合同编号： (2025)SJ010

福田区网络和信息系统安全大数据监测分析和管理服务合同（2025-2026 年）

甲方：深圳市福田区民意速办和智慧城市建设中心

统一社会信用代码：124403046610332564

负责人：

地址：深圳市福田区华富街道深南大道 1006 号国际创新中心 F 座 3 层

乙方：杭州安恒信息技术股份有限公司

统一社会信用代码：913301086623011957

负责人：

地址：浙江省杭州市滨江区西兴街道联慧街 188 号

根据《中华人民共和国民法典》及 2025 年 4 月 9 日“福田区网络和信息系统安全大数据监测分析和管理服务项目（项目编号：FTCG2025000031）”招标结果（中标通知书）和“招标文件”，就乙方承担福田区政府网络和信息系统安全大数据监测分析和管理服务的相关事宜，经双方协商一致，达成本合同。

第一条、合同金额

1、本合同总金额为人民币:**壹佰壹拾伍万贰仟元整（￥1,152,000.00 元）**。本合同服务期自 2025 年 4 月 24 日至 2026 年 4 月 23 日，共计 12 个月。本合同以人民币进行结算。

2、乙方的开户银行资料：

乙方开户银行：

乙方开户名称：杭州安恒信息技术股份有限公司

乙方银行账号：

第二条、合同的服务内容

乙方承担福田区政府政务网络的网络和信息系统安全大数据监测分析和管理服务。本合同的具体服务要求如下：

1、网络和信息系统安全大数据监测分析和管理服务的要求

（1） 协助建立统一的“资产管理、漏洞管理、安全监测和安全技术保障”闭环管理机制，形成安全管理工作流程。

（2） 结合现有安全态势感知大数据系统，进行每日安全态势大数据监测，利用各设备威胁情报、机器学习、用户行为画像等技术对报警数据进行综合研判，输出分析报告，报告每月一次。

（3）策略优化反馈，基于日常监测成果，完善相应防护策略，负责监测资产梳理核查，定期更新监测范围，防止因资产遗漏引发的安全盲区。

（4） 针对目标地址段不明确的资产，通过流量还原和大数据平台的用户行为分析功能，对福田区各单位访问部署在互联网的应用系统的行为进行识别、过滤，发现私自搭建的业务系统要发出安全预警通告，需发现当天发出通告。

（5） 经过研判，核定的安全事件发出安全通告，须包含事件详情、溯源过程、分析结果、解决方案。发现安全事件的当天需发出安全通告。

（6） 网络和信息系统安全大数据监测分析相关系统对 APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等各类高级网络攻击进行监测，并对恶意攻击源 IP 进行封堵，需形成工作记录表，每日更新。

（7） 担任采购人的网络安全顾问，在网络和主机系统进行升级、扩建时，提供安全修补建议。

（8） 需监控的网络资产数量：信息系统不少于 150 个；安全设备不少于 70 套；服务器不少于 1000 台（包括云虚拟服务器）；终端电脑不少于 15000 台（包括桌面云主机）。

2、网络流量监测服务的要求

（1） 监测政务网各节点网络流量数据，分析全区网络的带宽、网络设备转发瓶颈、各类网络协议流量分配情况，研判增长趋势，提出合理的网络资源控制策略。监测各个重要业务系统访问用户量、访问流量、响应速率、应用负载状态、

DNS 服务器状态等，保障重要业务系统稳定运行。

（2） 协助各业务系统运维团队排查业务系统网络问题，分析性能瓶颈，排查僵尸业务、服务器、终端主机等。

（3） 应急响应服务。需提供 24 小时的应急响应服务。一旦发生网络安全故障，需半小时内赶到现场提供应急响应技术支持，协助网络系统运维团队在指定时间内恢复网络正常运行。

