天富网络安全加固及数据安全治理项目（项目名称）设备采购

（招标编号：E6608004006260393）

招标文件

招标人：新疆天富能源股份有限公司

招标代理机构：新疆生产建设兵团招标有限公司石河子分公司（电子签章）

日期：2026-03-04 13:13:52

目 录

第一章 招标公告（适用于不见面开标）

天富网络安全加固及数据安全治理项目（项目名称）天富网络安全加固及数据安全治理项目（标段名称）招标公告

一、招标条件

天富网络安全加固及数据安全治理项目已经由新疆生产建设兵团第八师发展和改革委员会以发改委备[2025]234 号文批准建设。招标人为新疆天富能源股份有限公司，设备采购所需资金来源为企业自筹。项目已具备招标条件，现对该项目的天富网络安全加固及数据安全治理项目进行公开招标。本工程拟采用资格后审方法选择合格的投标报名人参加投标。

二、项目概况与招标范围

1.招标项目所在实施地区：新疆生产建设兵团·八师

2.本次招标项目的建设地点:石河子市北一东路 2 号 52 小区天富数据中心及下属电厂关键区域

3.工程规模：对数据中心各信息系统现存漏洞开展专项加固治理，新增 4 套万兆级边界安全设备强化区域边界防护，部署数据库审计与专业防勒索设备提升风险识别、阻断及恢复能力，建设数据脱敏系统防范人员操作引发的安全风险，同时开展 2026 年天富网络安全风险评估及加固。

4.标段工程规模：

E660800400626039300l001 天富网络安全加固及数据安全治理项目，【标段工程规模】:对数据中心各信息系统现存漏洞开展专项加固治理，新增 4 套万兆级边界安全设备强化区域边界防护，部署数据库审计与专业防勒索设备提升风险识别、阻断及恢复能力，建设数据脱敏系统防范人员操作引发的安全风险，同时开展 2026 年天富网络安全风险评估及加固。

5.本次公告共划分为 1 个标段

标段编号	标段名称	招标范围	交货期
E66080040062 60393001001	天富网络安全加固及数据安全治理项目	为构建统一的数据安全管控平台，建立健全数据资产管理体系和数据安全防护体系，采购天富网络安全加固及数据安全治理项目的中新建数据治理统一定制化管控系统、威胁监测与分析系统、数据静态脱敏系统、数据库运维管控系统、数据动态脱敏系统、数据库加密系统、数据环境安保系统、数据库审计系统、数据资产梳理系统、API 审计系统、服务器密码机、加密机等**（具体详见供货要求中的技术标准和要求）**	90 日历天

三、投标人资格要求：

1. 资质要求

投标人须具有独立承担民事责任能力的法人或者其他组织，且具有合法有效的营业执照或其他有效证明文件，须提供主要设备厂商针对本项目的唯一授权（主要设备为：威胁监测与分析系统”、“数据库审计系统”、“服务器密码机”）；并具有完成本项目相适应的人员、设备、资金和项目管理能力；

2.财务要求

投标人没有处于被责令停业、投标资格被取消，没有处于财产被接管、冻结、破产状态；并提供企业近三年（2023 年至 2025 年，若 2025 年尚未完成，则提供 2022 年至 2024 年）经审定的财务审计报告，若成立不足三年的则提供自成立至今的经审定的财务审计报告，成立不足一年的提供开户行出具的银行资信证明；

3.业绩要求

投标人自 2023 年 1 月 1 日起至投标截止之日（以中标通知书签发日期或合同签订日期为准），具有类似项目业绩 2 项（证明材料：合同或中标通知书扫描件）。

4.信誉要求

（1）未被列入“信用中国”网站（www.creditchina.gov.cn）严重失信名单、经营异常；

（2）未被列入“中国执行信息公开网”网站（www.zxgk.court.gov.cn）失信被执行人；

（3）未被列入“全国企业信用信息公示系统”https://www.gsxt.gov.cn 列入经营异常名录信息、列入严重违法失信名单（黑名单）；

注：投标人须提供网络截图或信用报告或承诺书。

5.其他要求

（1）与招标人存在利害关系可能影响招标公正性的法人、其他组织或者个人，不得参加投标；

（2）单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一标段投标或者未划分标段的同一招标项目投标，否则投标无效；

（3）投标人不得存在新兵办发[2021]100 号文“兵团办公厅关于印发《新疆生产建设兵团招标投标管理办法（试行）》的通知”第十九条、第二十条予以限制的情形。

6.本项目**不接受**联合体投标。

四、招标文件的获取

1.领取时间：2026 年 8 月 5 日 00:00 至 2026 年 8 月 10 日 00：00。

2.领取方式：新疆生产建设兵团公共资源交易信息网平台下载。

五、投标须知

投投标单位须办理标证通手机移动 CA 证书或实体 CA 证书，通过“标证通”APP 扫码或插入实体 CA 证书登陆兵团公共资源交易系统进行填报入库信息；信息审核后方可进行在兵团公共资源交易系统各主体类型下领取招标文件。

具体注册事宜见兵团公共资源交易信息网通知公告《关于注册兵团公共资源交易中心交易主体信息库有关问题的说明》、《关于兵团公共资源交易平台启用“标证通”的通知》、《关于办理兵团公共资源一体化平台网上交易系统 CA 数字

证书和电子签章的通知》。

六、资格审查方式

本招标工程项目对投标申请人的资格审查采用资格后审方式，主要资格审查标准和内容详见招标文件。

本项目采用不见面开标，投标人无需递交纸质投标文件及原件，投标人在投标前应及时完善企业主体库中企业信息及扫描件（项目经理、人员、资质、业绩、财务等投标所需材料），提交并审核通过。评标时以电子投标文件及企业主体库中已通过的企业信息为准。

七、投标文件的递交

1．本项目采用不见面开标、投标人需要递交电子投标文件，无需递交纸质文件。

2．投标文件的上传/递交截止时间（投标截止时间，下同）和地点见招标文件。加密电子投标文件（.BTTF 格式）应在投标截止时间前通过兵团公共资源交易电子交易平台（https://ggzy.xjbt.gov.cn）上传完成。

3.本项目采用远程不见面交易的模式。开标当日，投标人无需到达开标现场，仅需在任意地点通过新疆生产建设兵团不见面开标系统（登录地址详见网站操作手册）完成远程解密、评标办法与系数抽取、文件传输、提疑澄清、开标唱标、结果公布等交互环节。投标人必须使用能正确解密投标文件的“标证通手机移动 CA 证书或实体 CA 证书”在规定的时间内完成远程解密，因投标人原因未能解密、解密失败或解密超时，视为投标人撤销其投标文件，系统内投标文件将被退回；因招标人原因或网上招投标平台发生故障，导致无法按时完成投标文件解密或开、评标工作无法进行的，可根据实际情况相应延迟解密时间或调整开、评标时间（友情提示：若投标人已领取副锁（含多把副锁）请注意正副锁的使用差别，务必使用生成投标文件的那把锁解密）。

4.远程开标前，投标人务必在兵团公共资源交易电子交易平台（https://ggzy.xjbt.gov.cn）投标文件上传模块中使用“模拟解密”功能，验

证本机远程自助解密环境。

5.逾期上传/送达的或者未上传/未送达指定地点的投标文件，招标人不予受理。

八、发布公告的媒介

本招标公告同时在“**新疆生产建设兵团公共资源交易信息网”和“石河子政府网”**上发布。

九、联系方式

招 标 人：新疆天富能源股份有限公司

地　　址：新疆石河子市北一东路 2 号

联 系 人：袁靖宇

电　　话：13579767251

招标代理机构：新疆生产建设兵团招标有限公司石河子分公司

地　　址：石河子市 57 小区左岸阳光 1 栋 4 单元 8 楼

联 系 人： 李艳辉、朱雪彤

电　　话：18935708511

2026 年 8 月 4 日

第二章 投标人须知

投标人须知前附表

条款号	条款名称	编列内容
1.1.2	招标人	名称：新疆天富能源股份有限公司 地址：新疆石河子市北一东路 2 号 联系人：袁靖宇 电话：13579767251
1.1.3	招标代理机构	名称：新疆生产建设兵团招标有限公司石河子分公司 地址：石河子市 57 小区左岸阳光 1 栋 4 单元 8 楼 联系人：李艳辉、朱雪彤 电话：18935708559
1.1.4	招标项目名称	天富网络安全加固及数据安全治理项目
1.1.5	工程项目名称	天富网络安全加固及数据安全治理项目
1.2.1	资金来源及比例	企业自筹 100%
1.2.2	资金落实情况	已落实
1.3.1	招标范围	为构建统一的数据安全管控平台，建立健全数据资产管理体系和数据安全防护体系，采购天富网络安全加固及数据安全治理项目的中新建数据治理统一定制化管控系统、威胁监测与分析系统、数据静态脱敏系统、数据库运维管控系统、数据动态脱敏系统、数据库加密系统、数据环境安保系统、数据库审计系统、数据资产梳理系统、API 审计系统、服务器密码机、加密机等。 **（具体详见供货要求中的技术标准和要求）**
1.3.2	交货期	自合同签订之日起 90 日历天
1.3.3	交货地点	货到招标人指定地点。
1.3.4	技术性能指标	详见第五章 供货要求
1.4.1	投标人资质条件、能力	1. 资质要求 投标人须具有独立承担民事责任能力的法人或者其他组织，且具有合法有效的营业执照或其他有效证明文件，须

条款号	条款名称	编列内容
		提供主要设备厂商针对本项目的唯一授权（主要设备为：威胁监测与分析系统”、“数据库审计系统”、“服务器密码机”）；并具有完成本项目相适应的人员、设备、资金和项目管理能力； 2.财务要求 投标人没有处于被责令停业、投标资格被取消，没有处于财产被接管、冻结、破产状态；并提供企业近三年（2023年至2025年，若2025年尚未完成，则提供2022年至2024年）经审定的财务审计报告，若成立不足三年的则提供自成立至今的经审定的财务审计报告，成立不足一年的提供开户行出具的银行资信证明； 3.业绩要求 投标人自2023年1月1日起至投标截止之日（以中标通知书签发日期或合同签订日期为准），具有类似项目业绩2项（证明材料：合同或中标通知书扫描件）。 4.信誉要求 （1）未被列入“信用中国”网站（www.creditchina.gov.cn）严重失信名单、经营异常； （2）未被列入“中国执行信息公开网”网站（www.zxgk.court.gov.cn）失信被执行人； （3）未被列入“全国企业信用信息公示系统”https://www.gsxt.gov.cn 列入经营异常名录信息、列入严重违法失信名单（黑名单）； **注：投标人须提供网络截图或信用报告或承诺书。** 5.其他要求 （1）与招标人存在利害关系可能影响招标公正性的法人、其他组织或者个人，不得参加投标； （2）单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一标段投标或者未划分标段的同一招标项目投标，否则投标无效； （3）投标人不得存在新兵办发[2021]100 号文“兵团办公厅关于印发《新疆生产建设兵团招标投标管理办法（试行）》的通知”第十九条、第二十条予以限制的情形。
1.4.2	是否接受联合体投标	☑不接受

条款号	条款名称	编列内容
		☐接受， 应满足下列要求：
1.4.3	投标人不得存在的其他情形	/
1.9.1	投标预备会	☑不召开 ☐召开 召开时间： 召开地点：
1.9.2	投标人在投标预备会前提出问题	时间：/
		形式：使用标证通手机 CA 移动证书或实体 CA 证书证书登录“兵团公共资源交易系统”，在“网上提问”菜单将提出的问题送达招标人。
1.9.3	招标文件澄清发出的形式	通过“兵团公共资源交易系统”发出招标文件澄清
1.10.1	分包	☑不允许 ☐允许
1.11.1	实质性要求和条件	满足招标文件要求
1.11.3	其他可以被接受的技术支持资料	/
1.11.4	偏差	☑不允许 ☐允许 偏差范围： 最高项数：
2.1	构成招标文件的其他资料	招标文件的修改、澄清等在新疆生产建设兵团公共资源交易信息网发布的本项目的其他信息、通知、公告
2.2.1	投标人要求澄清招标文件	时间：递交投标文件截止之日 15 日前
		形式：使用标证通手机 CA 移动证书或实体 CA 证书登录“兵团公共资源交易系统”，在“网上提问”菜单要求招标人对招标文件予以澄清。
2.2.2	招标文件澄清发出的形式	通过“兵团公共资源交易系统”发出招标文件澄清
2.2.3	投标人确认收到招标文件澄清	时间：递交投标文件截止之日 10 日前
		形式：使用标证通手机 CA 移动证书或实体 CA 证书登录“兵团公共资源交易系统”，在“网上提问”菜单要求招标人对

条款号	条款名称	编列内容
		招标文件予以澄清。
2.3.1	招标文件修改发出的形式	通过“兵团公共资源交易系统”发出招标文件修改
2.3.2	投标人确认收到招标文件修改	时间：开标截止时间前 15 日内 形式：投标人自行查看并下载最新的澄清答疑文件进行制作。否则，由投标人自行承担所造成的不良后果
3.1.1	构成投标文件的其他资料	/
3.2.1	增值税税金的计算方法	根据国家相关规定计算
3.2.4	最高投标限价	☐无 ☑有 **最高投标限价：998.00 万元（投标人投标报价高于最高投标限价的按否决投标处理。）**
3.2.5	投标报价的其他要求	以人民币的形式一次性报价
3.3.1	投标有效期	90 天
3.4.1	投标保证金	投标人应在投标截止时间前提交**壹拾捌万元**投标保证金，并确保投标保证金在投标截止时间前缴纳。 投标保证金的形式：现金或电子保函 1、以现金形式缴纳保证金的，应以电汇或转账形式汇缴至系统指定生成的保证金专用账户。 投标保证金必须以企业网银转账的形式由投标人的基本账户汇出，并汇入兵团第八师交易中心投标保证金监管专户。 中国农业银行股份有限公司石河子东苑（兵团）支行 保证金缴纳账号：新疆生产建设兵团第八师石河子市公共资源交易中心 保证金缴纳账号：下载招标文件成功后，系统会根据标段（包）自动生成对应的唯一的保证金缴款账号。投标单位根据该账号从基本户进行保证金缴纳。 **＊ 各投标单位在缴纳投标保证金时，必须由投标单位基本账户转入到平台随机生成的虚拟账户中，否则不予认可。** 注：投标单位下载招标文件后，系统会根据标段（包），自动生成对应的唯一的保证金缴纳账户（27 位账户），投标单位需先在“业务管理->保证金账户->网页右上角的《兵

条款号	条款名称	编列内容
		团公共资源电子交易平台保证金操作手册》（投标单位）”下载保证金操作手册并查看保证金缴纳的注意事项，然后由基本户足额缴纳保证金，缴纳成功后在系统中自行查询保证金入账情况。 制作电子投标文件，上传投标保证金缴纳的复印件是指： **（1）投标保证金银行汇款凭证或银行回单。** **（2）投标人基本账户开户许可证。** 2、采用电子保函形式应按以下要求办理： （1）电子保函按照“一标段一保函”的原则。 （2）电子保函须在招标文件规定的投标截止时间前办理完成。 （3）具体办理流程详见兵团公共资源交易网《关于办理电子保函操作指南》。 投标人以保函形式缴纳投标保证金的，应通过“兵团公共资源电子交易金融服务平台”，使用其标证通手机 CA 移动证书或实体 CA 证书申请购买电子投标保函。购买投标电子保函应从投标企业基本账户转出，同时将电子投标保单作为电子投标文件组成部分在投标时一并提交。 （备注：如采用电子保函形式缴纳的，在投标截止日之前须从兵团电子保函服务管理平台中确认是否生效。电子保函服务管理平台技术人员联系方式：0512-58188553；0991-8844613） 递交方式：详见 3.4
3.4.4	其他可以不予退还投标保证金的情形	1.投标人在投标有效期内撤销投标文件； 2.中标人在收到中标通知书后，无正当理由不与招标人订立合同，在签订合同时向招标人提出附加条件，或者不按照招标文件要求提交履约保证金； 3. 虚假资料 4.串标、围标等违法违规行为 5.国家相关法律法规规定的不予退还的其他情形。
3.5	资格审查资料的特殊要求	☑无 ☐有 具体要求：
3.5.2	近年财务状况的年份	详见本表 1.4.1 条款要求

条款号	条款名称	编列内容
	要求	
3.5.3	近年完成的类似项目情况的时间要求	2023 年 1 月 1 日至投标截止之日前
3.5.5	近年发生的诉讼及仲裁情况的时间要求	2023 年至 2025 年
3.6.1	是否允许递交备选投标方案	☑不允许 ☐允许
3.7.3	投标文件副本份数及其他要求	☐采用见面开标： 投标文件副本份数： 是否要求提交电子版文件： 使用兵团公共资源交易平台投标文件制作工具，制作完成需将加密投标文件在投标截止时间前上传至兵团公共资源交易平台对应位置，密封提供不加密的电子版标书（一张 U 盘和三张光盘） 其他要求： ☑采用不见面开标： 加密的电子投标文件壹份(.BTTF 格式)在兵团公共资源交易系统指定位置上传。 **其他要求：开标结束后，中标单位请将纸质版投标文件正本 1 份，副本 2 份。寄至：新疆生产建设兵团招标有限公司石河子分公司 地址：石河子市 57 小区左岸阳光 1 栋 4 单元 8 楼。** **联系人：李艳辉、朱雪彤　　联系电话：18935708511**
3.7.3	投标文件是否需分册装订	☑不需要 ☐需要 分册装订要求：
3.7.3	投标文件所附证书证件要求	按兵团公共资源交易平台及招标文件的要求提供相关证书的扫描件，模糊无法辨认评标信息的视为其未提供。
3.7.3	投标文件签字或盖章要求	投标人应在投标文件封面、投标函加盖投标人和法定代表人的电子印章及电子签名。由委托代理人签字或盖章的在投标文件中须同时提交投标文件签署授权委托书。具体生成投标文件的方法及电子签名请详见《新疆生成建设兵团

条款号	条款名称	编列内容
		公共资源交易平台》网上招投标（投标人业务）操作手册”。
4.1.1	投标文件加密要求	网上投标上传的投标文件应使用 CA 数字证书认证并加密，具体详见《新疆生成建设兵团公共资源交易平台》“网上招投标系统操作手册”。未按上述要求加密和数字证书认证的投标文件，将被视为无效投标文件，其投标文件将被拒绝，招标人不予受理。
4.1.2	封套上应载明的信息	招标人名称：新疆天富能源股份有限公司 招标人地址：新疆石河子市北一东路 2 号 项目名称：天富网络安全加固及数据安全治理项目 招标项目编号：E6608004006260393001001 在 2026 年 8 月 25 日 10 时 30 分前不得开启
4.2.1	投标截止时间	2026 年 8 月 25 日 10 时 30 分
4.2.2（A）	递交投标文件地点	加密电子投标文件（.BTTF 格式)应在投标截止时间前通过兵团公共资源交易电子交易平台(https://ggzy.xjbt.gov.cn)上传完成
4.2.3	投标文件是否退还	☑否 ☐是 退还时间：
5.1（A）	开标时间和地点	☐采用见面开标： 开标时间：同投标截止时间 开标地点： ☑采用不见面开标： 开标时间：同投标截止时间（北京时间） 开标地点：远程不见面开标大厅
5.2（4）（A）	开标程序	☐采用见面开标： 开标顺序： ☑采用不见面开标： 1.不见面开标默认解密时长：30 分钟 2.关于能否延长解密时间的约定： 开标现场若发现默认解密时长不足，由招标人决定是否延长解密时长。 本项目采用远程不见面交易的模式。开标当日，投标人无需到达开标现场，仅需在任意地点通过新疆生产建设兵团不见面开标系统（登录地址详见网站操作手册）完成远程

条款号	条款名称	编列内容
		解密、评标办法与系数抽取、文件传输、提疑澄清、开标唱标、结果公布等交互环节。投标人必须使用能正确解密投标文件的“标证通手机 CA 移动证书或实体 CA 证书”在规定的时间内完成远程解密，因投标人原因未能解密、解密失败或解密超时，视为投标人撤销其投标文件，系统内投标文件将被退回；因招标人原因或网上招投标平台发生故障，导致无法按时完成投标文件解密或开、评标工作无法进行的，可根据实际情况相应延迟解密时间或调整开、评标时间（友情提示：若投标人已领取副锁（含多把副锁）请注意正副锁的使用差别，务必使用生成投标文件的标证通过手机 CA 移动证书或实体 CA 证书解密）。
6.1.1	评标委员会的组建	评标委员会构成：5 人 其中招标人代表 0-1 人，专家 4-5 人； 评标专家确定方式：从公共资源交易平台专家库是随机抽取。
6.3.2	评标委员会推荐中标候选人的人数	3 名
7.1	中标候选人公示媒介及期限	公示媒介:“新疆生产建设兵团公共资源交易信息网”和“石河子政府网” 公示期限：3 日
7.4	是否授权评标委员会确定中标人	□是 ☑否
7.6.1	履约保证金	□是否要求中标人提交履约保证金： 要求 履约保证金的形式： 履约保证金的金额： ☑不要求
9	是否采用电子招标投标	□否 ☑是 具体要求： （1）投标文件制作工具在“新疆生产建设兵团公共资源交易信息网（https://ggzy.xjbt.gov.cn/）自行下载使用，操作使用指南均可通过网站“下载中心”下载查看。

条款号	条款名称	编列内容
		（2）第六章投标文件格式文件要求盖单位章和（或）签字的地方，投标人均应使用标证通手机 CA 移动证书或实体 CA 证书加盖投标人的单位电子签章和法定代表人的个人电子签名。 （3）电子投标文件制作完成后，将生成一份加密的电子投标文件(后缀名为.BTTF)和一份不加密的电子投标文件(后缀名为.NBTTF），在业务系统上传加密投标文件（后缀名为.BTTF)。 （4)投标人将不加密的电子投标文件复制到一张 U 盘和三张光盘中，表面粘贴“标签贴”，并将项目名称、招标编号、投标人名称等信息填写在“标签贴”上。 （5)如果投标人电子投标文件无法制作或无法导入及导出等疑问，请与国泰新点软件股份有限公司联系。 联系人：国泰新点软件股份有限公司 联系电话：0512-58188553
10	需要补充的其他内容	1.各投标单位：如为现金形式缴纳保证金的，请务必在缴纳成功后在系统中及时查询保证金入账情况， 2.场地服务费：按新发改医价【2012】832 号文执行场地服务费缴纳方式为：兵团公共资源交易信息网（电子招标投标交易平台）场地设施费缴纳中进行缴纳，不支持现金缴纳。投标企业少于 6 家（含 6 家）的，按每个投标企业每次 1000 元收取；投标企业超过 6 家（不含 6 家）的，按单个招投标项目 6000 元由投标企业平均分摊，余款退回。各投标单位在不见面开标系统中按照附件《兵团公共资源交易平台场地及设施服务费操作手册（投标单位)》在 30 分钟内将场地费交到八师公共资源交易中心，由交易中心开具场地费相关票据。场地服务费缴纳方式在开标时另行通知;缴费时须备注项目名称、缴费单位、联系人及联系方式。 3.根据招标人和招标代理机构委托代理合同的约定，本项目招标代理服务费：由中标人支付，计算基数是中标通知书中载明的中标金额,按下列费率收取，不足 4000 元按 4000 元计取。

<table>
<tr><th>条款号</th><th>条款名称</th><th>编列内容</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>序号</th><th>中标金额</th><th>收费比例</th><th>备　注</th></tr>
<tr><td>1</td><td>1 亿元以下</td><td>1.50%</td><td>工程、货物、服务</td></tr>
<tr><td>2</td><td>1-5 亿元</td><td>1.20%</td><td>工程、货物、服务</td></tr>
<tr><td>3</td><td>5-10 亿元</td><td>1.00%</td><td>工程、货物、服务</td></tr>
<tr><td>4</td><td>10 亿以上</td><td>0.80%</td><td>工程、货物、服务</td></tr>
</table>
开户名称：新疆生产建设兵团招标有限公司石河子分公司
开户银行：中国农业银行股份有限公司石河子金穗（兵团）支行
开户账号：30731501040005046
支付时间： 在发出《中标通知书》同时。
</td></tr>
<tr><td>11</td><td>特别补充</td><td>1.开标当日，投标人无需到达开标现场，仅需在任意地点通过新疆生产建设兵团不见面开标系统（登录地址详见网站操作手册)完成远程解密、答疑澄清、开标唱标、结果公布等交互环节。
2.因招标文件为电子招标文件版本，招标文件格式、内容等要求前后不一致时，以投标须知前附表为准。
3.参与“不见面”开标的投标人应当按照规定使用 CA 数字证书及电子签章。各方主体在系统中的所有操作均具有法律效力，并承担法律责任。
4.投标人参加“不见面”开标项目，应通过兵团公共资源交易“一体化”平台“不见面”系统严格按采购文件模板要求制作，在投标截止时间前完成经过 CA 数字证书电子签章并加密的交易文件上传至平台指定位置（加密和解密须用同一数字证书)。
5.投标人应在解密指令发出后采购文件规定时间内完成解密，投标人未按规定完成解密，视为放弃投标。
6.开标、评标过程中，投标人参与远程音视频交互的法定代表人或授权代理人应始终为同一人，中途不得更换，并保持在席和通讯通畅。投标人端口操作人员均视为投标人法定代表人或授权委托人，投标人自行承担随意更换人员所导致的一切后果。
7.异常情况处理依据《兵团公共资源交易“不见面”开标</td></tr>
</table>

条款号	条款名称	编列内容
		管理办法》中的规定执行。 8.因本项目为不见面电子开标，投标文件内审查的资料为原件的扫描件，清晰可辨。投标文件内漏放资料或所放的资料不清晰，自行承担评审后果。 9.招标文件的澄清将在投标人须知前附表规定的投标截止时间 15 天前澄清或修改，澄清或修改的内容不影响投标人编制投标文件的内容除外。 10.本项目不在开标现场宣布中标候选人的名单，请各投标人关注兵团公共资源交易信息网（https://ggzy.xjbt.gov.cn）和石河子政府网所发布的本项目中标候选人公示及中标结果公告，招标人及招标代理机构不再另行通知;《中华人民共和国招标投标法实施条例》第五十四条依法必须进行招标的项目，招标人应当自收到评标报告之日起 3 日内公示中标候选人，公示期不得少于 3 日。投标人或者其他利害关系人对依法必须进行招标的项目的评标结果有异议的，应当在中标候选人公示期间提出。招标人应当自收到异议之日起 3 日内作出答复；作出答复前，应当暂停招标投标活动;、《中华人民共和国招标投标法实施条例》第六十条 投标人或者其他利害关系人认为招标投标活动不符合法律、行政法规规定的，可以自知道或者应当知道之日起 10 日内向有关行政监督部门投诉。投诉应当有明确的请求和必要的证明材料。就本条例第二十二条、第四十四条、第五十四条规定事项投诉的，应当先向招标人提出异议，异议答复期间不计算在前款规定的期限内。 ★11、企业银行账户许可已取消（银发[2019]41 号），基本账户开户许可证和基本存款账户信息证明具有同等效力。

