络环境、主机及相关系统、安全管理制度等。在充分了解被测系统的情况下,结合系统构成特点,确定具体的测评对象。建立测评方案和测评指导书,通过访谈、检查和工具测试等方式判断该系统安全管理和安全技术的各个方面相对于测评指标的符合程度,形成整改建议并协助整改,最终并出具正式的等级测评报告。

2.1 本次测评的信息系统等保定级情况如下:

“重庆市产业大脑应用”的信息系统为等级保护 3 级。

2.2 测评指标项:

测评范围主要包括: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、安全运维管理等方面,并根据系统实际情况选择相应的扩展测评内容。

2.2.1 技术测评:

2.2.1.1 安全物理环境测评(物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护);

2.2.1.2 安全通信网络测评(网络架构、通信传输、可信验证);

2.2.1.3 安全区域边界测评(边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证);

2.2.1.4 安全计算环境测评(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、数据备份恢复、剩余信息保护、个人信息保护);

2.2.1.5 安全管理中心测评(系统管理、审计管理、安全管理、集中管控)。

2.2.2 管理测评:

2.2.2.1 安全管理制度测评（安全策略、管理制度、制定和发布、评审和修订）；

2.2.2.2 安全管理机构测评（岗位设置、人员配备、授权和审批、沟通和合作、审核和检查）；

2.2.2.3 安全管理人员测评（人员录用、人员离岗、安全意识教育和培训、外部人员访问管理）；

2.2.2.4 安全建设管理测评（定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统支付、等级测评、服务乙方选择）；

2.2.2.5 安全运维管理测评（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、外包运维管理）。

3. 数据安全协查

乙方应根据《关于进一步做好网络和数据安全保护工作的通知》（渝等保办〔2025〕1号）有关要求，协助开展数据安全监督检查评估的有关工作，提供数据安全相关咨询服务，以满足数据安全合规工作的开展，以及落实国家数据安全协调机制相关工作要求和数据安全保护义务。在接到甲方的协助需求时，安排项目组成员到指定位置驻场服务。

4. 项目成果要求

乙方应形成针对待测评系统的网络安全等级保护测评报告，主要包括系统测评记录、安全扫描及渗透测试报告、系统风险分析、系统等级测评报告等（可合并输出）。

5. 实施要求

（1）乙方应根据项目实际情况制定项目实施计划，严格按照项目实施计划推动项目实施，确保项目进度。

（2）为保障测评工作的顺利推进，乙方应指定一名专职服务人员，通过现场或远程支撑的方式为测评过程中的技术问题（包括但不限于需整改的问题）提供技术支撑服务。

(3) 乙方应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。乙方应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

(4) 乙方应组织应急技术支撑队伍，在服务期限内加强与业主单位的联防、联动，积极配合处理网络安全事件，提升业主单位应对网络安全事件的应急处理能力。

(三) 密码应用安全性评估服务内容及要求

1. 项目需求

乙方应依据 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》《信息系统密码测评要求》《商用密码应用安全性评估测评过程指南》《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》和信息系统自身的安全需求分析，对本单位信息系统“重庆市产业大脑应用”进行商用密码应用安全性评估，为重要网络和信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为，推动提升被测系统密码应用水平。在项目实施过程中，投标方应做好计划与安排，确保项目实施不影响系统的正常运行，测评中应严格按照《GM/T 0116-2021 信息系统密码应用测评过程指南》标准的要求实施，加强质量监督和评审，确保测评工作质量。

2. 采购服务内容

2.1 测评指标项

乙方提供的商用密码应用安全性评估应参照《中华人民共和国密码法》《中华人民共和国网络安全法》《信息安全技术信息系统密码应用基本要求》(GB/T39786-2021)、《信息系统密码测评要求(试行)》《商用密码应用安全性评估测评过程指南(试行)》等国家行业现行有效的标准、规范，测评指标和对象选择须符合《GB/T 43206-2023 信息安全技术 信息系统密码应用测评要求》标准的相关要求。

按照商用密码应用安全性分类分级评估的要求，依据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）要求及信息系统等级保护定级情况，测评至少应该包括以下内容：系统通用要求、物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等，具体要求如下表所示：