3、重要业务系统运行状态监测要求

（1）每天利用网络和信息系统安全大数据监测分析相关系统对各业务系统运行安全状态进行监测，监测内容包括业务访问量，网络流量、响应延时、业务会话量等指标，发现异常立即预警并分析问题，并协助各系统管理排查和解决问题，每月提交系统安全状态监测报告。

（2）每日监控应用负载和 DNS 服务器状态，包括业务日志、响应速率等，做好安全维护工作，保障全区业务系统对外提供访问能力及办公终端访问互联网能力正常。

（3）应急响应服务。需提供 24 小时的应急响应服务。一旦发生业务安全故障，需半小时内赶到现场提供应急响应技术支持，协助业务系统运维团队在指定时间内恢复业务系统正常运行。

4、渗透测试要求

（1）每 3 个月对机关单位的互联网系统开展至少一次渗透测试，找出存在的安全漏洞及风险，出具渗透报告，并督促责任单位完成漏洞整改。

（2）组织专业力量对采购方指定的福田区党政机关、事业单位、医院、学校、国企等单位业务系统每半年进行一次全方面深层次的渗透，在系统运行状态通过对目标进行模拟黑客入侵，进行非破坏性质的攻击性测试，直观地暴露系统所面临的威胁与风险点，最大程度挖掘潜在安全漏洞和威胁，以攻促防，最终形成详细的漏洞位置，成因，修复建议等内容的专业安全渗透测试报告，解决存在的或潜在的深层次安全漏洞。

5、网络安全攻防演练服务要求

做好省、市、区网络安全攻防演练防守和保障工作。 在网络实战攻防演练期间组建防守队伍。演习前开展安全检查、整改与加固，演习期间进行网络安全

监测、预警、分析、验证、处置，演练结束后复盘分析防护工作，总结经验与不足，为后续常态化的网络安全防护措施提供优化依据。

6、移动 APP 安全漏洞及个人信息保护合规性检测要求

（1）每月对福田区的移动应用开展一次安全检测，安全检测服务范围涵盖福田区移动 APP 客户端（含 IOS）、微信小程序、微信公众号、通信链路和服务器端的多方面和多维度。检测内容主要包含以下七个方面：运行环境安全检测、软件自身安全检测、用户操作安全检测、数据安全检测、通信安全检测、业务安全检测、服务器端安全检测。每月提交给客户单位 App 安全检测报告。

（2）移动应用系统上线前根据《中央网络信办、工业和信息化部、公安部、市场监督总局关于开展 App 违法违规收集使用个人信息专项治理的公告》《App 违法违规收集使用个人信息自评指南》《APP 违法违规收集使用个人信息行为认定方法》等文件要求开展 App 的个人信息保护合规性评估。根据评估结果指导 App 开发单位完成整改。

7、配合做好上级主管部门信息安全检查要求

（1）协助采购人做好每年上级党政机关信息安全及培训工作，以及做好迎接上级主管部门对福田区信息安全检查的准备工作。

（2）配合采购人对福田区党政机关单位信息安全检查和绩效评估：协助采购人做好每年对福田区党政机关单位的信息安全检查和绩效评估工作。

8、互联网外部攻击面管理服务要求（含暴露面监测、攻击面管理、敏感数据泄露监控、暗网监控）

8.1、功能要求

（1）乙方提供可以管理互联网资产探查结果和风险情况的统一的技术平台，甲方只需提供查询和线索即可，无须自助发起任务和人工复核，并以 SaaS 服务形式将结果展示给甲方。

（2）支持暴露面检测功能，要求输出结果包括子域名、IP 资产、端口、指纹等信息，并支持将结果导入资产中心，实现对资产的全面掌握。

（3）支持泛资产线索管理，支持添加标题、网页 body 关键字、证书、ICON 图标等内容作为泛资产进一步发现影子资产的线索管理。

（4）支持对攻击面资产风险类型进行筛选展示，类型包括 DNS 解析、疑似

敏感应用、高危端口、内容安全、漏洞。

（5）支持对暗网数据泄漏风险、telegram 黑灰产数据贩卖情报、网盘泄漏风险（国内十大网盘）、代码泄漏（github、gitlab、gitee）、文库泄漏风险（csdn、百度文库、道客巴巴）、邮件互联网暴露情况进行监测与发现。