1. 总则

1.1 招标项目概况

1.1.1 根据《中华人民共和国招标投标法》、《中华人民共和国招标投标法实施条例》等有关法律、法规和规章的规定，本招标项目已具备招标条件，现对设备采购进行招标。

1.1.2 招标人：见投标人须知前附表。

1.1.3 招标代理机构：见投标人须知前附表。

1.1.4 招标项目名称：见投标人须知前附表。

1.1.5 工程项目名称：即招标项目所属的工程建设项目，见投标人须知前附表。

1.2 招标项目的资金来源和落实情况

1.2.1 资金来源及比例：见投标人须知前附表。

1.2.2 资金落实情况：见投标人须知前附表。

1.3 招标范围、交货期、交货地点和技术性能指标

1.3.1 招标范围：见投标人须知前附表。

1.3.2 交货期：见投标人须知前附表。

1.3.3 交货地点：见投标人须知前附表。

1.3.4 技术性能指标：见投标人须知前附表。

1.4 投标人资格要求

1.4.1 投标人应具备承担本招标项目资质条件、能力和信誉：

（1）资质要求：见投标人须知前附表；

（2）财务要求：见投标人须知前附表；

（3）业绩要求：见投标人须知前附表；

（4）信誉要求：见投标人须知前附表；

（5）其他要求：见投标人须知前附表。

投标人为代理经销商的，对投标人的资质要求包含对制造商的资质要求，对投标人的业绩要求包含对投标设备的业绩要求。

需要提交的相关证明材料见本章第 3.5 款的规定。

1.4.2 投标人须知前附表规定接受联合体投标的，联合体除应符合本章第 1.4.1 项和投标人须知前附表的要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体牵头人和各方权利义务，并承诺就中标项目向招标人承担连带责任；

（2）由同一专业的单位组成的联合体，按照资质等级较低的单位确定资质等级；

（3）联合体各方不得再以自己名义单独或参加其他联合体在本招标项目中投标，否则各相关投标均无效。

1.4.3 投标人不得存在下列情形之一：

（1）与招标人存在利害关系且可能影响招标公正性；

（2）与本招标项目的其他投标人为同一个单位负责人；

（3）与本招标项目的其他投标人存在控股、管理关系；

（4）与本招标项目其他投标人代理同一个制造商同一品牌同一型号的设备投标；

（5）为本招标项目提供过设计、编制技术规范和其他文件的咨询服务；

（6）为本工程项目的相关监理人，或者与本工程项目的相关监理人存在隶属关系或者其他利害关系；

（7）为本招标项目的代建人；

（8）为本招标项目的招标代理机构；

（9）与本招标项目的监理人或代建人或招标代理机构同为一个法定代表人；

（10）与本招标项目的监理人或代建人或招标代理机构存在控股或参股关系；

（11）被依法暂停或者取消投标资格；

（12）被责令停产停业、暂扣或者吊销许可证、暂扣或者吊销执照；

（13）进入清算程序，或被宣告破产，或其他丧失履约能力的情形；

（14）在最近三年内发生重大产品质量问题（以相关行业主管部门的行政处罚决定或司法机关出具的有关法律文书为准）；

（15）被工商行政管理机关在全国企业信用信息公示系统中列入严重违法失信企业名单；

（16）被最高人民法院在“信用中国”网站（www.creditchina.gov.cn）或各级信用信息共享平台中列入失信被执行人名单；

（17）法律法规或投标人须知前附表规定的其他情形。

1.5 费用承担

投标人准备和参加投标活动发生的费用自理。

1.6 保密

参与招标投标活动的各方应对招标文件和投标文件中的商业和技术等秘密保密，否则应承担相应的法律责任。

1.7 语言文字

招标投标文件使用的语言文字为中文。专用术语使用外文的，应附有中文注释。

1.8 计量单位

所有计量均采用中华人民共和国法定计量单位。

1.9 投标预备会

1.9.1 投标人须知前附表规定召开投标预备会的，招标人按投标人须知前附表规定的时间和地点召开投标预备会，澄清投标人提出的问题。

1.9.2 投标人应按投标人须知前附表规定的时间和形式将提出的问题送达招标人，以便招标人在会议期间澄清。

1.9.3 投标预备会后，招标人将对投标人所提问题的澄清，以投标人须知前附表规定的形式通知所有购买招标文件的投标人。该澄清内容为招标文件的组成部分。

1.10 分包

1.10.1 投标人拟在中标后将中标项目的非主体设备进行分包的，应符合投标人须知前附表规定的分包内容、分包金额和资质要求等限制性条件，除投标人须知前附表规定的非主体设备外，其他工作不得分包。

1.10.2 中标人不得向他人转让中标项目，接受分包的人不得再次分包。中标人应当就分包项目向招标人负责，接受分包的人就分包项目承担连带责任。

1.11 响应和偏差

1.11.1 投标文件应当对招标文件的实质性要求和条件作出满足性或更有利于招标人的响应，否则，投标人的投标将被否决。实质性要求和条件见投标人须知前附表。

1.11.2 投标人应根据招标文件的要求提供投标设备技术性能指标的详细描述、技术支持资料及技术服务和质保期服务计划等内容以对招标文件作出响应。

1.11.3 投标文件中应针对实质性要求和条件中列明的技术要求提供技术支持资料。技术支持资料以制造商公开发布的印刷资料，或检测机构出具的检测报告或投标人须知前附表允许的其他形式为准，不符合前述要求的，视为无技术支持资料，其投标将被否决。

1.11.4 投标人须知前附表规定了可以偏差的范围和最高偏差项数的，偏差应当符合投标人须知前附表规定的偏差范围和最高项数，超出偏差范围和最高偏差项数的投标将被否决。

1.11.5 投标文件对招标文件的全部偏差，均应在投标文件的商务和技术偏差表中列明，除列明的内容外，视为投标人响应招标文件的全部要求。

2. 招标文件

2.1 招标文件的组成

本招标文件包括：

（1）招标公告（或投标邀请书）；

（2）投标人须知；

（3）评标办法；

（4）合同条款及格式；

（5）供货要求；

（6）投标文件格式；

（7）投标人须知前附表规定的其他资料。

根据本章第 1.9 款、第 2.2 款和第 2.3 款对招标文件所作的澄清、修改，构成招标文件的组成部分。

2.2 招标文件的澄清

2.2.1 投标人应仔细阅读和检查招标文件的全部内容。如发现缺页或附件不全，应及时向招标人提出，以便补齐。如有疑问，应在投标人须知前附表规定的时间前通过兵团公共资源交易平台以“网上提问”方式，要求招标人对招标文件予以澄清。

2.2.2 招标文件的澄清将在投标人须知前附表规定的投标截止时间 15 天前通过兵团公共资源交易平台以答疑文件形式发给所有购买招标文件的投标人，但不指明澄清问题的来源。如果澄清发出的时间距投标截止时间不足 15 天，相应延长投标截止时间。

2.2.3 招标文件澄清发出的同时，投标人应注意及时浏览网上发出的澄清，并登录平台查

看具体澄清内容，因投标人自身原因未及时获知澄清内容而导致的任何后果将由投标人自行承担。

2.3 招标文件的修改

2.3.1 在投标截止时间 15 天前，招标人可以通过网上制作答疑文件形式修改招标文件，并以公告形式通知所有已购买招标文件的投标人。如果修改招标文件的时间距投标截止时间不足 15 天，相应延长投标截止时间。招标文件修改发出的同时，投标人应注意及时浏览网上发出的修改，并登录平台下载答疑澄清文件来制作最新的投标文件，因投标人自身原因未及时获知澄清内容而导致的任何后果将由投标人自行承担。

2.3.2 投标人收到修改内容后，应按投标人须知前附表规定的时间和形式通知招标人，确认已收到该修改。

2.4 招标文件的异议

投标人或其他利害关系人对招标文件有异议的，应在投标截止时间 10 日前登录“兵团公共资源交易系统”通过“网上提问”菜单提出。招标人将在收到异议之日起 3 日内登录“兵团公共资源交易系统”在“提问回复”菜单作出答复；作出答复前，将暂停招标投标活动。

3. 投标文件

3.1 投标文件的组成

3.1.1 投标文件应包括下列内容：

（1）投标函；

（2）法定代表人（单位负责人）身份证明或授权委托书；

（3）联合体协议书；

（4）投标保证金；

（5）商务和技术偏差表；

（6）分项报价表；

（7）资格审查资料；

（8）投标设备技术性能指标的详细描述；

（9）技术支持资料；

（10）技术服务和质保期服务计划；

（11）投标人须知前附表规定的其他资料。

投标人在评标过程中作出的符合法律法规和招标文件规定的澄清确认，构成投标文件的组成部分。

3.1.2 投标人须知前附表规定不接受联合体投标的，或投标人没有组成联合体的，投标文件不包括本章第 3.1.1（3）目所指的联合体协议书。

3.1.3 投标人须知前附表未要求提交投标保证金的，投标文件不包括本章第 3.1.1（4）目所指的投标保证金。

3.2 投标报价

3.2.1 投标报价应包括国家规定的增值税税金，除投标人须知前附表另有规定外，增值税税金按一般计税方法计算。投标人应按第六章“投标文件格式”的要求在投标函中进行报价并填写分项报价表。

3.2.2 投标人应充分了解该项目的总体情况以及影响投标报价的其他要素。

3.2.3 投标报价为各分项报价金额之和，投标报价与分项报价的合价不一致的，应以各分项合价累计数为准，修正投标报价；如分项报价中存在缺漏项，则视为缺漏项价格已包含在其他分项报价之中。投标人在投标截止时间前修改投标函中的投标报价总额，应同时修改投标文件“分项报价表”中的相应报价。此修改须符合本章第 4.3 款的有关要求。

3.2.4 招标人设有最高投标限价的，投标人的投标报价不得超过最高投标限价，最高投标限价在投标人须知前附表中载明。

3.2.5 投标报价的其他要求见投标人须知前附表。

3.3 投标有效期

3.3.1 除投标人须知前附表另有规定外，投标有效期为 90 天。

3.3.2 在投标有效期内，投标人撤销投标文件的，应承担招标文件和法律规定的责任。

3.3.3 出现特殊情况需要延长投标有效期的，招标人通过兵团公共资源交易平台变更公告形式通知所有投标人延长投标有效期。投标人同意延长的，应相应延长其投标保证金的有效期，但不得要求或被允许修改或撤销其投标文件；投标人拒绝延长的，其投标失效，但投标人有权收回其投标保证金。

3.4 投标保证金

3.4.1 投标人在递交投标文件的同时，应按投标人须知前附表规定的金额、形式和第六章“投标文件格式”规定的投标保证金格式递交投标保证金，并作为其投标文件的组成部分。境内投标人以现金或者支票形式提交的投标保证金，应当从其基本账户转出并在投标文件中附上基本账户开户证明。联合体投标的，其投标保证金可以由牵头人递交，并应符合投标人须知前附表的规定。

3.4.2 投标人不按本章第 3.4.1 项要求提交投标保证金的，评标委员会将否决其投标。

3.4.3 招标人最迟将在与中标人签订合同后 5 日内，向未中标的投标人和中标人退还投标保证金。投标保证金以现金或者支票形式递交的，还应退还银行同期存款利息。

3.4.4 有下列情形之一的，投标保证金将不予退还：

（1）投标人在投标有效期内撤销投标文件；

（2）中标人在收到中标通知书后，无正当理由不与招标人订立合同，在签订合同时向招标人提出附加条件，或者不按照招标文件要求提交履约保证金；

（3）发生投标人须知前附表规定的其他可以不予退还投标保证金的情形。

3.4.5 如开标时投标人对本单位投标保证金缴纳情况有疑义，投标人应在开标结束前向招标人提交书面申请核实保证金缴纳情况。由银行或保险公司核实后出具书面材料予以答复。

3.4.6 开标结束后，转账、电汇、网银形式缴纳的保证金由招标代理或招标人统一办理中标人和未中标人的保证金退还事宜。如本项目招标中遇质疑，投诉，复议等特殊情况，保证金退还时间按相关规定执行。银行电子保函、保险电子保函形式缴纳的投标保证金按协议执行，无需办理退款手续。

3.4.7 电子保函的应急措施

开标时电子保函系统，若出现下列原因，导致电子保函无法正常使用，应采取应急措施。

（1）开标时，系统获取明文保函文件异常，无法正常获取保函文件；

（2）金融机构/电子保函系统的软件或数据库出现错误，不能进行正常操作；

（3）金融机构/电子保函服务器发生故障或停电等情况，无法访问或无法使用电子保函；

（4）金融机构/电子保函服务器受到病毒或其他外来的攻击；

（5）其他影响电子保函出具的异常情形。

具体措施：

（1）出现上述情况，应通过交易中心、平台系统维护方以及金融保函机构核实原因。若投标人提交有效电子保函购买相关凭证或证明材料，且经招标人、代理机构确认同意后，可以继续进行开标。

（2）若投标人无法出具有效电子保函购买相关凭证或证明材料，则招标人可在开标时当场拒收其投标，不得进入评标。

3.4.8 企业可以以银行转账、电汇、电子保函及纸质保函的方式缴纳投标保证金、履约保证金、工程质量保证金、农民工工资保证金，任何单位和部门不得排斥、限制或拒绝。

3.5 资格审查资料（适用于已进行资格预审的）

投标人在递交投标文件前，发生可能影响其投标资格的新情况的，应更新或补充其在申请资格预审时提供的资料，以证实其各项资格条件仍能继续满足资格预审文件的要求，且没有实质性降低。

3.5 资格审查资料（适用于未进行资格预审的）

除投标人须知前附表另有规定外，投标人应按下列规定提供资格审查资料，以证明其满足本章第 1.4 款规定的资质、财务、业绩、信誉等要求。

3.5.1 “投标人基本情况表”应附投标人及其制造商（适用于代理经销商投标的情形）资格或者资质证书副本和投标材料检验或认证等材料的复印件以及：

（1）投标人为企业的，应提交营业执照和组织机构代码证的复印件（按照“三证合一”或“五证合一”登记制度进行登记的，可仅提供营业执照复印件）；

（2）投标人为依法允许经营的事业单位的，应提交事业单位法人证书和组织机构代码证的复印件。

3.5.2 “近年财务状况表”应附经会计师事务所或审计机构审计的财务会计报表，包括资产负债表、现金流量表、利润表和财务情况说明书的复印件，具体年份要求见投标人须知前附表。投标人的成立时间少于投标人须知前附表规定年份的，应提供成立以来的财务状况表。

3.5.3 “近年完成的类似项目情况表”应附中标通知书和（或）合同协议书、设备进场验收证书等的复印件，具体时间要求见投标人须知前附表。每张表格只填写一个项目，并标明序号。

3.5.4 “正在供货和新承接的项目情况表”应附中标通知书和（或）合同协议书复印件。每张表格只填写一个项目，并标明序号。

3.5.5 “近年发生的诉讼及仲裁情况”应说明投标人败诉的设备买卖合同的相关情况，并附法院或仲裁机构作出的判决、裁决等有关法律文书复印件，具体时间要求见投标人须知前附表。

3.5.6 投标人须知前附表规定接受联合体投标的，本章第 3.5.1 项至第 3.5.5 项规定的表

格和资料应包括联合体各方相关情况。

3.6 备选投标方案

3.6.1 除投标人须知前附表规定允许外，投标人不得递交备选投标方案，否则其投标将被否决。

3.6.2 允许投标人递交备选投标方案的，只有中标人所递交的备选投标方案方可予以考虑。评标委员会认为中标人的备选投标方案优于其按照招标文件要求编制的投标方案的，招标人可以接受该备选投标方案。

3.6.3 投标人提供两个或两个以上投标报价，或者在投标文件中提供一个报价，但同时提供两个或两个以上供货方案的，视为提供备选方案。

3.7 投标文件的编制

3.7.1 投标文件应按第六章“投标文件格式”进行编写，如有必要，可以增加附页，作为投标文件的组成部分。

3.7.2 投标文件应当对招标文件有关供货期、投标有效期、供货要求、招标范围等实质性内容作出响应。投标文件在满足招标文件实质性要求的基础上，可以提出比招标文件要求更有利于招标人的承诺。

3.7.3 投标文件的制作应满足以下规定：

（1）投标文件由投标人自行在“新疆生产建设兵团公共资源交易信息网（https://ggzy.xjbt.gov.cn/）下载使用“兵团公共资源交易平台投标文件制作工具”制作生成投标文件。

（2）投标人在编制投标文件时应建立分级目录，并按照标签提示导入相关内容。

（3）投标文件中证明资料的“复印件”均为“原件的扫描件”，应以附件形式直接导入，未标示“复印件”的证明资料均应直接制作生成。

（4）投标文件中的已标价报价清单数据文件应与招标人提供的报价清单数据文件格式一致。

（5）第六章“投标文件格式”中要求盖单位章和（或）签字的地方，投标人均应使用标证通手机 CA 移动证书或实体 CA 证书加盖投标人的单位电子印章和（或）法定代表人的个人电子印章或电子签名章。联合体投标的，投标文件由联合体牵头人按上述规定加盖联合体牵头人单位电子印章和（或）法定代表人的个人电子印章或电子签名章。

（6）投标文件制作完成后，投标人应使用标证通手机 CA 移动证书或实体 CA 证书对投标文件进行文件加密，形成加密的投标文件。

（7）电子投标文件使用兵团公共资源交易平台提供的投标文件制作工具以及招标文件要求进行制作编制。投标文件制作时，将招标文件导入制作工具中，按照招标文件中明确的投标文件目录和格式进行编制，保证目录清晰、内容完整。投标文件制作的具体方法详见新疆生产建设兵团公共资源交易中心信息网-下载中心-操作手册。

3.7.4 电子招投标文件具有法律效力，与其他形式的招投标文件在内容和格式上等同，若投标文件与招标文件要求不一致，其内容影响中标结果时，责任由投标人自行承担。投标人递交的电子投标文件因投标人自身原因而导致无法导入电子辅助评标系统，该投标文件视为无效投标文件，将导致其投标被拒绝。

3.7.5 使用兵团公共资源交易平台投标文件制作工具，电子投标文件制作工具在生成加密投标文件时，同时生成非加密投标文件一份，制作完成需将加密投标文件在投标截止时间前上传至兵团公共资源交易平台对应位置，密封提供不加密的电子版标书（一张 U 盘和三张光盘）和纸质版投标文件，具体其他要求见投标人须知前附表。

是否采用不见面开标详见投标人须知前附表，若采用不见面开标方式只需加密的电子投标文件壹份（.BTTF 格式，在会员系统指定位置上传）。

3.7.6（1）投标文件应用不褪色的材料书写或打印，投标函及对投标文件的澄清、说明和补正应由投标人的法定代表人（单位负责人）或其授权的代理人签字或盖单位章。由投标人的法定代表人（单位负责人）签字的，应附法定代表人（单位负责人）身份证明，由代理人签字的，应附授权委托书，身份证明或授权委托书应符合第六章“投标文件格式”的要求。投标文件应尽量避免涂改、行间插字或删除。如果出现上述情况，改动之处应由投标人的法定代表人（单位负责人）或其授权的代理人签字或盖单位章。

（2）投标文件正本一份，副本份数见投标人须知前附表。正本和副本的封面右上角上应清楚地标记“正本”或“副本”的字样。投标人应根据投标人须知前附表要求提供电子版文件。

（3）投标文件的正本与副本应分别装订，并编制目录，投标文件需分册装订的，具体分册装订要求见投标人须知前附表规定。

4. 投标

4.1 投标文件的密封和标记

4.1.1 投标人应当按照招标文件和电子招标投标交易平台的要求加密投标文件，具体要求见投标人须知前附表。（若需投标文件应密封包装，并在封套的封口处加盖投标人单位章或由投标人的法定代表人或其授权的代理人签字）

4.1.2 投标文件封套上应写明的内容见投标人须知前附表。

4.1.3 未按本章第 4.1.1 项要求密封的投标文件，招标人将予以拒收。

4.1.4 是否采用不见面开标方式详见投标人须知前附表，若本项目采用不见面开标，无需提供电子投标文件 U 盘、纸质投标文件。

4.2 投标文件的递交

4.2.1 投标人应在投标人须知前附表规定的投标截止时间前递交投标文件。

4.2.2 投标人通过下载招标文件的电子招标投标交易平台递交电子投标文件。投标人应在第一章“招标公告”或“投标邀请书”规定的投标截止时间前，通过互联网使用标证通手机 CA 移动证书或实体 CA 证书登录“兵团公共资源交易系统”，将加密的投标文件上传。投标人应充分考虑上传文件时的不可预见因素，未在投标截止时间前完成上传的，视为逾期送达，招标人（兵团公共资源交易系统）将拒绝接收。

4.2.3 除投标人须知前附表另有规定外，投标人所递交的投标文件不予退还。

4.2.4 逾期送达的投标文件，电子招标投标交易平台将予以拒收。

4.2.5 是否采用不见面开标方式详见投标人须知前附表，若采用不见面开标，各投标人应在投标截止时间前上传加密的电子投标文件（*.BTTF 格式）到兵团公共资源交易系统的指定位置。上传时必须得到电脑“上传成功”的确认回复后方为上传成功。请投标人在上传前务必认真检查上传投标文件是否完整、正确。

4.3 投标文件的修改与撤回

4.3.1 在本章第 4.2.1 项规定的投标截止时间前，投标人可以修改或撤回已递交的投标文件。投标人对加密的投标文件进行撤回的，应在“兵团公共资源交易系统”直接进行撤回操作（撤回流程为使用本单位标证通手机 CA 移动证书扫描二维码或插入实体 CA 证书，在上传投标

文件界面点击撤回投标文件，然后输入标证通手机 CA 移动证书或实体 CA 证书密码即可）；投标人对加密的投标文件进行修改的，应在投标截止时间前完成上传。

4.3.2 投标人修改投标文件的，应使用“投标文件制作工具”制作成完整的投标文件，并按照本章第 3 条、第 4 条规定进行编制、加密和递交。对采用网上递交的加密的投标文件，以投标截止时间前最后完成上传的文件为准。

5. 开标

5.1 开标时间和地点

A.招标人在本章第 4.2.1 项规定的投标截止时间（开标时间）,通过电子招标投标交易平台公开开标，所有投标人的法定代表人（单位负责人）或其委托代理人应当准时参加。

B. 采用不见面开标方式（是否采用详见投标人须知前附表）

招标人在本章第 4.2.1 项规定的投标截止时间（开标时间）和投标人须知前附表规定的地点开标。投标人的法定代表人或其委托代理人无需到达开标现场，仅需在任意地点通过新疆生产建设兵团不见面开标系统，使用标证通手机 CA 移动证书或实体 CA 证书完成远程解密、评标办法与系数抽取、文件传输、提疑澄清、开标唱标、结果公布等交互环节。

法定代表人或法定代表人授权委托人参与远程交互，中途不得更换，在废标、澄清、提疑、传送文件等特殊情况下需要交互时，投标人一端参与交互的人员将均被视为是投标人的授权委托人或法人代表，投标人不得以不承认交互人员的资格或身份等为借口推脱，投标人自行承担随意更换人员所导致的一切后果。

5.2 开标程序

主持人按下列程序进行开标：

A. 采用见面开标方式

（1）宣布开标纪律；

（2）公布在投标截止时间前递交投标文件的投标人名称；

（3）宣布开标人、唱标人、记录人、监标人等有关人员姓名；

（4）投标人通过电子招标投标交易平台对已递交的电子投标文件进行解密，公布招标项目名称、投标人名称、投标保证金的递交情况、投标报价、交货期、交货地点及其他内容，并记

录在案；

（5）投标人代表、招标人代表、监标人、记录人等有关人员使用本人的电子印章在开标记录上签字确认；

（6）开标结束。

开标补救措施

5.2.1 开标过程中因本章第 5.2.2 项、第 5.2.3 项所列原因，导致开标无法正常进行，应采取补救措施。

5.2.2 投标人在投标截止时间前已经成功上传加密投标文件（.bttf），由于系统故障导致无法解密时，允许使用光盘/U 盘导入非加密投标文件。当出现下列情形之一，导致无法解密文件时，投标文件应予以退回：

（1）投标人开标现场未携带标证通手机 CA 移动证书或实体 CA 证书导致无法解密投标文件的；

（2）投标人开标现场携带的标证通手机 CA 移动证书或实体 CA 证书与加密投标文件的标证通手机 CA 移动证书或实体 CA 证书不一致的；

（3）投标人解密时标证通手机 CA 移动证书或实体 CA 证书已过期的；

（4）加密投标文件时，标证通手机 CA 移动证书或实体 CA 证书未过期，因开标前进行标证通手机 CA 移动证书或实体 CA 证书延期导致开标现场无法解密的；

（5）投标人个人原因导致无法解密的其他情形

上述无法解密之外的情形，需结合开标现场，依据行政主管部门的意见来定。

5.2.3 当出现以下情况时，应对未开标的中止电子开标，并在恢复正常后及时安排时间开标：

（1）系统服务器发生故障，无法访问或无法使用系统；

（2）系统的软件或数据库出现错误，不能进行正常操作；

（3）系统发现有安全漏洞，有潜在的泄密危险；

（4）出现断电事故且短时间内无法恢复供电；

（5）其他无法保证招投标过程正常进行的情形。

5.2.4 采取补救措施时，必须对原有资料及信息作出妥善保密处理。

B．采用不见面开标方式，（是否采用详见投标人须知前附表）

本工程采用远程不见面电子开标。投标截止时间到达后，各投标人按时对电子投标文件进行解密。解密完成后各投标人的电子投标文件的实质性内容将自动显示在网页中。投标人在投标截止时间前未上传电子投标文件的将被视为放弃投标。

主持人按下列程序进行开标：

（1）宣布投标截止时间已到，不再接收投标文件；

（2）宣布开标纪律；

（3）宣布开标人、监标人等有关人员姓名；

（4）公布投标人名单；

（5）电子投标文件解密；

（6）电子唱标并记录在案；

（7）由主持人启动抽取评标 K 值程序；（如需要抽取 K 值）

（8）招标人代表在开标记录上签字确认；

（9）开标结束。

5.2.5 开标时出现下列情况的，招标人将拒绝其投标文件。

（1）经检查数字证书无效的投标文件；

（2）投标人未按投标人须知表 5.1 项规定的时间内因投标人自身原因，导致电子投标文件无法解密的；

（3）投标人在投标须知前附表规定时长内未解密完成的，按未按时参加开标会处理。

5.3 开标异议

投标人对开标有异议的，应当在开标现场提出，招标人当场作出答复，并制作记录。

6. 评标

6.1 评标委员会

6.1.1 评标由招标人依法组建的评标委员会负责。评标委员会由招标人或其委托的招标代理机构熟悉相关业务的代表，以及有关技术、经济等方面的专家组成。评标委员会成员人数以及技术、经济等方面专家的确定方式见投标人须知前附表。

6.1.2 评标委员会成员有下列情形之一的，应当回避：

（1）投标人或投标人主要负责人的近亲属；

（2）项目主管部门或者行政监督部门的人员；

（3）与投标人有经济利益关系，可能影响对投标公正评审的；

（4）曾因在招标、评标以及其他与招标投标有关活动中从事违法行为而受过行政处罚

或刑事处罚的；

（5）与投标人有其他利害关系。

6.1.3 评标过程中，评标委员会成员有回避事由、擅离职守或者因健康等原因不能继续评标的，招标人有权更换。被更换的评标委员会成员作出的评审结论无效，由更换后的评标委员会成员重新进行评审。

6.2 评标原则

评标活动遵循公平、公正、科学和择优的原则。

6.3 评标

6.3.1 评标委员会按照第三章“评标办法”规定的方法、评审因素、标准和程序对投标文件进行评审。第三章“评标办法”没有规定的方法、评审因素和标准，不作为评标依据。

6.3.2 评标完成后，评标委员会应当向招标人提交书面评标报告和中标候选人名单。评标委员会推荐中标候选人的人数见投标人须知前附表。

6.3.3 评标及补救措施

评标委员会按照本章第 6.3.1 项的规定在电子评标系统上开展评审工作。如果评标过程中出现异常情况，导致无法继续评审工作的，可暂停评标，对原有资料及信息作出妥善保密处理，待电子评标系统恢复正常之后，应重新组织评审。

7. 合同授予

7.1 中标候选人公示

招标人在收到评标报告之日起 3 日内，按照投标人须知前附表规定的公示媒介和期限公示中标候选人，公示期不得少于 3 天。

7.2 评标结果异议

投标人或者其他利害关系人对评标结果有异议的，应当在中标候选人公示期间提出。招标人将在收到异议之日起 3 日内作出答复；作出答复前，将暂停招标投标活动。

7.3 中标候选人履约能力审查

中标候选人的经营、财务状况发生较大变化或存在违法行为，招标人认为可能影响其履约能力的，将在发出中标通知书前提请原评标委员会按照招标文件规定的标准和方法进行审查确认。

