美创 MEICHUANG

2022 年版

合同编号：MMCZJ2025062518S

签订地点：德清

2025-2026 年数据库运维服务

合同书

甲方（委托方）：德清县人力资源和社会保障信息中心

乙方（受托方）：杭州美创科技股份有限公司

甲乙双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》之规定，签订本合同，并由双方共同恪守。

第一条　服务内容及费用

数据库运维服务	年	1	包含但不限于标准库、生产库和政务云上的所有类型数据库。
NBU 备份运维服务	年	1	\
操作系统服务	年	1	\
中间件服务	年	1	\
智能监控运维平台服务	年	1	\
CDP 灾备一体化服务	年	1	本地 CDP 灾备一体化的运维服务。
数据安全审计运维服务	年	1	本地数据库审计设备及安全策略的运维服务。
现场应急保障支持	年	2	要求出具书面或电子报告。
非应急类现场运维服务	年	次数不限	配合上级及其他各项网络、数据安全及重大保障产生的要求，可与巡检及应急保障支持一起做服务。
定期巡检服务	年	2	要求出具书面或电子报告。
数据内控管理运维服务	年	1	本地数据内控管理设备及安全策略的运维服务。
数据脱敏运维服务	年	1	本地数据库脱敏设备及安全策略的运维服务。
数据加密运维服务	年	1	本地数据库审计设备及安全策略的运维服务。
数据安全评估服务	年	1	在服务期内，提供一次数据安全评估服务，通过数据安全综合评估，对系统基本情况综合了解，作为开展符合性判定的参考意见，以便尽快落实法律中关于评估的相关要求。
数据库迁移服务	年	1	支持数据库的迁移工作，类型为不同操作系统同类型数据库，工作内容包括：项目系统调研，制定数据库迁移方案，数据库软件安装，模拟迁移及正式迁移和迁移后的保障工作
合计：	小写：￥ 219000 （大写：人民币 贰拾壹万玖仟 元整）		

一、数据库运维服务要求

（一）7*24 小时 400 电话不间断支持

对数据库系统故障或与数据库系统相关联的系统故障，提供 7*24 小时不间断非现场(可以是 400 电话、e-mail、VPN、QQ 等形式)支持服务，通过以上方式直接联络服务供应商的技术工程师，寻求问题的解决方案、技术文档以及技术指导，提供故障处理案例。

在接到采购方故障申告后应于 5 分钟内响应，如故障未能在 15 分钟内通过远程支持得到解决，应承诺根据采购方要求派指定服务工程师在 1 小时内赶到采购方现场，提供不间断故障处理服务。

（二）故障管理和查询回顾

（1）客户管理报告

要求记录所有的故障 ID，并处理之后可以让采购方随时跟踪故障 ID 的处理状况。

对故障 ID 的报告要显示问题的状态，问题描述和解决方法、解决过程等等内容。要定期将所记录的故障 ID 进行汇总之后传真或者 E-mail 给采购方。报告中除包含特定的日期、产品、客户资料、平台等基本内容之外，还包括故障 ID、故障 ID 的严重等级、故障 ID 及问题解决的状态、处理该问题的技术支持工程师、问题说明、问题进展等。

客户管理报告一个季度的为单位的方式进行整理，并对这一段时间的问题进行一个分类总结、在定期的时间内进行讨论，并提出某些常见问题上的建议，在后续的维护中尽可能避免类似错误，更好的保障数据库运行。

（2）客户关系管理 （系统配置和故障处理库）

要求服务供应商技术团队做好数据库维护的同时，建立档案。档案内容包括客户联系人、地点、电话等基本信息之外，还包括数据库的基本状况，从而准确的把数据库环境和运行状态交接给采购方。

（3）年度总结报告

在服务年度结束前最后一周，要求出具一年来的工作报告，内容包括现场服务报告，电话支持报告，技术方案，技术工作文档等一切技术性文字。

（4）专职责任工程师提供二对一的服务

要求保证固定的专职的主备责任工程师，最少有两位专业的工程师，一名主责任工程师，一名副责任工程师，固定提供服务响应支持。该服务为最高级别的常规服务，主要针对可用性要求极高的系统。要求主责工程师将定期对客户进行访问，进行数据库状况检查。责任工程师将免费提供系统健康检查顾问服务以及协助客户建立数据库日常管理规范。

（5）案例查询和故障回顾

要求详细记录 ORACLE、RDS、达梦等数据库发生的事故及解决方案，并及时提供案例技术交流。

（三）现场应急保障支持

当遇到复杂性问题，需要到现场进行综合诊断或者采购方要求现场支持服务的时候，服务团队人员乃至专家后援服务团队人员在 1 小时内到达支持现场，同时在路途中不中断电话支持以求快速解决问题。

用户出现系统问题时，为了保证故障得到及时、准确定位和处理。服务供应商应提供服务工程师根据用户的合理安排到达现场提供技术支持服务。工程师应配合用户和其他相关厂商工程师对故障进行分析定位并及时解决故障。

配合用户对系统进行优化实施

根据系统的运行情况，按照用户的优化实施安排，服务供应商提供现场技术支持服务。服务供应商提供的服务工程师会配合用户和其他相关厂商工程师对系统参数和运行情况进行分析，提出改进方案并协助用户进行调整。

根据用户要求实施的其他现场技术支持服务，如系统安装、补丁安装、系统升级、巡检等。

到场时间：

服务工程师于 1 小时内到达用户现场。

系统恢复时间：

服务工程师到达用户现场后，于 2 小时内恢复系统的正常运行，并收集现场信息以便完成故障分析。如遇到重大故障，4 小时内无法解决问题，则会提出应急方案，确保可以在 6 小时内恢复系统运行。

故障分析时间：

在系统恢复正常运行后，应对系统运行情况进行跟踪，并结合故障现场信息对故障产生原因进行分析，5 日内提交故障分析报告及解决方案。

不间断故障处理：

服务工程师在到达现场后，开始进行不间断服务直至系统恢复正常运行，得到确认后方可离开。

（四）数据库现场巡检服务

日常检查应至少包括以下内容：

- 提供一年四次的现场日常巡检服务。

- 检查相关软硬件、数据库配置和 SGA、PGA 的配置情况；
- 检查数据库、备份结果集、各表空间的变化情况等，并对数据变化情况作评估；
- 统计当前表空间、文件系统和数据文件的使用情况；
- 检查数据库 alert.log 日志文件和相关 trace 文件；
- 检查操作系统用户、数据库用户、系统本身的安全性；
- 收集数据库运行期间的负载情况和 Instance 各性能指标；
- 检查数据库备份是否正常；