（6）数据泄露 Telegram 部分支持展示泄露信息发送者、发送者 ID、社群名称、发现时间等内容。

8.2、服务要求

（1）乙方的服务专家需对平台自动监测的数据进行复核，同时对文档资产、代码库资产等进行人工确认、剔除无效的噪音数据，并最终提供完整的互联网暴露面监测报告，报告内容需至少包括互联网资产、攻击面信息、数字资产及敏感信息泄露检测结果。一年提供两次互联网暴露面监测报告。

（2）乙方每月进行一次互联网暴露面检测服务。

（3）服务时间内对互联网暴露面监测报告及相关服务工作提供技术咨询服务。

（4）具备 7*24 服务热线，满足用户报障及咨询需求。

（5）提供具备完整的事件处理系统，具备不同等级事件的响应和处理时间定义。

8.3、投入设施要求

（1）乙方需具备互联网暴露面监测 SaaS 平台。

（2）乙方需提供给用户互联网 SaaS 用户界面来查询结果。

8.4、其他要求：

（1）一年提供两次外部攻击面管理服务报告。

（2）提供互联网暴露面监测 SaaS 用户端 1 年平台使用授权来随时查看服务状态；

9、其他要求

（1）乙方负责提供并保管其安全技术服务人员的工作电脑；服务期间若发生的交通费、午餐费等均由乙方承担。

（2）乙方负责其安全技术服务人员的工资、奖金、福利待遇及其他一切费用，必须为其安全服务人员购买劳动保险，对其安全服务人员做好安全生产教育。如乙方的安全技术服务人员在甲方工作现场发生工作事故或工伤事故的，由乙方

负全责。

（3）若乙方指派到甲方现场服务的安全技术服务人员的工作表现不能符合甲方要求，且经过教育后仍不能改正的，甲方可要求乙方更换相关技术服务人员。

（4）甲方的政务办公网、政务公共网及其主机系统发现有安全问题时，安全服务公司在接到甲方通知（含电话通知）后，即安排资深安全维护工程师前往甲方现场，查明发生问题的原因，采取有效的措施尽快恢复网络和主机的正常运行。一般问题安全服务公司维护人员应在 2 小时内到达，重大问题应在 1 小时内到达。

对于每次安全服务，安全服务公司应保存现场资料，分析产生问题的原因，记录维护使用的方法、步骤和参数，制定防止类似问题发生的解决方法。安全服务公司将保存的现场资料和有关文档资料提交给甲方。

第三条、付款方式

对本合同第一条的合同总金额，双方约定按照服务进度进行付款，具体付款步骤如下：

1、本合同签字生效后，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后15个自然日内，甲方向乙方支付合同总金额的30%作为订金，即人民币（大写）**叁拾肆万伍仟陆佰元整（￥345,600.00元）**。

2、乙方完成半年服务工作，乙方按合同履行服务工作任务并通过双方组织的验收合格后，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后15个自然日内，甲方向乙方支付合同总金额的20%服务费，即人民币（大写）**贰拾叁万零肆佰元整**（￥230,400.00元）。

3、合同服务期满，乙方按合同履行服务工作任务并通过双方组织的验收合格，在甲方收到乙方提供的等额合法有效的税务发票后，甲方办理相关付款资料，审批流程完成且财政资金到账后 15 个自然日内，甲方向乙方支付合同剩余的服务费，即人民币（大写）**伍拾柒万陆仟元整**（￥ 576,000.00 元）。