7.4 定标

按照投标人须知前附表的规定，招标人或招标人授权的评标委员会依法确定中标人。

7.5 中标通知

在本章第 3.3 款规定的投标有效期内，招标人以书面形式向中标人发出中标通知书，同时将中标结果通知未中标的投标人。

7.6 履约保证金

7.6.1 在签订合同前，中标人应按投标人须知前附表规定的形式、金额和招标文件第四章“合同条款及格式”规定的或者事先经过招标人书面认可的履约保证金格式向招标人提交履约保证金。除投标人须知前附表另有规定外，履约保证金为中标合同金额的 10%。联合体中标的，其履约保证金以联合体各方或者联合体中牵头人的名义提交。

7.6.2 中标人不能按本章第 7.6.1 项要求提交履约保证金的，视为放弃中标，其投标保证金不予退还，给招标人造成的损失超过投标保证金数额的，中标人还应当对超过部分予以赔偿。

7.6.3 企业可以以银行转账、电汇、电子保函及纸质保函的方式缴纳履约保证金，任何单位和部门不得排斥、限制或拒绝。

7.7 签订合同

7.7.1 招标人和中标人应当在中标通知书发出之日起 30 日内，根据招标文件和中标人的投标文件订立书面合同。中标人无正当理由拒签合同，在签订合同时向招标人提出附加条件，或者不按照招标文件要求提交履约保证金的，招标人有权取消其中标资格，其投标保证金不予退还；给招标人造成的损失超过投标保证金数额的，中标人还应当对超过部分予以赔偿。

7.7.2 发出中标通知书后，招标人无正当理由拒签合同，或者在签订合同时向中标人提出

附加条件的，招标人向中标人退还投标保证金；给中标人造成损失的，还应当赔偿损失。

7.7.3 联合体中标的，联合体各方应当共同与招标人签订合同，就中标项目向招标人承担连带责任。

8.纪律和监督

8.1 对招标人的纪律要求

招标人不得泄露招标投标活动中应当保密的情况和资料，不得与投标人串通损害国家利益、社会公共利益或者他人合法权益。

8.2 对投标人的纪律要求

投标人不得相互串通投标或者与招标人串通投标，不得向招标人或者评标委员会成员行贿谋取中标，不得以他人名义投标或者以其他方式弄虚作假骗取中标；投标人不得以任何方式干扰、影响评标工作。

8.3 对评标委员会成员的纪律要求

评标委员会成员不得收受他人的财物或者其他好处，不得向他人透露对投标文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。在评标活动中，评标委员会成员应当客观、公正地履行职责，遵守职业道德，不得擅离职守，影响评标程序正常进行，不得使用第三章“评标办法”没有规定的评审因素和标准进行评标。

8.4 对与评标活动有关的工作人员的纪律要求

与评标活动有关的工作人员不得收受他人的财物或者其他好处，不得向他人透露对投标文件的评审和比较、中标候选人的推荐情况以及评标有关的其他情况。在评标活动中，与评标活动有关的工作人员不得擅离职守，影响评标程序正常进行。

8.5 投诉

8.5.1 投标人或者其他利害关系人认为招标投标活动不符合法律、行政法规规定的，可以自知道或者应当知道之日起 10 日内向有关行政监督部门投诉。投诉应当有明确的请求和必要的证明材料。

8.5.2 投标人或者其他利害关系人对招标文件、开标和评标结果提出投诉的，应当按照投标人须知第 2.4 款、第 5.3 款和第 7.2 款的规定先向招标人提出异议。异议答复期间不计算在第 8.5.1 项规定的期限内。

9. 是否采用电子招标投标

本招标项目是否采用电子招标投标方式，见投标人须知前附表。

10. 需要补充的其他内容

需要补充的其他内容：见投标人须知前附表。

第三章 评标办法（综合评估法）

评标办法前附表

条款号		评审因素	评审标准
1	评标方法	中标候选人排序方法	
2.1.1	形式评审标准	投标人名称	与营业执照、资质证书一致
		投标函签字盖章	有法定代表人（单位负责人）或其委托代理人签字或加盖单位章。由法定代表人（单位负责人）签字的，应附法定代表人（单位负责人）身份证明，由代理人签字的，应附授权委托书，身份证明或授权委托书应符合第六章“投标文件格式”的规定
		投标文件格式	符合第六章“投标文件格式”的规定
		备选投标方案	除招标文件明确允许提交备选投标方案外，投标人不得提交备选投标方案
2.1.2	资格评审标准	营业执照和组织机构代码证	符合第二章“投标人须知”第 3.5.1 项规定，具备有效的营业执照和组织机构代码证
		资质要求	符合第二章“投标人须知”第 1.4.1 项规定
		财务要求	符合第二章“投标人须知”第 1.4.1 项规定
		业绩要求	符合第二章“投标人须知”第 1.4.1 项规定
		信誉要求	符合第二章“投标人须知”第 1.4.1 项规定
		其他要求	符合第二章“投标人须知”第 1.4.1 项规定
		不存在禁止投标的情形	不存在第二章“投标人须知”第 1.4.3 项规定的任何一种情形
		投标设备制造商的资质要求（如有）	符合第二章“投标人须知”第 1.4.1 项规定
		投标设备的业绩要求（如有）	符合第二章“投标人须知”第 1.4.1 项规定
2.1.3	响 应 性	投标报价	符合第二章“投标人须知”第 3.2 款规定

	评审标准	投标内容	符合第二章“投标人须知”第 1.3.1 项规定
		交货期	符合第二章“投标人须知”第 1.3.2 项规定
		交货地点	符合第二章“投标人须知”第 1.3.3 项规定
		技术性能指标	符合第二章“投标人须知”第 1.3.4 项规定
		投标有效期	符合第二章“投标人须知”第 3.3.1 项规定
		投标保证金	符合第二章“投标人须知”第 3.4.1 项规定
		权利义务	符合第二章“投标人须知”第 1.11.1 项规定和第四章“合同条款及格式”中的实质性要求和条件
		投标设备及技术服务和质保期服务	符合第五章“供货要求”中的实质性要求和条件
		技术支持资料	符合第二章“投标人须知”第 1.11.3 项规定
条款号		**条款内容**	**编列内容**
2.2.1		分值构成(总分 100.00 分)	商务部分：30.00 分 技术部分：40.00 分 投标报价：30.00 分 其他评分因素：.00 分

2.2.2	评标基准价计算方法	有效投标报价少于等于 5 家直接取平均值作为评标基准价，大于 5 家少于 10 家（含 10 家）去掉一个最高一个最低取平均值作为评标基准价，大于 10 家去掉两个最高一个最低取平均值作为评标基准价。
2.2.3	投标报价的偏差率计算公式	偏差率=（投标报价-评标基准价）/评标基准价*100%，百分率计算结果保留小数点后两位，小数点后第三位四舍五入。

条款号	评分因素（偏差率）		**评分标准**
2.2.4(1)	商务评分标准	企业综合实力（0.0-6.0）	1.具有 CMMI 认证证书(三级及以上)资质的得 1.5 分； 2.具有 ITSS 信息技术服务运行维护标准证书（三级及以上）资质的得 1.5 分； 3.具有有效的 ISO27001 信息安全管理体系证证书的得 1.5 分； 4.具有有效的 ISO20000 信息技术服务管理体系认证证书的得 1.5 分；

			（注：须提供证书复印件或官网查询截图，并加盖投标人公章，未提供者不得分）
		项目业绩（0.0-6.0）	在满足招标文件要求的基础上，每增加一项类似项目业绩得 1.5 分，满分 6 分。 注：须提供证明文件（合同或中标通知书扫描件）
		项目实施能力（0.0-18.0）	拟投入本项目项目团队人员中： 1.具有高级信息系统项目管理师证书的，每有一人得 3 分，本项最高得 6 分； 2.具有高级系统分析师证书的，每有一人得 3 分，本项最高得 3 分； 3.具有注册信息安全工程师证书(CISE)的，每有一人得 3 分，本项最高得 6 分； 4.具有网络工程师证书的，每有一人得 3 分，本项最高得 3 分。 注：1、投标人拟投入本项目所有人员须为本单位在职人员，须提供上述证书复印件加盖公章及由本单位缴纳连续三个月（2026 年 1 月至 3 月）社会保险缴费记录复印件加盖公章（材料二者缺一不可），未提供或提供不全或提供评委不认可的，不得分。 2、如同一人有多个证书，不重复计分，评审时只计取一次。
2.2.4(2)	技术评分标准	主要产品配置及技术参数（0.0-26.0）	根据投标人的产品质量、性能对招标文件的响应程度进行打分：全部提供且符合要求得 26 分，第五章供货要求的“5.3 产品类技术参数要求”和“5.4 平台测试仿真配套资源”中标★参数和要求一项不符合扣 2 分(须提供产品功能页面截图，未提供不得分)。须按照招标文件要求提供相关证明文件或功能截图。中标后要进行功能验证，若发现虚假应标将取消中标资格并自行承担相应后果。
		供货进度计划安排（0.0-3.0）	进度满足要求，安排合理，并且有提前的进度计划，得 3 分；进度满足要求，安排基本合理，无提前的进度计划，得 2 分；进度满足要求，安排不合理，无提前的进度计划，酌情给分。
		售后及培训（0.0-5.0）	1、售后服务方案内容完整，并有具体可行的服务措施，具备详细的培训方案和计划，培训形式多样，可以提供全面的培训教材，所配备的培训人员，具有丰富的培训经验得 3-5 分；

			2、售后服务方案内容简单、粗略，无具体保证措施和方法，售后人员无法 2 小时内到达现场， 培训方案、计划和教材，但内容简单、不够全 面，配备培训人员缺乏专业和实践经验，得 1-2 分。 3、该项内容未进行描述的，得 0 分。
		投标货物的先进性、可靠性、经济实用性和可信度（0.0-3.0）	设备的功能性、整体配套性、经济实用性、先进性、稳定性是否最佳化。设备的选材是否符合或优于招标文件技术要求。全部符合或优于得 3 分，否则酌情扣分。
		售后技术实施保障（0.0-3.0）	投标人承诺：在本项目实施过程中，如涉及与招标人现有应用系统（含营销系统、财务系统等）的对接工作，投标人无条件免费配合调试，直至系统稳定运行，所有对接相关的开发、协调、测试、人工等成本均由投标人自行承担，招标人不再另行支付费用。提供加盖公章的承诺函，且承诺内容完整、明确，得 3 分；未提供承诺函，或承诺内容不完整、不明确的，得 0 分。
2.2.4(3)	投标报价评分标准	投标报价（0.0-30.0）	当投标报价大于基准价时，按偏差率每 1%扣 0.5 分，得分=30-0.5*|（投标报价-评标基准价）|/评标基准价×100； 当投标报价小于基准价时，按偏差率每 1%扣 0.1 分，得分=30-0.1*|（投标报价-评标基准价）|/评标基准价×100； 报价得分等于基准价时，得 30 分。
废标条款		1、投标文件没有对招标文件的实质性要求和条件作出响应，或者对招标文件的偏差超出招标文件规定的偏差范围或最高项数； 2、有串通投标、弄虚作假、行贿等违法行为。	

1. 评标方法

本次评标采用综合评估法。评标委员会对满足招标文件实质性要求的投标文件，按照本章第 2.2 款规定的评分标准进行打分，并按得分由高到低顺序推荐中标候选人，或根据招标人授权直接确定中标人，但投标报价低于其成本的除外。综合评分相等时，以投标报价低的优先；投标报价也相等的，以技术得分高的优先；如果技术得分也相等，按照评标办法前附表的规定确定中标候选人顺序。

2. 评审标准

2.1 初步评审标准

2.1.1 形式评审标准：见评标办法前附表。

2.1.2 资格评审标准：见评标办法前附表。

2.1.3 响应性评审标准：见评标办法前附表。

2.2 分值构成与评分标准

2.2.1 分值构成

（1）商务部分：见评标办法前附表；

（2）技术部分：见评标办法前附表；

（3）投标报价：见评标办法前附表；

（4）其他评分因素：见评标办法前附表。

2.2.2 评标基准价计算

评标基准价计算方法：见评标办法前附表。

2.2.3 投标报价的偏差率计算

投标报价的偏差率计算公式：见评标办法前附表。

2.2.4 评分标准

（1）商务评分标准：见评标办法前附表；

（2）技术评分标准：见评标办法前附表；

（3）投标报价评分标准：见评标办法前附表；

（4）其他因素评分标准：见评标办法前附表。

3. 评标程序

3.1 初步评审

3.1.1 评标委员会可以要求投标人提交第二章“投标人须知”规定的有关证明和证件的原件，以便核验。评标委员会依据本章第 2.1 款规定的标准对投标文件进行初步评审。有一项不符合评审标准的，评标委员会应当否决其投标。

3.1.2 投标人有以下情形之一的，评标委员会应当否决其投标：

1、投标文件没有对招标文件的实质性要求和条件作出响应，或者对招标文件的偏差超出招标文件规定的偏差范围或最高项数；

2、有串通投标、弄虚作假、行贿等违法行为。

3.1.3 投标报价有算术错误及其他错误的，评标委员会按以下原则要求投标人对投标报价进行修正，并要求投标人书面澄清确认。投标人拒不澄清确认的，评标委员会应当否决其投标：

（1）投标文件中的大写金额与小写金额不一致的，以大写金额为准；

（2）总价金额与单价金额不一致的，以单价金额为准，但单价金额小数点有明显错误的除外；

（3）投标报价为各分项报价金额之和，投标报价与分项报价的合价不一致的，应以各分项合价累计数为准，修正投标报价；

（4）如果分项报价中存在缺漏项，则视为缺漏项价格已包含在其他分项报价之中。

3.2 详细评审

3.2.1 评标委员会按本章第 2.2 款规定的量化因素和分值进行打分，并计算出综合评估得分。

（1）按本章第 2.2.4（1）目规定的评审因素和分值对商务部分计算出得分 A；

（2）按本章第 2.2.4（2）目规定的评审因素和分值对技术部分计算出得分 B；

（3）按本章第 2.2.4（3）目规定的评审因素和分值对投标报价计算出得分 C；

（4）按本章第 2.2.4（4）目规定的评审因素和分值对其他部分计算出得分 D。

3.2.2 评分分值计算保留小数点后两位，小数点后第三位“四舍五入”。

3.2.3 投标人得分=A+B+C+D。

3.2.4 评标委员会发现投标人的报价明显低于其他投标报价，使得其投标报价可能低于其个别成本的，应当要求该投标人作出书面说明并提供相应的证明材料。投标人不能合理说明或者不能提供相应证明材料的，评标委员会应当认定该投标人以低于成本报价竞标，并否决其投标。

3.3 投标文件的澄清

3.3.1 在评标过程中，评标委员会可以书面形式要求投标人对投标文件中含义不明确、对同类问题表述不一致或者有明显文字和计算错误的内容作必要的澄清、说明或补正。澄清、说明或补正应以书面方式进行。评标委员会不接受投标人主动提出的澄清、说明或补正。

3.3.2 澄清、说明或补正不得超出投标文件的范围且不得改变投标文件的实质性内容，并构成投标文件的组成部分。

3.3.3 评标委员会对投标人提交的澄清、说明或补正有疑问的，可以要求投标人进一步澄清、说明或补正，直至满足评标委员会的要求。

3.4 评标结果

3.4.1 除第二章“投标人须知”前附表授权直接确定中标人外，评标委员会按照得分由高到低的顺序推荐中标候选人，并标明排序。

3.4.2 评标委员会完成评标后，应当向招标人提交书面评标报告和中标候选人名单。

第四章 合同条款及格式

工程项目工业品买卖合同

出卖人：____　　合同编号：__

买受人：新疆天富能源股份有限公司　　合同名称：工程（ ）

项目单位：_____　　签订地点：新疆石河子市

项目编号：_____　　签订时间：　　年　月　日

项目名称：_____

根据《中华人民共和国民法典》，出卖人、买受人双方经过友好协商，就买受人向出卖人购买以下产品及服务有关事宜，签订并信守下列条款。

合同含税总价为：元　（　　元整）

合同不含税总价为：元（　　元整）

第一条　产品名称、型号、数量、金额等

序号	物资名称	型号规格	单位	数量	不含税单价	不含税总价	含税单价	含税总价	备注
1									

以上合计价格为合同总价，包括但不限于设备费、备品备件、专用工具、包装费、运保费、卸货费、安装指导费、调试费等合同项下的义务；也包括买受人、出卖人双方签订的技术附件中出卖人承诺的其它系统配件，并满足最终施工图纸的要求。出卖人按买受人货物的明细要求开具增值税发票，合计金额不变。

第二条　质量标准：

1、所有产品均为原厂包装。外观无瑕疵，标识齐全。

2、出卖人保证产品质量全部符合下列标准：以国家或相关行业较高标准为准。有技术协议的，需同时满足技术协议要求。

3、出卖人随货向买受人提供产品合格证书、质检报告等证明产品质量的文件。同时出卖人需配合买受人提供有国家主管部门验收所需的相关资料。

第三条　合同产品包装、运输、交货

1、合同产品的包装

由出卖人负责货物的妥善包装，应符合国家包装标准和适合长途运输、多次搬运及叉车装卸，并具有防潮、防晒、防震、防腐等保证措施，包装上有明显运输、方位标识，确保货物在任何情况下的安全。

2、合同产品的运输

运输及保险费用由出卖人承担，出卖人需送货上门。出卖人在买受人指定地点将合同产品交付给买受人，视为交货完成。出卖人交付合同产品前，风险（包括但不限于第三人侵权、货物合理损耗、不可抗力、第三方违约等）由出卖人承担，交付后风险由买受人承担，，卸车费由出卖方承担

3、合同货物的交货

交货时间：按买受人要求时间到货。

交货地点：买受人指定的石河子市到货现场。

交货方式：汽运，就地交货。

第四条　质量验收

1、按技术协议以及双方协商确认的质量标准和图纸作为验收依据，由买受人进行验收。

2、质量不符合验收要求的，买受人有权随时退货，并拒绝接受。

3、到货验收后，出卖人应及时到达产品安装地点进行安装指导、调试，必须达到国家或相关行业标准以及双方技术协议的规定。

4、发现质量问题，出卖人应及时采取补救措施，给买受人造成损失的，由出卖人承担相应责任。

第五条　售后服务

1、出卖人需承诺服务及质量，并负责货物的补充及供应（货物质量应符合本合同的有关要求），供应单价不得高于本合同约定的价格。

2、出卖人按制造厂的产品安装维护使用说明书的各项要求，保证设备能正确存放、安装和使用，产品质量保证期限为投入运行 72 小时试运行后之日起 3 年；在质保期内发生质量问题的，出卖人应在接到买受人通知后 48 小时内作出服务响应，10 个工作日内履行更换、维修，确保所提供的产品合格率达到 100%，质保期内本合同产品出现的任何非因买受人原因发生的故障，出卖人免费为买受人现场解决，负责包修、包退、包换并承担相应违约责任；质保期后，出卖人应提供维修服务，只收取材料费。质保期从货物验收合格后重新起算。

3、出卖人提供工作时间的投诉服务电话或质量负责人手机：　　。

第六条　结算方式

付款方式为电汇或汇票方式；付款方式为电汇或汇票方式；合同签订后 30 日内甲方向乙方支付合同总金额的 30%，按要求初验完成后，甲方向乙方支付合同总金额的 30%，竣工验收合格后，甲方向乙方支付合同总金额的 30%，剩余合同总额的 10%作为质量保证金，系统竣工验收合格一年后，甲方 10 日内向乙方支付合同总金额的 10%。

第七条　不可抗力

1、不可抗力指战争、严重火灾、政策变更等政府行为、洪水、地震等或其它双方认定的不可抗力事件。

2、签约双方中任何一方由于不可抗力影响合同执行时，发生不可抗力一方应尽快将事故通知另一方。在此情况下，出卖人仍然有责任采取必要的措施加速供货，双方应通过友好协商尽快解决本合同的履行问题。

第八条　索赔

1、在运行过程中，发生问题包括但不限于产品质量、出卖人指导安装错误、指导说明有误等出卖人原因，

给买受人造成损失的，出卖人承担赔偿责任。

2、在合同执行期间，如果出卖人对买受人提出的索赔和差异负有责任，出卖人应按照买受人同意的下列方式解决索赔事宜：出卖人同意退货，并按合同规定的数额将货款退还给买受人，并承担由此发生的一切损失和费用。

3、如果在买受人发出索赔通知后 30 天内，出卖人未作书面答复，上述索赔应视为已被出卖人接 受。买受人将从合同款项中扣回索赔金额。如果这些金额不足以补偿索赔金额，买受人有权向出卖人提出不足部分的赔偿，赔偿范围包括但不限于违约金、诉讼费、鉴定费、律师费等。

第九条　违约责任

1、出卖人未能按质量标准按时交货，每拖延一周，需向买受人支付合同金额的 3‰的违约金，并继续履行合同，不足一周的，按一周计算。扣除违约金上限为合同总价的 10%。

2、若出卖人未按约定提供售后服务或逾期提供服务，则视为出卖人违约，出卖人承担合同价款 10%违约金。

3、如果出卖人所供设备或产品的规格、质量、性能没有达到合同、技术协议中任何一条款要求或出卖人应提供的技术服务未能按照其合同、技术协议（要求）执行都是出卖人违约，出卖人均应向买受人支付合同总金额 20%违约金。如果本合同项下约定的违约金合计达到最高限额（即合同总价 30%）,买受人将考虑终止合同。

4、若出卖人不履行合同或履行合同不符合合同的约定，向买受人承担合同总金额 20%违约金，若违约金不足以弥补损失，按实际损失向买受人承担。

第十条　合同解除

如果一方严重违反合同义务，并在收到对方通知书后在 30 天内仍未能改正的，另一方有权解除本合同，合同至通知书到达对方之日起解除，违约方承担一切法律后果。

第十一条　合同争议的解决方式

本合同在履行过程中发生的争议由双方当事人协商解决；协商不成的，依法向合同签订地新疆石河子市有管辖权的人民法院起诉解决。

第十二条　其它事项：

1、详细价格、技术说明及其它有关合同设备的特定信息由合同附件说明。所有附件及本项目的招投标文件、技术协议、供货合同等均为本合同不可分割部分。

2、本合同一式捌份，出卖人两份，买受人陆份。

3、出卖人、买受人双方签字盖章后本合同正式生效。

第十三条　其它约定：／

出卖人	买受人
单位名称 ：	单位名称：新疆天富能源股份有限公司

地址：	地址：新疆石河子市北一东路 2 号
电话：	电话：0993-2904050
开户银行：	税号：91650000718900147A
账号：	开户银行：中国银行石河子市三山支行
法人代表：	账号：107004669637
委托代理人：	法人代表：
纳税号：	委托代理人：
传真：乙方传真	传真：
邮政编码：832000	邮政编码：832000

第五章 供货要求

一、项目概况

新疆天富能源股份有限公司成立于1999年3月，于2002年2月28日在上交所发行上市，是一家以电力、热力生产、销售及天然气销售为主体，发、供、调一体化的综合性能源企业。公司采用先进的技术、优质的服务提供安全、高效、清洁的电力、热力、天然气供应，成为新疆石河子地区的能源支柱企业。

随着公司信息系统的不断发展，营销系统与财务系统所承载的数据规模不断扩大，数据安全风险也逐步显现。经综合分析，天富能源在数据安全管理方面主要存在以下问题：

1、缺乏统一的数据安全管理体系

目前尚未建立统一的数据治理统一定制化管控平台，各系统的数据安全管理能力相对分散，缺乏统一的数据资产管理和数据安全管控机制。

2、数据资产管理能力不足

尚未开展系统化的数据资产梳理工作，缺乏对重要数据资产的全面识别与管理，无法准确掌握企业核心数据资源分布情况。

3、数据分类分级体系尚未建立

目前尚未建立数据分类分级管理体系，无法对敏感数据进行分级保护，数据安全管理缺乏统一标准。

4、测试环境数据安全风险较高

营销系统测试环境及仿真环境使用真实业务数据运行，但未进行有效的数据脱敏处理，存在敏感数据泄露风险。

5、数据安全平台及测试环境信创底座缺失

数据安全治理平台、态势感知平台等新建系统需存储海量审计日志及策略数据，目前缺乏国产数据库支撑；同时营销系统仍沿用Oracle 12c，不仅不符合能源行业信创替代要求，且与生产环境数据库同构，一旦测试环境因使用真实数据而遭受攻击，极易利用同构漏洞横向渗透至生产核心。

6、数据共享安全管理能力不足

营销系统存在对外数据共享和内部数据交换需求，目前缺乏统一的数据共享安全管理机制，数据访问行为审计能力不足。

7、数据库访问安全防护能力不足

目前财务系统无论在网络安全还是数据安全方面均未采用技术手段进行有效保护，系统网络边界防护能力下降，同时数据库访问缺乏专门的安全监控与审计机制。

8、数据安全运营能力尚未建立

尚未建立数据安全持续运营机制，缺乏数据安全风险监测、分析及处置能力，数据安全管理仍处于被动防护阶段。

9、应对数据资产爆发式增长的治理需求

随着企业数字化转型深入，数据量呈指数级增长，数据类型日趋复杂（结构化、半结构化、非结构化）。传统人工梳理方式已无法满足全域数据资产的发现、分类与管控需求，亟需建设自动化、智能化的数据治理平台，实现数据资产的可视、可管、可控。

10、满足日益严格的数据安全合规要求

《数据安全法》《个人信息保护法》及等保 2.0 等法规明确要求企业建立数据分类分级、风险监测、安全审计等能力。平台通过内置的分类分级策略、全流程操作审计、风险事件闭环管理等功能，可有效支撑合规自查与监管审计，降低合规风险。

11、云化趋势带来的安全盲区亟待填补

随着企业业务系统加速上云，传统基于网络镜像的审计方案在虚拟化、容器化环境中面临“数据流不经过网络”的盲区问题。平台通过应用层探针技术，从源头采集数据，彻底解决云环境下的审计死角，实现全链路可视。

12、缺乏完善的管理制度

目前尚未建立覆盖数据全生命周期的统一数据安全管理制度体系，缺少数据分类分级、数据访问权限、数据共享交换、数据脱敏加密、数据备份恢复、数据销毁、应急处置、人员管理、第三方管理、安全考核等规范化、可落地的制度文件。现有管理要求分散、不成体系，责任边界不清晰、流程不明确，导致数据安全管理无据可依、执行不到位，难以形成长效管理机制。

13、未建立常态化的安全风险评估机制

未建立定期、全面、闭环的数据安全风险评估工作机制，未按法规要求开展常态化风险识别、分析、评价与整改跟踪。对营销、财务等核心系统的数据安全风险、漏洞隐患、权限风险、流程风险缺乏周期性排

查；未形成 “评估 — 发现 — 整改 — 复查 — 再评估” 的闭环管理，风险隐患长期存在，无法提前预警、主动防范，难以满足监管与合规要求。

上述问题在一定程度上影响了数据安全管理水平，也对核心业务系统的安全运行带来潜在风险，亟需通过建设系统化的数据安全防护体系进行有效解决。

二、项目建设目标

本项目以国家数据安全相关法律法规和行业监管要求为指导，以全面提升企业数据安全防护能力为目标，围绕营销系统与财务系统开展数据安全能力建设，构建覆盖数据全生命周期的完备数据安全管理体系。

项目总体目标为：构建统一的数据安全管控平台，建立健全数据资产管理体系和数据安全防护体系，实现企业数据资产“可识别、可管理、可控制、可审计、可追溯”的核心数据安全管理目标。

