**用户需求书**

**一、项目概况**

（一）采购单位

东莞市水务集团有限公司

（二）项目名称：2025年东莞市水务环境集团有限公司网络安全保障服务项目

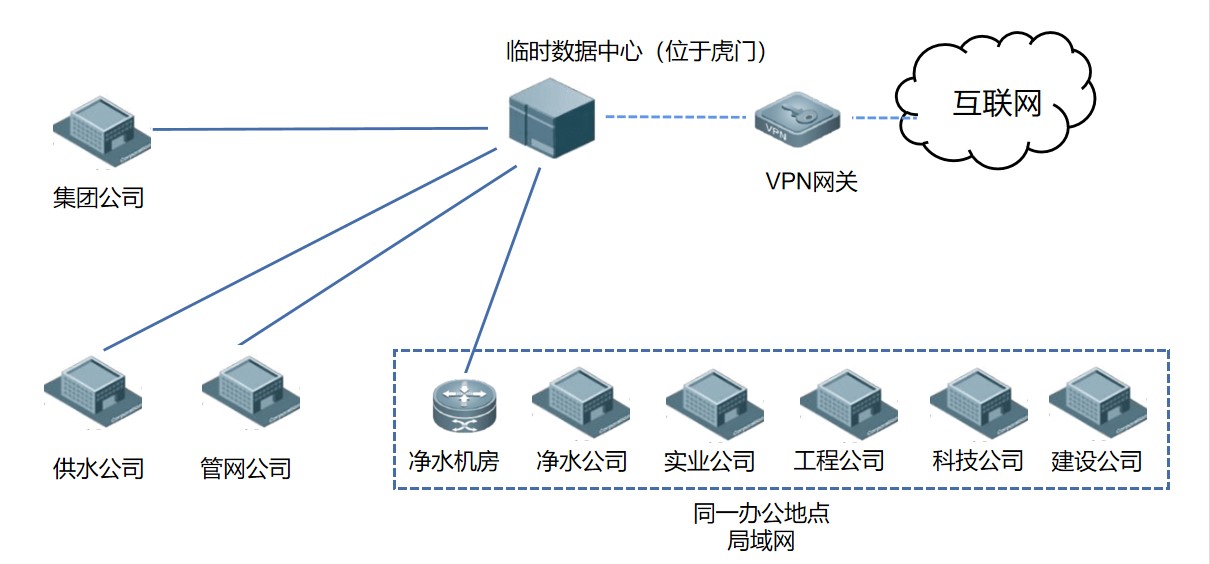
（三）项目性质：服务类

（四）项目概况

本项目建设目的是为了加强集团信息安全建设，减轻网络安全运维压力，完善集团运维体系和网络安全管理体系，更好的保障“莞盾”“粤盾”以及“两会”等重要时段的网络安全，保障集团业务的正常运作。

**二、基本情况**

目前东莞水务环境投资控股集团有限公司下设**8家直属企业**，分别为：供水公司、净水公司、管网公司、碧水公司、建设公司、实业公司、科技公司、福地公司，其中集团公司建有2个机房（集团本部机房、集团临时数据中心），除福地公司外，7家直属企业各自建有1个机房，即**共有9个机房**，每个机房均之间通过专线及零信任进行访问。



信息化建设情况：**水务环境集团建有信息化系统22个**，包括集团公司5个、供水公司2个、净水公司3个、管网公司4个、建设公司1个、碧水公司0个、科技公司6个、实业公司1个，业务系统部署于各自机房，已通过组网专线连通了各集团及直属企业的机房、办公网络。

机房设备情况：集团及各直属企业机房已有网络安全设备（含防火墙、上网行为管理器、网络安全探针等）30余台，服务器（含存储服务器、业务系统服务器）有40余台。

注：1.以上数量信息仅用于数量参考，本次项目涉及的设备、信息化系统数量以实际为准。2.根据招标人经营情况，办公地点有可能进行调整，办公地点以甲方实际为准，投标人应充分考虑相关风险。

表1 各单位地址

|  |  |
| --- | --- |
| 单位 | 详细地址 |
| 集团公司（包括办公地点） | 东莞市东城街道育华路1号 |
| 供水公司 | 东莞市莞城街道莞龙路莞城段141号 |
| 净水公司 | 东莞市南城街道滨河路100号二期1号楼 |
| 管网公司 | 东莞市东城街道运河路5号 |
| 实业公司 | 东莞市南城区滨河路100号二期3号楼 |
| 碧水公司 | 东莞市南城街道滨河路100号二期2号楼 |
| 科技公司 | 东莞市南城街道滨河路100号 |
| 建设公司 | 东莞市南城街道滨河路100号 |
| 集团临时数据中心机房 | 东莞市虎门镇东引路10号 |

