**数据脱敏系统应用需求**

**（如完全响应，请盖公章）**

1. 项目背景

《中华人民共和国网络安全法》自2017年6月1日起施行，其中明确指出相关方“应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。” 华润万家在跟第三方进行数据交换时，在对外部机构提供相关的报告时，在系统的开发和测试过程中，均需要使用生产数据，这容易造成会员、商品、供应商信息泄露, 需要引进数据脱敏系统对生产数据进行脱敏处理。

1. 项目目标

购买数据脱敏系统：对生产数据涉及会员、商品、供应商的信息进行脱敏处理， 防止会员和商品、供应商数据的隐私数据进入第三方机构、华润万家的开发及测试环境引起信息泄露；

1. 项目范围
2. 组织范围

 全华润万家

1. 业务范围

|  |  |
| --- | --- |
| **场景** | **内容** |
| 数据库脱敏 | 对数据库中包括的敏感信息进行脱敏处理后方可进行测试环境和开发环境， 保持数据库中数据库的完整性 |
| 文件脱敏 | 对结构性的文本文件中的个人隐私数据核心商密进行脱敏处理， |

1. 系统功能要求

|  |  |  |
| --- | --- | --- |
| **系统功能** | **要求** | **定义举例** |
| 数据库数据脱敏 | 支持主要的关系型数据库作为源和目的数据库 | 支持ORACLE、Mysql、Informix、MS SQL SERVER、DB2 |
| 支持隐私数据类型的自动发现功能 | 能够根据数据本身的特征，包括类型、长度等进行分析，发现隐私数据 |
| 支持中国地区特定隐私数据自动漂白脱敏功能 | 如中文姓名、身份证号码、电话号码、纳税人识别号等 |
| 支持自定义隐私数据类型 | 可以自定义隐私数据， 如字段数据、或者正则表达式等方式 |
| 支持元数据的数据装载 | 能够生成目标数据库的DDL语句创建数据表、索引、约束、用户、权限、表空间、存储过程、触发器等 |
| 漂白算法能够保持数据的关联性 | 如能够支持数据的跨表关联 |
| 生成的脱敏数据必须为高仿真数据 | 例如姓名脱敏后仍为姓名，证件号码脱敏以后仍然是同种类的证件号码且符合该种证件号码的编码规则 |
| 数据脱敏后必须保证数据的完整性 | 数据的行数和列数必须和原始数据相等，不能出现数据丢失。必须支持CLOB/BLOB/LONG等大对象字段的装载。 |
| 支持源库脱敏 | 支持在源库上进行脱敏，脱敏后直接写入源数据库 |
| 数据文件脱敏 | 支持带有特定格式的结构性文本文件脱敏 | 带有特定分隔符的文本文件进行数据脱敏 |
| 系统管理 | 提供必要的系统管理功能 | 除了发现、抽取、漂白、装载等功能外， 提供系统监控、访问控制功能等功能 |
| 用户管理 | 对平台用户的账号进行管理和授权管理，支持用户的行为审计功能 |

1. IT技术要求
* 支持以下种类的数据库作为源和目标数据源：ORACLE、INFORMIX、MYSQL；
* 支持带有一定格式的结构化文本文件作为目标数据源；
* 脱敏过程中， 数据不在脱敏系统落地。
1. 工作说明书

工作说明书的内容应包含但不限于下列事项：

|  |  |  |  |
| --- | --- | --- | --- |
| **项目阶段** | **分类** | **项目工作** | **实施商职责划分** |
| **项目过程管理** | 项目管理 | **项目执行管理** |  |
| 项目管理 |  项目规划 | 参与 |
| 项目管理 | 项目进度监控 | 参与 |
| 项目管理 | 风险管理 | 参与 |
| 方案 | **方案设计** |  |
| 方案 | 数据脱敏方案设计 | 主责 |
| 实施 | **交付与部署策略** |  |
| 实施 | 系统部署和设置 | 主责 |
| 测试 | **系统测试** |  |
| 测试 | 测试方案 | 主责 |
| 实施 | 脱敏算法调整 | 主责 |
| 培训 | 系统培训和知识转移 | 主责 |
| 运维 | 上线后问题解决 | 参与 |

1. 项目周期要求

 项目周期预计5个月

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **招采** | **启动** | **设计** | **上线** | **验收** |
| 实际完成为准 | 1个月 | 1个月 | 2个月 | 1个月 |

1. 实施团队要求
2. 实施团队

原厂实施团队成员必须参与项目实施，应保证参与人员的稳定性，实施过程中不得进行更换。

1. 实施范围

负责实施方案的制定，文档加密安全策略的定义与实施，培训课件的制作，并完成知识转移和交接。

1. 项目经理要求

项目经理全职现场参加项目。须为原厂项目经理，负责本项目的计划、组织、实施、协调、人员配置并监督工作情况及进度等工作，负责与各方的沟通联系。具有预见和应对项目风险的能力。

