建信信托官网系统重构项目采购需求

**一、业务需求**

本期项目建设业务需求主要包括三大部分：公司官网前端页面功能、移动端页面功能、后台管理功能以及技术类需求。

1、前端页面功能

（1）现有菜单栏目展示功能

目前，公司官网设有8个一级菜单和36个二级菜单，一级菜单包括关于我们、投资银行、资产管理、财富管理、信息披露、客户服务、建信洞察、消费者保护；二级菜单包括公司简介公司新闻、加入我们、联系我们等。

本次项目应满足以上菜单体系的展示、增加、删除、更新等管理配置。

（2）新增个人客户登录、查看信息披露报告的功能

公司官网面向个人客户提供建信尊享APP下载、注册二维码，支持客户下载注册建信尊享APP；支持客户通过输入密码、手机动态验证码或扫描二维码方式登录公司官网；支持客户身份识别认证，提供其名下持仓产品的信披报告（含有客户信息水印）。

（3）新增机构客户登录、查看信息披露报告的功能

官网支持管理员预埋机构客户账户与密码，并通过邮件、短信方式通知客户；支持客户通过初始密码登录系统，查看本机构所代销产品的信披文件（含有机构信息水印）。

（4）其他功能

公司官网支持按内容的按标题或全文检索；支持视频在线播放；支持首页浮动广告展示， 可以通过后台对浮动广告内容、是否显示浮动广告进行管理配置；支持一键变灰；支持留言板等功能。

2、移动端页面功能

移动页面功能与PC端一致，适用手机端浏览器展示，支持微信、QQ等主流社交媒体分享。

3、后台管理功能

（1）用户管理

用户角色与权限管理：创建、编辑和删除不同用户角色（如管理员、机构客户管理员等），并为每个角色分配特定的访问权限，确保数据安全和操作合规性。账户信息变更生效后通过邮件/短信的方式通知客户。

用户信息管理：集中管理所有注册用户的基本信息，包括姓名、邮箱、电话号码、注册日期等。

用户行为监控：跟踪用户登录、操作日志，识别异常行为，提升账号安全性。

（2）内容管理

页面编辑与发布：提供可视化编辑器，支持富文本、图片、视频、音频等多种内容格式的编辑，以及即时预览和一键发布功能。

文章内容管理：分类管理文章，支持标签、分类设置，便于内容组织和搜索优化。

多媒体资源管理：上传、存储、分类和管理图片、视频等多媒体资源，支持批量上传和URL链接管理。

模板与主题管理：允许管理员切换网站主题或模板，自定义网站风格和布局，快速响应品牌形象变化。

（3）信托产品、信披报告、客户关系维护

支持信托产品、信披报告、客户标签管理及关系维护。

（4）数据分析与报告

网站访问统计：集成分析工具，追踪网站访问量、页面浏览量、用户行为路径等，生成可视化报告。

SEO性能监控：监控关键词排名、网站索引情况，提供SEO建议，提升搜索引擎可见度。

（具体需求详见附件）

**二、技术相关要求**

1.平台支持要求

（1）用户登录系统需要支持微软EDGE、苹果Safari、火狐、谷歌、360极速模式等主流浏览器。

（2）应加强系统浏览器兼容性测试（对客户端应用场景，应有对应的适配测试）。要明确应用系统可兼容浏览器的类型及版本范围，当通过非兼容浏览器访问应用系统时，提示用户升级浏览器版本或者更换合适类型的浏览器。

2.完整性和独立性要求

供应商提供服务所需的硬件设备、软件产品、文档资料、源代码（算法）等，并保证其拥有合法的使用权，不包含任何侵犯他人知识产权的物品、文档或内容。同时，要求供应商提供的软件产品、源代码（算法）等不能对其他第三方软件产生依赖并且需甲方支付额外费用。

根据建信信托提出的业务需求所开发形成的全部业务及技术知识产权（含本项目所有源代码）均归建信信托所有。

3.性能要求

（1）支持同时在线用户数不少于500人。

（2）实时查询服务平均响应时间小于等于1秒。

（3）复杂数据处理场景服务平均响应时间小于等于3秒。

4.安全性要求

为更好的保障数据安全，系统需满足金融银行系统级别安全要求，包括但不限于SQL注入、平行越权、常规安全攻击防范等。

（1）应用程序不得与操作系统的用户名/密码相关，应采用参数的模式记录所连接数据库的IP地址、数据库实例名、用户名/密码等信息，以支持定期修改操作系统、数据库的用户密码。密码不能以明文形式存储在文件或配置中。