第四条、双方的责任

（一）甲方责任：

1、应按合同第三条的约定按时向乙方支付合同款。

2、在本合同执行过程中，甲方应为乙方提供方便并积极配合。

3、在乙方的协助下，制定和不断完善计算机网络安全管理制度，强化网络安全管理。

4、有义务保守乙方与本合同执行有关的所有技术和商业机密，不向第三方泄漏。

（二）乙方责任：

1、乙方应投入投标承诺的足够的技术力量，以确保按期完成本合同第二条规定的服务内容。在安全服务期间，未经甲方同意，乙方不得随意抽调或更换乙方承诺的驻场服务人员，如果甲方认为乙方的驻场服务人员的技术能力或管理能力不能胜任本合同的服务要求，甲方可以要求乙方更换有关人员。乙方不得拒绝甲方要求，如乙方拒绝甲方要求，即构成违约，造成后果由乙方自负并应向甲方支付本合同总金额3%的违约金。

2、承诺向甲方提供及时、准确、高效、优质的安全服务，以保证甲方的网络和主机系统具有高安全性。

3、遵守福田区政府及甲方在网络及信息安全方面的要求，承诺将保守甲方网络和主机系统所有参数和系统资源的秘密，不向第三方泄漏。

4、承诺需精通电子政务网络及信息安全体系，对相关安全重点具有敏锐洞察力；

5、承诺有较强的信息安全技术服务力量和服务团队；

6、承诺具有安全等级保护定级、安全域规划实施和访问控制的实际工作经验；

7、承诺掌握信息安全防护的最新技术，了解电子政务网络和安全体系的弱点，有一定的先知先觉的预判能力；

8、承诺具有网络攻防经验，可以应对任何复杂的信息安全问题，在信息安全领域有较强的研发能力；

9、若乙方指派的安全服务人员的工作表现不能符合甲方的要求，且经过教育后仍不能改正时，乙方须按甲方的要求更换服务人员。

10、安全服务人员的工作电脑由乙方提供并负责保管，服务期间发生的交通费、误餐费等由乙方承担。

11、承诺所有参与本合同的乙方人员，在安全服务前须与甲方、乙方签订保密协议（详见附件）。在安全维护和安全服务期间及安全维护期满后的 5 年内，等所有安全信息（含文档、资料等），提供给其它第三方的单位或个人查看或使用。

12、乙方负责安全服务人员的工资、奖金、福利待遇及其他一切费用，乙方必须为其安全服务人员购买劳动保险，并对进入甲方工作现场的工作人员加强安全生产教育，为现场工作人员购买安全保险。若出现安全事故造成乙方工作人员伤亡的情况完全由乙方承担责任，甲方对此不负任何责任。

13、乙方有义务加强对本单位工程实施人员的安全保密教育，遵守福田区政府及甲方在网络及信息安全方面的要求。

第五条 人员及投入设施要求

人员要求：

根据本项目的招标要求，乙方应派驻不少于 3 个正式原厂身份的人员常驻甲方办公场所，其中 1 人为项目经理。驻场服务人员需按照甲方的作息时间和甲方的工作安排开展工作，非驻场服务人员的安全服务工作根据需要由甲、乙双方具体商定。需常备 1 名机动安全专家，以便于在紧急情况或工作量较大时，可随时抽调熟悉相关环境的工程师进行补充。机动安全专家需具有网络安全工程相关专业的中级职称，CISP-DSG 证书、CCRC-DCO 证书、CISAW 证书、系统集成项目管理工程师证书。未经过甲方单位同意，不得更换驻场服务人员；甲方可对拟安排的驻场服务人员进行提前面试，如面试未通过，乙方须提供与投标文件同等资质的其他人员进行替换。

项目经理权利和责任如下：

1、项目联络；

2、组织和协调项目进展；

3、代表委派方签署合同变更的文件（包括但不限于项目相关文件的签字确认权）。

乙方如需更换项目经理，需经甲方同意后进行更换，更换的项目经理具有至少五年与本项目类似的安全服务工作经验。

技术服务人员素质要求：

1、项目负责人具有信息技术（信息安全）专业的高级工程师职称、具有国家信息安全漏洞共享平台(CNVD)原创漏洞证书、信息系统项目管理师证书、CISP-CISO 证书。