数据库巡检为客户定期（每个季度）执行一次，提供现场操作系统例行检查服务，内容涉及到操作系统的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。操作系统巡检工作由现场检查和系统数据分析构成，提供一份内容详尽的操作系统巡检报告。

提供现场数据库预防性维护服务，内容涉及到数据库的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。定期维护工作由现场检查和系统数据分析构成，并提供一份内容详尽的数据库巡检报告。

定期维护包括以下内容：

- 检查相关软硬件、数据库配置和 SGA、PGA 的配置情况；
- 检查数据库、备份结果集、各表空间的变化情况等，并对数据变化情况作评估；
- 统计当前表空间、文件系统和数据文件的使用情况；
- 检查数据库 alert.log 日志文件和相关 trace 文件；
- 协助确认数据库中出现的无效对象合理性；
- 检查操作系统用户、数据库用户、系统本身的安全性；
- 收集数据库运行期间的负载情况和 Instance 各性能指标；
- 检查数据库备份是否正常；

基于收集的数据库性能信息，针对数据库系统可能存在的问题和性能瓶颈提出合理的建议。

数据库检查主要从数据库的多个方面进行，包括：

- 收集系统配置信息；
- 收集数据库配置信息；
- 收集数据库资源和负载大小；
- 检查数据库各方面的空间管理，包括整库变化状况、表空间变化情形、数据文件变化情形、回滚文件和日志文件等；

- 检查数据库的对象管理，尤其是大型对象管理，包括大型表格、大型索引、占用空间很大的对象、无效对象、垃圾箱空间占用等；
- 检查数据库的安全措施管理，包括变化的用户信息、变化的权限信息、用户的大权限管理、DBA权限管理等；
- 检查数据库的性能状况，主要关注典型业务时间段、高峰业务时间段的数据库性能表现，从性能管理里可以看出哪些资源开销很大；
- 检查数据库的备份系统运行情况，备份策略是否执行成功，备份日志是否有报错等。
- 检查数据库的告警日志文件，从上一次检查以来是否发生过报错告警等痕迹。

（五）数据库迁移服务

对采购方现有数据库全面梳理，确认需要迁移的数据库，通过升级和迁移评估规划，制定在线迁移方案，使数据库迁移后运行效率更高，包括：

评估云上数据库迁移所需资源；

评估数据库迁移带来的优点和可能产生的问题；

保证数据库迁移的过程中数据的安全性；

对于还在应用的业务系统，顺利、快速地完成迁移，减少业务的停机时间；

从oracle至达梦数据库迁移等。

（六）数据库安装、升级服务

从实际应用角度出发，根据具体的硬件环境，应用类型进行分析，结合当前数据库系统的最新补丁情况，为用户的新系统提供安装建议，从而提供数据库最安全可靠，适合应用的数据库、补丁安装服务以及相关应用上线现场支持服务。

根据实际应用角度出发，根据硬件环境，应用类型进行分析，推荐多种升级方案，每种升级方案中明确升级需要的条件、升级时间、业务停止时间、升级技术、风险、数据一致性、回退措施等，协助用户选择最适合的升级方案。为用户系统数据库提供最安全可靠，适合应用的 Oracle、MySQL、SQL Server 数据库、补丁等升级服务。

（七）数据容灾服务

提供数据容灾服务，集中对采购方数据进行连续性备份，尽可能实现完整的业务连续性解决方案。

（八）数据安全审计运维服务

提供数据安全审计运维服务，集中对采购方标准生产库和政务云的所有类型数据库的日志进行详细记录，针对风险操作进预警，同时保障数据安全审计运维系统的正常运行，尽可能的保障数据库资产安全。

（九）非应急类现场运维服务

对数据库系统故障或与数据库系统相关联的非紧急类系统故障，允许每季度次数累计，当单一季度内累计满 5 次时，提供一次现场服务予以集中解决，解决后累计次数清零；若未满 5 次则统一由下一季度的现场巡检服务时统一解决。

二、中间件软件服务要求

（一）7*24 小时 400 电话不间断支持

对中间件系统故障或与中间件系统相关联的系统故障，提供 7*24 小时不间断非现场(可以是 400 电话、e-mail、VPN、QQ 等形式)支持服务，通过以上方式直接联络服务供应商的技术工程师，寻求问题的解决方案、技术文档以及技术指导，提供故障处理案例。

在接到采购方故障申告后应于 5 分钟内响应，如故障未能在 15 分钟内通过远程支持得到解决，承诺根据采购方要求派指定服务工程师在 1 小时内赶到采购方现场，提供不间断故障处理服务。

（二）软件安装、升级服务

从实际应用角度出发，根据具体的硬件环境，应用类型进行分析，结合当前中间件系统的最新补丁情况，为用户的新系统提供安装建议，从而提供中间件最安全可靠，适合应用的中间件、升级安装服务以及相关应用上线现场支持服务。

（三）现场应急保障支持

当遇到复杂性问题，需要到现场进行综合诊断或者采购方要求现场支持服务的时候，服务供应商服务团队人员乃至专家后援服务团队人员在 1 小时内到达支持现场，同时在路途中不中断电话支持以求快速解决问题。

用户出现系统问题时，为了保证故障得到及时、准确定位和处理。服务供应商提供的服务工程师会根据用户的合理安排到达现场提供技术支持服务。工程师会配合用户和其他相关厂商工程师对故障进行分析定位并及时解决故障。

配合用户对系统进行优化实施

根据系统的运行情况，按照用户的优化实施安排，服务供应商提供现场技术支持服务。服务供应商提供的服务工程师会配合用户和其他相关厂商工程师对系统参数和运行情况进行分析，提出改进方案并协助用户进行调整。

根据用户要求实施的其他现场技术支持服务，如系统安装、补丁安装、系统升级、巡检等。

到场时间：

服务工程师于 1 小时内到达用户现场。

系统恢复时间：

服务工程师到达用户现场后，于 2 小时内恢复系统的正常运行，并收集现场信息以便完成故障分析。如遇到重大故障，4 小时内无法解决问题，则会提出应急方案，确保可以在 6 小时内恢复系统运行。