2.1.1 通用要求：

通用要求	密码算法	密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求
	密码技术	密码技术应遵循密码相关国家标准和行业标准
	密码产品	密码产品、密码服务应符合法律法规的相关要求

2.1.2 技术要求：

技术要求	物理和环境安全	身份鉴别
		电子门禁记录数据存储完整性
		视频监控记录数据存储完整性
		密码服务
		密码产品
	网络和通信安全	身份鉴别
		通信数据完整性
		通信过程中重要数据的机密性
		网络边界访问控制信息的完整性
		安全接入认证
		密码服务
		密码产品
	设备和计算安全	身份鉴别
		远程管理通道安全
		系统资源访问控制信息完整性
		重要信息资源安全标记完整性
		日志记录完整性
		重要可执行程序完整性、重要可执行程序来源真实性
		密码服务
		密码产品
	应用和数据安全	身份鉴别
		访问控制信息完整性
		重要信息资源安全标记完整性
		重要数据传输机密性
		重要数据存储机密性
		重要数据传输完整性
		重要数据存储完整性
		不可否认性

		密码服务
		密码产品

2.1.3 管理要求：

技术要求	管理制度	具备密码应用安全管理制度
		密钥管理规则
		建立操作规程
		定期修订安全管理制度
		明确管理制度发布流程
		制度执行过程记录留存
	人员管理	了解并遵守密码相关法律法规和密码管理制度
		建立密码应用岗位责任制度
		建立上岗人员培训制度
		定期进行安全岗位人员考核
		建立关键岗位人员保密制度和调离制度
	建设运行	制定密码应用方案
		制定密钥安全管理策略
		制定实施方案
		投入运行前进行密码应用安全性评估
		定期开展密码应用安全性评估及攻防对抗演习
	应急处置	应急策略
		事件处置
		向有关主管部门上报处置情况

2.2 测评内容

在系统真实环境下，乙方应采用访谈、查看配置、工具测评等方式评估信息系统密码应用及保障是否安全有效，密码使用和管理是否满足合规性、正确性、有效性。并且通过测评来发现信息系统存在的密码应用安全性隐患和风险，提出可行性整改建议。

乙方需协助甲方找出信息系统密码安全与国家相关政策标准要求的差距，有针对性的出具《差距分析报告及整改建议》，供甲方后续密码安全规划、建设、整改提供参考依据。

3. 数据安全协查

乙方应根据《关于进一步做好网络和数据安全保护工作的通知》（渝等保办〔2025〕1号）有关要求，协助开展数据安全监督检查评估的有关工作，提供数据安全相关咨询服务，以满足数据安全合规工作的开展，以及落实国家数据安全协调机制相关工作要求和数据安全保护义务。在接到甲方的协助需求时，安排项目组成员到指定位置驻场服务。

4. 项目成果要求

乙方需要按照国家密码管理局要求的报告模板，出具《商用密码应用安全性评估报告》及《差距分析报告及整改建议》。

5. 实施要求

(1) 乙方应根据项目实际情况制定项目实施计划，严格按照项目实施计划推动项目实施，确保项目进度。

(2) 为保障测评工作的顺利推进，乙方应指定一名专职服务人员，通过现场或远程支撑的方式为测评过程中的技术问题（包括但不限于需整改的问题）提供技术支撑服务。

(3) 乙方应加强本项目资料的保密管控，必须针对本项目建立项目纸质、声音、影像、图像、电子等各种形态资料及其载体的保密管控措施，记录资料由生成到销毁整个生命周期内的使用日志，并根据实际工作情况及时对制度进行调整。乙方应加强本项目在用户工作场所使用设备，特别是笔记本电脑、移动存储介质等便携设备使用的保密管理。接入系统网络内使用的设备，必须遵守该系统关于终端安全管理、移动存储介质管理等要求。