具体建设目标包括：

信息系统漏洞纵深加固：对现有 21 台核心信息系统开展全覆盖漏洞扫描，制定专项针对性加固方案，完成全部高危漏洞闭环修复，确保系统长期安全稳定运行。

勒索病毒主动防御设备部署：部署专业防勒索设备，针对当前日益严峻的勒索病毒攻击态势构建主动防护机制，全面提升天富数据中心对勒索攻击的精准识别、快速阻断及应急恢复能力。数据脱敏与运维安全治理系统建设：

建设数据脱敏系统，在内部不可信环境中构建可信防护防线，重点防范人员不当操作引发的安全风险。

完成营销及财务业务系统全量数据资产梳理，建立数据资产台账，实现数据资产全局统一管理；

建立规范的数据分类分级管理体系，落实差异化防护策略，实现数据精准分级保护与分级管控措施落地；

完成营销系统测试环境及仿真环境全量数据脱敏处理，明确敏感数据脱敏规则、方法与使用限制，有效降低数据泄露风险；

建立全链路数据库访问审计机制，实现开发运维人员操作、数据导出行为全程可追溯、日志可审计；

升级财务系统数据库访问管控策略，严格管控外包人员访问权限，大幅提升核心财务数据安全防护能力；

实现数据共享及接口访问行为的持续安全监测，规范数据提供及传输流程，及时预警异常访问风险；

建立数据安全常态化持续运营机制，构建风险监测、分析、处置闭环能力，全面提升企业数据安全管理水平；

建立健全数据安全管理制度体系，完善数据存储、备份、删除、传输、跨境等全流程规范，确保制度落地执行；

明确数据安全负责人，落实数据安全责任制度，配齐数据安全岗位与资源投入，满足数据安全保护需求；

制定数据安全事件应急预案，每年至少开展 1 次应急演练，提升安全事件应急处置与恢复能力；

常态化开展数据安全风险评估，建立 “评估 — 整改 — 复查”闭环机制，及时消除安全隐患；

开展全员数据安全培训与考核，建立重要岗位员工录用前背景调查机制，强化人员安全管理；

启用堡垒机实现远程运维全过程审计，确保运维操作可监控、可追溯、可审计；

制定数据存储安全策略，按需实施重要数据加密存储，全面满足合规与监管要求。

同时，天富在规划建设数据中台系统，本期建设内容未来要应用到数据中台环境之中，保障中台中数据的安全。

三、规范依据

涉及数据安全部分核心条款如下：

条目	内容	具体措施
第 40 条	网络运营者应采取技术措施（如加密、访问控制、审计日志）防止数据泄露、损毁或丢失。	加密、访问控制、日志审计等等
第 42 条	要求对用户信息严格保密，并在发生数据泄露时及时向主管部门报告。	保密、及时报告安全事件
第 45 条	发生数据安全事件时，应立即启动应急预案，采取补救措施并上报。	启动应急预案、及时不久、上报安全事件与处理结果

（1）数据安全法

条目	内容
第 4 条	要求数据处理活动应当采取必要措施（包括技术和管理措施），确保数据安全，防止数据泄露、篡改、丢失。
第 21 条	建立数据分类分级保护制度，对数据实行差异化管控。 对重要数据、核心数据需采取更严格的保护措施（如加密、访问控制、网络隔离等）； 制定内部数据安全管理制度和操作规程。
第 27 条	明确要求通过技术手段保障数据安全，包括： 数据加密、脱敏； 访问权限控制； 安全审计日志；
第 29 条	重要数据的处理者应当定期开展风险评估，并向主管部门报送报告； 发生数据安全事件时，立即采取处置措施并上报。

（2）关键信息基础设施安全保护条例涉及网络安全加固部分

条目	内容
第 10 条	● 建设网络安全监测预警系统，实时监测网络运行状态和威胁； ● 每年至少开展一次网络安全应急演练。
第 11 条	● 优先采购安全可信的网络产品和服务（需通过国家安全审查）； ● 对可能影响国家安全的设备和服务进行风险评估。
第 15 条	● 定期开展漏洞扫描、渗透测试； ● 对发现的漏洞立即修复，并向主管部门报告重大风险。

涉及数据安全部分

条目	内容
第 12 条	对 CII 运营者提出更高要求： ● 重要数据和核心数据需单独存储、加密传输； ● 建立数据备份和容灾机制（如异地灾备）。
第 13 条	CII 运营者境内收集的重要数据原则上不得出境；确需出境的，需通过国家网信部门的安全评估（与《数据安全法》衔接）
第 14 条	处理个人信息需遵循最小必要原则，并采取去标识化或匿名化技术

在 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》条例中，

涉及网络加固相关要求如下：

（1）安全物理环境

网络设备物理隔离：关键网络设备应部署在独立机房，配备防盗、防火、防电磁泄漏设施。

（2）安全区域边界

边界防护（G3）：

- 部署防火墙或访问控制设备，禁止非授权跨边界通信；
- 关闭非必要端口和服务（如 Telnet、SNMPv1/2）。

入侵防范（G3）：

- 应在网络边界处部署 IDS/IPS，检测/阻断端口扫描、暴力破解等攻击行为；
- 定期更新攻击特征库（至少每周一次）。

恶意代码防范（G3）：

- 在网络边界及核心节点部署防病毒网关或沙箱检测系统。

安全审计（G3）：

- 记录网络设备、安全设备的运行日志，留存日志不少于 6 个月。

（3）安全计算环境

终端防护：

- 服务器和终端安装防病毒软件，并启用主机防火墙；
- 禁用默认账户（如 Administrator）或强制修改默认口令。

（4）数据安全

在 GB/T22239-2019《信息安全技术网络安全等级保护基本要求》条例中，涉及数据安全相关要求如下：

- 数据完整性（G3）：采用校验技术或密码技术（如 HMAC-SHA256）保

障重要数据在存储和传输过程中的完整性。

- 数据保密性（G3）

（5）传输加密：

- 敏感数据通过 VPN 或 TLS1.2+协议加密传输；
- 禁止使用 HTTP、FTP 等明文协议传输口令或业务数据。

（6）存储加密：

- 核心数据（如用户密码、密钥）需使用国密 SM4 或 AES-256 加密存储；
- 密钥与数据分离存储。

（7）数据备份恢复（G3）

- 重要业务数据每日增量备份，每周全量备份；
- 备份数据异地保存（如灾备中心）。
- 每年至少进行一次备份数据恢复演练。

（8）个人信息保护（新增）

- 收集个人信息时需脱敏处理（如手机号显示为 1381234）；
- 查询权限需与角色绑定，避免越权访问。

四、项目材料清单

区域位置	设备名称	硬件配置要求	具体内容	建设规模（套/台）
III 区	中新建数据治理统一定制化管控系统	国产化服务器，千兆电口≥4个，万兆光口≥4个，冗余电源；CPU≥16 核，内存≥64G，硬盘≥4T。	建设面向企业级全域数据资产的智能化治理中枢，遵循“全域全量采集、湖仓一体存储、分类分级驱动、资产价值提升”的建设原则，基于 AI 增强的自动化检测与动态质量模型，构建覆盖数据全生命周期的治理与安全管控体系。（包含三方系统如营销系统、财务系统等接入）	1 台
III 区	威胁监测与分析系统	标准机架式设备，≥4 个千兆电口、≥2 个万兆 SFP+插槽、内置≥4T 硬盘，具备液晶屏，冗余电源。	为应对 APT、勒索、挖矿等高级威胁的持续演进，满足合规与实战化防护要求，部署一套业界领先的高级威胁监测与分析系统。系统需具备全流量实时捕获与深度解析能力，覆盖南北向及东西向流量，集成威胁情报、动态沙箱、机器学习及 AI 大模型，实现已知与未知威胁的自动化精准识别与告警降噪。支持 ATT&CK 攻击链可视化溯源、全包存储取证，并提供高级旁路阻断及 SOAR 编排联动，实现威胁监测—分析—响应—预警的闭环运营。系统应具备分布式集群、云原生部署能力，全面提升网络安全主动防御与应急响应水平。	1 台
III 区	数据静态脱敏系统	国产化服务器，千兆电口≥4个，万兆光口≥4个，冗余电源；CPU≥8 核，内存≥32G，硬盘≥4T。	以数据仿真为核心点，可实现自动化发现源数据中的敏感数据，并对敏感数据按需进行随机、仿真、变形、遮盖等处理，可以满足为开发环境、测试环境、培训环境等提供脱敏后的生产数据，也可以为数据交易、数据交换、数据分析等第三方数据应用场景提供适用的敏感信息泄露防护作用。避免敏感信息泄露的同时又能保证脱敏后的输出数据能够保持数据的一致性和业务的关联性。最大限度地保证脱敏后数据的特征、逻辑及各类数据间的一般性、业务性关联。。	1 台
III 区	数据库运维管控系统	国产化服务器，千兆电口≥4个，万兆光口≥4个，冗余电源；CPU≥8 核，内存≥32G，硬盘≥4T。	将事前审批、事中控制、事后溯源贯穿整个运维过程，产品汇集了数据库准入、数据资产展示、运维访问控制、敏感数据脱敏、高危操作管控、审计、统计等核心功能，实现数据库运维侧多元化管理。 广泛数据库兼容：全面支持 Oracle、MySQL、SQL Server、PostgreSQL、达梦、金仓、瀚高、Hive、HBase、MongoDB 等超 20 种国内外主流及大数据数据库。 集中化可视管理：基于 B/S 架构的 HTTPS 远程 Web 管理平台，集成资产、风险、工单、防护等多维度统计仪表盘，并提供网络流量抓包与数据备份还原工具。	2 台
III 区	数据动态脱敏系统	国产化服务器，千兆电口≥4个，万兆光口≥4个，冗余电源；CPU≥8 核， 内存≥32G，硬盘≥4T。	通过反向代理部署方式，对业务系统数据库中的敏感数据进行透明实时的脱敏。产品依据用户的角色、职责和其他 IT 定义身份特征，动态地对生产数据库返回的数据进行专门的屏蔽、隐藏和审计，可确保不同级别的用户按照其身份特征恰如其分地访问敏感数据，并且不需要对生产数据库中的数据进行任何改变。	1 台
III 区	数据库加密系统	国产化服务器，千兆电口≥4个，万兆光口≥4	在敏感数据存储加密的基础上增加访问授权机制，任何访问被加密数据的人或应用事先必须经过授权，拥有合法访问权限才能访问加密数据，非授权用户访问	2 台

		个，冗余电源；CPU≥8 核， 内存≥32G,硬盘≥4T。	加密数据只能看到密文或者无效内容。 可直接部署于原生操作系统，无需依赖特定定制系统。	
III 区	数据环境安保系统	国产化服务器，千兆电口≥4个,万兆光口≥4个，冗余电源；CPU≥8 核， 内存≥32G,硬盘≥4T。	环境安保系统采用了一种安全可信策略管控下的运算和防护并存的主动免疫的新计算节点体系结构,以密码为基因实施身份识别、状态度量、保密存储等功能。及时识别“自己”和“非己”成份，从而排斥与破坏进入机体的有害物质,相当于为网络信息系统培育了免疫能力。	1 台
III 区	数据库审计系统	国产化服务器，千兆电口≥4个,万兆光口≥4个，冗余电源；CPU≥8 核， 内存≥32G,硬盘≥4T。	基于数据库通讯协议和 SQL 解析技术的数据库安全产品,能够实时监控记录用户对数据库的所有访问行为，并对数据库所遭受的风险行为进行告警，帮助用户快速生成事后合规性报表与对事故的追根溯源。通过全面监控内、外部数据库的访问行为，进一步保护数据资产的安全。	2 台
III 区	数据资产梳理系统	国产化服务器，千兆电口≥4个,万兆光口≥4个，冗余电源；CPU≥8 核， 内存≥32G,硬盘≥4T。	全数据（结构化数据和非结构化数据）梳理为核心目标,依靠数据资产智能挖掘和扫描技术为用户建立精准的数据资产台账,并依据内置数据分类分级模块对已发现的数据,根据不同分类及重要程度进行分类分级打标处理，且形成数据资产管理、账户管理、数据管理、数据流向、数据分布等可视化看板，帮助用户一站式解决数据在管理、使用、统计、合规上的问题，并为数据安全防护提供强有力支撑。	1 台
III 区	API 审计系统	国产化服务器，千兆电口≥4个,万兆光口≥4个，冗余电源；CPU≥8 核， 内存≥32G,硬盘≥4T。	通过对 web 应用系统的流量进行旁路（镜像）采集和分析，记录对应用系统的操作，可对 web 应用系统中的操作全审计，监视重点账号操作，监视重要业务模块的访问。该产品着重对应用系统操作合规性进行分析，发现异常操作和越权行为，同时标记出哪些 API 会访问敏感数据、风险的 API，从而做到 API 风险的提前预防和管控；同时，产品可对业务系统安全性进行分析，可以检测常见的 web 攻击行为和业务风险。	1 台
III 区	服务器密码机	机架式硬件设备，≥2 个 100/1000M 自适应网口。	产品严格遵循国家相关产品技术规范,内置经国家密码管理局审批的高速密码模块,能够为各类业务系统提供数据加解密、数字签名/验签以及密钥管理等高性能密码服务。产品具有商用密码产品认证证书。(包含三方系统如营销系统、生产系统等密钥改造)	1 台
III 区	加密机	机架式硬件设备，接口方式：RJ-45 &RS-232 最大传输速率：TCP/IP10M/100M 自适应，并支持 1000M 的传输速率； 异步 115 ,200 bps MTBF≥25 ,000 小时 频率：50~60 Hz	支持 3 DES、SM1\SM2\SM3\SMS4\SM7 算法,算法可选；密码机内共保存有 50 组本地主密钥，支持 192Bits 长度本地主密钥； 主密钥的存储采用完整性校验以及硬件冗余机制,以保证主密钥的一致性； 采用哑终端密钥管理模式，终端通讯参数可配置，密钥管理和联机交易可并行处理;支持中文(本地语言)操作界面； 具备客户端访问密码机的 IP 地址过滤和 MAC 绑定功能； 具备独立的密钥管理端口、TCP/IP 端口； 消息鉴别：支持 MAC/HMAC/TAC 的产生和验证； 支持多种 PIN 格式的加密和转换。包括 ANSI X9.8 格式即 ISO 95641－格式 0，Docutel 格式，Diebold 和 IBM 格式，ISO 95641－格式 1； 真随机数产生功能。使用硬件产生随机数，产生的随	2 台

			机数符合国家密码管理局颁布的《随机数检测规范》； 具有打印密码信封功能，支持串行或并行打印机； 密钥管理功能：支持产生、传输、存储、导入、销毁； 在三表、小额支付、一卡通、金融领域有广泛应用。	

五、项目技术要求

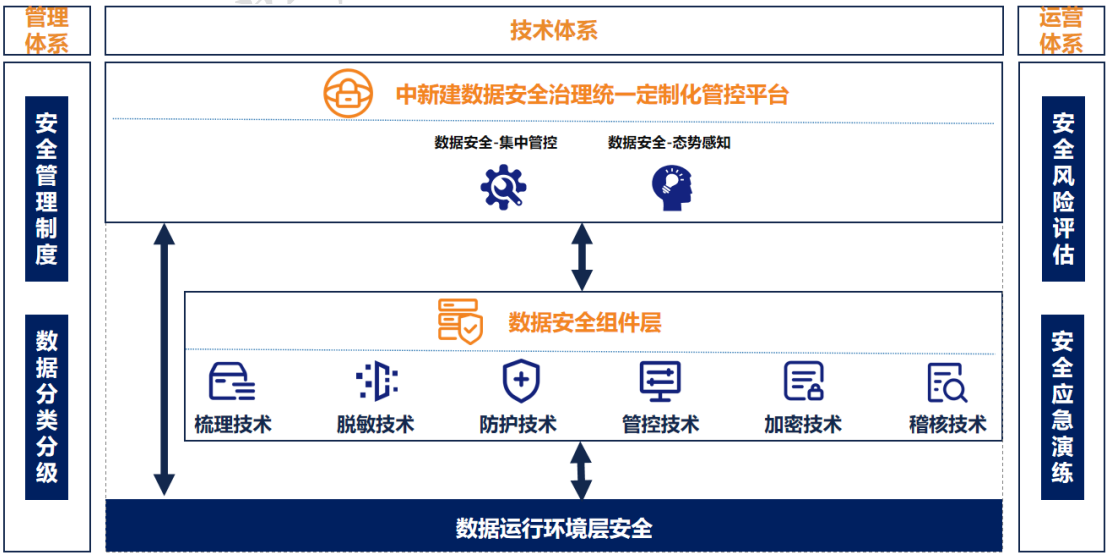
5.1 数据安全治理能力要求

5.1.1 总体建设要求

数据安全建设不是单纯的技术堆叠，也不仅是制度文本，而是面向全业务、全生命周期的系统化、可落地、可持续运营的能力建设。数据安全建设应实现从制度设计到技术执行，再到运营落地的完整闭环，确保每一项安全措施都能在实际业务中落地、可监控并可持续改进。

整体建设形成三大协同体系：数据安全管理体系、数据安全技术体系以及数据安全运营体系。这三个体系互为支撑，共同形成从战略规划、技术支撑到日常运营的闭环能力，使数据安全建设能够长期沉淀、持续优化并符合监管要求。

数据安全管理体系作为顶层治理架构，明确全域的数据安全责任，规范业务操作流程，建立风险识别与监控机制，为技术体系和运营体系提供规则和责任保障。数据安全技术体系通过分层架构实现对数据运行环境、数据使用过程以及集中管控分析的全面防护，确保管理策略在业务系统中可执行。数据安全运营体系则将管理制度和技术能力转化为日常可执行的运营状态，实现风险发现、事件响应、整改复盘和能力优化的闭环管理。



5.1.2 功能总体架构要求

整体功能层面包含数据治理统一定制化管控平台和数据安全防护组件：

中新建数据治理统一定制化管控平台提供数据安全统一管理与分析能力，实现数据资产管理、策略统一下发、风险监控及告警分析。通过数据治理统一定制化管控平台，各类资产信息、策略配置和风险数据得以集中管理，实现策略执行监督和效果验证。该层还提供实时分析能力，将技术执行结果转化为运营指标，为运营体系提供决策依据，支持风险事件的快速响应及持续改进。

数据安全防护组件重点保障数据在全生命周期中的安全。

数据资产梳理，在数据采集阶段对数据进行梳理，并且按照既定的分类分级标准进行自动化数据分类分级打标，确保数据的类别和等级可在系统中清晰呈现。

数据库加密，通过数据加密技术对数据库中敏感表或者字段进行落盘加密存储，确保数据存储安全。

数据静态脱敏，通过脱敏算法对生产数据进行脱敏处理，在保障安全的同时也保障了脱敏后数据的可用性，为开发测试场景提供安全可用的脱敏数据。

数据库运维管控，通过访问控制技术，对数据库运维人员的权限进行细粒度管控，确保敏感数据访问必须经过审批后才可进行相关操作。

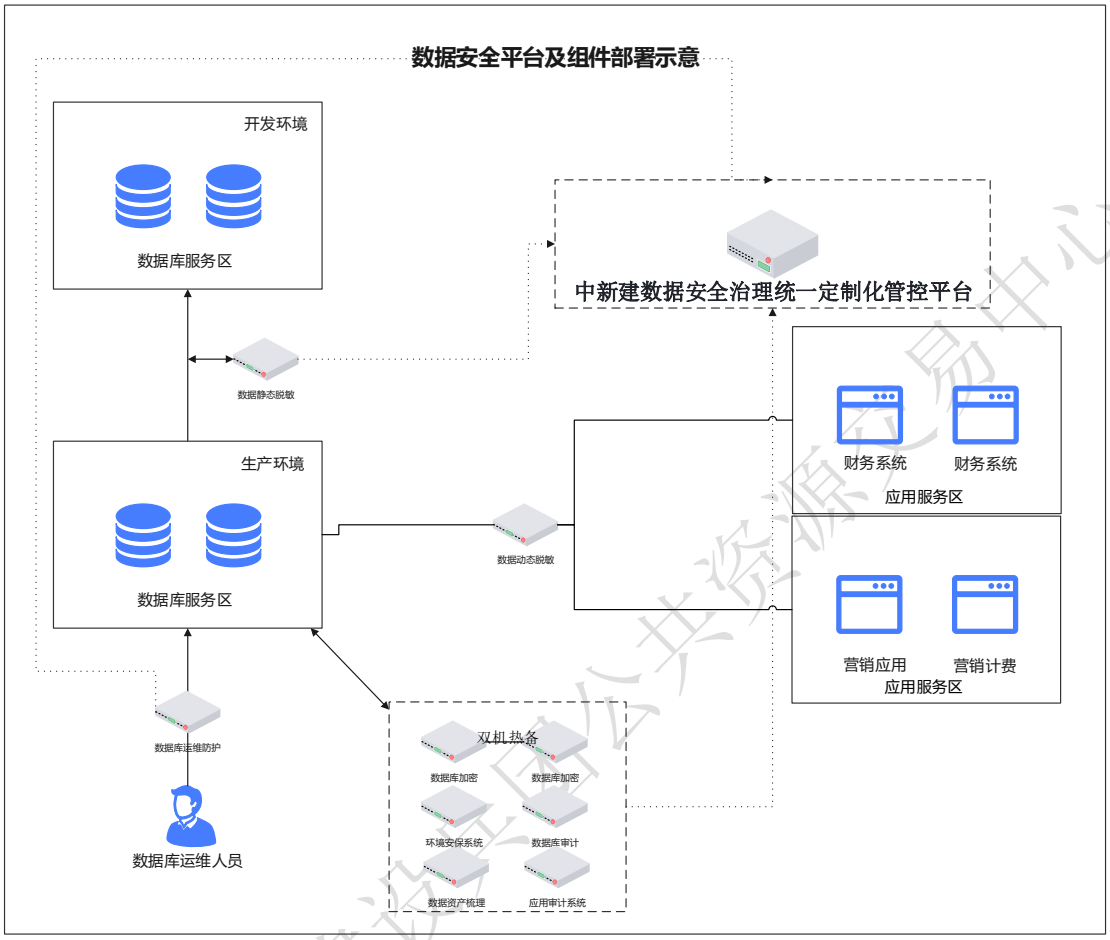
数据动态脱敏，通过动态脱敏技术对数据查询过程中的敏感数据进行有效保护，基于查询者的身份及查询的目标数据，实时返回脱敏后的数据。

环境安保系统，通过安全可信策略管控下的运算和防护并存的主动免疫的新计算节点体系结构，以密码为基因实施身份识别、状态度量、保密存储等功能。及时识别“自己”和“非己”成份，从而排斥与破坏进入机体的有害物质，相当于为网络信息系统培育了免疫能力。。

数据库审计，对数据库的访问及操作行为进行实时监测和记录。

应用审计，对应用系统的 API 接口调用情况进行实时监测与记录。

5.1.3 系统部署架构要求



数据安全治理统一定制化管控平台，采用旁路方式部署，需满足各数据安全组件网络可达即可；

数据资产梳理系统、应用审计系统、数据库加密系统、数据静态脱敏系统、数据库审计系统、环境安保系统采用旁路方式部署，需满足与数据库服务器网络可达即可；

数据库运维防护系统、数据动态脱敏系统采用反向代理方式部署，需满足与数据库服务器网络可达即可；

服务器密码机部署：

采用旁路或直连方式部署于数据库专区核心交换区，与数据库加密系统建立专用通信链路，为营销系统和财务系统的数据库加密提供统一密钥管理服务。

3.4.1.4 数据安全服务

为更好的让数据安全治理体系落地，需要开展以下数据安全服务工作：

数据安全制度编制服务，制度建设以战略目标为导向，梳理数据安全总体目标和原则，制定顶层策略文件，并将制度模板落地到各业务单元，包括数据分类分级、访问审批、数据共享、备份管理、风险评估及事件处理等操作流程。同时，为保证制度落地，集团为不同层级人员设计分层培训方案，通过操作手册、审批模板和流程指导，将策略转化为具体的操作行为，从而实现制度执行的可控性。

数据分类分级服务，在数据资产管理与分类分级方面，管理体系要求对全集团数据资产进行全面梳理，包括营销数据、财务数据等，并建立统一资产目录。资产目录上的数据按照敏感性、业务价值及风险等级进行分类分级，高敏感数据在访问、共享和操作过程中均需绑定审批流程、审计策略及告警策略，以应对业务变更和新数据上线的场景。

数据安全风险评估服务，风险评估是管理体系的核心环节，新业务上线、数据共享或跨境传输等关键场景需进行风险登记与评估。评估结果结合数据分类分级和业务影响形成风险等级，为技术体系配置相应防护策略提供依据。

数据安全应急演练服务，依据国家法律法规与行业规范，编制贴合实际的数据安全事件应急预案，明确应急组织架构、处置流程、责任分工与响应时限。服务围绕数据泄露、数据库非法访问、勒索病毒攻击、系统故障宕机等高风险场景，开展实战化应急演练，完成应急启动、事件研判、威胁处置、数据恢复、复盘整改全流程实操。通过演练检验预案有效性、技术防护能力与协同处置水平，形成演练记录、评估报告与整改清单，推动闭环改进，全面提升企业数据安全应急响应与快速恢复能力，满足监管与合规核查要求。

5.2 数据治理统一定制化管控平台要求

5.2.1 数据安全管控要求

为提升数据安全运维效率，降低运维成本，以数据为核心，结合数据分级策略，统一纳管、灵活调用数据安全工具，双向打通数据安全管理和技术瓶颈，能够针数据实现敏感数据识别、数据脱敏、数据加密、数据库审计等数据安全能力的联动高效管理。

5.2.1.1 安全态势要求

● 综合安全态势

大屏展示纳管业务系统的安全概况信息。包括总日志数量、总风险数量、当日新增日志数量、当日新增风险数量、未处置风险数量；已纳管业务系统数量、风险业务系统数量、风险业务系统占比；纳管应用资产数量、风险应用资产数量、风险应用资产占比；纳管数据库资产数量、风险数据库资产数量、风险数据库资产占比；数据库表数量、敏感数据库表数量、敏感数据库表占比；数据库字段数量、敏感数据库字段数量、敏感数据库字段占比；资产访问热度排行、风险类型排行、风险资产排行、风险用户排行、日志接入趋势、实时未处置风险滚动展示。

● 资产分布态势

大屏展示平台纳管的业务系统的数据分布情况。包括：业务系统、数据库资产数量、数据表总数、字段总数、涉敏字段总数以及文件数量等；

图标展示数据类型统计、字段统计、文件统计、数据访问热度 TOP5，敏感数据分布 TOP5、数据类别业务分布 TOP5 和数据等级业务分布 TOP5 统计等。

● 数据库资产安全态势

大屏展示数据库访问风险的综合信息，包括风险来源 IPTOP5，操作类型 TOP5，防护类型统计、高危指令分布、慢语句分布、风险分布、实时风险滚动展示等。

● 应用资产安全态势

大屏展示 API 资产访问风险的综合信息，包括 API 资产分布，API 接口标签，域名/IP 总数、API 接口总数、涉敏 API 总数、API 漏洞攻击分布、API 风险类型分布、API 实时风险滚动展示等。

5.2.1.2 综合安全管理要求

以纳管数据安全设备日志为基石，提供全面的安全设备监控。通过大屏展示，一目了然地掌握数据安全系统的流量信息与资产分布信息，同时基础安全风险信息。实现数据安全设备的全面管理和监控。

5.2.1.3 设备运行管理要求

通过大屏展示，可以直观地监控所有本方案中的数据安全系统的运行状态。简洁的界面展示系统的整体健康状态，同时提供详细信息以显示具体设备的运行状态。可以切换系统，查看不同系统的详细状态。

运行状态信息涵盖主机运行时间、主机 CPU 核数、主机物理内存总量、CPU 使用率、内存使用率以及磁盘根分区使用率。还提供时间区间内主机 CPU 的 sys 态最大使用率、最小使用率，user 态的最大使用率、最小使用率等详细数据。