故障分析时间：

在系统恢复正常运行后，应对系统运行情况进行跟踪，并结合故障现场信息对故障产生原因进行分析，5 日内提交故障分析报告及解决方案。

不间断故障处理：

服务工程师在到达现场后，开始进行不间断服务直至系统恢复正常运行，得到确认后方可离开。

（四）软件性能优化服务

根据采购方提出的具体需求，制定中间件性能调优方案。

在采购方的同意下进行中间件性能优化。

性能优化服务内容如下：

- 调优 TCP 连接缓存数
- WebLogic EJB 调优
- JDBC 应用调优
- JSP 调优
- JMS 代码调优
- 使用 EJB 和 WebLogic 的特性
- JRockit 调优
- Server 调优
- 调整默认执行线程数
- 调整连接参数
- Web 调优
- 优化事务隔离级别和事务属性

（五）软件现场巡检服务

中间件巡检为采购方定期（每个季度）执行一次，提供现场中间件例行检查服务，内容涉及到中间件的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。中间件巡检工作由现场检查和系统数据分析构成，提供一份内

容详尽的中间件巡检报告。

（六）NBU 备份软件运维

提供 NBU 备份软件的日常巡检服务（每季度一次），保障 NBU 备份软件的正常运行。

（七）非应急类现场运维服务

对中间件系统故障或与中间件系统相关联的非紧急类系统故障，允许每季度次数累计，当单一季度内累计满 5 次时，提供一次现场服务予以集中解决，解决后累计次数清零；若未满 5 次则统一由下一季度的现场巡检服务时统一解决。

三、操作系统运维服务要求

（一）7*24 小时 400 电话不间断支持

对操作系统故障或与操作系统相关联的系统故障，提供 7*24 小时不间断非现场(可以是 400 电话、e-mail、VPN、QQ 等形式)支持服务，通过以上方式直接联络服务供应商的技术工程师，寻求问题的解决方案、技术文档以及技术指导，提供故障处理案例。

在接到采购方故障申告后于 5 分钟内响应，如故障未能在 15 分钟内通过远程支持得到解决，根据采购方要求派指定服务工程师在 1 小时内赶到采购方现场，提供不间断故障处理服务。

（二）操作系统安装和升级服务

从实际应用角度出发，根据具体的硬件环境，应用类型进行分析，结合当前操作系统的最新补丁情况，为采购方的新系统提供安装、升级建议，从而提供操作系统最安全可靠，适合应用的操作系统、升级安装服务以及相关应用上线现场支持服务。

（三）操作系统性能监控服务

监控操作系统性能，主要包括：CPU、内存、磁盘，同时设定阀值报警。

采购方目前使用的服务器，服务期内免费提供操作系统资源监控平台，采购方利用该监控平台可以进行 7×24 小时实时系统监控，监控整个系统的资源状况、性能状况等。

操作系统资源监控后，可以定期形成性能分析报告。根据性能评估报告，及时发现性能问题，并采用有效的优化手段。

（四）操作系统性能分析和优化

提供服务器运行状态、性能分析、评估和调整服务，并根据系统资源利用的历史记录，对操作系统定期进行优化。

操作系统性能调优应包括以下内容：

- Share Pool Tuning
- I/O Tuning
- Buffer Cache Tuning
- Redo Log Buffer Tuning
- 内存资源冲突
- IO 资源冲突
- CPU 开销资源冲突
- 回滚段资源冲突
- 临时段资源冲突
- 数据“热”块资源冲突
- 索引效率低下
- SQL 语句调整
- 可能影响操作系统性能的其它方面。

（五）现场应急保障支持

当遇到复杂性问题，需要到现场进行综合诊断或者采购方要求现场支持服务的时候，服务供应商服务团队人员乃至专家后援服务团队人员在 1 小时内到达支持现场，同时在路途中不中断电话支持以求快速解决问题。

采购方出现系统问题时，为了保证故障得到及时、准确定位和处理。提供的服务工程师会根据采购方的合理安排到达现场提供技术支持服务。工程师会配合采购方和其他相关厂商工程师对故障进行分析定位并及时解决故障。

配合采购方对系统进行优化实施

根据系统的运行情况，按照采购方的优化实施安排，服务供应商提供现场技术支持服务。服务供应商提供的服务工程师会配合用户和其他相关厂商工程师对系统参数和运行情况进行分析，提出改进方案并协助用户进行调整。

根据采购方要求实施的其他现场技术支持服务，如系统安装、补丁安装、系统升级、系统迁移、巡检等。

■ 到场时间：

服务工程师于 1 小时内到达用户现场。

■ 系统恢复时间：

服务工程师到达用户现场后，于 2 小时内恢复系统的正常运行，并收集现场信息以便完成故障分析。如遇到重大故障，4 小时内无法解决问题，则会提出应急方案，确保可以在 6 小时内恢复系统运行。

■ 故障分析时间：

在系统恢复正常运行后，应对系统运行情况进行跟踪，并结合故障现场信息对故障产生原因进行分析，5 日内提交故障分析报告及解决方案。

■ 不间断故障处理：

服务工程师在到达现场后，开始进行不间断服务直至系统恢复正常运行，得到确认后方可离开。

（六）操作系统现场巡检服务

操作系统巡检为客户定期（每个季度）执行一次，提供现场操作系统例行检查服务，内容涉及到操作系统的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。操作系统巡检工作由现场检查和系统数据分析构成，提供一份内容详尽的操作系统巡检报告。

提供现场数据库预防性维护服务，内容涉及到数据库的方方面面，主要包含错误日志管理，性能管理，空间管理，对象管理，安全管理，备份管理等方面内容。定期维护工作由现场检查和系统数据分析构成，并提供一份内容详尽的数据库巡检报告。

定期维护包括以下内容：

- 检查相关软硬件、数据库配置和 SGA、PGA 的配置情况；
- 检查数据库、备份结果集、各表空间的变化情况等，并对数据变化情况作评估；
- 统计当前表空间、文件系统和数据文件的使用情况；
- 检查数据库 alert.log 日志文件和相关 trace 文件；
- 协助确认数据库中出现的无效对象合理性；
- 检查操作系统用户、数据库用户、系统本身的安全性；
- 收集数据库运行期间的负载情况和 Instance 各性能指标；
- 检查数据库备份是否正常；