(4) 乙方应组织应急技术支撑队伍，在服务期限内加强与业主单位的联防、联动，积极配合处理网络安全事件，提升业主单位应对网络安全事件的应急处理能力。

三、甲方的权利及义务

3.1 甲方具有对乙方提供的服务活动进行监督与检查的权利。

3.2 甲方具有对项目计划、实施进度、项目质量进行控制，对乙方服务人员进行管理的权利。

3.3 甲方具有要求乙方更换不合格服务人员的权利。

3.4 为保证服务相关活动的正常展开，甲方须为乙方提供必要的配合与支持，包括但不限于：

(1) 确保被服务系统具备开展相关服务工作的条件。

(2) 如实提供乙方实施服务所需的文档资料和图纸等。

(3) 提供必要的工作场地，安排合适的人员配合。

3.5 如甲方与被服务单位非同一主体时，甲方应当保证被服务单位能够按照本协议之约定履行相应的协作，否则造成履行期限延误、服务工作无法开展等不利后果的，由甲方承担相应违约责任。

四、乙方的权利和义务

4.1 乙方应按照双方约定完成服务实施，并对服务报告的客观性、真实性、合法性负责，保证服务的质量符合国家及行业等相关规定。

4.2 乙方应向甲方提供合格的服务人员，完成技术支持、项目实施和项目质量等工作。

4.3 乙方应确保服务实施团队的稳定性，确保项目顺利完成。

4.4 乙方应严格遵守甲方的各项规章制度并严格执行甲方的工作安排。

五、知识产权和保密义务

5.1 甲方承诺甲方（或被服务单位）所提供的系统包括安全产品、软件产品如操作系统、数据库系统、应用软件等具有合法知识产权，没有任何侵犯他人知识产权的行为。若有侵权行为，甲方（或被服务单位）承担由此而引起的一切后果。

5.2 甲方在中华人民共和国境内使用乙方提供的服务时免受第三方提出的侵犯其专利权或其它知识产权的起诉或索赔。如果第三方提出侵权指控，乙方应承担由此而引起的一切法律责任和费用。

5.3 服务工作的成果和结论属被服务单位所有，乙方对其引用和公开应得到甲方（或被服务单位）的授权。

5.4 甲、乙双方应签署“附件1”的《保密协议》，对双方的保密责任和义务进行约定。乙方在本项目执行过程中应对所获悉的所有项目内容进行保密，未经甲方允许不得随意公布、不得转交给第三方。乙方在签订协议时与甲方签订保密协议，若有违反按保密协议规定进行处理，情节严重的，甲方将有权追究其相关法律责任。

乙方必须对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。乙方必须遵守与甲方签订的保密协议，未经甲方书面许可，乙方不得以任

何形式向第三方透露本项目规范书以及本项目的任何内容。如在第三方处发现有涉及甲方内部资料、技术文档和信息等文件，查明确实属于乙方泄露的，甲方将有权追究乙方的法律责任。

5.5 甲方（或被服务单位）如果要引用乙方出具的服务报告，若部分引用会产生歧义或不完整，则甲方必须完整引用，不得作部分内容引用。服务结果仅对被服务系统当时的状态有效，当服务工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行服务，原报告不再适用。

六、履行期限

6.1 服务预定时间为：测评服务从协议签订生效之日起至“重庆市产业大脑应用开发项目”验收完成为止。

6.2 因不可抗力或甲方（或被服务单位）原因导致测评服务工作无法按期完成的，测评服务时间期限将在本协议约定的期限基础上顺延。

6.3 因相关政策调整等不可抗力原因致使项目延期或取消或调整的，或因客观原因致使协议无法订立或订立后因无法履行而解除的，甲方不承担任何责任。

七、工作验收方法

7.1 乙方根据服务结果，针对被服务系统出具正式的《网络安全等级保护测评报告》（含整改建议等）、《商用密码应用安全性评估报告》（含整改建议等）、《系统检测报告》（含整改建议等）、服务成果，报告一式三份，甲方（或被服务单位）签收乙方提供的正式报告并按照验收标准完成验收视为完成验收工作。

7.2 乙方完成所有工作后提请验收，甲方在7个工作日内按照已经确认的协议、国家及行业相关标准、竞争性磋商文件规定对乙方完成情况进行验收（验收单格式详见附件2）。如验收达不到相关规定要求的，乙方应立即进行整改，整改后仍不合格的，则视为验收不合格，甲方有权立即终止协议。由此对甲方造成一定的损失，乙方应承担一切责任，并赔偿所造成的损失。