（2）应用开发前应及时对IP地址、DNS 域名、端口、协议进行确认。严禁采用远程桌面或类似的应用程序作为业务系统组件,严禁使用类似P2P的特殊协议。

1）对用户口令的长度及复杂度的要求描述：并需要防范SQL注入、恶意用户注册、恶意批量注册等攻击行为。

2）应用登陆（包括密码重置），能抵抗暴力猜解。

3）对于非互联网系统，应对接SSO（Single Sign On - 单点登录）系统，例如内部用户拟通过对接我司认证及授权系统系统产生系统用户。

4）授权应满足最小权限原则，满足基本需求即可。

（3）数据保护-安全要求，如涉及相关场景则需按此标准实施：

1）数据存储：敏感信息的存储方式的说明，例如“应用涉及用户口令存储，需在存储前通过安全的单向hash函数转化为不可还原的形式”。

2）数据传输：敏感信息传输的方式的说明，例如“数据涉及互联网传输场景，需使用https加密传输，对证件类信息返回前端时进行额外脱敏处理”。

3）数据使用：敏感信息使用的方式说明，例如“数据展现上，涉及后台管理页面，用户可进行批量查询，最多单词查询N条数据，拟通过脱敏进行展示”。

5.高可用要求

（1）系统应具备应用备份机制，通过负载均衡、应用系统备份等机制，确保不得出现单点故障，确保系统具备切换条件，支持异地灾备。

（2）数据库应用应制定数据备份策略，定期对生产数据进行备份，可设定定期备份时间、路径，可以采用手动和自动两种方式，并对备份结果进行提示和检查。数据备份应包括数据库、保存系统信息的和各类配置文件、参数文件、上有数据文件等。

（3）应具有应用级恢复建议方案，该方案的实施应保证系统在出现故障时能够迅速恢复,其中RPO、RTO时间均为240分钟。

6.底线原则

（1）系统间数据访问：禁止使用DBLINK方式进行数据交互，原则上不允许跨系统JDBC。

（2）软件及技术组件：支持在建行云上部署，同时操作系统、中间件以及开源软件（包含前后端开发框架及系统软件）等需要符合建信信托标准，如开源软件禁止低于底线版本、相关软件配置项要求。

（3）互联网系统访问：要求使用https，禁止使用http非加密方式传输，原则上不使用四层TCP/UDP监听。

（4）数据标准落实：对外输出共享以及定制开发的本地表的数据项需要按照建信信托数据标准落地（包含字段命名、长度精度、数据字典等）；对于产品内部数据表建议按照建信信托数据标准落地，覆盖我司业务实质和监管报送要求。

（5）系统交互形式：对于系统间的交互需要结合时效采用实时、消息队列、文件交换等方式；同时禁止在数据表上进行耦合交互（如视图交互方式等），需要增加接口或文件约束进行信息交互。

（6）组件依赖原则：信息系统的组件依赖要基于公司的业务及技术基础服务平台，按照通用性原则进一步分为应接尽接、按需对接两类系统，具体说明参考如下（系统定义说明参考附件-系统生态梳理）。

应接尽接：主要有统一认证&认证与授权中心&通讯录、消息中心、微服务治理平台、架构治理管控平台、企业级数据仓库、数据资产管理平台、文件交换平台、内容管理平台、建行公有云、开发云桌面、DEVOPS平台、应用监控中心、日志中心等系统。

（7）接口设计要求：系统间及系统内的接口需要按照系统或模块的边界进行分析设计、系统间交互需要使用Restful接口（HTTP+JSON）、微服务注册需要与我司微服务平台对接，支持RPC或Restful接口标准。

（8）对于日志部分的开发，按照信托日志规范进行通讯日志、运行日志、操作日志、中间件日志及日志脱敏实施。

日志审计描述：

1）明确主要应用日志级别设置策略，例如“默认设置为warning级别，在问题排查情况下，需通过在线配置刷新将日志级别升级为info级别”。

2）日志记录完整性说明，例如“日志记录满足关键业务活动审计，包括用户认证/登录、超时退出、数据修改等关键活动；日志中包含客户端请求原始IP”。

3）日志可用性说明，明确日志清理及备份策略。

（9）反爬虫防范要求，确保反爬虫措施不会对合法用户的访问造成影响，同时能够有效抵御恶意爬虫的攻击，保护网站数据安全。采取的反爬虫措施符合当地法律法规，避免侵犯用户的合法权益。尽量减少对正常用户的影响，保护客户数据的安全，防止非法获取敏感信息。

（10）安全漏洞及时修复要求。供应商加强产品或系统安全缺陷、漏洞的检测与监测，其中包括第三方、开源组件的相关缺陷、漏洞。对于已知缺陷、漏洞，供应商应按照国家相关法规要求妥善处置，并协助建信信托在符合要求的限定时间内完成整改与修复。