此外，可详细显示区间时间内磁盘 IO 最大读取速率、最大写入速率、最小读取速率、最小写入速率等。同时，还可以查看区间时间内最大上行网络流量、最大下行网络流量、最小上行网络流量、最小下行网络流量等详细数据。

实时监控数据安全设备的运行状态，提供全方位的数据分析和报告，及时发现并解决问题，确保数据安全系统稳定运行，全面提升数据安全防护能力。

5.2.1.4 统一策略管理要求

平台可以对接入的本方案中的数据安全系统进行统一化的策略管理，通过 API 接口将策略模块集成，实现在平台中完成各类数据安全策略配置及下发。

5.2.1.5 设备注册登记要求

在数据治理统一定制化管控平台中添加数据安全设备进行注册，注册后的设备在管理平台中进行统一管理，包括策略设置、风险监控、状态监控、告警监控等。

5.2.1.6 单点登录管理要求

在数据治理统一定制化管控平台中对安全设备的单点登录进行管理，如开启、关闭单点登录等。开启单点登录后的设备通过平台进行统一身份认证，关闭单点登录的设备可以直接登录设备进行操作。

5.2.1.7 多设备管理要求

支持多种类型安全设备同时接入；

支持多台同类型设备同时接入；

支持设备分域管理，如：网络可达的情况下，不同数据中心的设备可以同时接入平台，并且该设备及该设备纳管的资产仅对具有管理权限的用户可见。

5.2.2 数据库审计要求

针对业务系统和运维人员访问数据库专区中数据库时，通过部署数据库审计系统，以安全事件为中心，以全面审计和精确审计为基础，对数据库的各类操作行为进行监测、记录、分析，生成审计报表。对于监测到的风险事件（包含数据库攻击和数据违规操作），及时生成告警并以邮件、短信等方式通知相关人员，确保用户的系统符合各类法律法规对数据库审计的要求。

5.2.2.1 数据库资产自动梳理要求

基于数据库协议嗅探技术（协议解析），自动梳理数据库资产，快速添加审计对象进行审计。自动梳理数据库的基本信息包括：数据库服务器 IP、端口号、数据库类型。同时支持自动发现自动添加审计对象的能力，解放人工。可以根据 IP 范围指定要发现的 IP 列表，仅发现这些 IP 内的数据库资产。

5.2.2.2 精确审计要求

能对 SQL 语句的执行结果（成功或失败）、错误码、错误信息、执行时长、返回行数、绑定变量值进行深度解析，帮助客户有效地提升审计内容的精确性。

5.2.2.3 高性能检索和海量存储要求

该系统在大量审计日志的情况下（几百亿甚至千亿）可以快速检索出结果、并且这些数据都是在线可查看，查询结果没有行数限制，实现了在不归档情况下的海量存储与快速检索。

5.2.2.4 安全规则要求

提供了内置规则、自定义规则、高危操作、漏洞攻击（CVE）、SQL 注入等 500+条以上的内置规则，帮助客户及时发现威胁，并告警。

多维度的规则管理，规则配置是以规则维度去关联审计对象（数据库），实现了把同一个规则应用到多个数据库上的灵活性。同时支持规则名称、规则组、规则类型、漏洞类型等维度的规则快速过滤方便查找规则。规则关联是以审计对象（数据库）为维度去关联和解除关联规则，方便对某个数据库上规则的灵活配置与优先级调整。

分组管理，对常用的 IP、数据库用户、工具等进行分组配置，方便在规则里直接引用组，实现分类管理。

5.2.2.5 多样的告警方式要求

当系统检测到数据库攻击、异常、违规等行为时，会自动触发系统预置访问规则进行实时告警，风险和数据外送的方式包括：syslog、kafka，可以灵活选择要外送的字段。

系统告警方式包括：邮件、短信平台、企业微信、syslog、kafka、snmp、站内信，方便使用者第一时间以不同的途径收到产品的异常告警。

5.2.2.6 丰富的报表模板要求

提供丰富的审计合规性报表、综合性报表、专项报表、自定义报表等报表模板，内置 30 多张报表，满足用户各种报表要求，自定义报表可以根据预设维度进行生成报表。

5.2.2.7 多维度统计要求

拥有流量统计、风险统计、会话统计、对象统计、SQL 统计、对比分析等多维度聚焦，可以分析出一定时间内数据的走向，以及访问频度。

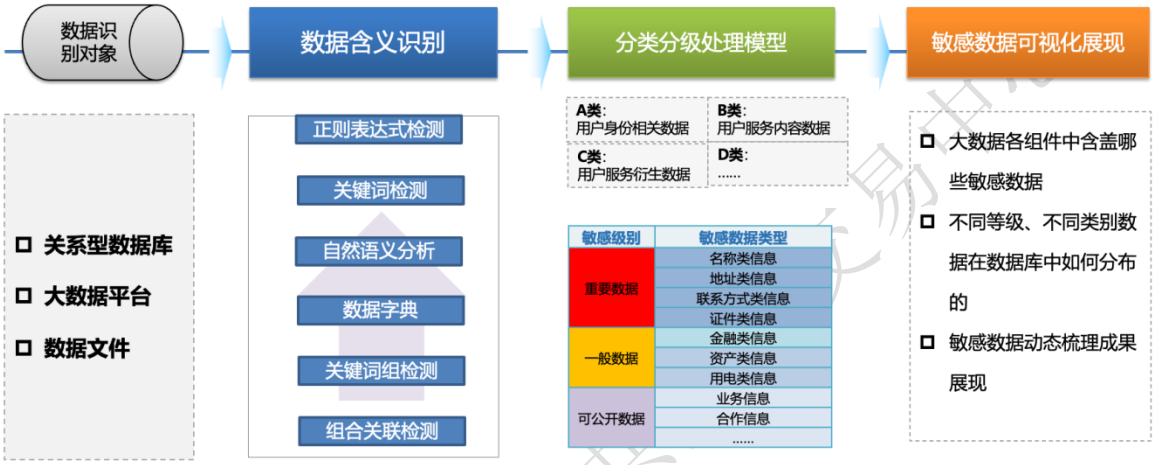
5.2.2.8 实时用户行为监控要求

对网络的入侵行为、用户的异常行为和违规行为进行监控，首页会展现风险数量、最近风险详情。

5.2.3 数据资产梳理要求

通过在数据库专区部署数据资产梳理系统，采用旁路部署模式，需实现与后端应用及数据库专区中各数据库节点之间路由可达，对整体业务无影响。系统以全数据（结构化数据和非结构化数据）梳理为核心目

标，采用静态网络扫描和动态流量识别相结合的方式，为数据库专区各业务系统数据库建立精准可靠的数据资产台账、形成完整数据分类分级清单，进而一站式解决各业务系统数据资产的管理、使用、统计、合规问题，并为数据安全防护提供基础策略支撑。



5.2.3.1 资产发现要求

系统可指定 IP 网段或数据库，建立资产发现任务，可对数据库、文件、图片等进行发现，并可按照设定的周期展开定时发现任务，帮助用户快速、准确地发现数据资产。

5.2.3.2 资产梳理要求

- 资产组

系统可根据 IP 段建立数据组，帮助用户查找数据资产、划分部门数据资产，便于用户管理与统计。资产清单

系统将所发现的数据库、IP、端口等进行展示，用户可手动添加新数据库资产，并支持用户对现有资产进行导入导出操作。

支持账号权限清单查看，支持添加动态梳理引擎。敏感数据发现规则

系统可根据字段、关键字、正则表达式等内容设定敏感字段，帮助用户快速、准确识别数据库中相应的敏感数据。

- **配置管理**

系统支持用户自定义设置采样率及匹配率来识别敏感数据，帮助用户高效识别敏感数据。

- **数据特征统计**

根据标记的数据特征进行可视化展现。

- **类别统计**

根据分类分级进行数据库、表、字段的可视化展现。

- **数据变更状态**

监控数据库表字段的变化（增加删除等）。

- **梳理**

支持单 IP 梳理/IP 组梳理等，并通过模板进行自动打标；支持二次梳理。

- **打标**

对敏感数据库表、字段按照分类分级模板进行人工打标，对同一表相似数据库支持一键同步功能，支持核实功能，核实后的字段多次打标不会受影响。

5.2.3.3 分类分级要求

本系统可建立不同分类分级模板，根据数据重要程度进行分类分级打标，并以思维脑图形式建立数据分类分级视图，方便用户查看。

模板管理：

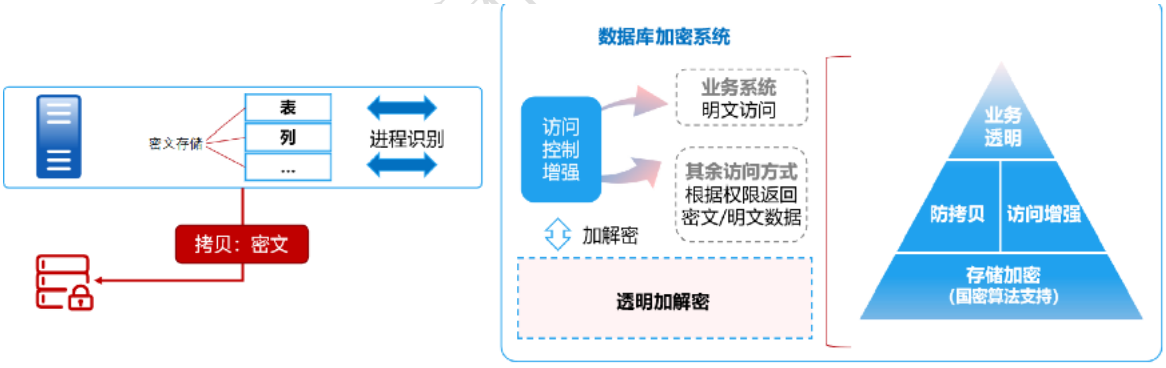
定制分类分级模板，并在梳理中进行关联使用。

分类修订：

对已打标的数据进行手工修订，避免重复梳理对数据库产生的压力。

5.2.4 数据库加密要求

针对数据库专区中数据库存储的重要数据，通过数据库加密系统部署，对数据库中各类重要数据进行加密，加密后的数据以密文形态存储。一方面，由于黑客缺乏密钥，即使硬盘失窃或遗失也不会轻易造成敏感数据泄露；另一方面，通过对密文数据施行访问控制，防止运维人员接触敏感数据。系统采用透明加密技术，即业务程序在访问加密的敏感数据时，无需改变任何代码，对于具备密文访问权限的业务程序自动进行加解密，对于缺乏密文访问权限的用户拒绝访问，加密对于业务程序来说是透明的，无需改变业务逻辑,不影响业务性能。



5.2.4.1 数据加密要求

数据库加密系统支持对数据库中各类常用的数据类型进行加密，加密后的数据以密文形态存储，由于黑客缺乏密钥，因此即使数据库文件因物理入侵造成失窃也不会导致敏感数据泄露：

- 支持列加密、表空间加密、文件系统加密三种加密模式，满足不

同场景需求。

- 支持对指定表或列的加密。
- 支持如 CHAR、VARCHAR2、VARCHAR、RAW、NUMBER、DATE 等数据类型的加密。

5.2.4.2 数据加密算法要求

数据库加密系统全面兼容多种国密、国际标准算法，如 SM4 国密算法，3DES、AES 等国际标准算法，实现为数据加密提供高效的密码运算和加解密服务，同时具备领先的加解密性能，保证敏感数据的机密性。

5.2.4.3 加密透明性要求

数据库加密系统无需改变应用，业务程序透明访问加密数据。

1、业务程序无需改变任何业务逻辑，透明访问业务

业务程序无需知道密钥，也无需改变任何代码，透明访问加密的敏感数据。

2、加解密过程透明，简化管理

对于具备密文访问权限的应用自动进行加解密，对于缺乏密文访问权限的应用进行敏感屏蔽。

3、透明加密的索引支持，业务性能几乎无损

索引是业务程序性能的关键措施，数据库加密系统无需改变索引策略，保证业务程序性能不损伤。

4、SQL 语句透明

对于增删改查操作，函数、存储过程等均透明；约束透明：主外键、唯一索引、NOTNULL 等重要约束透明。

5.2.4.4 加密密钥管理要求

为保护加解密密钥的安全性管理，数据库加密系统支持对安全密钥备份更新机制。同时加密系统支持多级密钥管理方案，将密钥分为主密钥和加密密钥，主密钥保护加密密钥，加密密钥用于保护被加密的目标（敏感表、字段）。支持三方密码产品对接，如密码机、密码平台等。

5.2.4.5 加密数据访问管控要求

支持 SQLPLUS、PLSQLDEV 等 SQL 管理工具查询加密数据时的访问控制，对未授权明文访问的账户禁止访问明文数据，起到防护效果。防止第三方运维人员接触重要的敏感数据信息和业务的个人隐私数据，提高数据安全运维能力。

5.2.4.6 密钥安全基础设施对接要求

数据库加密系统的密钥管理采用"软件+硬件"双重保护机制。核心加密密钥（主密钥、密钥加密密钥）由服务器密码机生成并安全存储于硬件密码模块内，通过标准接口与数据库加密系统进行对接，实现：

密钥不出机：所有密钥运算在密码机内部完成，私钥/主密钥不以明文形式导出至服务器内存或磁盘

分级密钥管理：支持主密钥保护工作密钥的二级密钥体系，支持密钥定期轮换和应急销毁

5.2.5 数据静态脱敏要求

针对数据对外共享分发场景（包含分发到开发测试环境以及分发到外界单位），部署数据静态脱敏系统，通过将数据库专区生产库数据经过脱敏后放入脱敏库，脱敏库用于搭建开发/测试/培训环境，以实现开

发/测试/培训环境与生产环境隔离，保障数据库生产环境数据安全。此外，脱敏库还可应用于数据交易、数据交换、大数据分析等第三方数据应用场景。

5.2.5.1 敏感数据自动发现要求

内置丰富的敏感数据发现规则，支持基于用户自定义敏感数据发现规则，实现对于目标数据源的敏感数据自动发现和标识。

5.2.5.2 数据子集定义要求

针对用户实际需求场景，特别定制了数据子集的定义和管理功能。该功能使得用户可以按照表对象、增量标签等方式定义管理数据子集。以满足用户对于生产库进行部分、增量分发脱敏的需求。

5.2.5.3 策略管理要求

支持对于系统内置的敏感数据自动发现策略以及数据脱敏策略进行规则管理的能力。支持在现有规则的基础上扩展新的敏感数据发现和脱敏规则，支持用户自定义敏感数据发现和脱敏规则。

5.2.5.4 任务管理要求

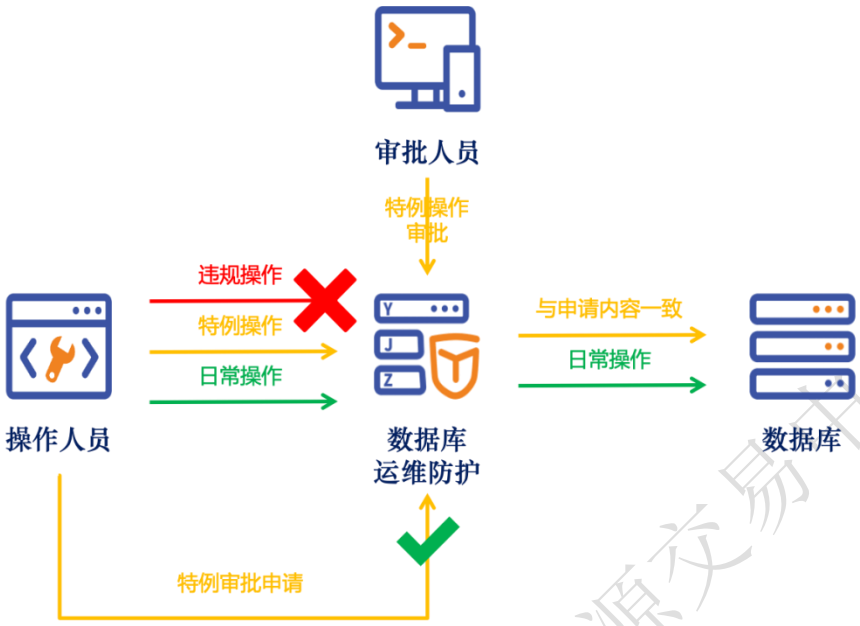
提供包括任务新增、查看、修改、启动、暂停等丰富的任务管理功能。

5.2.5.5 多种数据分发形式要求

支持多种形式的数据分发，包括数据库到数据库、数据库到文件、文件到文件、文件到数据库四种数据分发和输出方式，并且不需要在生产系统和本地安装任何客户端。

5.2.6 数据库运维管控要求

针对运维人员访问数据库专区中各类数据库时，通过部署数据库运维防护系统，对运维人员操作数据行为进行细粒度管控。内部运维人员往往拥有特权账户，如：SYSDBA、DBA、Schema User、其他 any 权限等。而这些运维人员为了工作方便还经常账户共用，存在数据泄露的安全隐患。为避免这类安全隐患，通过隔离 SYSDBA、DBA、Schema User、其他 any 权限等特权，使其权限最小化，只能访问授权范围内的敏感数据。一方面解决了运维人员拥有可访问数据库中任何数据的特权账户而带来的安全隐患，另一方面解决了黑客入侵后通过账户提权带来的安全隐患。



5.2.6.1 资产管理要求

- **资产发现**

系统可根据数据库类型、名称、IP 地址范围、端口等进行数据库的自动发现，并可对已发现的数据库进行具体信息核实及删除操作，帮助用户摸清数据库资产，减少管理员工作量，提高效率。

- **资产列表**

系统可对已发现的数据库进行防护开启、日常管理等操作。

- **资产数据**

对于数据繁杂的数据库类型，系统通过内置发现规则与自定义规则结合，帮助自动发现数据库中具有敏感数据特征的数据，如：姓名、手机号、住址、身份证号、社保账号、金融账号、企业等敏感信息，提高效率的同时，为数据安全防护提供依据。

- **资产账号**

系统可自动发现数据库中账号及数量信息，并可对已发现的数据库

账号进行管理，如账号信息核实、删除。

5.2.6.2 访问控制要求

- **模板白名单**

系统可对指定的数据库设置不同程度的可信模板并建立白名单，模糊匹配运维操作语句，避免不必要的防护，提高运维效率。

- **语句白名单**

系统可设置可信的 SQL 语句白名单，运维过程中无需对可信白名单中的 SQL 语句进行限制和阻断，提高运维效率。

- **策略规则**

数据库运维防护系统可针对不同维度设置风险策略规则，包括：管理资产信息、基本信息、来源信息、目标信息、访问信息等。

- **准入控制**

为防止非授权、非法用户登录并操作数据库，本系统通过运维预审方式，经管理人员逐条审阅、最终审批实现准入上的严格控制。

- **审批管理**

系统支持多级多人审批机制，可设置黑白名单及操作行为来限制运维人员操作，可对运维人员提交的运维申请详情进行查看、一键处理。

5.2.6.3 运维访问脱敏要求

系统可根据不同权限如管理账户、运维账户、外包人员账户等，对不同敏感数据（如姓名、身份证号、手机号、社保账号、住址、金融账号等）进行动态脱敏，防止内部人员利用职权非法收集、泄漏敏感数据，提高整体运维安全。

5.2.6.4 统计分析要求

系统支持多维度分析与统计，包括：来源分析、来源统计、目标统计、行为统计、申请统计、脱敏统计等，满足用户多角度统计分析需求。

5.2.6.5 报表分析要求

系统支持多种形式的报表，如综合报表、合规性报表、专项报表等，用户可根据自身需要自定义报表模板，可满足用户各场景需求。

5.2.6.6 合规审计要求

系统支持以下细粒度行为审计，如账号、SQL 语句、操作时间、IP 地址、使用终端、目标数据库、操作对象等,并支持精准审计检索能力，帮助用户准确、快速实现合规审计。

5.2.7 数据动态脱敏要求

针对业务人员通过应用系统访问后台数据时，通过部署数据动态脱敏系统，防止未授权的业务人员接触敏感数据，在未授权的业务人员通过业务账户访问敏感数据时，对敏感数据进行脱敏处理，避免敏感信息泄露。以业务用户识别技术为基准，以业务数据访问对象为保护目标，形成智能化的在线业务系统数据访问脱敏机制。在合法用户访问应用系统时，根据其业务需求，返回其必要的数据，而非其业务需要的敏感信息对其仅部分内容可见。

5.2.7.1 统计分析要求

可以统计数据库、敏感表、敏感列、数据库类型等信息；

可以统计终端访问、脱敏字段、资产访问等信息，并以 TOP5 方式进行展现，方便用户通过首页直观查看系统的整体运行和管理情况。

5.2.7.2 数据发现要求

- **数据库发现**

提供数据库自动发现和识别功能，减少管理员手工添加数据库的工作量。系统可以通过 IP 范围、端口范围自动识别数据库，已识别数据库可以由人工进行核实或删除。

- **数据库管理**

可以以数据库为防护目标，所有待防护的数据库需要添加到系统中进行管理。本功能提供手工添加待防护数据库的功能，并可对已添加数据库进行管理，包括编辑和删除。

- **识别规则**

内置针对符合特征的敏感数据的发现规则，规则包括：身份证等通用证件号、银行卡号、电话号码（手机、座机）、中文姓名、日期、Email

地址等。系统提供自定义识别规则功能，用户可以通正则表达式进行自定义。

- **数据字典**

提供数据字典功能，可以通过数据字典定义敏感数据发现规则，适用于无规律但可穷举型的数据目标。数据字典功能支持导入、导出，用户可以直接将数据库表结构信息导入到系统中，自动生成数据字典。

- **字段字典**

提供字段字典功能，可通过字段字典直接定义某个字段的数据类型，提高数据发现效率。

- **发现任务**

能够根据敏感数据识别规则，自动扫描检测数据源中的敏感数据。用户可以自主创建数据发现任务，针对指定的数据库进行自动扫描发现，并对任务进行管理。

- **敏感字段梳理**

能够针对自动识别的结果提供手动梳理能力，让用户可以对自动发现的结果进行敏感字段核实并进行调整。

5.2.7.3 脱敏方案要求

- **基于账号身份的脱敏规则**

为适配各类业务场景的数据脱敏需求，系统提供了基于应用系统账号识别能力，通过对应用系统账号识别，可对不同业务身份访问敏感数据时进行差异化管控，无论应用系统采用 B/S 架构还是 C/S 架构，系统均具备账号身份解析和对应动态脱敏能力。

- **脱敏算法管理**

内置针对符合特征的敏感数据脱敏规则，规则包括：身份证、日期、Email 地址、数值、英文字母、数字、汉字。

支持设置脱敏算法参数，如脱敏开始位置、替换字符长度等。

支持用户根据自身需求，自定义脱敏算法。

- **脱敏规则管理**

系统支持精确脱敏、模糊脱敏以及 API 脱敏三种模式。

（1）精确脱敏

以 SQL 改写为核心的脱敏模式，用户可以定义精确脱敏规则。

（2）模糊脱敏

以结果集改写为核心的脱敏模式，用户可以定义模糊脱敏规则。

（3）API 脱敏

系统可以代理数据接口 API，解决 API 接口数据交互过程中的敏感数据安全问题。

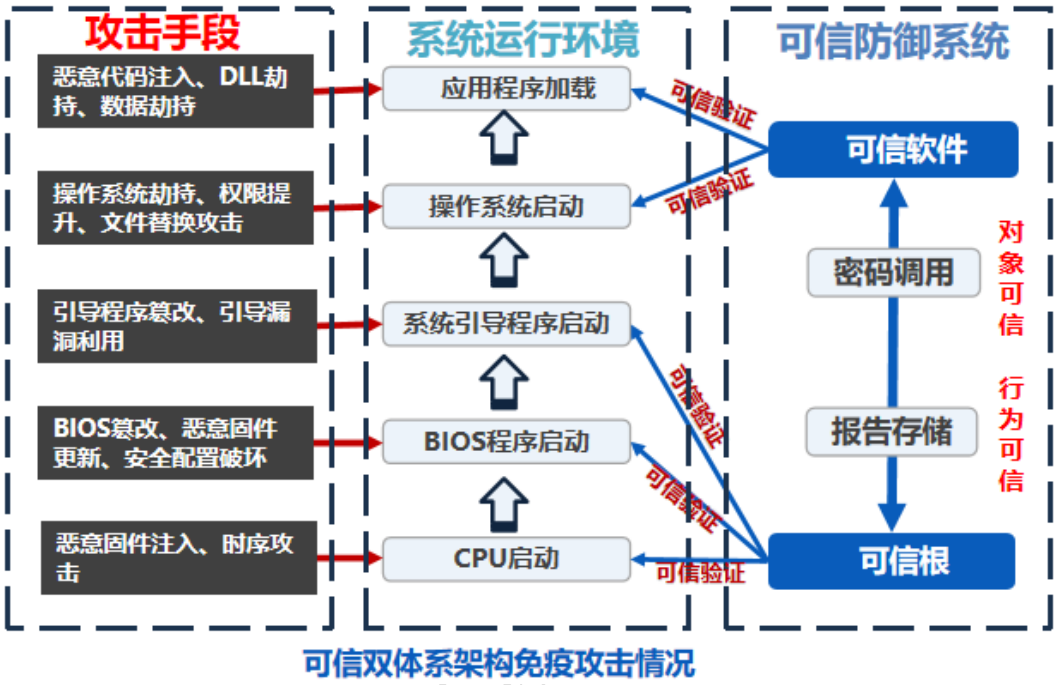
5.2.7.4 脱敏日志要求

系统提供脱敏审计功能，能够记录所有触发脱敏规则的数据访问行为。审计内容包括：数据库类型、来源地址、数据库名称、数据库地址、数据库端口、映射端口、访问的表名、访问的列名、规则名称、登录账户、时间等信息。

5.2.8 环境安保系统要求

融合先进的可信计算技术理念，深入挖掘当前主流安全软、硬件产品急需的主动防御需求，在涵盖主机安全软件常用功能的基础上，进一步提供符合网络安全等级保护要求（等级保护 2.0）的具有中国安全需

求和特色的可信产品，为现有系统构建自主防御体系，打造可信应用环境，抵御一切未知病毒、木马、恶意代码的攻击，形成我国自主创新的安全软件。



可信双体系架构免疫攻击情况

5.2.8.1 资源可信监控要求

可信安全管理平台可定时监控被控终端 CPU、网卡、硬盘、内存、主板、端口、资源、操作系统、进程、用户、服务、软件安装等一系列资源状况进行监控，使资源使用情况可视化、清晰化。

5.2.8.2 策略管理要求

对一个终端或一组终端进行策略的管理（增加、删除、下发），包括静态度量策略、动态度量策略、自主访问控制策略、强制访问控制策略、外设控制等。

5.2.8.3 审计管理要求

支持对终端审计、可信软件库和可信安全管理平台自身审计的展示、查询。

5.2.8.4 静态度量

恶意代码主动防御

能够对操作系统中可执行程序的执行请求进行度量，只允许经过可信度量的安全程序在系统中运行，并且可以拦截已知、未知病毒、木马及其他恶意软件。

软件行为控制

与可信软件库内策略进行联动，只有通过软件库认证检查过的软件才可以使用。阻止未授权软件和恶意软件安装使用。

软件安全分发

与可信软件库内软件分发策略进行联动，对多个终端进行不同软件的分发控制。

软件防卸载

保障正常业务程序及软件运行的完整性，阻止非法卸载。

程序完整性保护

为白名单中的程序提供完整性保护，所有在白名单的程序都受到系统安全机制的保护，禁止对白名单程序篡改。

5.2.8.5 动态度量要求

内核关键数据保护

支持对内核代码段、制度数据段、关键跳转表等操作系统正常运行过程中的关键数据，进行度量。保障系统重要数据结构的可信性，进而保障安全机制不被旁路和篡改，保障系统安全运行。