乙方必须在协议执行完毕之日准备好全套验收资料，因乙方递交不全或不及时对验收工作造成的影响由乙方承担相应责任。

7.3 若有需要，乙方应配合甲方完成项目审计。

八、服务费用及其支付方式

8.1 经甲、乙双方协商，本项目的服务费用总金额为人民币（含税）：426500元（大写：肆拾贰万陆仟伍佰元整）。协议价格明细表详见附件3，本协议的价格应包括完成项目的全部费用，包括但不限于系统测评费、评估服务费、劳务费、税费等完成本项目所需的一切费用。甲方除此以外不支付其它费用。因乙方自身原因造成漏报、少报皆由其自行承担责任，甲方不再补偿。

8.2 支付方式：

本项目为包干价项目，由甲方付款。

协议签订后，乙方向甲方提供协议总额100%的正规发票及与预付款同等额度的担保函，甲方在收到发票及担保函后5个工作日内办理支付协议金额的服务费100%。

如乙方收到预付款后不履行相关义务，甲方可通过担保函收回已支付的预付款。

九、违约金或者损失赔偿额的计算方法

9.1 乙方不履行本协议义务或履行义务不符合约定的，甲方有权要求乙方承担继续履行、赔偿损失或支付违约金等违约责任。

9.2 因乙方原因造成服务完成时间延期的，每延期1天，则乙方向甲方支付本协议约定的未付款项的3%作为违约金，延后时间超过10天的，甲方有权终止协议，不支付协议款并追究乙方相关法律责任。

9.3 甲方将不定期对乙方的工作内容进行审核（审核表详见附件4），出现一次审核不达标的，甲方予以口头警告；出现两次不达标的，乙方应向甲方支付协议金额5%的违约金；出现三次不达标的，乙方应向甲方支付协议金额10%的违约金；出现四次不达标的，甲方有权终止协议，没收乙方的履约保证金，并追究相关法律责任。

9.4 因甲方（或被服务单位）提供的被服务系统、相应协作、配合工作不足服务实施要求造成乙方服务工作无法开展，乙方有权要求甲方（或被服务单位）配合完成服务工作或补充完善相应材料；若因不可抗力或甲方（或被服务单位）原因导致未按期完成测评服务工作、出具测评服务报告及验收等工作的，乙方不承担违约责任，乙方的测评服务时间期限将在本协议约定的期限基础上顺延。

9.5 甲方不履行本协议义务或者履行义务不符合约定的,乙方有权要求甲方承担继续履行、支付违约金等违约责任。

9.6 协议生效后,甲方未能在约定日期或协议双方所同意的延期期限内,向乙方支付协议约定的款项的,每超期 30 天,甲方应向乙方支付逾期款项 0.5% 的违约金,且该违约金累计最高不超过协议总金额的 5%。

十、争议的解决办法

本协议在履行过程中发生争议,双方应本着诚信友好协商解决。若双方不愿协商、调解解决或者协商、调解不成的,可向甲方所在地的人民法院提起诉讼;违约方应当承担守约方为实现债权产生的诉讼费、保全费、保全担保费、律师费等费用。

十一、协议生效及终止

11.1 本协议自甲乙双方加盖双方公章或合同专用章后生效,在双方履行完毕本协议约定的所有义务后终止。

11.2 在本协议终止的情形下,甲、乙双方除应对相关费用/违约金进行清算外,乙方有义务向甲方提供必要的交接和协助。

11.3 本协议如有未尽事宜双方可以协商签订补充协议,补充协议与本协议具有同等效力,补充协议与本协议不一致的以补充协议为准。

11.4 协议各方一致确认协议中的通讯地址和联系方式为各方履行协议、解决协议争议时接收其他方商业文件信函或司法机关(法院、仲裁机构)诉讼、仲裁文书的地址和联系方式。上述确认的通讯地址和联系方式真实有效,如有错误,导致的商业信函和诉讼文书送达不能的法律后果由自己承担。

11.5 协议一式肆份,甲、乙双方各持贰份,具有同等法律效力。

(以下为签字页,无正文内容。)