**三、需求内容**

结合招标人网络安全建设及网络安全运营情况，拟采购第三方网络安全服务单位为招标人提供网络安全保障服务，具体内容如下：

**（一）设备状态及网络监控**

服务范围：集团及各直属企业

服务要求：1.每周一次出具《巡检报告单》；通过线上巡查，对网络设备、网络安全设备、服务器等重要设备进行状态巡检，对网络设备及网络状态进行监测，对网络安全设备的日志进行分析，排查设备、网络以及安全隐患问题，保障网络安全。

2.针对发现安全隐患问题以及设备和线路调整、重大活动日加强防护等原因，对设备（包括但不限于交换机、防火墙、服务器等设备）安全策略、系统设置等进行调优。

交付内容：《巡检报告单》

**（二）信息化系统及设备安全检测**

服务范围：集团及各直属企业

服务要求：一年两次，对集团及直属企业信息化系统及各类设备进行安全扫描、弱口令检查、基线扫描以及渗透测试等，协助对系统进行升级和漏洞封堵，具体内容包括但不限于：

1.操作系统安全检查：病毒防护、系统补丁、系统账户、远程管理、审计策略、密码策略、账户锁定策略、审计日志策略和备份、端口开放等。

2.数据库安全检查：身份鉴别、访问控制、安全审计、通信保密信息、数据保密性和资源控制等。

3.中间件安全检查：身份鉴别、访问控制、安全审计、通信保密性、软件容错、资源控制和数据完整性等。

4.服务器安全分析：进程分析、会话分析、冗余软件分析、冗余服务分析、访问互联网和内网权限分析、关键位置木马检测、入侵痕迹分析等。

5.渗透测试：在得到我司渗透测试授权后，安全服务单位以模拟黑客常用的攻击手段，尝试入侵授权范围内的互联网开放系统，找出各种潜在的安全漏洞，以验证企业的设备与资料是否可被破坏或窃取，避免系统受到非法攻击者的恶意攻击。渗透测试内容包括但不限于信息收集、中间件漏洞测试、目录文件漏洞测试、注入攻击测试、跨站脚本漏洞测试、访问控制测试、敏感信息泄露测试、缺省的或可猜测的（字典攻击）用户账户测试、身份认证和会话管理、跨站请求伪造测试。

6.设备网络安全排查：对机房各类设备、终端进行网络安全检查，包括但不限于设备硬件检查、设备安全策略检查、设备漏洞补丁修复等。

交付内容：《安全检测报告》《渗透测试报告》

**（三）IT资产运维**

服务范围：集团公司（包含集团临时数据中心）

服务要求：对集团IT资产（包括但不限于办公IT设备、网络设备、安全设备、服务器、办公终端等设备）进行盘点和梳理，定期对资产信息进行维护和更新，建立相关台账，梳理相关管理流程，实现有效管理。

交付要求：《IT资产台账》

**（四）IT运维体系建设**

服务范围：集团及各直属企业

服务要求：（1）根据集团实际情况，协助梳理运维流程，建立健全网络安全、网络数据安全工作机制、运维机制以及协助制定相关制度等。

（2）服务期内要求提供网络安全管理软件工具，支撑集团及各级单位网络安全运维工作，工具功能包括不限于：集中全面监控集团的IT系统，包括服务器、网络设备、操作系统和数据库等，能够实时监测系统状态，及时发现潜在问题并进行智能预警，从而提升运维效率、缩短响应时间，保证业务系统的数据安全和稳定运行。

**（五）应急响应及运维服务**

服务范围：集团公司本部及集团临时数据中心。

★**服务要求：（1）提供不少于1人IT工程师现场驻点，提供IT设备运维服务及网络安全保障服务，保障集团公司本部及集团临时数据中心各类IT资产各类终端设备（包括但不限于办公电脑、交换机、AP、防火墙、服务器）、终端桌面、网络、各类线路及业务系统等的正常运作，保障网络安全和各类设备的正常运作（须附驻点人员的身份证、职称证、社会保障部门出具距今的近6个月在投标人单位缴纳社会养老保险有效凭证等证明材料复印件并加盖投标人法人公章）。**

1. **要求：**

**1.驻点时间和招标人工作时间相同；特殊情况除外（遇应急情况需及时处理）**

**2.驻点人员应优先处理“应急响应及运维服务”的服务内容，本项目其他服务项原则上应由团队其他人员完成。**

交付要求：驻点人员接受招标人考核，提供包括考勤打卡记录、应急响应处理台账、运维台账以及其他材料。

**（六）安全评估与规划**

服务范围：集团及各直属企业

服务要求：每年一次，对集团及直属企业的网络安全情况进行综合评估，评估应包含各网络设备盘点、服务器盘点、安全评测以及整改方案等，对集团及直属企业的网络安全进行评估，并提出整改计划和未来建设规划，协助各单位进行整改。