基于收集的数据库性能信息，针对数据库系统可能存在的问题和性能瓶颈提出合理的建议。

数据库检查主要从数据库的多个方面进行，包括：

- 收集系统配置信息；
- 收集数据库配置信息；
- 收集数据库资源和负载大小；
- 检查数据库各方面的空间管理，包括整库变化状况、表空间变化情形、数据文件变化情形、回滚文件和日志文件等；
- 检查数据库的对象管理，尤其是大型对象管理，包括大型表格、大型索引、占用空间很大的对象、无效对象、垃圾箱空间占用等；
- 检查数据库的安全措施管理，包括变化的用户信息、变化的权限信息、用户的大权限管理、DBA 权限管理等；

◆ 检查数据库的性能状况，主要关注典型业务时间段、高峰业务时间段的数据库性能表现，从性能管理里可以看出哪些资源开销很大；

◆ 检查数据库的备份系统运行情况，备份策略是否执行成功，备份日志是否有报错等。

◆ 检查数据库的告警日志文件，从上一次检查以来是否发生过报错告警等痕迹。

（七）非应急类现场运维服务

对与操作系统相关联的非紧急类系统故障，允许每季度次数累计，当单一季度内累计满5次时，提供一次现场服务予以集中解决，解决后累计次数清零并在该季度内重新累计；若未满5次则统一由下一季度的现场巡检服务时统一解决。

四、数据安全服务要求

（一）数据安全评估服务

在服务期内，提供一次数据安全评估服务，通过数据安全综合评估，对系统基本情况综合了解，作为开展符合性判定的参考意见，以便尽快落实法律中关于评估的相关要求。

（二）数据内控管理服务

在服务期内，提供数据内控管理服务，服务要求如下：

服务要求	部署方式	1.支持反向代理部署； 2.支持分布式部署，通过管理中心对分布式部署的各网关节点进行集中配置管理、分析、统计等。
	高可用	支持集群，可随业务随时平滑扩展。
		支持主备HA部署。
	权限模版	针对不同敏感等级的敏感资产，支持通过内置的权限模版，实现身份的初始化授权，1级敏感资产默认授权只读且可查询明文，其余敏感等级资产默认授权数据只读且脱敏权限，确保资产数据安全，实现基于资产的零信任防护；内置的权限模版无法编辑、删除；
		支持设置数据操作、数据库对象操作两种类型的权限模版；支持通过数据操作模版，自定义对敏感资产的DQL、DML操作权限；支持通过数据库对象操作模版，自定义表、视图、存储过程、函数等各种实体的DDL、DCL操作权限。
		支持通过权限模版，为特定身份授予数据操作、数据库对象操作权限；支持限制授权有效期，可将授权有效期约束在指定时间段、指定时间周期、指定时间域；当需要变更某身份所使用的授权模版时，应当在变更前，进行授权前后的权限对比，明确标注操作变更项，防止因平台误操作造成不合理授权。
		支持为不同等级的敏感资产，自定义设置不同的权限模版；

	准入控制	支持数据库登录授权，通过身份的多因素认证，至少应支持应用名称、应用签名、主机名、证书、数据库用户、操作系统用户、用户名、IP 地址、MAC 地址等因素的任意组合，系统根据多维身份管理策略，自动判别登录主体的合法性，如不符合设定的身份管理策略，登录失败。
		支持为每个用户绑定 USB KEY 证书或软证书，实现在数据库用户密码被泄露的情形下，仍能阻止非法用户登陆目标数据库，解决仅依靠密码认证带来的安全不足问题。
		支持通过不删除账户的方式，在系统中回收资产授权权限。
	防绕过	可通过在数据库服务器安装探针，实现直连阻断、本地操作管控，防止非法身份绕过安全系统，违规对数据库进行访问。
		具备应用防假冒功能，至少支持通过安装安全客户端进行 MD5 值和应用程序名校验、及提取数据库的动态访问内容作为动态指纹两种方式实现应用防假冒；针对假冒应用，可进行行为阻断或告警；
	数据库账号安全	具备免密登录功能，通过安装安全客户端，将数据库账号与运维终端的数字证书进行绑定，实现在运维终端无需输入数据库用户名密码就可登录数据库，减少因数据库帐密公开造成的泄露问题；免密登录至少支持 Toad、PL/SQL DEV 两种运维工具。
		支持产品 OTP 登录二次身份认证。
		具备账号托管功能，支持将真实数据库账号映射至自定义的托管账号，并通过 OTP、或系统动态生成的动态码作为配套密码，实现运维人员通过托管账号及动态码校验即可访问数据库，防止因数据库帐密公开造成的泄露问题；动态码应当脱敏显示，查看动态码时应当输入平台密码进行二次校验，动态码支持在线手动更新、自定义；
		支持安全客户端的短信二次认证功能，当登录安全客户端时，使用短信验证码验证成功才会登陆放行。
	权限管控	针对敏感数据集合的访问，任何账户（包括 DBA\SYSDBA\Schema User\any 权限等用户）都需要通过授权才可以访问，对不具备访问权限的操作，明确阻断拒绝，实现用户权限分离管理。
		支持通过标准 SQL、原始 SQL、正则 SQL 等方式自定义高危 SQL，用以精细化控制针对指定对象的 ALTER、DROP、CREATE 、TRUNCATE 等高危操作行为；支持将访问日志中的原始 SQL 进行标准化，形成标准 SQL，方便运维人员从访问日志中直接拷贝标准 SQL 用以自定义高危 SQL。
		支持 oracle 同义词表访问管控。
		支持 DB2 数据库联邦表管控。
		支持无需进行 SQL 语句自定义，即可在系统页面直接设置