1. 知识转移要求

在项目阶段针对万家的项目人员进行知识转移和培训工作，并确保质量，使华润万家人员具备参与本项目的技能和实施后的运维能力。

1. 知识产权要求
2. 乙方承诺所使用软件、技术等的合法性，无相关法律瑕疵；
3. 乙方应向甲方提供本项目开发实施的所有源代码，并保证代码的完整性；
4. 乙方保证由乙方负责开发实施的成果（包括但不限于运行程序、代码等）未侵犯任何第三方的知识产权，否则由此引起的有关法律责任及全部损失赔偿由乙方承担。
5. 验收和交付成果要求

实施商需要根据万家定义的范围为基础，参考实施方法论，列出项目生命周期不同阶段提交的阶段成果和各类交付物清单，交付范围与交付质量须符合万家项目管理要求。另外，实施商需要对交付成果以及各类交付物给出验收标准和验收流程建议。

1. 运维服务要求

项目验收后，供应商需要提供一年免费维护服务，其中，1个月的全程现场支持，并将现场运维工作移交给万家。完成运维工作移交后，采用7\*24电话或远程登入的方式支持，如遇紧急问题需安排合适人员进行现场支持。

一年免费维护期结束后，如万家提出后续维护服务的需求，供应商不得拒绝，且后续维护服务费（含许可续期费，如有）双方应约定收费规则，维护服务合同双方另行签订。预计本系统使用年限为5年以上。

运维服务包括但不限于以下内容：

**电话服务：**7\*24（每周7天，每天24小时）电话支持服务；

远程支持：日常使用中遇到的问题通过打电话、邮件等咨询方式没有解决问题，产商运维工程师须远程排查分析问题；

**顾问服务：**在系统正式运行期间，厂商须提供各类关于系统维护、安全管理等方面的技术资料，对用户在实际应用中的相关问题提供专业的解决方案，提供技术安装、调试、使用、维护、升级和新技术推荐等方面的免费咨询服务；

**现场支持：**日常使用中遇到的问题通过打电话、邮件等咨询、远程等方式没有解决问题，可联系项目经理，由项目经理安排工程师上门解决问题。

1. 驻场人员管理规定

实施商驻场人员应严格遵守《华润万家IT项目供应商驻场人员管理规定》，见附件。如乙方驻场人员违反规定中的“一类规定”，视为乙方根本违约，乙方应承担所有责任，且甲方有权解除合同，并要求乙方赔偿损失（包括但不限于甲方自身遭受的损失、被政府相关部门处罚以及被第三方追偿的损失等等）。如乙方驻场人员违反规定中的“二类规定”，合同期内前3次违规，甲方有权给予警告并处以100元/次罚款，从第4次开始，甲方有权对乙方处以1000元/次罚款，所有罚款均可在合同付款时直接扣除。

  **华润万家IT项目供应商驻场人员管理规定**

**一类规定：**

1. 严禁在甲方服务器安装使用未经华润万家书面许可的远程控制工具；
2. 未经甲方书面授权，乙方不得从事下列活动：
3. 以甲方名义进行考察、谈判、签约、招投标、竞拍等；
4. 以甲方名义提供担保、证明；
5. 以甲方名义对外发表意见、消息；
6. 以甲方名义出席公众活动；
7. 以甲方名义对华润万家外部客户和业务关联单位做出书面或口头承诺；
8. 对外演讲、交流或授课时涉及甲方的内容；
9. 将甲方资产赠与、转让、出租、出借、抵押给其他单位或个人。
10. 禁止对甲方人员有恐吓、敌对、性骚扰等行为。

**二类规定：**

1. 计算机终端须安装防病毒软件及最新高危漏洞补丁后方可接入甲方网络；
2. 不在任何场合诋毁甲方及其关联单位，以及甲方的其他供应商和个人；
3. 工作时间应注意仪容仪表，整体要求是：得体、大方、整洁；
4. 工作时间不得在甲方食堂就餐，用餐时间不得插队；
5. 工作时间不得睡觉、嬉笑打闹、高声喧哗、玩游戏、观看影视剧等与工作无关的活动；
6. 工作时间不得擅离职守，常驻乙方如需外出或休假，需提前向甲方对接人提出邮件或其他书面申请并获得批准；
7. 未经甲方对接人邮件或书面批准，常驻IT乙方人员每日出勤未满8小时的情况每月不得超过3次；
8. 办公桌面应干净整洁，不得堆放有气味的食物等；
9. 不得在指定吸烟点之外的区域吸烟；
10. 工作期间必须佩戴甲方临时工牌；
11. 不得带无关人员进入甲方办公区；
12. 乙方应指定专人进行人员管理，包括但不限于以下管理内容：

进场管理：项目合同签订后，乙方指定专人填写《进场申请单》、《驻场登记册》及《人力投入计划》，邮件发送甲方对接人并获得批准；

实施过程管理：乙方指定专人每月更新《驻场登记册》及《人力投入计划》并邮件发送甲方对接人并获得批准；

离场管理： 乙方指定专人填写《离场申请单》并邮件发送甲方对接人并获得批准。