进程状态监测

支持对系统内的任意进程状态实现对运行时注入式攻击的检测，增强访问控制机制的安全性和有效性。

5.2.8.6 自主访问控制要求

用户自主访问控制

控制终端内主体为用户对客体目录、文件的访问，防止其他用户对自己的客体进行的攻击。

进程自主访问控制

控制终端主体为进程对客体目录、文件的访问，防止其他进程对自己的客体进行攻击。

5.2.8.7 强制访问控制要求

进程强制访问控制

提供基于内核层实现的主客体为进程的强制访问控制。

文件强制访问控制

提供基于内核层实现的主客体为文件强制访问控制，有效解决操作系统自身文件访问控制机制薄弱和操作系统超级用户权限过大带来的安全风险。

服务强制访问控制

提供基于内核层实现的主客体为服务强制访问控制，不准随意增加、删除、更改服务状态。

注册表强制访问控制

对于 Windows 操作系统提供基于内核层实现的注册表强制访问控制，保护 Windows 系统敏感注册表项或值不被删除或篡改。

外设强制访问控制

对 USB 存储设备进行访问控制。

操作系统账号强制访问控制

5.2.8.8 本地白名单要求要求

终端上的程序只有在白名单中才能运行，不在白名单的程序将拒绝执行。白名单在终端软件安装时可自动采集本地执行程序形成白名单，以后需通过管理中心下发白名单策略。

5.2.8.9 配置完整性要求

针对文件、进程、服务、注册表项、驱动进行信息预设、检查，并提供配置还原服务。

5.2.8.10 异常进程上报审批要求

支持对异常进程信息进行采集和上报，在可信安全管理平台可对其进行审核、批准。

5.2.8.11 进程保护要求

支持对系统内任意指定进程安全保护。保证其可用性，不被非法停止、篡改、注入等。

5.2.8.12 执行程序保护要求

对在白名单内的所有二进制可执行文件进行完整性保护，在未授权状态下无法对其进行修改，保证了所有执行程序的完整性、可用性。

5.2.8.13 可信软件信息采集要求

能够对操作系统中的业务应用软件、工具软件等程序信息进行采集，为内部服务器提供高可用的安全策略保障。可采集软件安装包，可执行程序，动态库，内核模块，驱动。

5.2.9 应用审计要求

5.2.9.1 全量资产梳理要求

- API 资产梳理

API 安全监测产品采用了先进的流量分析技术，可以从复杂的网络数据流中精准识别各类 API 接口路径及相关信息，如接口名称、请求方法、URL 路径、参数格式等；API 安全监测产品在成功识别出 API 接口之后自动化归类展示形成资产清单。

- 敏感数据梳理

系统内置敏感数据检测策略，对请求和返回中传输的敏感数据进行识别并打标，内置敏感数据识别规则包含身份证、手机号、银行卡、统一社会信用代码、军官证、车牌号、电子邮箱、护照号、手机 IMEI、固化号码、GUID/UUID、国内地址、邮政编码、车辆识别码、香港身份证号、澳门身份证号、台湾身份证号等常见敏感数据类型。结合用户已有分类分级策略或系统内置分类分级策略实现业务数据分类分级打标。

对于非常见的敏感数据类型支持自定义创建识别策略，通过内置结合自定义方式进行识别，提升数据敏感类型识别度；

- 应用账号梳理

基于对业务系统与用户交互信息的深入解析能力，该系统能够灵活采用多种方式实现应用系统账号信息的有效提取和识别。具体包括但不限于：

表单登录解析：通过监控并分析用户在网页表单中提交的登录信息，如用户名、密码等字段内容，自动捕获并解析相关账号数据。

Cookie 解析：利用内置的 Cookie 分析机制，从客户端发送到服务

器的 HTTP 请求头中读取包含用户会话信息或认证信息的 Cookie 内容，以识别用户账号。

HEADER 解析：通过对 HTTP 请求头部（Header）的深度挖掘，提取诸如 Authorization（认证授权）、Referer（来源地址）以及其他可能携带用户标识信息的 Header 字段，从而实现账号信息的精准解析。

JSON 解析：对于采用 JSON 格式传输的 API 请求体，系统能高效解析其中嵌台的用户身份属性，确保准确获取并记录账号信息。

读取会话信息：通过对接口调用过程中的会话管理机制，实时读取并解析用户在交互过程中产生的会话 ID、令牌（Token）等会话状态信息，进一步确认用户身份及其访问权限。

系统凭借多元化的解析手段，实现了对各类业务系统中应用账户信息的全面、准确识别和管理，为后续的安全策略制定与执行打下坚实基础。

- API **拆分合并**

一方面，系统支持按照应用、域名、HOST 以及 Path 等多种方式对 API 接口进行智能合并，这一特性有助于简化 API 资产管理，将具有相似属性或服务于同一功能模块的 API 接口归类整合，从而便于整体性的安全管理、性能优化和维护升级。

另一方面，系统支持按照 Query Param（查询参数）和 Header 参数等标准对 API 接口进行精细化拆分。这项功能有助于实现对 API 接口的微细化控制，特别是当需要根据不同的参数组合或请求头信息来区别对待 API 访问权限、日志记录或安全策略时，能够提供更为精确和有针对性的管理措施。

5.2.9.2 安全风险监测要求

系统集成了丰富且精细的内置安全策略，针对不同类型的潜在安全风险提供全方位的识别能力：

- **数据泄露类安全风险**

系统能自动检测并预警一系列可能导致敏感信息过度暴露的安全事件，如单次接口响应中返回过多敏感数据、超出常规阈值的敏感数据访问频率、来自境外对敏感数据的异常访问增加（境外敏感数据访问过量）、恶意翻页遍历以获取大量数据、通过参数遍历尝试挖掘隐藏信息等行为。

- **账户身份类安全风险**

针对账户登录与认证环节的安全隐患，系统能够有效识别多种账户威胁行为，包括但不限于账号登录失败次数超限、使用弱口令尝试登录、URL 中直接包含密码信息、用户账号在非常用地点或设备上登录（异地登录）、单一 IP 地址频繁使用多个账号登录（单 IP 多账号登录）、利用已泄露数据库进行批量验证（撞库攻击）以及暴力破解密码企图。

- **业务类安全风险**

对于影响业务正常运行和用户体验的风险场景，系统也具备强大的防范机制，可及时发现并阻止接口扫描攻击、短信轰炸式骚扰、验证码系统的滥用与爆破攻击、不合理的高频访问请求等行为。

- **Web 应用攻击风险**

针对常见的 Web 应用层漏洞与攻击手段，系统集成有先进的探测技术，能够实时监测并拦截 SQL 注入攻击、跨站脚本（XSS）攻击、Log4J 日志框架漏洞利用、远程文件包含（RFI）攻击、敏感文件的非法访问

和扫描活动、外部漏洞扫描器的探测行为、Java 反序列化漏洞利用尝试、Unix/Linux 命令注入测试以及路径穿越遍历攻击、服务器端请求伪造（SSRF）等高级 Web 攻击方式。

- 自定义风险识别规则

系统具备高度灵活的安全风险识别规则自定义配置功能，能够紧密围绕用户业务的具体特点和安全需求进行个性化设置。这一特性使得用户可以根据自身服务的性质、数据敏感程度、业务逻辑复杂性等因素来创建、调整或细化各类安全策略。

5.2.9.3 安全风险统计分析要求

系统具有强大的多维度风险分析功能，能够对各种类型的风险事件进行全面且细致的统计与分析。系统支持从多个关键视角展开统计：

按风险类型划分：针对 Web 攻击类、账户身份类、账号类及业务类等不同类型的安全风险，系统可以精准统计各类风险事件的发生数量，并提供详细的每一起风险事件的具体信息。

基于域名视角：系统能实时追踪并汇总各个域名下所发生的全部风险事件及其详细情况，包括但不限于风险事件总量、不同类型的攻击趋势以及具体受影响的资源和服务。

以 HOST 主机为单位：针对各台主机（HOST），系统可精确记录在预设时间段内与之相关的每个域名遭遇的数据安全威胁次数及其详尽统计报告。

用户层面统计：对于不同的用户，系统能够统计他们在特定时间范围内的所有触发风险事件的情况，帮助识别异常用户行为和潜在的内部威胁源头。

客户端 IP 地址统计：系统具备按客户端 IP 地址进行分类的能力，能够汇总来自不同 IP 地址的用户触发的风险事件数量，并展示相关风险指标如访问时间、来源 IP、风险等级、风险类别描述以及具体的告警消息内容。

系统通过多元化的统计手段，不仅能够宏观把握整个系统的风险分布和态势，还能深入微观层面剖析每一项风险事件的具体详情，同时提供了日志级别的追溯能力，方便进一步调查和处理，从而为管理者提供了全方位的风险评估依据和应对措施的基础数据支持。

5.2.9.4 业务访问审计要求

系统解析并记录用户访问行为，包括访问数据的 IP 地址、登录日期时间、应用账号、访问方式、是否是敏感数据、访问结果、数据对象等，支持详细记录所有应用接口数据完整的请求内容，包括请求时间、请求参数值、URL、账号、源 IP、域名、REFERER、COOKIE、UA、请求体、请求类型、返回长度、返回类型等。

基于监测日志提供多维度的统计分析能力，以及事件溯源能力，满足用户安全监测要求的同时法规和监管机构对日志记录要求。

5.2.9.5 加密流量解析要求

目前众多企业为了确保应用系统的安全性普遍采用 HTTPS 协议，因此对于加密的流量解析就成了一项难题。本方案采用 eBPF 技术对加密流量进行处理，eBPF（扩展的伯克利包过滤器）是一种强大的内核技术，能够在不修改内核源码的情况下，动态地插入自定义代码来监控和处理网络流量。对于 HTTPS 流量的解析，eBPF 可以通过挂载到网络协议栈的特定点（如 TCP 层或 TLS 层）来捕获加密前的明文数据。通过解析 TLS

握手过程中的 ClientHello 和 ServerHello 消息，eBPF 可以提取出服务器名称指示（SNI）等关键信息，从而识别 HTTPS 流量的目标域名。尽管 eBPF 无法直接解密 HTTPS 流量（因为加密发生在应用层），但它可以通过与内核事件（如连接建立、数据包传输）的关联，提供对加密流量的元数据分析和监控能力。

5.2.9.6 事件溯源分析要求

系统不仅具备实时监控和识别安全风险的能力，还集成了访问行为审计日志功能；在检测到潜在风险事件时，用户能够基于详尽的审计日志快速下钻至具体事件详情，对风险源头进行精准定位和深度溯源分析。一旦核实告警事件为正常业务行为或误报后，系统支持将这些事件加入白名单机制，确保在未来不再针对此类行为产生不必要的风险提示。

通过这种从风险发现、分析、处置跟踪管理的闭环流程设计，系统有效实现了安全事件的全生命周期管理；既避免了过度打扰正常的业务运行，又确保了在真正发生安全威胁时能迅速响应并采取相应措施，极大地提升了整体的安全运维效率和防护效果。

5.3 产品类技术参数要求

5.3.1 中新建数据治理统一定制化管控平台要求

序号	名称	平台系统内容			备注
		类别	模块介绍	功能参数要求	
1	中新	基本功能	综合安全态势	大屏展示纳管业务系统的安全概况信息。包括总日志数量、总风险数量、当日新增日志数量、	中新建数据安全治理统一定制化管控

	建数据治理统一定制化管控平台	要求		当日新增风险数量、未处置风险数量；已纳管业务系统数量、风险业务系统数量、风险业务系统占比；纳管应用资产数量、风险应用资产数量、风险应用资产占比；纳管数据库资产数量、风险数据库资产数量、风险数据库资产占比；数据库表数量、敏感数据库表数量、敏感数据库表占比；数据库字段数量、敏感数据库字段数量、敏感数据库字段占比；资产访问热度排行、风险类型排行、风险资产排行、风险用户排行、日志接入趋势、实时未处置风险滚动展示。	平台数据安全集中管控平台是数字化时代保障数据资产安全的核心枢纽，旨在打破数据安全单点防护壁垒，实现全域数据的集中化、标准化、智能化管控。平台全面覆盖结构化与非结构化数据，贯穿数据收集、存储、使用、传输、销毁全生命周期， 平台可自动发现全域数据资产并完成分类分级，通过统一接口联动各类安全设备，实现策略统一下发与集中管理。依托 AI 智能分析技术，平台能精准识别异常访问、数据泄露等风险并及时告警，同时生成合规报表，满足《数据安全法》《个人信息保护法》等监管要求。其适配混合云、本地部署等多环境，兼顾安全防护与业务连续性，筑牢数据安全底座，实现从被动合规向主动治理转型。
			资产分布态势	大屏展示平台纳管的业务系统的数据分布情况。包括：业务系统、数据库资产数量、数据表总数、字段总数、涉敏字段总数以及文件数量等； 图标展示数据类型统计、字段统计、文件统计、数据访问热度 TOP5，敏感数据分布 TOP5、数据类别业务分布 TOP5 和数据等级业务分布 TOP5 统计等	
			数据库资产安全态势	大屏展示数据库访问风险的综合信息，包括风险来源 IPTOP5，操作类型 TOP5，防护类型统计、高危指令分布、慢语句分布、风险分布、实时风险滚动展示等	
			应用资产安全态势	大屏展示 API 资产访问风险的综合信息，包括 API 资产分布，API 接口标签，域名/IP 总数、API 接口总数、涉敏 API 总数、API 漏洞攻击分布、API 风险类型分布、API 实时风险滚动展示等	
			★设备运行态势	大屏展示纳管安全设备的运行状态，简洁显示全部纳管设备的健康状态，详细显示具体设备的运行状态。可切换设备，显示不同设备的详细状态。运行状态信息包括：主机运行时间、主机 CPU 核数、主机物理内存总量、CPU 使用率、内存使用率、磁盘根分区使用率。可详细显示时间区间内主机 CPU 的 sys 态最大使用率、最小使用率，user 态的最大使用率、最小使用率等。可详细显示区间时间内磁盘 IO 最大读取速率、最大写入速率、最小读取速率、最小写入速率等。可详细展示区间时间内最大上行网络流量、最大下行网络流量、最小上行网络流量、最小下行网络流量等（投标文件中提供截图证明）	
			业务系统管理	支持自定义资产层级结构，用户可配置地域、部门、业务系统等层级关系，并且与数据资产进行绑定，以业务视角对资产进行直观展示	
			数据资产管理	支持对数据库的资产进行展示，并且可以通过手动任务去发现资产或者通过同步标品的资	

				产到平台，通过平台可以对某些资产做安全防护措施	
			应用资产管理	支持对应用审计的的资产进行展示，并且可以通过手动创建资产或者通过同步标品的资产到平台，通过平台可以对某些资产做安全防护措施	
			资产自动发现	通过 IP 网段定义，自动扫描网段内的数据库资产，支持多网段同时扫描； 支持扫描任务编辑、单次执行、定时执行设置； 支持扫描历史查看，分析任务历史执行情况；	
			数据资产扫描	支持对资产通过梳理任务进行扫描 支持对扫描的情况通过日志记录 支持将扫描结果展示并且以图表的形式展示分析	
			资产目录	通过数据资产发现、数据资产扫描，以及分级分类打标结果，形成资产台账。包括业务系统维度、数据库资产维度、数据库表维度、数据库字段维度的分类展示。展示内容涵盖资产组织结构、业务名称、资产名称、资产类型、资产标识、资产描述、资产负责人等信息。	
			字段目录	通过数据资产自动扫描、人工核实后，形成数据目录。以资产组织结构逐层下转，盘点数据资产详细信息，支持丰富的图表统计展示；	
			账户目录	通过自动扫描发现的数据库账号信息、人工核实后形成数据库账号目录。以资产组织结构展示数据资产账号信息。账号信息包含：数据资产名称、资产账号、拥有权限、禁止权限、是否锁定、账号过期时间等。	
			文件目录	通过数据资产梳理、人工核实后，形成文件数据目录。以资产组织结构逐层下转，盘点数据资产详细信息，支持丰富的图表统计展示；	
			变更目录	通过对数据资产做定时扫描梳理，自动生成和台账信息对比的差异数据。如新增表、新增字段、新增账号、删除表、删除字段、删除账号等信息。为管理员提供一目了然的数据变化情况展示。管理员对变更数据进行确认后，更新台账信息。	
			重要数据管理	通过数据资产扫描，自动标识业务系统中的重要数据。可自定义重要数据识别规则，可手动修改重要数据标识； 可通过手动添加或者批量导入维护重要数据	
			核心数据管理	通过数据资产扫描，自动标识业务系统中的核心数据。可自定义核心数据识别规则，可手动修改核心数据标识； 可通过手动添加或者批量导入维护核心数据	
			数据分级分类	内置多种行业的数据分级分类规则； 可自定义数据分级分类规则；	

				根据定义好的分级分类规则，在资产扫描时，自动进行分级分类；	
			数据打标	对具有敏感特征的数据自动进行打标； 打标数据可手工调整； 对打标的数据可通过修改关联的分级分类规则进行批量修正； 支持按照目录、分级分类、数据特征不同维度进行筛选打标；	
			★AI 打标	支持通过输入少量打标样本，进行深度学习，对大量数据进行自动打标，减少人工打标的工作量。支持对单一字段的分类分级 AI 推荐。AI 智能打标训练时具备自我验证能力，并能够在线查看分类正确率。（投标文件中提供截图证明）	
			文件打标	对具有敏感特征的数据自动进行打标； 打标数据可手工调整； 对打标的数据可通过修改关联的分级分类规则进行批量修正； 支持按照库表、分级分类模板、数据特征不同维度进行筛选打标；	
			分级分类统计	支持按照特征、类别、级别对文字进行统计 支持按照特征、类别、级别对文件进行统计	
			数据识别策略	支持通过页面设置扫描规则以及扫描模板从而灵活应用	
			数据动态脱敏	支持对数据库敏感数据的访问进行遮蔽、随机替换等方式的脱敏； 支持敏感数据识别、并根据敏感数据生成脱敏规则； 支持基于 SQL 改写和基于结果集改写的双模脱敏方式；	
			数据静态脱敏	支持库到库、库到文件、文件到文件、文件到库等脱敏方式； 支持敏感数据识别，并形成数据台账； 支持数据子集管理，对选定的数据子集做周期性脱敏； 支持脱敏方案管理，方便灵活配置数据子集、脱敏算法的关联； 支持脱敏任务管理，可直观展示脱敏任务状态，可启动、暂停、恢复、停止脱敏任务；	
			数据透明加密	支持数据库表级加密、列级加密； 支持创建密文索引，保证字段加密后不影响查询性能； 支持秘钥管理，对秘钥进行备份、恢复，支持对秘钥进行周期轮换；	
			数据运维管控	支持自动发现数据库资产以及手动发现数据库资产 系统支持自定义访问控制规则功能，规则设置	

				条件大于 30 种，至少包括等级、优先级、响应动作、时间、IP、时间组、数据库账号、MAC、源程序、主机名、系统用户名、数据库账户组、阈值、动作、对象、字段、表、数据库、schema、SQL 关键字等； 支持语句白名单，可以自定义无需审计的语句名单，降低时间溯源扰乱因素，提高系统分析效率，系统支持模板白名单，过滤工具自动生成的无害语句，提高审计效率，过滤无用信息，模板白名单支持自学习建立功能； 支持自学习功能，可以自动建立访问基线并开展准入管控； 支持库到库、库到文件、文件到文件、文件到库等脱敏方式； 支持敏感数据识别，并形成数据台账； 支持数据子集管理，对选定的数据子集做周期性脱敏； 支持脱敏方案管理，方便灵活配置数据子集、脱敏算法的关联； 支持脱敏任务管理，可直观展示脱敏任务状态，可启动、暂停、恢复、停止脱敏任务； 支持用户的操作行为通过工单审批控制	
			数据安全审计	支持数据库操作行为审计，会话审计、风险审计； 内置丰富的风险规则，并按照不同数据库类型默认分组，同时支持自定义添加。 支持按 SQL 操作类型、风险类型、风险级别、客户端来源、SQL 流量等多维度进行统计分析，支持对统计数据进行下钻分析、以列表方式展示分析结果。 支持 30+种报表分析，支持报表预览、报表导出、报表定时生成等	
			数据风险列表	支持对审计的数据库风险信息以列表方式展示，并且可以去处理这些风险	
			数据风险分析	支持对审计的数据库风险以二维柱状图、折线图的方式分析展示	
			应用资产审计	支持从流量里对应用系统、API 接口等做自动梳理，形成应用列表、API 接口列表； 支持 API 接口审计，对 API 调用进行详细日志记录； 支持通过规则配置，对 API 调用风险进行识别，并通过图形化方式展现； 支持对 API 调用风险进行分析及溯源	
			应用风险列表	支持对审计的应用接口风险信息以列表方式展示，并且可以去处理这些风险	
			应用风险分析	支持对审计的应用接口以二维柱状图、折线图的方式分析展示	

			用户认证管理	支持大数据组件的统一用户认证，提供 LDAP、Kerbors 等认证服务体系	
			资产权限管理	支持大数据组件的统一数据权限管理功能	
		定制化研发服务	设备注册登记	在数据安全管控平台中添加数据安全设备进行注册，注册后的设备在管控平台中进行统一管理，包括策略设置、风险监控、状态监控、告警监控等。	
			多设备管理	支持多种类型安全设备同时接入； 支持多台同类型设备同时接入； 支持设备分域管理，如：网络可达的情况下，不同数据中心的设备可以同时接入平台，并且该设备及该设备纳管的资产仅对具有管理权限的用户可见。	
			安全能力页面级接入	支持多种类型、多台设备页面级接入，无需跳转到单独的设备页面进行操作； 支持页面级集成的策略管理，无需对策略二次下发；	
			设备授权统一管理	在数据安全平台中对数据安全设备进行统一授权、授权查看、授权更新等	
			设备告警统一管理	在数据安全平台中统一设置安全设备的告警参数，并进行统一告警。如 CPU、内存、磁盘占用率阈值设置、告警接收人设置、告警方式设置等。告警方式支持邮件、Syslog、Kafka 等方式。	
			设备操作统一审计	可集中监控安全设备的策略配置、策略修改等操作行为，并形成日志，方便审计员集中对设备操作进行审计。	
			部门管理	支持按照组织结构管理部门，包括增加、删除、修改部门信息。	
			角色管理	平台内置安全管理员、系统管理员、审计管理员三个角色；	
			用户管理	支持按照组织结构的分层用户管理。如集团公司，省公司、地市公司，每个层级可以有自己的管理员，对自己层级内的用户和设备做管理。	
			主机设置	支持设置主机名称、时间、时间服务器；支持主机网络设置。	
			安全设置	支持设置密码策略，如密码过期时间、非法登录保护、登录保护锁定时长、登录操作过期时间、密码复杂度等； 支持设置 web 访问限制、ssh 访问限制，如白名单、黑名单。	
			外发配置	支持全局数据外发的配置，供系统其他模块调用。外发至少包含邮件外发，syslog 外发，kafka 外发	

5.3.2 威胁监测与分析系统要求

序号	指标要求
1	性能与授权规格：混合流应用层处理能力≥15Gbps，包含基础系统软件一套，包括网页漏洞利用检测、webshell 上传检测、网络攻击检测、威胁情报检测功能，提供离线 pcap 包导入检测、基础旁路阻断和基础 SSL 解密功能。提供 3 年威胁情报更新授权与规则升级授权。
2	威胁检测功能：支持网页漏洞利用、反病毒引擎、webshell 上传、网络攻击、威胁情报、ICMP 隧道、HTTP 隧道、网络渗透测试工具 MSF、挖矿流量、代理流量、暗网流量、弱口令、SSH 爆破登录成功等检测功能，且上述功能可单独开启或关闭，提供上述功能截图。
3	★平台接入功能：流量传感器作为分析平台的流量采集组件，可通过监听口接收交换机镜像流量进行分析检测，并通过管理口上传检测数据至分析平台，提供 CNAS 认可检测机构出具的针对上述检测环境图的检测报告关键页证明。
4	AI 检测能力：支持灵活开启机器学习模型，增强检测精度，模型至少包括：ICMP 隧道检测、DNSTunnel 检测、HTTP 隧道检测、CS 流量检测、MSF 检测、挖矿流量检测、代理流量检测、暗网流量检测、弱口令检测、SSH 爆破登录成功检测。【可提供第三方检测报告证明】
5	隧道封装识别：支持多层 VLAN、VXLAN、MPLS、GRE 等网络流量的解析检测；云场景下，支持 GENEVE 协议双层隧道封装流量的解析检测。【可提供第三方检测报告证明】
6	加密流量攻击检测：支持针对 SSL 加密协议的攻击检测。【可提供第三方检测报告证明】
7	API 资产发现：支持识别 API 资产中的敏感信息，包括手机号、银行卡号等，同时敏感信息支持高亮并脱敏显示。
8	SSL 解密功能：支持对 HTTPS、IMAPS、SMTPS、POP3S 等 SSL 加密流量进行解密，提供上述功能截图。
9	安全检测能力：原厂商具备较强漏洞挖掘能力，可将挖掘的漏洞信息生成相关检测规则提升设备检测能力，2022—2024 年任意一年向国家漏洞共享平台 CNVD 提交漏洞数≥30000 个，提供 CNVD 出具的提交证明。
10	资质证书要求：产品具备公安部销售许可证证书或网络安全专用产品安全检测证书、信息技术产品安全测评证书 EAL3+，各证书及相关功能检测报告登记的产品名称、软件版本一致，提供证书复印件证明。

5.3.3 数据静态脱敏系统要求

序号	指标项	指标要求
1	性能参数	默认支持数据库类型：10 种 峰值脱敏速度：80G/h 最大脱敏能力：800000 单元格/秒 视用户数据库吞吐性能而定
2	资产兼容	支持主流、国产、大数据类型 oracle、mysql、sqlserver、postgres、达梦、hana、hive 等，支持文件 csv、txt、excel、xml、dmp、json、dicm、docx 文件等（投标文件中提供截图证明）
3	管理平台	系统基于 B/S 架构，采用 HTTPS 方式远程管理，中文图形管理界面
4		系统支持管理平台进行资产配置、扫描发现、方案配置、任务配置等
5	脱敏方式	系统支持库到库、库到文件、文件到文件、文件到库等方式进行脱敏
6		系统支持 oracle、mysql、sqlserver、postgre 间的资产异构方式脱敏
7		系统支持通过 FTP,SFTP,NFS 协议访问 NAS 盘中的文件,对存储的数据文件进行脱敏
8	资产管理	系统支持在资产添加时进行连接测试
9		系统支持文件资产的本地上传
10		系统资产管理应支持脱敏源、脱敏目标进行区分，防止数据误操作覆盖
11	敏感数据识别	系统内置敏感数据特征规则库，应支持手机号、座机号、中文地址、日期、社会统一信用代码、银行卡号、电子邮箱、身份证号、ip 地址、姓名、车牌号、车架号、港澳居民来大陆通行证号、中文大写金额、金额数字、营业执照注册号、企业组织机构代码、税务登记号码、房屋产权证号、不动产权登记号等不少于 20 种敏感类型特征特征进行自动识别发现
12		系统支持基于字段、内容方式进行数据的识别发现
13		系统支持按照模式、表对象等方式进行扫描对象的选择，抽样方式支持按照全表、行数、百分比方式进行选择，取样数据支持前、后、随机方式进行取样并支持过滤空值，命中判断支持满足行数、百分比两种方式且支持选择是否统计数据源表对象行数
14		系统支持增量敏感发现能力、枚举敏感发现算法，敏感发现算法支持互斥性属性（投标文件中提供截图证明）
15		系统支持按照需求配置组合发现策略，单张表同时包含组合策略中的多种敏感类型判别为敏感对象
16		系统支持对多次执行敏感任务对发现结果做比对
17		系统支持自定义发现规则添加
18	数据台账	系统支持对扫描的结果形成台账，数据台账支持按照表、字段两个视图维度进行展示，台账信息支持数据库、模式名、表名、字段名、字段类型、敏感类型、敏感类型种类、样本数据等信息进行展示
19		系统支持台账信息敏感类型进行调整；支持台账信息的导出和导入功能