		针对数据库角色、数据库对象、数据库系统等进行数据库授权相关操作的管控授权；数据库角色授权中，应当包含对 DBA、SYSDBA、SYSADMIN、服务器管理员、安装管理员、ADMIN、DBADMIN、USERADMIN、SECURITYADMIN 等数据库角色的授权；数据库对象授权中，应当包含对访问敏感对象、访问业务用户对象、访问系统对象的授权；数据库系统授权中，应当包含对任意对象及任意数据的删除、创建、修改等。
		支持无需进行 SQL 语句自定义，即可在系统页面直接设置针对数据库用户代码的操作管控授权，包括存储过程、函数、包、触发器、视图、索引等代码进行创建、删除、修改。
		支持无需进行 SQL 语句自定义，即可在系统页面直接设置针对数据库账号的操作管控授权，包括对用户、角色的创建、删除和修改，以及对密码的更改。
		支持无需进行 SQL 语句自定义，即可在系统页面直接设置针对数据表对象的操作管控授权，包括对数据库、SCHEMA、敏感数据表、业务用户表格、系统表格、以及表空间的删除、清空、修改、创建。
		支持数据访问频次控制，当请求超过自定义的阈值时，阻断请求；支持查询行数控制，当查询行数超过自定义的阈值时，超过的行数进行脱敏显示，防止返回过多明文导致批量数据泄漏。
		支持删除行数控制，当删除行数超过自定义的阈值时，可实现在不阻断删除操作的前提下，不删除任何数据；支持更新行数控制，当更新行数超过自定义的阈值时，可实现在不阻断更新操作的前提下，不更新任何数据；
		支持运维连接数控制、以及对单次请求关联的表个数进行管控，以降低大量恶意连接、复杂 SQL 等因素对数据库性能的影响。
		支持对已分类分级资产、未分类分级资产进行动态管控；实现将新增或变更的数据资产自动纳入管控；动态管控策略至少包含阻断、脱敏两种方式。
		数据资产未进行分类分级时，支持基于表和 schema 进行快速授权到某些身份或组。
		支持对通过 DBeaver 等三方运维工具进行数据导出的行为进行管控，未授权身份无法实现数据导出。
	SQL 窗口	支持直接通过 SQL 窗口进行数据库操作，提供可审计、可管控的数据访问方式。
		支持通过 SQL 窗口访问阻断时，可直接发起工单进行权限申请。
		支持 SQL 输入时数据库对象与关键字智能提示、SQL 美化。
		支持 SQL 查询结果集可视化查看、修改、添加、删除，并通过访问身份进行权限控制。

		支持对通过 SQL 窗口导出查询结果集的行为进行管控，并支持通过工单申请数据导出权限；结果集导出格式至少包含 XLSX、CSV、TXT、SQL 等。
		支持查看及生成指定数据库表的 DDL 语句。
	安全防御	支持僵尸账号检测，对僵尸账号进行永久锁定，防止僵尸账号造成数据泄露。
		支持数据库口令暴力破解防御，对口令攻击行为进行防御，防御数据库爆破行为。
		支持数据库防扫描，防止黑客或恶意用户对数据库进行扫描、侦查和探测，以发现潜在的安全漏洞和攻击目标。
		支持超时登出，当登录数据库后一定时间不操作时，自动断连。
	敏感数据脱敏	支持数据脱敏，可通过自定义脱敏策略，实现通过运维工具进行数据访问时，部分字段可返回脱敏后的结果；应当支持对敏感类型进行自定义分段处理；脱敏算法至少支持空值、随机映射、遮盖、加密等。
		支持 MongoDB 三层结构数据返回全解析，全脱敏。
	误操作恢复	支持误操作恢复，可在永久时间段或指定时间段内记录误操作的时间、数据库名称、SCHEMA、对象名称、SQL 语句、恢复状态等信息；支持设置误操作前的数据保留时间；支持对 DROP、Truncate 类型的操作进行一键恢复。
	工单管理	提供工单申请功能，可通过工单针对数据库登录、访问授权、自定义 SQL 执行、高危 SQL 执行等操作进行在线申请；工单采用逐级审批机制；实时展示待办工单审批状态；支持通过浙政钉进行移动端审批。
		申请人员提交工单申请后，支持通过预先设定好的审批流程，根据工单申请涉及的不同数据库，流向不同的审批人员。

（三）数据脱敏服务

在服务期内，提供数据脱敏服务，服务要求如下：

服务要求	系统架构	采用 B/S 架构，全中文操作界面，支持主流浏览器，支持 https/SSL 等加密传输协议。
		支持集群部署、可横向扩展，实现平滑扩容。
		采用微内核富插件化设计，支持外嵌插件对产品进行功能扩展。
	用户权限	根据三权分立原则进行职权分离，系统内置安全管理员、安全保密员和安全审计员三种用户角色。
		提供用户管理、角色管理功能，支持用户角色自定义，每个角色可关联不同的操作功能权限；同时支持不同用户拥有对应的数据资产管理权限，包括对特定资产进行敏感数据发现、执行脱敏作业等。
	资产适配	支持主流关系型数据库脱敏，包括 Oracle、MySQL、SQLServer（mssql）、PostgreSQL、MariaDB、MongoDB、AS400、Cache、DB2 等。

		支持国产数据库脱敏，包括但不限于达梦 dm、人大金仓 kingbase、华为 GaussDB、OceanBase、TDSQL（mysql_td）、TiDB、GoldenDB、Gbase 8a/8t/8s、Vastbase、opengauss、巨杉 sequoiadb、星环 Transwarp、qianbase、崖山 yashan。
		支持大数据平台脱敏，包括 Hive Apache、HANA、impala、Hbase、HDP、Hive FusionInsight、Greenplum、巨杉 sequoiadb、星环 Transwarp、ODPS（MaxCompute）、Teradata、Elasticsearch 等。
		支持云数据库脱敏，包括 RDS、阿里云 ODPS（MaxCompute）、腾讯云 TDSQL（mysql_td）、腾讯云 Hive 等。
		支持直接读取文件脱敏，包括 OFD、txt、csv、excel、xml、json 文件、DICOM 医疗影像文件、oracle dump（exp/expdp）、mysql dump（sql 文件）等。
		支持对本地、远程（ftp、sftp）的文件夹中的文件进行脱敏。
	脱敏方式	支持多场景脱敏，包括跨库脱敏、原库脱敏、库到文件、文件到文件（包括 FTP 和 SFTP 方式）、文件到库的脱敏场景。
		支持异构脱敏，包括 Oracle 与 MYSQL、Oracle 与 PostgreSQL、Hive 与 MYSQL 之间的异构脱敏。
		支持通过时间戳、自增列等增量标识对关系型数据库、大数据平台等不同数据源进行增量脱敏。
		支持对单个大表进行分片处理，可自定义大表数据量，同时支持多线程并发以提升脱敏效率。
	敏感类型	内置常见敏感类型，包括中文姓名、英文姓名、姓名拼音、韩文姓名、电话号码、邮箱、邮编、金额、日期、企业营业执照、组织机构代码证、银行卡号、军官证、港澳通行证、往来台湾通行证、护照、香港身份证、澳门身份证、税务登记证、身份证、组织机构名称、地址、IP 地址、社会统一信用代码、开户许可证、医疗机构登记号、医师资格证书、医师职业证书、证券代码、证券名称、基金名称、基金代码、车牌号码、车架号等。
		支持混合敏感类型，包括单个字段中多种敏感类型、一个数据单元内包含多种敏感类型的情况。
		支持自定义敏感类型，发现规则可选择根据内容正则匹配、内容字典匹配、字段名正则匹配、Javascript 脚本等方式。
	敏感数据发现	支持自定义数据子集进行敏感发现，支持按字段条件配置筛选条件。
		支持通过抽样的方式进行敏感数据发现，可自定义敏感类型发现范围、抽样比例和匹配率，支持自上而下或随机抽取等抽样方式。
		支持对自动发现的敏感类型进行手动调整，支持单个/批量修改。
		支持对拥有一定规律的半结构化文本进行敏感数据发现，如电子病历等。
		支持自动检测源数据库 DDL 的变动，识别增量的新数据表的敏感信息。
	脱敏规则算法	支持多种脱敏算法，包括固定映射、随机映射、遮盖、置空、替换、截取、截断、范围随机、随机浮动、偏移、取整、分段、MD5 加密、SHA1 加密、SHA256 加密、SM4 加密、AES 加密、RSA 加密、归一算法、数据水印以及自定义算法等。
		支持归一化算法，实现数据标准化处理。