签署页

甲 方	单位名称	重庆市经济和信息化委员会 (签章)		
	法定代表人或委托代理人	(签章)		
	统一信用代码			
	地 址			
	电 话			
	开户银行			
	银行账户			
	项目联系人		电话	
	签订时间	2025 年 12 月 22 日		
乙 方	单位名称	重庆巽诺科技有限公司 (签章)		
	法定代表人或委托代理人	(签章)		
	统一信用代码	91500104585207799X		
	地 址	重庆市两江新区金开大道西段 106 号 13 幢 5 层 /3 层		
	电 话	02363410769		
	开户银行	中国民生银行股份有限公司重庆分行营业部		
	银行账户	647992035		
	项目联系人		电话	
	签订时间	2025 年 12 月 22 日		

附件 1

保密协议

甲方：重庆市经济和信息化委员会

乙方：重庆巽诺科技有限公司

第一条 保密资料的范围

在（以下简称“本项目”或“项目”）磋商及项目执行过程中，甲方将/已向乙方披露或乙方将/已从甲方知悉保密信息。为保护甲方的合法权益，经平等自愿协商一致，甲乙双方特就保密事宜签订本协议，共同遵照履行。

1、保密资料指在协议签订和履行过程中由甲方或其授权代表以文字、图纸或任何其他形式透露给乙方，或者乙方以任何其他形式从甲方获取的与协议有关的任何资料。

2、任何包含保密资料的手册、说明、报告、图纸、信函、电传、电子邮件和其他资料或载体，均视为保密资料。

3、在甲方告知乙方时，已经是公开资料的，不是保密资料。

第二条 保密义务的内容

1、乙方应对任何保密资料保密并促使、监督其雇员对保密资料保密。

2、未经甲方书面同意，不得向第三方透露任何关于保密资料存在的信息或为第三方使用、复制保密资料或以任何形式了解保密资料的内容提供便利。

3、除为协议的履行外，不得将保密资料用于任何其他目的。

第三条 保密对象

保密对象包括但不限于乙方、其关联公司及其相关人士。相关人士包括但不限于公司及其所属集团各自的董事、监事、高级管理人员、雇员、咨询者、代理人、顾问等。

第四条 保密期限

乙方应在职责范围内对所接触的甲方资料负有保密义务，该保密义务自签署之日起生效，

不因协议的解除或终止而失效。

第五条 其他

1. 任何保密资料的版权，除有明确规定外，都归甲方所有。

2. 当协议履行完毕或被解除时，乙方应立即将保密资料归还给甲方。不能归还的，应在按照甲方的要求或者在甲方指定人员的监督下将其销毁。

因履行协议的需要或根据本协议，保密资料需要为第三方所知时，乙方应取得甲方的书面同意，且确保第三方签署一份与协议中的保密义务相等的保密承诺书。

4. 如乙方未按上述条款所述义务保密从而导致甲方遭受损失，乙方应承担由此造成的全部损失，包括但不限于甲方因乙方的违约行为而受到的索赔、支出、法庭或仲裁庭或任何其它监管机构作出的处罚。

5. 本协议经甲乙双方签字盖章后生效。

(以下无正文)

甲方：重庆市经济和信息化委员会

联系
电



签章日期：2025年12月20日

乙方：重庆巽诺科技有限公司

联系
电



签章日期：2025年12月22日

附件 2

重庆市经济信息委验收单	
处室名称:	
采购类别: 货物 ☐ 服务 ☐ 工程 ☐	
项目名称:	
协议金额: 验收金额:	
服务时间:	
服务地点:	
主要内容	执行情况
软件测评服务 (包一)	
网络安全等级保护测评 (包二)	
密码应用安全性评估 (分包三)	
供应商名称 (盖章)	供应商签字: 时间:
使用处室验收意见 (盖章)	验收人签字: 时间:
其他参与处室验收意见 (若有)	验收人签字: 时间:
备注	

附件 3

协议价格明细表

单位：元

序号	费用名称	相关信息	数量	单价	合计
1	软件测评服务	软件测评服务（包一）	1	275800	275800
2	网络安全等级保护测评	网络安全等级保护测评（包二）	1	75200	75200
3	密码应用安全性评估	密码应用安全性评估（分包三）	1	75500	75500
总计（元）：426500.00(肆拾贰万陆仟伍佰元整)					

附件 4

重庆市产业大脑应用开发软测、密评与等保服务（分包 ） 服务质量审核表				
成交供应商 名称	审核日期	审核结果及说明	审核人签字	成交供应商代表 签字