（11）严格落实我司关于供应商安全的相关要求，具体按照《供应商安全相关要求》文件执行。

（具体技术需求详见附件）

**三、项目进度要求。**

根据业务需求紧迫性要求，系统功能应在2025年12月31日前实现，并且系统上线验收后提供免费维护期12个月。

**四、项目实施各阶段的服务内容和要求。**

（一）服务内容

拟采购建信信托官网整体改造需求事项业务功能。具体参照一业务需求说明部分。

（二）上线要求

根据业务需求紧迫性要求，系统功能应在2025年12月31日前实现。

（三）验收要求

1.验收标准

（1）功能性验收

1）功能项验收。以用户测试验收为准，针对所提供的功能点逐项进行验收确认。功能要求详见需求说明书。

2）业务流程验收。对业务中使用的流程逐项进行验收确认。

（2）非功能性验收

1）安全性验收

系统是否存在未修复的安全漏洞；开源组件版本是否满足建信信托技术栈要求；安全性方面是否能够通过建信信托安全性测试（包括人工渗透测试和代码审计）。

2）容错性验收

系统对用户常见的误操作是否能进行提示。

系统对用户的操作错误和软件错误，是否有准确、清晰的提示。

系统对重要数据的删除是否有警告和确认提示。

系统是否能判断数据的有效性，屏蔽用户的错误输入，识别非法值，并有相应的错误提示。

3）性能验收

通过模拟多种正常、峰值以及异常情况下系统所承载的业务压力或使用场景，对系统的性能指标进行测试验收。

4）易用性验收

用户界面是否友好，是否出现中英文混杂的界面。

提示信息是否清楚、易理解，是否存在原始的英文提示。

各个模块的界面风格是否一致。

查询结果的输出方式是否比较直观、合理。

5）适应性验收

对所需满足的软、硬件环境逐一进行测试验收。

（3）文档材料验收

文档材料包括：安装手册、操作手册、维护手册、数据字典、架构设计、系统详细设计等。系统文档材料验收内容包括:

1）文档材料是否齐全、是否包含产品使用所需的全部信息和所有的功能模块；

2）文档材料描述的信息是否准确，是否没有歧义和错误的表达；

3）文档材料是否容易理解，是否通过使用适当的术语、图形表示、详细的解释来表达；

4）文档材料对主要功能和关键操作是否提供应用实例；

5）文档材料是否有详细的目录表和索引表。

6）对于前期已上线功能做的优化需求，需更新对应产品手册，系统设计手册等，并提交最新版本，作为验收材料。

**五、供应商投入项目的人员数量、资质经验、角色等方面的要求。**

供应商人员项目团队至少包含以下人员角色和要求，并进行详细介绍，包括参与本项目人员清单，以及对应的具体角色、级别、职责，并附简历、身份证明、资质证明文件等。应保证具备充足的响应技术人员储备及完整的变更协调机制，并且保证参与项目的主要人员稳定。如需更换项目组成员，需至少提前20个工作日告知，经我司同意后方可变更。若项目人员技术能力、态度等不满足我司要求，应在5个工作日内更换入场人员以满足要求。若出现人力不足的情况，应在5个工作日内协调满足我司要求的人员，并完成入场手续。项目实施期间人员变动应少于20%，实施团队需具备以下资质：

（1）项目经理（至少1人）

职责：负责本项目的计划、组织、实施、协调、人员配置并监督工作情况及进度等工作，负责各方沟通联系，及时进行项目跟进，要求全程驻场，积极配合建信信托各项规定要求。

人员要求：具有5年以上金融行业互联网系统建设相关项目实施、管理经验，具有5个（含）以上互联网平台相关项目管理实施经验（银行、金融行业相关）；具有丰富的业务场景分析、集成、实施的项目经验和较强沟通协调能力；具有遇见和应对项目风险的能力。

（2）技术经理（至少1人）

职责：负责本项目的计划、组织、实施、协调、人员配置并监督工作情况及进度等工作，负责各方沟通联系，及时进行项目跟进，要求全程驻场，积极配合建信信托各项规定要求。

人员要求：具有5年以上金融行业互联网系统建设相关的项目实施、管理经验，具有3个（含）以上金融行业互联网系统建设相关项目管理实施经验（银行、金融行业相关）。

（3）需求经理/产品经理（前期需求分析阶段不少于1人）

职责：负责本项目的需求范围确定，需求收集，需求分析，软件规格说明书的编写，用例评审，对测试进行验收。

人员要求：应具备3年以上金融项目工作经验，参与3个以上大型金融机构软件项目或者业务规划项目；具有较强的业务洞察力，对金融行业互联网系统建设有深入的了解，业务设计具有前瞻性。

（4）实施人员

高级实施人员：要求具有5年以上项目实施经验，具有至少3个以上同类项目的系统分析经验，在系统研发、实施、上线等方面具有丰富的经验；精通投标人产品相关的各项技术，至少具有2个互联网平台的项目经验。熟悉系统业务，能够对应用机构、技术架构、数据架构及相关系统集成等方面提出专业建议，具有较强的系统性能分析、调优、排查能力，具有较好的沟通能力。