		支持自定义增加脱敏规则，包括规则名称、敏感类型、脱敏算法、分段配置；其中脱敏算法支持采用 JavaScript 语言自定义。
		支持组合脱敏，选择多个敏感类型形成组合，组合内所有敏感类型都存在时才进行脱敏。
		支持计算脱敏，数据脱敏后保留计算关系，如数据的分组求和、依赖计算等。
		支持依赖脱敏，可根据依赖本字段、其他字段的值对数据进行不同类型的脱敏处理。
		支持配置脏数据处理规则，规则内容至少包括不脱敏、置空处理、按敏感类型进行脏数据处理。
		支持对所有敏感类型进行自定义分段脱敏，分段方式包括位数、分隔符、指定位置、正则等。
	数据脱敏管理	支持脱敏后在目标库中自动创建数据库对象，数据库对象包括表、主键、外键、索引、约束、视图、同义词、序列、队列、DBlink、自定义类型、存储过程、函数、触发器、包等。
		支持在脱敏时自定义选择目标表空间，包括默认表空间、源库表空间（同名）、指定表空间等。
		支持数据一致性关联，如身份证脱敏后，相关的业务字段“生日”“年龄”可与脱敏后的身份证结果保持一致。
		支持脱敏前自动检测源数据库 DDL 的变动，识别增量的新数据表的敏感信息，自动同步变化的对象
		支持对单表指定列数据进行脱敏；支持剔除不相关的列。
		支持创建脱敏数据子集，仅对子集中的敏感信息进行脱敏，支持按 where 条件和按分区设置筛选，也可批量导入条件设置。
		支持黑白名单配置，白名单支持模板批量导入，添加到黑名单中的数据不会同步到目标端，添加到白名单的数据不进行脱敏保持原值同步到目标端。
		支持在脱敏前对真实数据进行预脱敏，确认脱敏效果。
		支持可视化展现脱敏作业运行状态，包含脱敏作业状态、脱敏速度、进度条、当前脱敏操作等监控指标；支持可视化展现作业运行日志，支持错误数据、错误步骤展现。
		支持脱敏暂停、终止、断点续做等操作；脱敏作业错误中断后，可进行错误部分重做，已完成部分无需重复脱敏。
		支持脱敏结果与原数据比对，数据脱敏后保持原有数据类型、结构、特征、业务逻辑关系。
		支持对已设置为数据源的库信息做强阻断性保护，防止操作不当导致的源数据被删除。
		支持配置脱敏作业定时调度计划，可在指定时间自动运行，支持按分、按时、按天、按周、按月执行以及执行一次，支持设置调度周期，支持自由启停脱敏计划。
		支持快速脱敏，可通过上传规定的表格文件完成脱敏配置，自动完成敏感数据的发现并进行脱敏作业。

	系统报表	提供针对敏感分布维度、脱敏作业维度的分析报表，支持自定义时间段进行报表查询和报表导出；敏感分布分析报表包含敏感源总量、表格总量、敏感表格量、字段总量、敏感字段量、敏感占比、敏感排名、脱敏源敏感分析等，可对脱敏源敏感分析的每一项数据进行排序查看；脱敏作业分析报表包含运行作业数、运行总次数、处理数据总量、处理敏感数据量、共计错误数、脱敏作业处理量分析、脱敏作业分析等，可对脱敏作业分析的每一项数据进行排序查看。
		提供针对用户行为维度、敏感发现作业维度的统计报表，支持自定义时间段进行报表查询和报表导出；用户行为统计报表包含用户登录总次数、用户登录总时长、脱敏源相关操作、作业调度次数、手动创建脱敏源数量等；敏感发现作业维度包括敏感发现耗时、发现表格数量和敏感表格数量等；同时支持对敏感字段进行统计，支持查询展示与导出。
	系统安全性	支持账号安全控制，包括登入防暴力破解、登入密码定期修改、密码有效期等，并对密码复杂度进行限制，以确保平台自身账户的安全。
		支持对访问身份进行强验证，验证因子包括生物特征-指纹、证书、OTP 等。
		用户密码应采用加密算法进行存储和验证，服务报文采用对称加密方式加密，并具有校验机制。
		要求提供详细有效的系统维护日志，支持一键下载，便于对故障、事件和错误等进行分析和定位，方便事件处理和审计追溯。
		要求提供详细有效的用户操作日志，包括不限于：操作时间、操作人、操作模块、客户端 IP 等，便于操作追溯和审计归档。
		支持对脱敏系统自身进行定时或者手动备份，备份存储方式包括 FTP/SFTP，支持从备份中恢复脱敏系统。
	告警通知	支持告警通知功能，告警方式包括邮件告警、钉钉告警、短信告警；告警内容设置为错误调度或全部调度。
	产品联动	支持与分类分级系统进行联动，通过 API 接口将分类分级结果自动同步，同时支持对分类分级的结果进行手动调整。
	API 接口	支持第三方通过 OpenAPI 方式直接调用脱敏能力，接口包括敏感发现接口、脱敏作业接口、作业调度接口，通过作业调度接口可对作业进行启动、终止操作；支持 Token、Accesskey 等接口安全鉴权验证方式。