2、派驻现场服务的人员须具有同类安全服务项目至少三年的工作经验，能够独立、按时完成现场服务工作，遵守甲方的工作作息时间。

3、派驻现场服务的人员须为投标方自有人员。

4、驻场技术服务人员具有 CISP 证书或 CISAW 证书。

5、乙方应按照投标文件指定的驻场服务人员到甲方现场进行驻场服务。乙方如需更换，需经甲方同意后进行更换，更换的现场服务的人员须具有同类安全服务项目至少三年的工作经验，并按甲方招标文件的要求和乙方投标文件的承诺，**具有不低于乙方投标文件所承诺的资格要求**，能够独立、按时完成现场服务工作，遵守甲方的工作作息时间。

投入设施要求：

为确保安全服务工作的稳定推进，乙方在服务期间提供专业网络检测安全服务工具至少 1 套。

成果要求：

服务过程产生的所有过程文档、原始数据、扫描报告、正式报告等必须进行电子或纸质归档，在项目结束后一并移交给甲方。

技术资料：

1、网络和信息系统安全大数据监测分析和管理服务的要求：每日进行安全数据识别、分析、处置，并针对发现的安全风险和安全时间编写预警报告及安全通告。安全数据要每日整理输出《信息安全威胁识别记录表》、《信息安全处置记录表》、《信息安全通报统计表》、《信息安全预警统计表》。每季度最后一个月提交《安全大数据监测分析报告》。

2、网络流量监测服务的要求：每日监测全区业务系统流量情况，针对发现的业务流量异常情况进行分析、并协助业务系统责任单位进行排障。每月提交《全区业务系统流量分析表》。

3、重要业务系统运行状态监测要求：监测重要业务系统的用户访问量、数据流量、响应性能，协助业务系统责任单位进行安全运维，提供应急响应安全

技术支持，排障完成后输出《排障报告》。

4、渗透测试要求：每半年对福田区的业务系统进行一次全方面深层次的渗透测试，形成详细的漏洞位置，成因，修复建议等内容的专业安全《渗透测试报告》

5、网络安全攻防演练服务要求：每年组织一次网络安全实战应急演练，演练结束后提交《应急演练方案》、《应急演练脚本》和《应急演练视频》。

6、移动 APP 安全漏洞及个人信息保护合规性检测要求：每月对福田区的移动应用开展一次安全检测，检测完成后需提交《每月 APP 安全检测报告》；移动应用系统上线前开展 App 的个人信息保护合规性评估，并提交《APP 个人信息保护合规性评估报告》

7、服务期内提供 5 次移动 APP（Android、iOS）安全加固服务要求：每次加固完成后需提供《APP 安全加固报告》。

8、一年提供两次互联网暴露面监测报告。乙方的服务专家需对平台自动监测的数据进行复核，同时对文档资产、代码库资产等进行人工确认、剔除无效的噪音数据，并最终提供完整的互联网暴露面监测报告，报告内容需至少包括互联网资产、攻击面信息、数字资产及敏感信息泄露检测结果。

第六条、违约责任

1、如甲方未在规定的时间内向乙方支付合同款，甲方应按超过的天数每天向乙方支付本合同第三条中到期应付而未付金额的**千分之三**作为违约金，但每次违约金支付不得超过当次到期应付而未付金额的 **5%**。

2、如甲方的政务办公网、政务公共网及其主机系统发现有安全问题时，乙方接到甲方通知后，重大问题应在 1 小时内（其它问题 2 小时内）仍未到达甲方现场进行服务，甲方将扣除当月的安全服务费，同时乙方须继续提供服务。如乙方在接到甲方通知后 24 小时仍未到达甲方现场，或者乙方不继续提供服务，乙方除当月维护费被扣除外，还须向甲方支付本合同总金额的 **10%**作为违约金，并自动解除本合同。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可直接在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