(5)中级实施人员：具有3年以上银行系统实施经验；熟悉业务及产品配置，具有较强的开发能力，能够解决技术难题，负责相关开发支持。

(6)初级实施人员：具有至少2年以上银行信息系统开发经验，可以按照系统设计进行开发和测试相关工作。

(7)人数要求：配备足够开发测试相关人员，高级实施人员不少于20%、中级实施人员不少于50%。

**六、项目实施的环境要求。**

支持在建行云上部署，并满足信创国产化相关要求。操作系统及数据库以建行云信创技术栈为标准执行；其余开源软件按如下版本及标准执行。

JDK: 1.8.0\_251及以上版本

Redis：6.0.4

中间件（建议Tomcat，比较轻）

Apache Tomcat 10.0.0-M10或更高版本

Apache Tomcat 9.0.40或更高版本

Apache Struts2 ：2.5.12

Spring Boot 2.6.8

Spring Web Service 2.4.4,3.0.6或更高版本

Spring Security 5.5.7及以上版本

Fastjson 1.2.83或更高版本

jackson-databind ：2.10.0

Weblogic：11g、2c

Log4j 2.17.1或更高版本

Shiro 1.10.0或更高版本

Vue 2.6.11或更高版本

**七、项目管理方面的要求。**

（一）项目沟通例会管理

1.项目组每周例会：每周一下午供应商项目经理与建信信托项目责任人开会，汇总项目状态，提出并解决问题，追踪问题、风险和依赖条件，制定下一步行动计划。供应商负责记录并分发会议记录。 每周四由PMO组织向业务科技领导汇报当前项目进展。

2.需求分析评审会：需求分析完成时，系统组，业务组及相关系统人员参加需求评审会，评审通过后对本系统需求分析说明书签字确认。

3.变更控制会议：业务提出重要变更后，需供应商项目经理组织需求变更会议，系统组、业务组及相关系统人员参会，从技术可行性、技术上的影响、技术上的问题等方面评估需求变更对业务、管理、系统的影响。

（二）项目事项报告反馈制度

1.项目周报：项目运行期间，供应商项目经理每周五提交项目周报，内容包括：项目里程碑及项目整体进度、项目范围管理、项目问题追踪等。

2.SIT测试报告：SIT完成后，提交SIT测试报告。

3.UAT测试报告、性能测试报告：UAT测试完成后，提交UAT测试报告、性能测试报告。

4.渗透测试报告、代码安全审计报告：渗透测试、代码审计完成后提交渗透测试报告、代码安全审计报告。

5.系统上线报告：系统上线后，提交系统上线报告。

**八、项目成果要求**

（一）知识转移及文档归档需求

1.源代码

供应商应提供本项目全部定制化开发的源码，本项目业务系统代码（官网系统前后端等）以及其他定制化开源代码。源代码包括：源代码、代码开发和编码规范，在开发过程中，应按照建信信托要求更新源代码以及相关的开发资料。

供应商应有完善的版本管理和文档管理机制，对于每个版本都有些详细说明，并能实时更新各种项目文档。

代码开发应做到规范化管理，源代码应具有良好的可维护性和详细注解，以便后续维护、修改和扩充。

2.设计稿

供应商应提供所有页面的设计稿，包括但不限于界面、图标及设计规范（所有设计元素：字体、图标、文档）均不存在版权问题，如需付费元素，则由供应商承担。

供应商应有完善的版本管理和文档管理机制，对于每个版本都有些详细说明，并能实时更新各种项目文档。

3.知识产权

本项目涉及所有定制化开发源代码知识产权归建信信托所有，未经建信信托同意，实施厂商不允许泄露给任何第三方，如违反，建信信托有权对厂商进行相关处理。

4.保密要求

项目实施过程中，所有入场人员对于建信信托的非公开信息、数据等承担保密义务，入场时需签订保密协议函。如违反保密协议函中相关条款，建信信托有权追究供应商及对应个人的法律责任，并要求承担相应损失。

**九、培训要求**

供应商需提供高技术、高质量的培训，包括研发、安装、维护、开发和使用等，满足系统从建设管理到维护运营等全生命周期的培训服务，以达到预定的培训目标。

所有培训服务（包括培训计划和培训课程）和费用必须在投标文件中分项列出，并计入总报价。

供应商负责为培训人员免费提供培训教师和培训资料，所有书面资料或电子文档用中文书写。

**十、项目验收后的技术支持和维护服务要求。**

在软件产品安装、调试完毕并通过验收上线后进入12个月免费维护保修期。

在保修期内，供应商必须对所有软件和系统免费提供定期预防性维护和临时性紧急维修服务。供应商需在1小时内对我司提出的临时性紧急维修做出回应，并提供派遣工程师进行现场支持，现场支持和回应不收取任何费用。

**十一、报价要求。**

供应商需明示本次改造涉及的收费标准及相关增值模块费用情况，并明示包括但不限于采购费用、相关模块、安装和部署费用、测试费用等实施费用，以及官网系统需求梳理、功能开发、部署运维、培训等费用。供应商不得以任何形式向建信信托索要报价清单之外的任何费用。