20	脱敏配置管理	系统支持脱敏子集的配置，子集应支持定义脱敏的表范围、表内数据支持配置过滤条件，过滤条件支持大于、小于、大于等于、小于等于、等于等条件并支持对 sql 进行预览调整；子集支持手动添加、从数据台账中直接生成等
21		系统支持脱敏方案的配置，脱敏方案支持关联模板算法或直接引用系统默认分配算法，支持按照敏感类型进行脱敏算法关联调整，支持按照字段级别为字段选择脱敏算法
22		系统支持对生成的脱敏方案进行脱敏预览功能，脱敏前进行脱敏预览检查脱敏结果是否符合数据使用质量（投标文件中提供截图证明）
23		系统支持从数据台账直接生成脱敏方案配置
24		系统支持脱敏前检查环境信息，检查环境是否具备脱敏环境条件
25		系统支持脱敏任务管理，任务启动应支持任务启动、停止、暂停、继续，支持对脱敏表并发、表内并发等参数设置（投标文件中提供截图证明）
26		★系统支持根据系统资源动态调优管理任务线程，增加脱敏性能（投标文件中提供截图证明）
27		系统脱敏任务支持对表对象以外的其它对象的迁移功能，如序列、视图、包、函数、存储过程、索引、约束、触发器等
28		系统脱敏任务支持对脏数据的处理，处理方式包括置空、迁移、随机生成方式
29		系统应支持增量脱敏功能，通过配置增量字段（自增、时间及其他类型）实现自动增量脱敏，实现定期调度源库进行增量脱敏（投标文件中提供截图证明）
30		系统支持多版本多行业分级分类脱敏方案，根据分级分类标准查看数据台账，生成脱敏方案，并进行脱敏。
31		系统支持快捷脱敏，用户仅仅关注源库、目标库，降低脱敏操作门槛
32		系统支持文件视图（上传/SFTP/FTP），显示文件列表，支持选择指定的文件进行脱敏后下载或脱敏后迁移
33		系统提供界面查看脱敏前后数据表的数据字段内容变化对比视图（投标文件中提供截图证明）
34	脱敏算法	产品内置丰富敏感数据自动发现规则，包含中文姓名、身份证号、固定电话、手机号码、银行卡号、电子邮箱、中文地址、邮政编码、企业单位名称、组织机构代码、营业执照代码、税务登记代码、企业三证合一代码等在内的常见敏感数据格式；并提供自定义数据类型添加功能，列名或者数据内容
35		系统内置置空、遮蔽算法、随机算法、仿真算法，可以根据实际需求转变为不同的脱敏效果
36		系统支持编写自定义算法，来满足个性化的脱敏需求；同时支持对混合数据、复合数据的脱敏支持，自定义码表算法支持还原，自定义算法导入导出。
37		系统支持复杂文本脱敏算法，XML 脱敏算法， JSON 脱敏算法，脱敏数据库字段中的复杂对象信息（投标文件中提供截图证明）
38		系统提供可视化编程能力,按业务表细粒度的控制脱敏范围和脱敏规则。支持表内字段逻辑关系保持，表内字段逻辑关系自定义，支持常用逻辑计算

39	模板管理	系统提供模板配置脱敏数据，并对选择的脱敏数据进行脱敏算法的选择，实现多组敏感数据、脱敏算法关联模板管理复用场景，模板导入导出。支持默认脱敏策略设置，并在敏感发现与数据方案处使用默认的脱敏策略
40	任务定时调度	系统支持对发现、脱敏任务创建定时调度任务
41	脱敏审批	系统支持审批能力可选择是否开启，开启后任务审批后才可进行脱敏任务执行（投标文件中提供截图证明）
42	分权分域	系统支持数据分权分域，数据资源隔离，提供项目组/项目管理。以项目组为管理单元，管理脱敏用户账号；以项目为管理单元，管理脱敏配置信息
43	系统维护	支持页面重启服务、重启设备、网络配置等功能
44	三权分立	系统应按照系统、操作、审计角色内置三权用户

5.3.4 数据库运维管控系统要求

序号	指标项	指标要求
1	性能参数	默认支持数据库授权（IP+PORT）：12 个 SQL 峰值处理能力：45000 条/秒 最大并发连接数：45000
2	数据兼容性支持	支持 Oracle 、Mysql、Sqlserver、PostgreSQL、DM、KingBase、Gbase8a、Gbase8s、Gbase8C、Hana、Informix 、Mariadb、Hana、Alisql、TD-SQL、MongoDB、瀚高、Hive、Hbase、CirroData、Kaiwudb 等国内外主流数据库。（投标文件中提供截图证明）
3	统计分析	统计并展示资产信息，包括数据库数量、数据库账号数量、敏感字段数量（投标文件中提供截图证明）
4		统计并展示运维工单信息，包括待审批工单数量、已审批工单数量、未通过工单数量（投标文件中提供截图证明）
5		统计并展示防护策略信息，包括语句白名单数量、防护策略数量、虚拟补丁数量（投标文件中提供截图证明）
6		统计并展示防护状态信息，包括语句总量、风险总量、脱敏次数（投标文件中提供截图证明）
7		统计并展示敏感数据以及敏感数据库的信息，包括已防护敏感数据类型及数量、未防护敏感数据类型及数量（投标文件中提供截图证明）
8		统计并展示防护趋势信息，包括白名单放行、审批放行、准入拦截、漏洞拦截、策略放行、策略拦截、策略阻断、审批拦截等数据（投标文件中提供截图证明）
9		统计并展示风险访问 TOP5，资产访问热度 TOP5（投标文件中提供截图证明）
10	管理平台	系统基于 B/S 方式，采用 HTTPS 方式远程 WEB 安全管理，无需安装管理客户端，中文操作界面；

11		系统自带网络流量抓包功能，帮助管理员分析流量、判断问题，支持根据流量包大小或者时间进行过滤，支持指定 IP、指定端口或者全部网络数据进行抓包。（投标文件中提供截图证明）
12		系统支持丰富的备份策略，包括配置备份、系统日志备份以及业务日志备份功能，用户可以根据需要进行灵活备份，在需要时可以进行数据还原。（投标文件中提供截图证明）
13	资产管理	支持自动发现数据库资产信息，可以自动获取数据库端口、类型、IP、版本等信息（投标文件中提供截图证明）
14		可以识别数据信息，可以识别敏感数据类型，支持自定义敏感数据识别规则
15		支持识别数据库账号信息并以列表形式展示（投标文件中提供截图证明）
16		支持资产分组管理和资产别名管理（投标文件中提供截图证明）
17	数据动态脱敏	系统支持数据动态脱敏功能，提高运维侧数据防护能力
18		系统内置常用脱敏算法，内置数量大于 20 条，同时支持精准脱敏和模糊脱敏两种模式（投标文件中提供截图证明）
19	访问控制	系统支持模板白名单、语句白名单功能（投标文件中提供截图证明）
20		系统支持自定义访问控制规则功能，规则设置条件大于 30 种，至少包括等级、优先级、响应动作、时间、IP、时间组、数据库账号、主机名、MAC、源程序、系统用户名、数据库账户组、阈值、动作、对象、字段、表、数据库、schema、SQL 关键字、结果集关键字、影响行数等（投标文件中提供截图证明）
21		系统支持分组设置，分组类型至少包括时间分组、数据库分组、查询类型分组、访问表分组（投标文件中提供截图证明）
22		系统支持自学习功能，可以自动建立访问基线并开展准入管控（投标文件中提供截图证明）
23		★系统支持虚拟补丁功能（投标文件中提供截图证明）
24	人员管理	系统支持创建审批人员账号，支持创建运维人员账号（投标文件中提供截图证明）
25		系统支持多级审批功能
26	工单管理	系统为审批人员提供待办工单界面，可以查看运维申请并进行审批（投标文件中提供截图证明）
27		系统为运维人员提供运维申请界面，可以提交运维申请
28		系统支持记录全部工单信息，便于管理人员进行回顾、分析
29		系统提供运维工单自动生成能力，当运维人员没有权限执行相关操作且需要通过审批才可操作时，系统将针对本次操作行为自动生成工单（投标文件中提供截图证明）
30	运维身份管理	系统提供运维身份管理功能，通过在系统建立运维账号，并与数据库账号进行关联，运维人员无需掌握数据库账号密码，使用运维账号登录访问数据库（投标文件中提供截图证明）
31	报表功能	系统内置丰富的报表模板，包括综合报表、合规报表、专项报表等
32	日志审计功能	系统支持全量日志记录及审计；
33		审计查询条件至少包括：风险等级、策略优先级、响应动作、时间、IP 地址、时间组、数据库账号、主机名、MAC 地址、源程序、系统用户名、数据库账户组、阈值、动作、对象、字段、表、数据库、schema、SQL 关键字、结果集关键字、影响行数等；
34		审计支持会话关联分析，SQL 回放；

35	部署方式	支持反向代理、透明代理的部署方式
36		支持 HA 部署模式
37		支持集群部署模式，且不需要额外的负载均衡设备
38		支持硬件 bypass

5.3.5 数据动态脱敏系统要求

序号	指标项	指标要求
1	参数要求	默认支持数据库授权（IP+PORT）：12 个 最大脱敏能力：60000 单元格/秒 最大并发连接数：7000
2	管理平台	系统基于 B/S 方式，采用 HTTPS 方式远程 WEB 安全管理，无需安装管理客户端，中文操作界面；
3		系统具备系统参数配置、资产管理、敏感数据的发现、脱敏规则配置、脱敏算法的管理、敏感数据特征等功能模块（投标文件中提供截图证明）
4	统计分析	资产统计：系统可以统计数据库、敏感表、敏感列、数据库类型等信息；
5		访问统计：系统可以统计终端访问、脱敏字段、资产访问等信息，并以 TOP5 方式进行展现；（投标文件中提供截图证明）
6	数据兼容性支持	支持 oracle、mysql、sqlserver、postgre、mariadb、hana、informix、clickhouse、sybaseASE、sybaseIQ、dm、kingbase、gbase8a、gbase8s、highgo、oscar、greenplum、teledb、Gbase_8c、KaiwuDB、Doris、DB2、行云、cirrodata、alisql、tdsql、hive、hbase 等国内外主流数据库。（投标文件中提供截图证明）
7	数据源管理	系统支持数据库资产的连通性测试。
8		系统支持按资产名检索
9		系统支持 ORACLE RAC 的数据脱敏（投标文件中提供截图证明）
10		系统支持 MYSQL 读写分离的数据脱敏
11		支持 Mysql ssl 加密链路的解析和脱敏
12		支持 Mysql 压缩传输协议的解析和脱敏
13		支持对数据库的资产按照分组的方式进行管理（投标文件中提供截图证明）
14	资产状态	支持对资产内的资产信息进行统计，统计数据包含敏感表统计、敏感列统计
15		支持查看资产的敏感数据发现结果（投标文件中提供截图证明）
16	分类分级	支持分类分级关联敏感规则创建分类分级模板（投标文件中提供截图证明）
17		支持分类分级导入，同时支持手动创建 支持分类分级增加修改删除等功能（投标文件中提供截图证明）
18	敏感数据智	系统内置至少 20 类预定义敏感数据智能发现规则；

19	能发现	支持自定义扩展敏感数据特征，新扩展的敏感数据特征可以通过数据发现功能进行识别
20		支持敏感数据的自动发现能力，能对姓名、地址、电话、手机号、身份证、统一信用代码、银行卡号等 20 种敏感信息智能识别。
21		系统支持数据字典功能，满足个性化敏感数据发现需求。（投标文件中提供证明截图）
22	脱敏算法支持	系统内置一些常用的算法类型，包括遮蔽脱敏、随机替换等；内置脱敏算法总数不少于 60 种
23		支持添加自定义脱敏算法，满足客户对脱敏效果的个性化需求
24		支持复杂 SQL 请求的脱敏，包含但不限于：select *，嵌台和多层嵌台，连接（左连接、右连接、内连接）查询，比较查询、模糊查询、范围查询、分组查询等（投标文件中提供证明截图）
25		支持 Mysql 的 SSL 证书导入，支持采用 SSL 连接的脱敏
26	脱敏规则	支持通过敏感特征，批量生成脱敏规则
27		★精确脱敏：以 SQL 改写为核心的脱敏模式，用户可以定义精确脱敏规则；（投标文件中提供证明截图）
28		★模糊脱敏：以结果集改写为核心的脱敏模式，用户可以定义模糊脱敏规则；（投标文件中提供证明截图）
29		API 脱敏:支持对 API 接口调用数据进行脱敏(投标文件中提供证明截图）
30		支持脱敏规则导入导出（数据发现规则、脱敏算法、脱敏规则）
31	部署方式	支持反向代理和透明代理的部署方式；脱敏系统无需在数据源安装任何代理程序，针对数据库环境仅通过 JDBC 数据接口配置。
32	高可用	支持集群部署模式，且不需要额外的负载均衡设备
33		管理端支持 HA 主备模式，主管理端宕机后，可以自动切换到备机并进行接管，主备之间保持配置同步。
34		系统支持 bypass 功能，避免单点故障。
35	三权分立	应能通过对授权用户给以不同的安全角色，赋予授权用户不同的访问权限，并且安全角色之间相互制约，重要功能(如用户/权限管理、审计记录管理、数据脱敏任务管理和对敏感数据进行操作)应由不同用户执行；
36		支持对每个管理员设置不同的管理权限，权限颗粒化设置，可有效的控制权限粒度，减少管理员误操作风险；

5.3.6 数据库加密系统要求

序号	指标项	指标要求
1	性能参数	默认支持数据库授权（IP+PORT）：8 个 最大加密列数：100 列 最大加密能力：30000 行/秒
2	部署方式	支持旁路模式部署
3		支持 HA 主备模式

4		任一部署模式下都无需修改应用系统代码，业务系统及数据库访问工具如 PL/SQL、JDBC、ODBC 等访问数据库时不受影响，实现透明加密
5	安装卸载	软件支持自动化安装和卸载，支持直接在原生操作系统上部署，不依赖原厂操作系统包
6	管理平台	系统基于 B/S 架构，采用 HTTPS 方式远程管理，中文图形管理界面
7		系统具备页面化管理功能，产品的自身管理、加解密管理、策略配置等
8	加解密功能	提供数据加解密、密文索引创建/删除等操作向导
9		支持对 Oracle、SQL Server、MySQL、人大金仓（Kingbase）、达梦等数据库的透明加解密
10		加密算法至少应支持 3DES、AES 等国际密码算法，SM4 国密算法
11		★支持列、表两种细粒度的加解密方式（投标文件中提供截图证明）
12		对于密文数据的增删改查操作、函数、存储过程等均透明
13		数据加密后不影响原表的主外键关联
14		支持 not null、default 值、唯一约束等重要约束列加密，且约束生效（投标文件中提供截图证明）
15	密文存储	加密后的数据文件以密文形式存储于磁盘
16	密文索引	支持对加密数据使用密文索引技术，提升密文数据检索速率
17	数据列变更	支持对密文表进行数据列的添加/删除，添加时可指定列名、数据类型、长度、not null、默认值、注释等（投标文件中提供截图证明）
18	访问管理	对业务无感知，加密对业务访问结果不产生影响
19		支持基于身份的密文访问控制，身份要素至少包括 IP 地址、数据库账户、操作命令等，根据用户权限进行数据库返回结果控制，只有拥有合法权限的数据库用户才可看到明文，无合法权限的用户禁止访问
20	秘钥管理	支持对加密后的密钥进行备份/恢复，包括本地备份和远程备份，防止密钥丢失带来的数据不可恢复问题
21		支持通过平台下载密钥。支持对密钥进行周期轮换（投标文件中提供截图证明）
22	任务队列管理	支持加解密任务队列信息可视化展示，包括资产名称、任务描述、资产类型、任务状态、耗时、查看子任务信息等
23	加密查询	支持根据数据资产查看加密的列表信息，以表加密、列加密两个维度查询当前的加密资产，并可对加密资产进行解密操作
24	告警信息	支持以图形、列表等方式查看告警信息，告警信息应当包含告警时间、告警内容等。

25		告警方式至少包括：企业微信、邮件、短信
26	三权分立	支持系统管理员，安全管理员，审计管理三权分立

5.3.7 数据环境安保系统要求

序号	指标项	指标要求
1	基本功能	采用主动防御机制，使用基于可信计算技术的操作系统内核级安全机制。
2		
3		软件自身具备安全防护机制，实现软件自保护功能。
4		支持远程推送安装，支持自动化静默安装。
5		产品采用 C/S 架构，B/S 管理的方式。
6		产品支持 Windows 操作系统平台；2003SP2 以上版本；Linux 开源系列，国产操作系统：银河麒麟 v7 V10、统信 V20、麒麟信安(全系列)、凝思（全系列）
7	可信程序列表	根据可信计算机制对可信程序进行维护和管理。
8	可信静态度量	支持在软件程序启动时通过可信度量机制对程序、重要配置参数进行完整性度量。只有在度量结果和预期值一致的前提下，才允许程序运行，否则拒绝运行，实现对已知/未知病毒、木马、攻击程序等恶意代码的防护能力。
9	可信动态度量	通过动态度量技术对程序、模块、文件系统等操作系统运行中的关键数据进行监控（投标文件中提供截图证明）
10	自主访问控制	支持基于 RBAC 模型的访问控制功能。控制用户和进程对目录、文件、注册表的访问和操作，非授权用户和进程对受控目录、文件、注册表的访问和操作。同时支持远程共享目录、文件的访问控制。
11	强制访问控制	支持基于 BIBA\BLP 模型的强制访问控制功能，主体是用户、进程，客体是文件、进程和设备。支持远程共享目录、文件的访问控制。
12	外设控制	支持对 USB 存储设备使用进行控制，未授权设备无法使用。
13	本地审计	支持受控节点（服务器和 PC 等，下同）存储安全审计信息，并且可本地查看。
14	文件完整性保护	支持对系统关键文件的保护，保障系统关键文件的完整性和可用性。受保护文件支持防篡改。
15	例外进程、目录	支持对指定的进程、目录通过静态度量时权限放开，允许指定进程、目录不受控制。（投标文件中提供截图证明）
16	异常程序上报	支持实时上报系统运行过程中非可信程序运行状态，并形成待审批模板。
17	可信进程	提供指定一个进程形成可信进程，会将此可信进程本身以及调用的执行文件自动加入可信基准库中。
18	重要配置文件保护	对操作系统中服务或应用的重要配置文件的操作如创建、删除、打开、重命名等进行控制保护，未经许可的操作不能执行。
19	进程保护	对系统关键进程进行保护，防止关键进程在运行过程中被强行关闭、停止。
20	统一管理	管理平台支持 B/S 管理模式，构建服务器“统一安全管理平台”，对系统

		中的所有受控节点进行统一策略管理、统一策略下发。
21	安全通信	管理中心与终端通信使用安全信道。
22	三权分立	管理平台支持三权分立管理模式，将管理员划分系统管理员、安全管理员、安全审计员；系统管理员对用户身份、平台身份系统资源等进行管理；安全管理员负责安全策略的配置等；安全审计员负责制定审计策略、查看审计记录等。通过“三权分立”的管理模式，使得系统中的不同角色各司其职，相互制约，共同保障信息系统的安全。
23	状态监控	支持管理中心对受控节点的身份管理；支持客户端在线、离线状态实时展示。
24	策略自适应	针对 web 中间件（例如：weblogic 等）采用自适的策略配置机制，自动化适配系统环境，部署安全策略，提供保护系统和业务的安全策略配置辅助能力。
25	审计管理	支持受控节点审计、 软件库和 安全管理平台自身审计的展示、查询。
26	审计日志转储	支持审计日志上传到指定的第三方平台或备份 FTP 服务器上。
27	信息采集	支持管理平台对受控节点硬件、软件、端口等信息进行采集，支持对受控节点的信息实时查询。
28	软件备案	通过对软件进行数据签名和可靠性校验，对软件来源进行标记，有效保障软件正版化用。（投标文件中提供截图证明）
29	软件统一管理	通过安全可靠的软件采集过程，将 Windows 和 Linux 平台的软件统一纳入软件库进行运维管理。
30	软件分发管理	根据不同受控节点的业务需求，主动推送相关用软件，实现最小化安装原则。（投标文件中提供截图证明）
31	软件统计和分类	对所有受控节点使用的软件进行分类登记和管理，可对软件的下载使用进行统计分析。
32	软件版本控制	根据受控节点环境灵活指定使用相同软件的不同版本，禁止非授权版本的软件进行安装，降低软件版本变化带来的兼容性等安全风险。
33	基本功能	采用主动防御机制，使用基于可信计算技术的操作系统内核级安全机制。
34		
35		软件自身具备安全防护机制，实现软件自保护功能。
36		支持远程推送安装，支持自动化静默安装。
37		产品采用 C/S 架构，B/S 管理的方式。
38		产品支持 Windows 操作系统平台; 2003SP2 以上版本；Linux 开源系列，国产操作系统：银河麒麟 v7 V10、统信 V20、麒麟信安(全系列)、凝思（全系列）
39	可信程序列表	根据可信计算机制对可信程序进行维护和管理。
40	可信静态度量	支持在软件程序启动时通过可信度量机制对程序、重要配置参数进行完整性度量。只有在度量结果和预期值一致的前提下，才允许程序运行，否则拒绝运行，实现对已知/未知病毒、木马、攻击程序等恶意代码的防护能力。
41	可信动态度量	通过动态度量技术对程序、模块、文件系统等操作系统运行中的关键数据进行监控。（投标文件中提供截图证明）

42	自主访问控制	支持基于 RBAC 模型的访问控制功能。控制用户和进程对目录、文件、注册表的访问和操作，非授权用户和进程对受控目录、文件、注册表的访问和操作。同时支持远程共享目录、文件的访问控制。
43	强制访问控制	支持基于 BIBA\BLP 模型的强制访问控制功能，主体是用户、进程，客体是文件、进程和设备。支持远程共享目录、文件的访问控制。
44	外设控制	支持对 USB 存储设备使用进行控制，未授权设备无法使用。
45	本地审计	支持受控节点（服务器和 PC 等，下同）存储安全审计信息，并且可本地查看。
46	文件完整性保护	支持对系统关键文件的保护，保障系统关键文件的完整性和可用性。受保护文件支持防篡改。
47	例外进程、目录	支持对指定的进程、目录通过静态度量时权限放开，允许指定进程、目录不受控制。（投标文件中提供截图证明）
48	异常程序上报	支持实时上报系统运行过程中非可信程序运行状态，并形成待审批模板。
49	可信进程	提供指定一个进程形成可信进程，会将此可信进程本身以及调用的执行文件自动加入可信基准库中。
50	重要配置文件保护	对操作系统中服务或应用的重要配置文件的操作如创建、删除、打开、重命名等进行控制保护，未经许可的操作不能执行。
51	进程保护	对系统关键进程进行保护，防止关键进程在运行过程中被强行关闭、停止。
52	统一管理	管理平台支持 B/S 管理模式，构建服务器“统一安全管理平台”，对系统中的所有受控节点进行统一策略管理、统一策略下发。
53	安全通信	管理中心与终端通信使用安全信道。
54	三权分立	管理平台支持三权分立管理模式，将管理员划分系统管理员、安全管理员、安全审计员；系统管理员对用户身份、平台身份系统资源等进行管理；安全管理员负责安全策略的配置等；安全审计员负责制定审计策略、查看审计记录等。通过“三权分立”的管理模式，使得系统中的不同角色各司其职，相互制约，共同保障信息系统的安全。
55	状态监控	支持管理中心对受控节点的身份管理；支持客户端在线、离线状态实时展示。
56	策略自适应	针对 web 中间件（例如：weblogic 等）采用自适的策略配置机制，自动化适配系统环境，部署安全策略，提供保护系统和业务的安全策略配置辅助能力。
57	审计管理	支持受控节点审计、 软件库和 安全管理平台自身审计的展示、查询。
58	审计日志转储	支持审计日志上传到指定的第三方平台或备份 FTP 服务器上。
59	信息采集	支持管理平台对受控节点硬件、软件、端口等信息进行采集，支持对受控节点的信息实时查询。
60	软件备案	通过对软件进行数据签名和可靠性校验，对软件来源进行标记，有效保障软件正版化用。（投标文件中提供截图证明）
61	软件统一管理	通过安全可靠的软件采集过程，将 Windows 和 Linux 平台的软件统一纳入软件库进行运维管理。
62	软件分发	根据不同受控节点的业务需求，主动推送相关用软件，实现最小化安装

	管理	原则。
63	软件统计和分类	对所有受控节点使用的软件进行分类登记和管理，可对软件的下载使用进行统计分析。
64	软件版本控制	根据受控节点环境灵活指定使用相同软件的不同版本，禁止非授权版本的软件进行安装，降低软件版本变化带来的兼容性等安全风险。

5.3.8 数据库审计系统要求

序号	指标项	指标要求
1	性能要求	★行为审计、风险审计检索效率：十亿在线数据查询耗时为 1 秒，五十亿在线数据查询耗时为小于 5 秒，百亿在线数据查询耗时为小于 10 秒。检索结果无行数限制。 检索可显示该检索条件命中总数，同时可以快速显示检索结果数据，提高使感受。 存储能力：在线日志存储无上限，视存储空间而定。（投标文件中提供证明截图）
2	部署方式	旁路部署：该模式下无须在被审计数据库系统上安装任何代理即可实现审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户）。
3		插件部署：该模式下支持在目标数据库服务器主机上安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计（不需要提供 DBA 账号和任何数据库账户，不需要创建任何数据库账户），审计平台可以实时监控插件 CPU 使用率、内存使用率、传输包个数以及宿主机的 CPU、内存使用率和网络流量。
4		插件参数支持自定义，可以配置过滤网卡或端口，可以配置插件 CPU 占用率、内存占用率来控制插件是否自动启动和停止，可以配置日志级别和关闭日志输出来减少插件宿主机的空间占用。
5		支持审计平台 WEB 界面管理插件，支持插件的配置、唤醒、挂起、启用、停用、中断、审计平台支持远程安装、卸载、下载。
6	协议支持	Oracle、SQL Server、MySQL、MariaDB、AnalyticDB for mysql、DB2、达梦、PostgreSQL、GreenPlum、Vertica、Sybase ASE、Gbase 8a、KingBase、OceanBase、PolarDB、Hive、CirroData、Rredis、HANA、TeleDB、TelePG、HighGo 等。
7		支持同时对传统数据库和大数据数据库进行审计。
8		支持对数据库协议的编码进行自识别。
9	数据库资产自动发现	支持基于深度协议解析技术自动发现数据库，并完成自动添加和审计。不主动扫描，避免对数据库性能造成影响。 支持指定 IP 范围进行数据库自动发现。
10	规则管理	内置高危操作，同时支持自定义添加。
11		内置不同数据库类型的默认规则组，同时支持自定义添加。