3、如乙方未按每季度提交一次《安全大数据监测分析报告》，每少一次，甲方将全额扣除该三个月内乙方的服务费，同时乙方应向甲方支付三个月的服务

费金额的 **10%**作为违约金，但由于甲方自身原因造成的除外。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

4、如乙方未按每月提交一次《全区业务系统流量分析表》和《每月 APP 安全检测报告》，每少一次，甲方将全额扣除该一个月内乙方的服务费，同时乙方应向甲方支付一个月的服务费金额的 **10%**作为违约金，但由于甲方自身原因造成的除外。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

5、如乙方在一个月内（当月一日至当月最后一天）未每天派乙方承诺的至少 3 名服务工程师驻场，甲方将扣除乙方当月的服务费外，同时乙方须向甲方支付该月服务费的 **10%**作为违约金，甲方可在支付给乙方的服务费中扣减该违约金（由于甲方自身原因造成的除外）。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

6、如乙方未按每半年提交一次《渗透测试报告》，甲方将扣除合同额的 10%服务费，同时乙方应向甲方支付一个月的服务费金额的 **10%**作为违约金，但由于甲方自身原因造成的除外。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

7、如乙方未按每年提交一次《应急演练方案》、《应急演练脚本》和《应急演练视频》，甲方将扣除合同额的 10%服务费，同时乙方应向甲方支付一个月的服务费金额的 **10%**作为违约金，但由于甲方自身原因造成的除外。因此导致甲方聘请第三方提供服务产生的费用等一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

8、在安全服务期间，若出现由于乙方人员泄露福田区政府网络和信息系统参数的情况，造成甲方网络系统、信息系统损失和产生不良政治后果的，甲方保留对其本人和乙方采取法律诉讼的权利。因此导致甲方的一切损失均由乙方承担，此项支出费用甲方可在乙方的安全服务费中扣除，不足部分甲方可向乙方继续追偿。

9、在合同服务期内，出现以下情况的视为安全技术服务质量没有达到要求，

将追究乙方的违约责任，违约金额从服务费中核减：

（1）因乙方原因导致信息安全工作被采购人上级点名批评的，每次扣除合同金额 1 万元。

（2）因乙方工作不到位，导致发生信息安全事件被上级部门通报，或导致采购人在市信息安全主管部门检查中扣分的，扣除合同总金额的 20%。

（3）因乙方工作不力，未能及时发现安全隐患，以致信息系统（网站）被上级部门渗透成功的，按每个系统（网站）扣除合同金额 1 万元。

（4）发现乙方技术服务人员在工作时间从事其他与信息安全工作无关的，第 1 次警告，从第 2 次起，每次扣除合同金额 1000 元。

第七条、资料及保密

1、对于一方向另一方提供或使用的资料和秘密信息，另一方负有安全保护和保密的责任，不得向任何第三方透露、不得随意丢弃而造成泄密；对于本合同项目的最终成果及阶段性成果，双方均负有保密义务。

2、未经双方授权代表签字认可，任何一方不得向第三方透露本合同内容。

3、本条款不因本合同或其下项目的变更、解除或终止而失效。

4、乙方人员通过本项目的实施接触到福田区电子政务网络、应用系统的资料、配置或业务数据，以及个人隐私、甲方的工作信息等，乙方均有义务和责任对甲方上述网络、网站、服务器系统和业务应用系统的信息资料或数据进行保密。若乙方及其工作人员未履行好保密职责，发生信息泄漏等行为，乙方需无条件承担甲方的一切损失，挽回对甲方造成的不利影响，并承担相应的法律责任。