（四）数据加密服务

在服务期内，提供数据加密服务，服务要求如下：

服务要求	部署方式	支持旁路模式部署，无需更改网络结构；支持分布式部署，通过管理中心对分布式部署的各网关节点进行集中配置管理、分析、统计。
	高可用	支持集群，可随业务随时平滑扩展。
		支持主备 HA 部署。
	数据加解密	支持根据数据库查看加密资产的信息，以库加密、schema 加密、表加密、列加密、表空间加密等维度查询当前的加密资产。
		至少支持整库、表空间、schema、表、列等数据加密粒度；支持针对不同敏感等级的数据进行加密。

		支持增量资产加密，支持新增列、表、schema、表空间的动态防护。
		支持多种加密模式，支持业务在线加密，不需要业务停机。
		支持以下特殊数据类型和索引类型的加密正常读写、等值查询和范围查询：BLOB 数据、CLOB 数据、IOT 表的 Mapping 表、B*Tree 索引、Bitmap 索引、全局索引等。
		对于增删改查操作、函数、存储过程等均透明；对于主外键、NOTNULL 等重要约束透明。
		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。
		支持通过指定进程或指定目录，新增进程白名单。
	数据存储完整性	支持 SM3-HMAC 国密验证算法，验证数据存储完整性，发生篡改时进行告警并记录告警时间、被篡改的目标对象。
	离线加解密	支持离线加解密工具下载，通过离线加解密工具，可对敏感数据文件进行加密，保障数据文件安全；实时记录用户名、邮箱、电话、加密内容、加密地址等信息；接收方需获取授权并验证信息后才可解密密文数据文件。
	加密资产授权	资产访问默认密文，支持通过工单审批机制，实现加密数据资产访问授权。
		支持基于身份的密文访问控制，身份要素至少包括应用名称、应用签名、IP 地址、主机名、数据库用户等，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，无合法权限的用户返回经过加密数据或禁止访问。
	密钥管理	加密算法至少应支持 3DES168、AES128、AES192、AES256 等国际密码算法，SM4 等国密算法。
		支持在加密前，根据不同加密算法，进行加密结果预览。
		支持使用 SM4 国密算法对工作密钥进行加密。
		支持分层密钥管理体系，通过引入主密钥，加密工作密钥，生成可备份保存的加密密钥。
		支持多级密钥管理体系，同一数据库中不同的数据表使用独立的工作密钥。
		支持对密钥进行更新；支持密钥备份至本地离线保存；支持通过将密钥导入至系统，实现密钥恢复；进入加密平台后，需再次经过当前安全管理用户的密码校验后，才能进行密钥更新、备份、恢复操作。
		支持对接三方密码设备，至少包括密码卡、密码服务平台、密码管理系统等。

五、数据库个性化运维服务要求

在服务期内，至少提供4人天的现场运维服务，以满足采购方定制化数据库运维需求或为重要活动提供保障。

第二条　服务期限

2.1 服务期限：自合同签订之日起一年

第三条　服务地点

3.1 服务地点及联系方式：

服务地址：德清县武康街道英溪南路399号

联系人：余旭　　联系电话：0572-8280010

第四条　款项结算

4.1 发票：乙方按以下内容向甲方开具相应支付金额的增值税专用发票

账户名称：德清县人力资源和社会保障信息中心

纳税人识别号：12330521669151548J

地址、电话：德清县武康街道英溪南路399号 0572-8280010

开户行及账号：浙江德清农村商业银行股份有限公司 231000002484526

4.2 甲方按以下方式支付款项。

合同签订生效并具备实施条件后7个工作日内，支付7万元作为预付款，服务期结束后稳定运行并通过服务质量评估（即服务验收）后支付余款。

4.3 收款账户

银　行：杭州银行

全　称：杭州美创科技股份有限公司

开户行：杭州银行求是支行

账　号：78808100148768

第五条　设备归还

5.1 乙方为满足甲方的服务需求所提供的软硬件产品，甲方仅拥有使用权，产品所有权及一切知识产权均归乙方所有。服务期满后或本协议终止、解除（不论何种原因）甲方应将乙方所提供的产品在 5 个工作日内归还乙方；若产品为软件形态的，则甲方需要在 5 个工作日内将软件进行卸载删除处理。

5.2 服务期间，甲方负责设备的安全性、完整性并且产品序列号标签不得磨损、丢失、修改。

5.3 服务期内，如果设备遗失或存在人为造成的损坏，则甲方必须向乙方照价赔偿，具体赔偿数额视设备损坏程度参照设备的账面价值及市场价格确定。

第六条　其他约定

6.1 服务期间，乙方负责设备硬件保修和软件升级。

6.2 服务期内乙方因提供服务必须使用的自有设备，运输成本和途中的风险由乙方自行承担。

6.3 乙方提供设备给甲方的运输成本和途中的风险由乙方自行承担。

6.4 甲方返还设备给乙方的运输成本和途中的风险由乙方自行承担。

6.5 非不可抗力原因，合同必须执行完整，不允许提前终止合同。

6.6 甲方在使用乙方提供的软硬件产品过程中，不进行反向工程、反向汇编、反向编译，或者以其他方式尝试发现相关产品的源代码；不得删除相关产品程序及其副本上关于著作权的信息。否则，乙方有权终止本合同并要求甲方支付合同总金额 30%的违约金。

第七条　违约责任

7.1 甲方未按合同约定如期付款的，每逾期一天，应向乙方支付合同总额千分之五（5‰）的违约金，逾期时间超过六十天的，乙方有权解除合同，甲方除须支付乙方合同全额货款外，

还须承担不低于合同总额30%的违约金，以及赔偿乙方因此产生的其他一应损失。乙方因追索债权产生的律师费等费用由甲方承担。

7.2 乙方未按合同约定如期交货的，每逾期一天，应向甲方支付合同总额千分之五（5‰）的违约金，逾期时间超过六十天的，甲方有权解除合同，乙方须承担不低于合同总额30%的违约金，以及赔偿甲方因此产生的其他一应损失。

7.3 如非因乙方过错，甲方不履行合同或拒绝接受符合合同约定的产品或服务的，为甲方单方违约，乙方有权解除合同并要求甲方支付不低于合同总额30%的违约金，甲方已支付预付款的，预付款不予退还，预付款不足合同总额30%的，甲方应补足违约金给乙方。