**十二、结算要求。**

1.合同生效并且收到供应商开具发票后十五个工作日内，向供应商支付软件系统对应合同总额的30%。

2.本合同下各软件系统完成竣工验收，并且收到供应商开具发票后十五个工作日内，向供应商支付各软件系统合同总额的60%。

3.本合同下各软件系统完成竣工验收之日起运行12个月（免费维护保修期）后，且收到供应商开具发票后十五个工作日内，向供应商支付各软件系统合同总额的10%。

**十三、供应商资质要求。**

1.未被“信用中国”网列入 “重大税收违法案件当事人名单”、未被“中国执行信息公开网”列入“失信被执行人名单”、未被“中国政府采购网”列入“政府采购严重违法失信行为信息记录名单”、未被“国家企业信用信息公示系统”列入网站“严重违法失信企业名单”、在参加本次采购活动前三年内未出现重大违法违规行为，未在行政处罚信息中涉及责令停业处罚，近三年在我司无不良行为记录。

**十四、其他要求。**

1.供应商所有入场人员需遵守《建信信托外包人员管理规定》相关要求，同时需签署《供应链企业安全责任与保密承诺函》并加盖公章。

2.系统中使用的软件工具，如调度、传数、加密等工具应经过全面的功能性测试及压力测试，不得使用未经验证或盗版的软件。

附件：

供应链企业安全责任与保密承诺函

建信信托有限责任公司：

我司（企业全称）根据与贵单位的约定，将为贵单位提供 产品/ 服务（服务时间： 、服务场地： ）。为落实供应链安全责任，防范网络安全重大风险，我司已组织相关人员学习本承诺函及附表所列内容，并知悉相应要求。承诺如下：

# 一、通用承诺

（一）我司不利用提供产品、服务的便利条件非法获取贵单位数据、非法控制和操纵贵单位设备，无正当理由不中断产品供应或必要的服务，不利用贵单位对产品的依赖性谋取不正当利益或迫使贵单位更新换代。

（二）我司为贵单位供应的产品、服务中未设置恶意程序和后门程序，没有任何可能导致泄密的风险装置且不存在安全漏洞。

（三）我司向贵单位供应的产品、服务不存在任何侵犯第三方及其授权许可人的知识产权情形。如含有商标、专利或者著作权等内容，我公司为合法的权利人或者授权许可人。

（四）我司保证拥有提供本合同约定服务的安全相关资质及许可，包括但不限于各类行政许可。

# 二、开发安全承诺

（一）安全检测。我司向贵单位供应软件产品或为贵单位定制开发系统时，我司将对提供的产品、系统开展安全检测、风险测评或源代码安全审计，并将向贵单位提供相关证明报告。

（二）源代码管理。我司承诺，将做好源代码的安全管控，防止源代码泄露。我司不将贵单位源代码托管至可公开访问的第三方代码平台，如需托管在不可公开访问的第三方代码平台时，我司应取得贵单位的事先书面同意并采取源代码安全管控措施，包括不限于访问控制、安全审计、安全防护策略等，防止人员违规访问源代码库。我司将加强源代码管理和技术资料泄露监测工作，及时发现违规在开放式代码管理平台、共享文档平台、网盘等上传、托管和存储情况，及时清理处置，采取措施消除影响并开展泄露溯源。合同或协议关系解除后，我司将及时删除贵单位相关源代码，不以任何方式保存或转移。

（三）漏洞管理。我司将加强产品或系统安全缺陷、漏洞的检测与监测，其中包括第三方、开源组件的相关缺陷、漏洞。对于已知缺陷、漏洞，我司将按照国家相关法规要求妥善处置，如涉及贵单位，将立即书面通知贵单位，准确传达缺陷、漏洞等风险，并协助贵单位进行整改与修复。同时对贵单位安全缺陷、漏洞等信息严格进行保密，在未经贵单位允许情况下绝不将其提供给第三方。不利用安全缺陷、漏洞信息等攻击贵单位信息系统。

（四）开发管理。我司将制定开发管理制度，明确开发过程的控制方法、管理流程、人员行为准则和代码安全规范等，并定期对相关人员开展安全开发培训。

（五）环境隔离。为贵单位提供开发服务或定制化产品时，如在我司场地实施，我司将对开发环境实施物理隔离，并对开发、测试、生产网实施有效隔离，对无线网络进行安全控制，避免开发、测试人员通过无线网络将贵单位相关源代码及敏感信息文件私自上传至互联网。

（六）知识产权。我司供应的产品或服务应用在贵单位关键信息基础设施时，承诺对产品和服务研发、制造过程中涉及的实体拥有或控制的已知技术专利等知识产权获得10年以上授权，或在产品和服务使用期内获得持续授权。