第八条、本合同的修改

对本合同的条款的任何修改，必须经甲乙双方协商同意后，以本合同的补充协议方式，以书面的形式订立，该补充协议与本合同具有同等法律效力。

第九条、其他事宜

1、本合同的适用法律：本合同的甲、乙双方应遵守《中华人民共和国民法典》及其他相关的法令和条例。因本合同或与本合同有关的争议，双方应通过协商解决；协商解决不成，向甲方所在地法院提起诉讼，诉讼裁判对双方均具约束力。

2、不可抗拒力：由于不可抗力的事故或自然灾害导致一方或双方违约，由甲、乙双方协商解决。但双方均有义务采取一切必要的措施减少损失。有义务采取措施而不采取造成严重后果，由有义务采取措施一方承担相应责任，并向另一方支付总金额3%的违约金。

3、乙方就本合同项目的“投标文件”与本合同具有同等的法律效力。投标文件中与本合同条款有差异的部分，按照本合同条款的规定执行。在本合同中未涉及但在乙方的“投标文件”中涉及的，按“投标文件”中的条款执行。

4、本合同未尽事宜，双方可协商解决，并可签订补充协议，该补充协议与本合同具同等法律效力。

5、本合同附件与本合同具有同等的法律效力。若附件与本合同有冲突的地方，以本合同为准。

6、本合同自甲、乙双方授权代表签字并加盖双方主体印章之日起生效。本合同壹式陆份，甲方执肆份，乙方执贰份，均具同等法律效力。

7、本合同服务期满前一个月，经履约考核合格的可按原合同条款续签合同，合同履行期限最长不得超过三十六个月，目前本服务合同履行期限已累计二十四个月。

8、如果后续年度经人大审议通过的部门预算中，该采购项目预算金额较提前采购计划金额发生变化的，双方可根据相关规定签订补充协议或终止协议执行。

甲方：深圳市福田区民意速办和智慧城市建设中心（盖章）

授权代表（签字）：[redacted]

日 期：2025 年 4 月 24 日

乙方：杭州安恒信息技术股份有限公司（盖章）

授权代表（签字）：[redacted]

日 期：2025 年 4 月 24 日

网络安全及数据安全保密协议

甲方：深圳市福田区民意速办和智慧城市建设中心

乙方：杭州安恒信息技术股份有限公司

乙方在甲方本合同的服务过程中，为确保甲方计算机网络及数据相关信息的保密性，依照《中华人民共和国计算机信息安全保护条例》、《中华人民共和国著作权法》、《计算机软件保护条例》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》及有关部门商业信息法规，达成此保密协议。

一、签订对象

参与甲方本合同服务项目的乙方技术人员，在进行服务前必须在本协议第六条的表格中签署本人名字，查验身份证，留存本人身份证复印件及工作简历。凡未在第六条的表格中签名备案的乙方人员，不能参与本合同的服务工作。

二、保密的内容和范围

乙方（含乙方参与服务的技术人员）在执行服务期间，掌握的或所接触到甲方的计算机网络系统和业务应用系统的一切技术秘密、网络设备信息、网络结构、IP 地址资源、安全设备信息、项目信息、业务信息、技术信息和以及工作中可能接触到的属于客户的数据、业务系统的资料和数据等，无论这些信息或数据采用何种媒介作为载体，如以有形形式披露、或通过电子通信，包括基于互联网提供。双方传输和接收的任何信息和资料，无论书面、口头或电子，以及本合同及其附件本身，均属于保密范围。

三、协议双方的权利和义务

1. 甲方有权拥有乙方在本合同的服务中所有技术资料及相关文档。

2. 甲方拥有对本合同的服务中的所有知情权、询问权及掌握项目进度的权利。

3. 乙方必须管理好自己的服务人员，乙方（含乙方参与施工的技术人员）不得将第 2 条所及的保密内容非法披露给外单位、转让给第三者或自行使用。

4. 乙方应严格遵守甲方规定的任何成文或不成文的信息安全及保密规章制度，履行与其工作岗位相应的信息安全及保密职责，防止泄密甲方或者虽属于他人但甲方承诺有保密义务的保密信息；