交付内容：《安全评估与规划报告》

**（七）重要时期网络安全保障服务**

服务范围：集团及直属企业

服务要求：（1）每年不低于4次（具体根据招标人实际需要为准），同时对集团及直属企业提供重要时期网络安全保障服务，要求该时期提供全天24小时网络安全保障，提供不低于两名工程师线上值守，提供应急响应服务，及时应对网络安全攻击，排查网络安全隐患，封堵网络安全漏洞，保障重要时期网络安全。

（2）在发生网络安全事件时，服务单位应在30分钟内响应，提供应急措施，需在1.5小时内到场，处理事故并提交书面安全事件调查分析报告，保证4小时内恢复系统正常运作，响应时间为每周7×24小时。

交付内容：《保障方案》《网络安全报告》以及其他材料（按招标人要求提供）

**四、其他要求**

1.服务单位应提供符合国家及用户提出的有关质量标准的服务；

2.在重要活动时期，服务单位应根据招标人网络安全梳理情况，提供应急网络安全检测或防御设施，加强网络安全体系。

**五、采购内容**

**（一）采购清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 服务项 | 内容 | 服务范围 | 次数 |
| 设备状态及网络监控 | 1.通过线上巡查，对网络设备、网络安全设备、服务器等重要设备进行状态巡检，对网络状态进行监控，排查设备、网络以及安全隐患问题，并出具相关巡查单、检查报告，安全日志分析、安全事件处置。  2.针对发现安全隐患问题以及设备和线路调整、重大活动日加强防护等原因，对设备（包括但不限于交换机、防火墙、服务器等设备）安全策略、系统设置等进行调优。  3.每周出具一份《巡查单》，每季度结合其他检查项目出具相关检查报告。 | 集团及直属企业 | 每周一次 |
| 信息化系统及设备安全检测 | 通过线上及线下检查，对信息化系统及各类设备终端进行安全扫描、弱口令检查、基线扫描、服务器安全分析、渗透测试等，出具相关报告及整改措施，协助对系统进行升级或漏洞封堵等。 | 集团及直属企业 | 每年两次 |
| IT资产运维 | 对集团IT资产（包括但不限于办公IT设备、网络设备、安全设备、服务器、办公终端等设备）进行盘点和梳理，定期对资产信息进行维护和更新，建立相关台账，梳理相关管理流程，实现有效管理。 | 集团公司本部及集团临时数据中心 | 不限 |
| IT运维体系建设 | 1.根据集团实际情况，协助梳理运维流程，建立健全网络安全、网络数据安全工作机制、运维机制以及协助制定相关制度等。  2.服务期内要求提供运维管理软件工具，工具功能包括不限于：集中全面监控集团的IT系统，包括服务器、网络设备、操作系统和数据库等，能够实时监测系统状态，及时发现潜在问题并进行智能预警，从而提升运维效率、缩短响应时间，保证业务系统的数据安全和稳定运行。 | 集团及直属企业 | 不限 |
| 应急响应及运维服务 | 1.提供不少于1人IT工程师现场驻点，提供IT设备运维服务及网络安全保障服务，保障集团公司本部及集团临时数据中心各类IT资产各类终端设备（包括但不限于办公电脑、交换机、AP、防火墙、服务器）、终端桌面、网络、各类线路及业务系统等的正常运作，保障网络安全和各类设备的正常运作（须附驻点人员的身份证、职称证、社会保障部门出具距今的近6个月在投标人单位缴纳社会养老保险有效凭证等证明材料复印件并加盖投标人法人公章）。  2.驻点要求：驻点时间和招标人工作时间相同；特殊情况除外（遇应急情况需及时处理）。 | 集团公司本部及集团临时数据中心 | 不限（驻点办公） |
| 安全评估与规划 | 对集团及直属企业的网络安全情况进行综合评估，评估应包含各网络设备盘点、服务器盘点、安全检测、漏洞扫描以及整改方案等，对集团及直属企业的网络安全进行评估，并提出整改计划和未来建设规划，协助各单位进行整改。 | 集团及直属企业 | 服务期内至少1次 |
| 重要时期网络安全保障服务 | 1.对集团及直属企业提供重要时期网络安全保障服务，要求该时期提供全天24小时网络安全保障，提供不低于两名工程师线上值守，提供应急响应服务，及时应对网络安全攻击，排查网络安全隐患，封堵网络安全漏洞，保障重要时期网络安全。  2.在发生网络安全事件时，服务单位应在30分钟内响应，提供应急措施，需在1.5小时内到场，处理事故并提交书面安全事件调查分析报告，保证4小时内恢复系统正常运作，响应时间为每周7×24小时。 | 集团及直属企业 | 服务期内不低于4次（具体根据采购人实际需要为准 |

**（三）服务期限**

自合同签订之日起计算，服务期为1年。