# 三、交付安全承诺

（一）我司承诺，将制定物流安全监督措施，保障交付给贵单位的产品物流安全，将采用可信或可控的产品分发、交付和仓储手段等。我司向贵单位提供产品、服务相关的技术文档时，将保证交付渠道的安全性。

（二）经贵单位认定的对关键信息基础设施、重要网络、大数据具有重大影响的核心部件，我司将提高物流安全等级，并及时将存储、交付、物流等信息报告贵单位。

（三）我司供应的产品或服务应用在贵单位关键信息基础设施时，将提供中文版运行维护、二次开发等技术资料。

# 四、维护安全承诺

（一）我司将对服务贵单位的维护人员开展安全培训、对维护人员行为进行监督与权限控制、利用合同或协议约束人员安全行为等。

（二）如在我司场地提供维护服务时，我司将采取控制手段，包括不限于记录维护的时间、人员、维护情况，对维护人员的权限审核与控制等。

（三）我司将严控人员权限管理，严禁我司人员非授权开展维护工作。

# 五、数据安全承诺

我司在供应产品、服务过程中，涉及接触或处理贵单位数据的，如客户个人信息、业务生产数据、重要工作文件、其他重要数据、系统源代码等，将履行下述承诺：

（一）我司具备符合贵单位要求的数据安全能力，保证采取适当的数据安全技术与制度措施充分保障贵单位数据的安全性、以及贵单位与相关信息主体的合法权益。我司保证该服务结果不会侵犯任何个人隐私、第三方商业秘密等其他合法权利。

（二）我司保证有权限处理（处理行为包括：收集、存储、使用、加工、传输、提供等）贵单位数据的我司工作人员于提供服务前接受数据安全相关专业化培训和考核，在服务期间内每年至少接受一次数据安全方面的相关培训；我司将妥善留存培训记录以供贵单位随时调取，保证我司工作人员均参加数据安全相关培训。

（三）我司将遵循法律法规、国家及行业标准以及本合同有关数据保护的相关约定，仅为本合同之目的处理贵单位数据。我司对贵单位数据的处理行为不超出贵单位的授权范围。

（四）我司将准确记录处理贵单位数据的情况，并依据贵单位需求定期或不定期向贵单位提交数据处理工作报告。我司数据处理工作报告的内容应包括但不限于我司处理贵单位数据的时间、场景、目的、行为、涉及的数据类型与字段，我司处理贵单位数据所采取的数据安全措施，我司负责处理贵单位数据的工作人员等。我司同意贵单位有权对我司进行现场或非现场检查，确保我司数据处理方式与安全要求一致。

（五）未经贵单位书面授权，我司不将贵单位授权我司开展的贵单位数据处理事项委托或提供给任何其他机构。如贵单位书面授权我司委托或授权其他第三方机构处理贵单位数据的，我司将保证其他机构具备符合贵单位要求的数据安全能力，在处理贵单位数据时采取相应的数据安全技术与制度措施保证数据安全，并就其合作机构的数据处理行为承担连带责任等。

（六）如我司或我司委托或授权的其他第三方机构发生与处理贵单位数据有关的数据安全事件，将立即以书面形式向贵单位报告，并迅速开展数据安全影响评估与安全事件调查，积极采取或配合贵单位采取止损措施，防止影响范围进一步扩大。

（七）我司保证对贵单位数据的收集、使用、存储（如适用）、销毁等处理行为均在中华人民共和国境内进行。

（八）我司保证采用加密、脱敏等安全措施传输数据，采取有效技术防护措施确保贵单位数据安全，防范贵单位数据传输过程中被第三方截获和利用。

（九）未经贵单位书面授权，我司不得存储、使用和共享其加工处理的贵单位数据或产生的服务成果（包括但不限于程序、文件、资料等）。我司为履行本合同约定而必须存储、使用和共享贵单位数据或产生的服务成果时，应获得贵单位书面授权，并向贵单位提供具备数据安全保护能力和对相应数据等采取保护措施的书面证明材料。

（十）如贵单位书面授权我司在履行本合同约定范围内存储贵单位数据的，我司将采取措施使贵单位数据与我司其他数据有效隔离，保证仅限于有权限的我司工作人员能访问贵单位数据。

（十一）我司将根据“业务需要”和“最小权限”原则，对贵单位数据的访问操作进行满足业务最小数据集的访问控制，并记录访问日志和全过程监控。

（十二）如我司在贵单位指定场所驻场提供服务，我司将遵守贵单位数据安全保护制度要求，未经贵单位书面授权不得以存储、传输等方式处理贵单位的任何数据。

（十三）我司承诺在合同终止后立即将获取的贵单位数据及相关衍生数据进行销毁并向贵单位为提供证据证明，不得以任何方式留存贵单位数据及相关衍生数据。我司承诺具备完善的数据销毁机制，对销毁过程保留记录以供贵单位调取。同时履行以下义务：