5. 乙方不得以任何形式将甲方或者虽属于他人但甲方承诺有保密义务的保密信息泄露或公布给甲方以外的任何其他人；

6. 乙方应正确使用甲方或者虽属于他人但甲方承诺有保密义务的保密信息，不得在履行职务之外使用这些保密信息；

7. 乙方不得利用甲方或者虽属于他人但甲方承诺有保密义务的保密信息为自己或者任何第三方牟利；

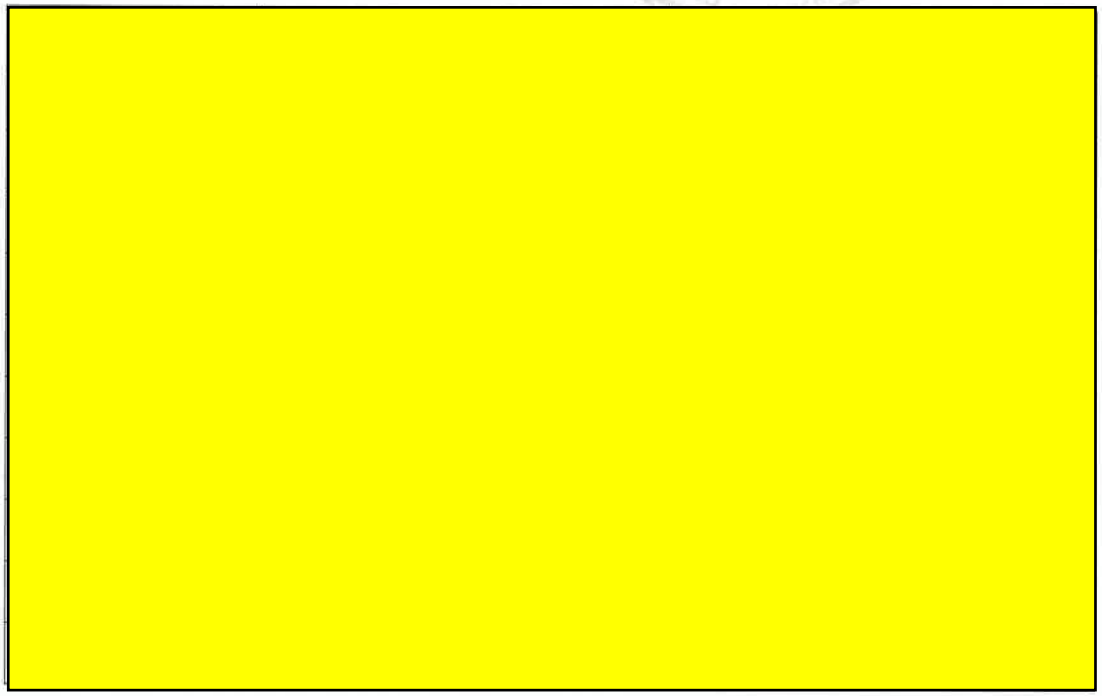
四、保密协议的期限

本协议自签订之日起，有效期为伍年。

五、违约责任

若乙方（含乙方参与服务的技术人员）泄密，需无条件向甲方赔偿因泄密所造成的相关损失，并承担相应的法律责任。

六、乙方在甲方进行安全服务的技术人员名单



说明：乙方的服务技术人员在执行服务前，必须在上表的“签字”栏内签字确认后，才能在甲方工作现场进行服务。

七、其他

本协议自甲、乙双方授权代表签字盖章之日起生效。本协议壹式伍份，甲方执叁份，乙方执贰份。

甲方： 深圳市福田区民意速办和智慧城市建设中心（盖章）

授权代表（签字）：[redacted]

日　　期：2025 年 4 月 24 日

乙方： 杭州安恒信息技术股份有限公司（盖章）

授权代表（签字）：[redacted]

日　　期：2025 年 4 月 24 日