7.4 按本合同约定应当偿付的违约金等各种经济损失，应当在明确责任后三个工作日内付清，未付清的，每逾期一天按应付违约金的千分之一（1‰）支付罚金。

7.5 若甲方在使用产品过程中，存在对产品软件进行反向工程、反向汇编、反向编译，或者以其他方式尝试发现相关产品的源代码，删除相关产品程序及其副本上关于著作权的信息等侵害乙方对产品享有的知识产权行为的，乙方有权解除本合同并要求甲方支付合同总额30%的违约金。

7.6 任何一方因违约向守约方支付的违约金不足以弥补守约方因此遭受的损失的，守约方有权要求违约方予以补足。任何一方因其他违约行为给守约方造成损失但未约定违约金的，守约方均有权要求其赔偿由此产生的所有损失。本合同所指“损失”包括但不限于守约方因此而遭受的经济损失、预期利益损失以及为处理此事而支付的费用（包括但不限于律师代理费、仲裁费、诉讼费、差旅费、公证费、鉴定费、公告费、材料费、调查费、评估费、第三方索赔费用等）。

第八条 不可抗力

8.1 因战争、自然灾害、政府行为、公共卫生事件、甲类及参照甲类管理的乙类传染病爆发

及非因乙方原因导致的互联网系统故障、互联网通讯提供商故障、黑客攻击或电力部门技术调整或故障等不可抗力因素或者第三方原因导致乙方不能履行本合同项下义务的，根据不可抗力因素或者第三方原因造成的影响，乙方可免责。

8.2 当不可抗力事故停止或消除后，受事故影响的一方应尽快以传真形式通知对方。

8.3 如果不可抗力的持续影响超过 10 周，被影响的一方通知另一方解决问题。如果另一方未能及时作出回应或在收到前者通知后 1 个月未能达成一致意见，被影响的一方有权解除部分或全部的合同。

8.4 如果本合同任何一方因受不可抗力事件（不可抗力事件指受影响一方不能合理控制的，无法预料或即使可预料到也不可避免且无法克服，并于本合同签订日之后出现的，使该方对本合同全部或部分的履行在客观上成为不可能或不实际的任何事件。此等事件包括但不限于水灾、火灾、旱灾、台风、地震、电脑病毒、疫情及其它自然灾害、交通意外、罢工、骚动、暴乱及战争（不论曾否宣战）以及政府部门的作为及不作为）影响而未能履行其在本合同下的全部或部分义务，该义务的履行在不可抗力事件妨碍其履行期间应予中止。

第九条 网络与数据安全责任

9.1 投标人在提供服务时应遵守《中华人民共和国网络安全法》《中华人民共和国保守国家秘密法》《浙江省信息技术服务外包网络安全管理办法》等法规。

9.2 投标人服务人员执行可能威胁网络安全的操作行为时，应先审批后操作。

9.3 采购人定期评估投标人服务活动中网络安全执行情况，发现异常或违规行为及时向投标人通报。

9.4 投标人收到采购人通报后，要及时开展内部惩戒，实行解除聘任合同、取消技术资质等措施，并及时将惩戒情况向采购人报告。

9.5 因投标人服务人员违规行为引发重大网络安全事件的，采购人有权单方面终止合同，经书面通知投标人后，投标人应当退还合同期内剩余未服务时间的服务费，并赔偿采购人合同总价款 10%的违约金，违约金不足以弥补因违约所造成的损失的，还应赔偿相应损失。

第十条　争议的解决

本合同为政府采购之合同，在发生所供商品（服务）的质量、售后服务等问题时，甲方有权直接向乙方索赔，签订必要的书面处理协议。如协商不成，任何一方有权提交甲方所在地仲裁委员会仲裁解决。

第十一条　附则

11.1 本合同一式伍份，甲方执叁份，乙方执壹份，招标代理公司执壹份，自双方加盖公章/合同章后生效，具有同等法律效力。

11.2 合同附件是本合同不可分割的一部分，与本合同具有同等法律效力。

附件一：《网络和数据安全责任协议》

11.3 本合同对应项目的招投标文件与本合同具有同等法律效力，与本合同不一致的，以本合同为准。

甲　方（盖章）：德清县人力资源和社会保障信息中心

地　址：德清县武康街道英溪南路399号

联系人：

电　话：0572-8280010

日　期：2025.7.10

乙方（盖章）：杭州美创科技股份有限公司

地　址：浙江省杭州市余杭区五常街道中福未来星宸金座4幢4-5层

联系人：

电　话：19818323266

日　期：

附件一：网络和数据安全责任协议

网络和数据安全责任协议

1、乙方在开展项目实施过程中应按照“安全第一、预防为主”的原则，并根据《浙江省信息技术服务外包网络安全管理办法》做好服务外包管理工作，应按照《网络安全法》、《数据安全法》等要求，采取科学有效的安全管理措施，确保信息安全的技术手段，建立权责明确、覆盖信息化全过程的岗位责任制，对信息化全过程实行严格监督和管理，确保网络和数据安全。

2、乙方应按照系统管理员、网络安全员、数据安全员、运维人员相互制约等原则设置服务人员岗位，并提供本单位服务人员的背景调查信息和保密承诺书，及对背景调查的结果负责。

3、乙方在对甲方敏感或重要数据进行操作时，应采取分类分级保护、数据备份和加密存储传输等技术手段，防止信息泄露、损毁、丢失。在信息发生泄露、损毁、丢失的情况时，应当立即采取补救措施，并第一时间告知甲方。由乙方服务人员不当操作或异常行为引起重大数据安全事故则由乙方承担，并扣除一定合同金。

4、甲方有权对乙方日常维护操作进行安全监督、检查和指导工作。由乙方服务人员不当操作或异常行为引起甲方业务停运或其他重大网络安全事故则由乙方承担，并扣除一定合同金。

5、未经甲方允许，乙方不得对建设、运营、运维的信息系统、应用、数据库等私开账户、擅自更改权限等操作，严禁乙方多名工作人员共用账号，严禁使用弱密码。

6、乙方应加强网络和数据安全风险监测，制定网络和数据安全应急预案，完善应急机制。发现自身高危安全风险时，应立即采取补救措施，并第一时间告知甲方。

6、乙方服务人员职责变更或离职时，应提前一个月向甲方提出申请，及时完成设备安全检查审核、技术资料移交等工作，并回收相关运维的工具及账号，签订离岗保密协议，严格禁止其向外传播。

甲方（盖章）： 德清县人力资源和社会保障信息中心

法人或受权委托人（签字）：

日期：2022 年 7 月 10 日

乙方（盖章）：杭州美创科技股份有限公司

法人或受权委托人（签字）：

日期： 年 月 日