1.返还包含贵单位数据及衍生数据信息的文件和资料，包括不限于复制件、电子文档等；

2.销毁无法返还的包含贵单位数据及衍生数据信息的文件和资料，包括不限于复制件、电子文档等；

3.提供一份书面声明，确认已销毁所有包含贵单位数据及衍生数据信息的文件、资料、电子文档和相关复制件，并附销毁材料清单。

# 六、人员安全承诺

（一）我司向贵单位提供服务时，我司将建立服务贵单位的人员台账并向贵单位报备，包括人员基本信息、联系方式、工作职责、在职离职情况、系统和服务权限等，台账将动态维护。

（二）我司将向服务贵单位的我司人员告知相关保密义务，并与其签署书面保密协议，使其承担不低于合同约定的及本承诺函承诺的保密义务。

（三）对于可接触贵单位关键信息基础设施、重要网络和大数据系统的我司服务人员，我司将开展人员背景调查和保密审查，调查结果应获得公安机关确认，并将调查结果、证明材料加盖公章后反馈贵单位，证明材料包括不限于人员的缴税证明、在职证明、学历证明、项目经历证明、社保证明、无犯罪证明、保密协议等。

（四）我司将组织服务贵单位人员，定期开展教育培训活动，提升人员安全意识，包括不限于制度规范、安全培训、应急流程、内部攻防演练等。在贵单位场地提供服务时，我司将制定符合贵单位管理要求的安全保密、工作场所行为规范等管理制度，并应组织我司服务人员学习上述制度。

（五）当服务人员离职时，我司将建立离职人员账号、权限、材料等交接、清理流程，并具有完整的离职交接记录。

# 七、运行安全承诺

我司为贵单位研发并运营的系统，如涉及贵单位重要数据或客户个人敏感信息，因特殊情况暂时不能在贵单位内部署时，我司将加强网络与信息安全、数据安全管理，如涉及第三方云平台，将密切跟踪第三方云平台内重要组件的更新管理，必要时对第三方云平台开展安全审计，我司将加强系统的安全防护和加固，并尽快组织向贵单位内迁移和部署。

# 八、连续性承诺

（一）我司将加强物理与环境安全，将提供必要的应急和灾备资源保障，强化备品备件管理，确保提供贵单位的产品、服务的持续性和可恢复性。

（二）根据贵单位认定，如我司属于重要等级产品、服务供应商，我司将针对安全类、运营类、管理类等事件进行分级分类，制定事件的监测发现、分析研判、上报、处置等措施。

（三）我司将加强与供应链上下游企业联动协同，密切关注上下游企业情况，做好风险防范与应急处置，根据贵单位需要，可向贵单位定期汇报上下游企业情况，防范供应链风险。

（四）根据贵单位认定，如我司属于重要等级产品和服务供应商，我司将制定供应链安全事件的应急响应预案，预案场景将至少包括供应链攻击、供应中断、敏感信息泄露等，预案中将明确，为贵单位提供应急响应和恢复的优先级为最高级，应急预案将定期报送贵单位。

（四）根据贵单位认定，如我司属于重要等级产品和服务供应商，我司将开展企业内部的应急演练。演练完成后，形成演练报告，评价演练效果，分析风险和不足并提出整改措施，及时整改，演练报告、问题发现及整改情况报送贵单位。同时我司将配合参加贵单位的应急演练。

# 九、保密承诺

我司与贵单位合作期间，如果我司以书面、介质或口头形式获得贵单位某些非公开的、保密的、专业的数据及相关衍生数据、服务成果等（以下统称“保密信息”），包括不限于涉及的客户个人信息、业务生产数据、重要工作文件、其他重要数据，密码本、网络拓扑图、系统源代码等信息（详见附表《保密信息范围》）。我司承诺对附表所列的贵单位保密信息承担下述保密义务：

（一）在保密期内，对保密信息保密，未经贵单位书面同意，不将保密信息用于合同以外的目的，并不将其泄漏给任何第三方，不将数据以任何形式转移、挪用或谋取合同约定以外的利益，不下载、分析和存储贵单位保密信息，不将保密信息带离*贵单位／我司*办公场所，而且我司应防止贵单位保密信息被销毁、丢失或改变。

（二）我司不出售、转让贵单位保密信息。不在公共场所或私人通信中谈及贵单位保密信息。不进行其他可能导致贵单位保密信息泄漏的活动。

（三）不利用合作之便获取贵单位与合作无关的保密信息。不利用贵单位保密信息从事损害贵单位利益和声誉的活动。

（四）我司人员如在为贵单位服务期间离职，不带走任何贵单位保密信息，在保密协议规定的保密期内不泄漏任何贵单位保密信息。

（五）如果法律规定或监管机构要求我司必须对保密信息或由保密信息得出的任何意见、判断等信息做出披露时，在法律允许的情况下，我司立即书面通知贵单位，以使贵单位能选择采取保护措施。且我司在披露前或披露时尽最大努力为被要求披露的保密信息获取保密措施或保密待遇，并将披露范围严格限定在有权机关或法律法规所要求必须披露的范围之内。