12		规则配置项涵盖客户端 IP、数据库用户、客户端工具、SQL 操作、数据库名、表名、字段名、SQL 语句关键字、where 条件、影响行数、关联表个数、时间等维度的配置。 规则元素支持等于、包含、正则、不包含、不等于等选项。
13		支持 IP 地址组、数据库用户组、客户端工具组、时间组等批量导入、可供配置规则时快速引用。
14		支持客户端地址过滤，用于对某些安全地址的排除。
15		支持口令攻击规则，用于检测撞库行为。（投标文件中提供证明截图）
16		支持语句过滤，用于减少工具语句或已知无风险语句的审计。
17		支持黑白名单语句规则，确切的控制某个语句模板。
18		★支持旁路阻断，风险行为进行会话阻断。（投标文件中提供证明截图）
19	审计功能	支持记录 SQL 语句执行时间、数据库用户、操作终端主机名及 IP 地址、PORT、客户端工具名、数据库名/Schema、操作类型、SQL 语句、SQL 长度、响应时间、影响行数，风险规则类型、规则名称、风险级别等。
20		会话回放。（投标文件中提供证明截图）
21		支持更精简的 SQL 摘要元素。
22		审计日志导出控制，需要输入密码认证。
23		支持风险批量处置。
24		支持在线会话和历史会话检索。
25		结果集审计。
26		长语句审计，单条语句长度可达到 8M。
27		敏感数据掩码，对敏感数据进行遮蔽，防止二次泄露。（投标文件中提供证明截图）
28	统计分析	支持从多维度对日志数量、风险数量、SQL 流量进行展示。
29		支持按 SQL 操作类型、风险类型、风险级别、客户端来源、SQL 流量等多维度进行统计分析。
30		支持对统计数据进行下钻分析、以列表方式展示分析结果。
31		支持对象统计、可查看对象访问的详情，支持桑基图统计对象操作信息。（投标文件中提供证明截图）
32		对比分析（可对审计对象整体或某个审计对象的 SQL、会话做日、周、月的周期性对比）。
33	统计报表	系统内置 PCI、SOX 行业报表模板。
34		系统内置数据库的风险命中、语句的成功失败、数据库压力流量、客户端工具、数据库用户等维度的统计分析报告。
35		系统内容 30+张不同维度的报表。
36		支持报表外送、可以配置发送时间和周期。
37		报表导出格式支持：PDF、EXCLE、WORD、HTML。
38	系统管理	支持三权分立，提供系统管理员、安全管理员、审计管理员，满足合规要求。
39		对系统运行进行实时监控并告警。系统监控内容包括：CPU、内存、磁盘超限，插件运行 CPU、内存超限等。
40		支持系统升级，可查看升级历史及当前版本信息。
41		支持系统诊断、网络配置等功能。

42		支持登录认证设置；包括登陆超时、密码强度、密码有效期。（投标文件中提供证明截图）
43		支持访问控制，可通过设置 ip 访问规则来限制对审计系统的访问。
44		支持本地备份配置（自定义备份审计对象、规则、系统配置），可以直接下载到本地计算机、备份配置文件到 FTP。（投标文件中提供证明截图）
45		支持 Kafka、Syslog 的审计数据、风险数据、会话审计外送。（投标文件中提供证明截图）
46		支持邮件、短信平台、企业微信等系统告警，SNMP 系统监控外送。

5.3.9 数据资产梳理系统要求

序号	指标项	指标要求
1	资产发现	支持国际主流数据库,包括:Oracle、MySQL、SQL Server、DB2、PostgreSQL、MariaDB、HANA、Informix、Mongodb、Redis、Hive、Hbase、Clickhouse、SybaseASE、SybaseIQ、AS400。（投标文件中提供截图证明）
2		支持国产数据库，包括：Gbase8a、Gbase8s、达梦、Kingbase、Cirrodata、TeleDB、Oscar、Oceanbase、Gaussdb。（投标文件中提供截图证明）
3		支持文件服务器，包括 FTP,SFTP,SMB,NFS,WebDAV。（投标文件中提供截图证明）
4	数据识别	支持国际主流数据库,包括:Oracle、MySQL、SQL Server、DB2、PostgreSQL、MariaDB、Informix、Hive、Hbase、MongoDb、Clickhouse、SybaseASE、SybaseIQ、AS400、Diors、starRocks 数据库。（投标文件中提供截图证明）
5		支持国产数据库，包括：Gbase8a、Gbase8s、Kingbase、Cirrodata、达梦、TeleDB、Oscar、Oceanbase、Gaussdb。（投标文件中提供截图证明）
6		支持 pdf,xls,xlsx,doc,docx,ppt,pptx,et,csv,txt,log,html 等格式文件扫描梳理。（投标文件中提供截图证明）
7	资产管理	支持手动添加数据库资产。
8		支持指定 IP 地址段和端口范围进行数据库资产的侦测、识别，自动发现网络中所有在线数据库，应覆盖所有支持的数据源。
9		自动发现数据库资产的任务支持定时自动执行，支持周期循环和单次执行两种模式。（投标文件中提供截图证明）
10		自动发现数据资产的发现方式支持静态扫描和动态发现两种方式。
11		支持数据库资产备案登记，备案登记信息应至少包括：归属部门、业务系统、负责人、状态等信息。（投标文件中提供截图证明）
12		具备系统列表便于日常资产管理，以树形结构呈现业务系统分组情况，以及各个系统的归属部门，以及各个系统底层支撑数据库资产等。（投标文件中提供截图证明）
13		支持批量导入、导出数据库资产清单。（投标文件中提供截图证明）
14	账户梳理	支持梳理数据库资产中所有的数据库账户。
15		支持梳理数据库账户具备的详细权限。
16	数据梳理	内置不少于 90 种数据识别规则。

17		支持自定义正则表达式、数据字典等方式扩展数据识别规则。
18		支持根据表名称、字段名称、字段内容、字段描述等方式进行数据识别梳理，支持与、或逻辑计算。（投标文件中提供截图证明）
19		支持自定义一键屏蔽数据库资产默认库/表。
20		支持自定义配置数据样本采集量、规则匹配率等规则，提升数据梳理识别的效率、准确率。
21		支持手动修正数据识别结果、数据类别标识等。
22		支持全新梳理、增量梳理、修正梳理三种梳理任务模式，应对不同场景下的梳理需求。（投标文件中提供截图证明）
23		支持根据数据特征批量自动修正数据分类标识。（投标文件中提供截图证明）
24		支持通过思维导图的方式，展示当前数据分类分级标识结构。（投标文件中提供截图证明）
25		支持数据资产分权管理，不同业务部门的用户只能对自己部门的资产进行管理。
26		支持定时执行梳理任务，在非工作时间段内自动执行梳理任务，避免在工作时间段内对业务造成影响。
27		内置不少于四个行业的分类分级标识。（投标文件中提供截图证明）
28	数据台账	支持通过梳理任务，形成资产目录、账户目录、字段目录、文件目录。
29		资产目录支持以系统、资产、表、字段、文件等五个维度对所有数据资产进行在线查看与管理。（投标文件中提供截图证明）
30		资产目录的台账数据支持导入、导出。（投标文件中提供截图证明）
31		字段目录支持按业务层级逐层下钻盘点目录下的资产，包括每一级目录包含的资产数量、表数量、字段数量、敏感字段数量、敏感字段占比。（投标文件中提供截图证明）
32		具备变更目录管理，能够查看字段变更清单、账户变更清单、文件变更清单。
33		支持自动识别重要数据，可在线编辑重要数据目录。
34		支持重要数据导入导出。（投标文件中提供截图证明）
35		支持 AI 智能打标，训练 AI 时应支持 TextCNN、TextRNN、TextRCNN 等算法。（投标文件中提供截图证明）
36		★AI 智能打标训练时具备自我验证能力，并能够在线查看分类正确率。（投标文件中提供截图证明）
37	报表展示	具备数据地图看板，能够展示数据总量、数据分类统计、数据分级统计、敏感数据分布、业务数据分布等情况。（投标文件中提供截图证明）
38		具备字段特征统计报表，展示不同数据特征命中量统计。（投标文件中提供截图证明）
39		具备字段类别统计报表，支持以树形结构逐层展示不同层级的数据类别统计标识量统计。（投标文件中提供截图证明）
40	系统管理	支持配置登录安全策略，安全策略包含：密码过期时间、密码输入错误、帐号锁定时间；
41		支持密码强度设置，包括设置密码最低长度，设置数字、小写字母、大写字母、特殊符号的密码复杂度；
42		提供系统管理员、安全管理员和审计管理员来管理资产梳理设备；
43		支持在线实时查看后台进程执行日志。查看日志包括：梳理结果日志、程序执行日志等。（投标文件中提供截图证明）

44		访问 WEB 管理界面时应采用 HTTPS 协议加密传输数据。

5.3.10 API 审计系统要求

序号	指标项	指标要求
1	性能参数	默认支持应用系统数量：20 个； 流量处理能力≥2Gbps
2	兼容性	支持 http/https 协议（投标文件中提供截图证明）
3	应用资产梳理	支持从镜像流量中识别应用资产，形成资产清单。支持对资产列表进行多条件查询，包括系统名称、系统 IP、审计状态等查询条件；支持一键导入或手动添加资产；支持一键关闭所有已开启审计的资产；支持为单个资产配置负责人、IP 或端口；支持通过鉴权特征进行策略配置；包括特征位置匹配、正则表达式等信息；支持资产分权；支持资产分组；（投标文件中提供截图证明）
4	API 清单管理	支持从镜像流量中，自动识别 API，形成 API 清单。支持对 API 清单列表进行多条件查询，包括 API、是否涉敏、已审计 API、未审计 API、已忽略 API、涉敏类型、新增 API、已认领 API、分类、分级、请求方式等查询条件；支持按系统维度统计 api 接口数量、展示 API 接口明细；支持对 API 接口进行审计、认领、删除、识别敏感类型、自动翻译 API 接口、重置敏感类型、修改分类、分级和一键认领等；（投标文件中提供截图证明）
5	API 台账管理	支持对 API 清单中的资产进行认领，形成 API 台账，并进行管理；包括删除 API 接口和配置 API 接口，支持对 API 接口的接口协议、接口负责人、接口状态、接口调用状态、系统名称、API 名称等进行配置；
6	白名单管理	支持 API 白名单管理：包括设置 IP 白名单、规则白名单、无效 API 接口等。
7	用户会话关联	支持记录单个会话 ID 的发现时间和结束时间
8	审计查询	支持对应用审计日志数据进行多条件查询，包括时间、系统名称、精确 API、模糊 API、域名、泛化 API、请求头、请求体、响应头、响应体、来源 IP、目标 IP、来源端口、目标端口、用户名、请求方式、agent、跳转 IP、响应包大小、是否涉敏、涉敏量、敏感明细、响应码状态、响应码明细、附件、附件名称、鉴权用户、匿名用户、特权账号、国外 IP、国内 IP、内网 IP、自定义网段 IP 等查询条件；支持对日志数据进行导出； 支持对应用日志数据进行高级检索，包括多个条件以“且”或“或”的关系进行组合检索；支持对常用检索条件进行收藏；支持对单个维度是否存在内容、是否包含某个内容、是否不包含某个内容等进行检索；（投标文件中提供截图证明）

9		支持对风险 API 列表进行多条件查询，包括时间、系统名称、API 名称、风险分类、风险名称、风险级别、处置结果、风险用户/IP、IP 所属地等查询条件。支持统计风险种类，并统计每类风险的风险数量；支持查询每类风险的风险原因、风险隐患以及处置建议等；支持对每类风险进行处置，包括逐条、批量或单类风险加入白名单处置等；支持统计账号共用、翻页遍历、参数遍历、异常响应、机器人访问行为、越权风险、数据缓慢泄露、附件下载频繁、非人操作匿名敏感信息、非人操作鉴权敏感信息、长期未使用涉敏 API、匿名扫描攻击、短时大量下行流量、用户/匿名大量下行流量、异常大量敏感信息、弱口令检测、尝试撞库、尝试暴力破解单个账户、验证码认证接口缺乏频率限制、明文密码传输、源代码泄露、配置文件泄露、接口信息泄露、备份文件泄露、任意短信发送、请求权限参数可控、敏感信息在 url 中、请求路径异常、未鉴权、请求头包含用户名和密码、登录页面存在账号密码、鉴权信息在 url 中、密码透出、登录认证不合理、单次过量敏感数据、未执行脱敏策略、sql 注入、命令执行、调试信息泄露、SSRF 攻击、CSRF 漏洞、XSS 攻击、webshell、允许上传恶意文件、任意文件读取、复活 API、认证令牌有效期过长、自定义级别的 API 接口等。支持一键导出风险数据，支持一键排除风险数据；
10		支持对异常行为进行查询，如附件下载、暴力破解、验证码认证接口缺乏频率限制、登录失败行为等行为进行查询。（投标文件中提供截图证明）
11	统计中心	支持按应用维度进行业务访问统计和风险行为统计，包括访问量、接口数量、用户数量等；包括风险系统总量、AI 类风险系统数量、高危系统数量等行为；
12		支持按 API 维度进行业务访问统计和风险行为统计，包括 API 数量、响应码异常数量统计等；包括包括风险 API 总量、风险处置数量、全量风险 API 及其 API 的风险数量等
13		支持按用户的维度进行业务访问统计和风险行为攻击，包括总访问量、用户访问量、访问附件数量、涉敏访问数量等；包括风险用户总量、单次涉敏超过基线值的用户数量、频繁登录失败的用户数量等行为；
14		支持按敏感信息业务访问统计和风险行为统计，包括敏感类型、下行敏感数量、上行敏感数量、匿名涉敏量等；包含频繁下载敏感数据，缓慢泄露敏感数据等行为；
15		支持统计应用流量和网络流量并以图表的形式展示；支持按流量统计排名前十的应用；支持统计单个应用的流量情况，包括 24 小时流量、与前一天或上周同期流量的对比情况；
16	溯源分析	支持根据具体线索、用户账号和敏感信息、攻击路径等四个方面进行溯源，对已发现的疑似风险行为进行溯源分析；用户账号方面包括手机号、应用和 token 等信息，敏感信息包括敏感类型及敏感数据等内容，攻击路径包括攻击规则和来源 IP 等；
17	报表分析	支持报表分析，包括生成报表、预览报表、导出报表；支持生成日报、周报、月报等；
18		支持根据用户不同需求进行自定义报表；支持自定义报表参数进行报表推送等；
19	规则管理	支持通过规则配置和机器学习两方面新增风险规则，配置条件包括策略名称、规则类型、规则组、规则级别、请求方法、API、时间规则、源 IP 规则、关键字规则、敏感信息规则、特权账号规则、作用域、频次规

		则、行为规则等内容。
20		支持通过设置时间规则、源 IP 规则、攻击规则、行为规则、频次规则和特权账号规则五个方面对风险规则进行设置，根据业务需求定制风险规则并识别相应风险。
21		★支持通过 AI 模型识别风险，训练维度包括访问数量、敏感数据、附件下载、来源 IP、响应码异常数据、agent 等，训练类型包括应用、API、鉴权用户、匿名用户等。支持展示训练结果，包括模型训练维度、模型训练时长、训练开始时间、训练结束时间、训练数据量、模型训练结果等。（投标文件中提供截图证明）
22	系统知识库	支持内置敏感数据规则库，包括用户自定义敏感信息规则；支持内置攻击漏洞库、人员信息配置库、IP 地址库、分类分级等；
23	探针管理	支持自动化和手工方式进行 agent 安装。支持探针状态监控，如 cpu，内存，网络包数量等。支持探针管理，如：暂停，启动，停止等。支持探针流量过滤；
24	数据外发	支持 syslog 外发和 kafka 外发，支持对风险告警数据、日志数据进行外发。可以自定义外发维度；
25	数据备份	支持备份模式包括全量备份和增量备份；支持不同策略备份：包括全库备份、日志表备份、风险告警数据备份、配置文件备份等；支持不同方式备份，包括单次备份和循环备份，其中循环备份；
26	高端扩展能力	系统可以与数据安全集中管控平台联动，实现统一管理和分析；
27	部署方式	支持旁路镜像部署；
28		支持探针部署；
29		支持旁路镜像、轻量级探针插件即混合方式获取流量，满足复杂网络环境、云环境等审计需求；
30	部署环境	支持本地虚拟化环境方式部署；
31		支持天翼云、华为云、阿里云、百度云等公有云环境部署；

5.4 平台测试仿真配套资源

★本项目所需的测试仿真服务器相关设备资源均由中标方承担，使用期限为三年，服务期内甲方享有资源的所有权和使用权，相关资源配置不低于《天富网络安全加固及数据安全治理项目仿真配套资源》的内容，允许通过租用云平台资源实施，但需满足系统整体网络安全要求，搭建专用网络环境。

天富网络安全加固及数据安全治理项目仿真配套资源			
序号	设备名称	配置规格	数量
1	测试仿真服务器 A	国产化服务器，千兆电口≥4 个，万兆光口≥4 个，冗余电源；CPU≥16 核，内存≥64G，硬盘≥4T。	1 台

2	测试仿真服务器 B	国产化服务器，千兆电口≥4 个，万兆光口≥4 个，冗余电源；CPU≥8 核，内存≥32G，硬盘≥4T。	10 台

六、运维服务要求

1.全面识别与梳理数据库、大数据平台、文件服务器等存储的数据资产，形成数据资产清单，明确数据分类分级初步范围。

2.审查现有数据安全管理制度、组织架构、人员职责、应急响应流程的完备性与执行有效性

3.通过访谈、日志审计、配置检查等方式，评估数据收集、存储、使用、共享、出境等活动的合法合规性与安全措施有效性。

4.对数据库、API 接口、数据传输通道等进行安全配置核查、漏洞扫描、渗透测试，验证技术防护措施强度。

5.编制全面的数据安全风险评估报告，包含问题清单、风险分析、等级评价及具体的整改措施与建设规划建议。

6.设计四级数据安全制度体系（方针政策、制度规范、操作细则、记录表单），确保体系完整、层级清晰。

7.调研企业现有相关制度，对标法律法规和最佳实践，识别差距与薄弱环节。

8.编写《数据安全管理总则》、《数据分类分级管理办法》、《数据全生命周期安全管理规范》等核心制度文件，组织内部评审与修订。

9.协助完成制度的正式发布，并对相关人员进行制度宣贯与培训，确保理解与执行。

10.结合行业特性（如参考金融、电信、能源等行业标准）、业务场

景和国家标准，制定企业内部的《数据分类分级指南》或《管控指南》。

11.基于资产清单，按照既定标准对数据进行分类，明确数据类别和子类。

12.根据数据泄露可能影响的对象、范围和程度，对已分类数据进行定级（如核心数据、重要数据、敏感数据、内部数据、公开数据等）。

13.形成最终的数据分类分级清单，并制定数据标识规则，为后续系统标识或人工标识提供指导。

14.围绕数据安全事件类型，设计覆盖核心场景的演练剧本，包括数据泄露事件、数据篡改与破坏事件、数据可用性事件

15.提供不同维度的演练形式，包括桌面推演、技术模拟演练、综合实战演练。

16.演练将覆盖应急响应的完整生命周期，包括监测与发现、研判与定级、上报与通报、应急处置、溯源与分析、复盘与总结。

七、免费运维服务期限

免费运维服务期间为系统竣工验收之日起3年，服务项目内容包括提供中新建电力集团兵团天富电力监控系统网络安全管理平台设备开展运行保障工作，其中：运行保障工作包括：故障处理、系统培训、客户服务、运维巡检。

八、质保要求

自验收合格之日起三年。

第六章 投标文件格式

_____（项目名称）设备采购招标项目

投 标 文 件

投标人：_____（单位电子签章）

法定代表人或其委托代理人：_____（法人电子签名）

_____年_____月_____日

目　　录

一、投标函

_____（招标人名称）：

1．我方已仔细研究了_____（项目名称）设备采购招标项目招标文件的全部内容，愿意以人民币（大写）_____（¥_____元）的投标总报价（其中，增值税税率为_____）提供_____（设备名称及技术服务和质保期服务），并按合同约定履行义务。

2．我方的投标文件包括下列内容：

（1）投标函；

（2）法定代表人（单位负责人）身份证明或授权委托书；

（3）联合体协议书（如有）；

（4）投标保证金（如有）；

（5）商务和技术偏差表；

（6）分项报价表；

（7）资格审查资料；

（8）投标设备技术性能指标的详细描述；

（9）技术支持资料；

（10）技术服务和质保期服务计划；

……

投标文件的上述组成部分如存在内容不一致的，以投标函为准。

3．我方承诺除商务和技术偏差表列出的偏差外，我方响应招标文件的全部要求。

4．我方承诺在招标文件规定的投标有效期内不撤销投标文件。

5．如我方中标，我方承诺：

（1）在收到中标通知书后，在中标通知书规定的期限内与你方签订合同；

（2）在签订合同时不向你方提出附加条件；

（3）按照招标文件要求提交履约保证金；

（4）在合同约定的期限内完成合同规定的全部义务。

6．我方在此声明，所递交的投标文件及有关资料内容完整、真实和准确，且不存在第二章“投标人须知”第1.4.3项规定的任何一种情形。

7．_____（其他补充说明）。

投 标 人：_____（单位电子签章）

法定代表人（单位负责人）或其委托代理人：_____（法人电子签名）

地　　址：_____

网　　址：_____

电　　话：_____

传　　真：_____

邮政编码：_____

_____年_____月_____日

二、法定代表（单位负责人）身份证明

法定代表人（单位负责人）身份证明

投标人名称：_____

姓名：_____性别：_____年龄：_____职务：_____

系_____（投标人名称）的法定代表人（单位负责人）。

特此证明。

附：法定代表人（单位负责人）身份证复印件。

注：本身份证明需由投标人加盖单位电子签章。

投标人：_____（单位电子签章）

_____年_____月_____日

三、授权委托书

授权委托书

本人_____（姓名）系_____（投标人名称）的法定代表人（单位负责人），现委托_____（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改设备采购招标项目投标文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：_____。

代理人无转委托权。

附：法定代表人（单位负责人）身份证复印件及委托代理人身份证复印件

注：本授权委托书需由投标人加盖单位公章并由其法定代表人（单位负责人）和委托代理人签字。

投　标　人：_____（单位电子签章）

法定代表人（单位负责人）：_____（法人电子签名）

身份证号码：_____

委托代理人：_____（签字）

身份证号码：_____

_____年_____月_____日

四、联合体协议书

联合体协议书

_____（所有成员单位名称）自愿组成_____（联合体名称）联合体，共同参加_____（项目名称）设备采购招标项目投标。现就联合体投标事宜订立如下协议。

1. _____（某成员单位名称）为_____（联合体名称）牵头人。

2. 联合体各成员授权牵头人代表联合体参加投标活动，签署文件，提交和接收相关的资料、信息及指示，进行合同谈判活动，负责合同实施阶段的组织和协调工作，以及处理与本招标项目有关的一切事宜。

3. 联合体牵头人在本项目中签署的一切文件和处理的一切事宜，联合体各成员均予以承认。联合体各成员将严格按照招标文件、投标文件和合同的要求全面履行义务，并向招标人承担连带责任。

4. 联合体各成员单位内部的职责分工如下：_____。

5. 本协议书自所有成员单位法定代表人（单位负责人）或其委托代理人签字或盖单位章之日起生效，合同履行完毕后自动失效。

6. 本协议书一式____份，联合体成员和招标人各执一份。

注：本协议书由法定代表人（单位负责人）签字的，应附法定代表人（单位负责人）身份证明；由委托代理人签字的，应附授权委托书。

联合体牵头人名称：_____（单位电子签章）

法定代表人（单位负责人）或其委托代理人：_____（法人电子签名）

联合体成员名称：_____（单位电子签章）

法定代表人（单位负责人）或其委托代理人：_____（法人电子签名）

联合体成员名称：_____（单位电子签章）

法定代表人（单位负责人）或其委托代理人：_____（法人电子签名）

_____年_____月_____日

五、投标保证金或保函

采用现金或电子保函的，投标人应在此提供汇款凭证或电子保单。

六、商务和技术偏差表

商务和技术偏差表

序号	招标文件章节及条款号	投标文件章节及条款号	偏差说明
1			
2			
3			
4			
5			
……			

投标人保证：除商务和技术偏差表列出的偏差外，投标人响应招标文件的全部要求。

七、分项报价表

分项报价表

1. 分项报价表说明
2. 分项报价表

单位：人民币元

序号	分项名称	单位	数量	单价（元）	总价（元）	备注
1	中新建数据治理统一定制化管控系统	台	1			
2	威胁监测与分析系统	台	1			
3	数据静态脱敏系统	台	1			
4	数据库运维管控系统	台	2			
5	数据动态脱敏系统	台	1			
6	数据库加密系统	台	2			
7	数据环境安保系统	台	1			
8	数据库审计系统	台	2			
9	数据资产梳理系统	台	1			
10	API 审计系统	台	1			
11	服务器密码机	台	1			
12	加密机	台	2			
合计报价						

八、资格审查资料

（一）基本情况表

投标人名称				
注册资金			成立时间	
注册地址				
邮政编码			员工总数	
联系方式	联系人		电话	
	网址		传真	
法定代表人（单位负责人）	姓名		电话	
投标人须知要求投标人需具有的各类资质证书	类型：	等级：	证书号：	
基本账户开户银行				
基本账户银行账号				
近三年营业额				
投标人关联企业情况（包括但不限于与投标人法定代表人（单位负责人）为同一人或者存在控股、管理关系的不同单位）				
投标设备制造商名称				
投标人须知要求投标设备制造商需具有的资质证书				
备注				

注：1. 投标人应根据投标人须知第 3.5.1 项的要求在本表后附相关证明材料。境内投标人以现金或者支票形式提交投标保证金的，还应附基本账户开户许可证复印件。

2. 如果投标人须知第 1.4.1 项对投标设备制造商的资质提出了要求，投标人应根据投标人须知第 3.5.1 项的要求在本表后附相关资质证书复印件。

（二）近年财务状况表

1. 投标人应根据投标人须知第 3.5.2 项的要求在本表后附相关证明材料。

2. 对于可以现货供应的标准设备（非定制设备），投标人的财务状况一般不宜作为审查投标人履约能力的因素。

（三）近年完成的类似项目情况表

设备名称	
规格和型号	
项目名称	
买方名称	
买方联系人及电话	
合同价格	
项目概况及投标人履约情况	
备注	

注：1. 投标人应根据投标人须知第 3.5.3 项的要求在本表后附相关证明材料。

2. 投标人为代理经销商的，投标人须知第 1.4.1 项要求投标人提供投标设备的业绩的，投标人应按照上表的格式提供投标设备的业绩情况并根据投标人须知第 3.5.3 项的要求在本表后附相关证明材料。

(四)正在供货和新承接的项目情况表

设备名称	
规格和型号	
项目名称	
买方名称	
买方联系人及电话	
签约合同价	
项目概况及投标人履约情况	
备注	

注：投标人应根据投标人须知第 3.5.4 项的要求在本表后附相关证明材料。

（五）近年发生的诉讼及仲裁情况

注：投标人应根据投标人须知第 3.5.5 项的要求附相关证明材料。

九、制造商授权书

致：_____（招标人）

我单位_____（制造商名称）是按_____（国家／地区名称）法律成立的一家制造商，主要营业地点设在_____（制造商地址）。兹授权按_____（国家／地区名称）的法律正式成立的，主要营业地点设在_____（投标人的单位地址）的_____（投标人名称）以我单位制造的_____（设备名称）进行_____（项目名称）投标活动。我单位同意按照中标合同供货，并对产品质量承担责任。

授权期限：_____。

投标人名称：_____（盖单位章）　制造商名称：_____（盖单位章）

签字人职务：_____　签字人职务：_____

签字人姓名：_____　签字人姓名：_____

签字人签名：_____　签字人签名：_____

十、投标设备技术性能指标的详细描述

投标设备技术性能指标的详细描述

十一、技术服务和质保期服务计划

技术服务和质保期服务计划

十二、不参与围标串标承诺书

不参与围标串标承诺书

本人作为（单位名称）_____的法人，清楚知晓我公司本项目投标活动，对以下事项作出承诺：

一、我单位遵循公开、公平、公正、诚实守信的原则，依法依规参与本项目竞标。

二、我单位在本项目招标投标活动中，未参与围标串标。

三、我单位如被查实在本项目招标投标活动中存在围标串标的，递交投标文件行为作为实施串通投标违法行为的关键环节，本人承担直接责任人员法律责任，接受相应行政处罚和失信惩戒。

项目编号：

标段号：

投标单位名称：

投标单位法人签名：

盖　章

年　月　日