（六）我司承诺上述保密义务的期限为永久，保密义务不随双方合作的终止而终止。

（七）我司同意，贵单位对所透露的保密信息有权不附带任何种类的保证。

（八）我司同意，对于我司因使用贵单位提供的保密信息而使我司受到的任何损害，贵单位无需承担赔偿责任。

# 十、风险管理承诺

（一）我司将根据贵单位要求，配合提供供应链产品及服务的相关信息，包括不限于版本、型号、生产厂商、开发类型、涉及的操作系统、是否有信息回传厂商、回传信息主要内容、联系人等基本要素。对于我司提供的产品、服务中包含的第三方或开源产品，我司将提供使用的第三方或开源产品信息。

（二）我司将积极配合贵单位的风险评估、监测、检查和审计等工作以及国家有关部门和银行业监管机构的检查，并根据贵单位或国家有关部门或银行业监管机构的整改要求及时纠正，整改结果将定期向贵单位汇报。

（三）我司承诺将做好网络安全保护工作，落实供应链安全责任，防范网络安全重大风险，保证不因我司及我司人员原因，导致外界获取贵单位保密信息或导致贵单位发生网络安全事件。

（四）供应链产品供应和服务过程中发生以下重大风险事件时，我司将立即向贵单位书面报告：

1.贵单位重要数据或客户个人信息泄露；

2.贵单位数据损毁或者重要业务运营中断；

3.由于不可抗力或我司重大经营、财务问题，导致或可能导致多家银行保险机构产品或服务中断;

4.产品或服务非正常中断、终止或我司非正常退出；

5.因我司不当行为或信息系统遭受网络攻击或其他原因，造成贵单位客户重大资金损失；

6.发现重大的我司违法违规事件;

7.国家及监管机构发现的其他重大事件。

（五）我司原因造成贵单位保密信息的泄露或发生贵单位网络安全事件时，我司将立即开展处置，最大限度降低影响，保障贵单位及客户权益，同时我司将承担相应责任。

（六）如我司或我司人员违反本承诺函的承诺，则贵单位有权采取以下措施中的一项或几项：

1. 要求我司立即停止侵害。

2. 暂停、中止或终止与我司的合作或我司所提供的服务，并要求我司退还已支付款项及同期存款利息。

3. 要求我司采取有效措施防止泄密范围及贵单位损失的扩大。

4. 要求我司赔偿给贵单位造成的直接和间接的损失和费用（包括但不限于律师费用、仲裁费用和执行费用等）。

5. 其他进一步追究我司法律责任的权利。

如违反上述承诺，我司愿意承担相应的法律责任。

附表：保密信息范围

XXXX公司（盖章）

\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

（多页请加盖骑缝章，如为联合体投标或代理商，原则上应由原厂商盖章）

**附表**

**保密信息范围**

|  |
| --- |
| **A.除贵单位书面表明为非保密信息外，我司从贵单位获取的所有信息及材料，不论是书面、口头、磁记录、光学记录、电子记录还是其它记录形式都属于保密信息，包括但不仅限于：**  1. 所有与贵单位的业务、经营、计划、交易、市场、财务、目前或将来拟采用的经营方式、财务、交易、信托资产等有关的不被公众领域所知的文件、资料和信息。  2．所有贵单位计算机应用系统的IT规划、软件设计方案、数据结构、设计方案、实施方案、技术细节、实现方式、设备参数配置、操作监控手段、数据加密算法、源代码、系统日志、密码本等相关信息和技术文档。  3. 所有贵单位计算机设备、网络设备、存储设备、安全设备、监控设备的参数配置、IP地址、口令、操作监控手段等相关信息；计算机主机系统和网络设备运行记录、运行报告及应急方案等。  4. 所有贵单位的生产数据、业务数据、生产经营信息及贵单位客户信息等相关信息。  5. 所有贵单位网络规划、网络架构、网络、IP地址信息及运行维护方案等相关信息。  6. 所有贵单位信息安全规划、策略、设计、实施方案等信息安全方面的相关信息。  7. 所有贵单位的工程实施文档、项目文档、管理文档等。  8. 所有贵单位及上下级单位的采购需求、采购计划及与第三方厂商签订的合作协议等信息。  9. 我司在工作过程中发现的贵单位系统、管理流程中存在的漏洞、缺陷等。  10. 我司在对贵单位进行服务时提交的工作成果。 |
| **B、贵单位的保密信息不包括：**  1. 已成为公共知识或可通过其他正当公开渠道获得的信息。  2. 我司从有权披露该信息的第三方合法获得的且我司对之不负有保密义务的信息。  3. 我司独立于本承诺函确定的保密信息而自主开发出来的文件、资料和信息。 |

附件1

附件2