项目验收报告

根据 福田区政府计算机网络安全和信息安全服务续签合同（2023-2024年） 合同的约定，我单位对 福田区政府计算机网络安全和信息安全服务续签合同（2023-2024年） 政府采购项目中标/成交供应商 深圳市安络科技有限公司 提供的服务进行了验收，验收情况如下：

<table>
<tr><td rowspan="4">项目基本情况</td><td>项目名称</td><td>福田区政府计算机网络安全和信息安全服务续签合同（2023-2024年）</td><td>项目编号（如有）</td><td></td></tr>
<tr><td>采购单位</td><td>深圳市福田区民意速办和智慧城市建设中心</td><td>中标/成交供应商</td><td>深圳市安络科技有限公司</td></tr>
<tr><td>中标/成交金额</td><td>2,996,000元</td><td>合同履约时间</td><td>自2023年3月1日至2024年2月29日</td></tr>
<tr><td colspan="4">货物型号规格、标准及配置（或者服务内容、标准）：

服务总体要求：在福田区政府政务网络安全系统集成防护的情况下，保障在线运行的信息系统安全，实现计算机网络主干不因安全原因而瘫痪，重要数据不被非法窃取，区政府网站页面不被篡改，保障互联网网站及信息系统的安全运行，信息系统安全管理有序进行的安全服务目标。
服务内容：
（1）网络及主机服务器安全服务；
（2）网站安全服务；
（3）信息安全服务；
（4）安全风险评估服务；
（5）安全等级保护服务；
（6）开展渗透测试服务；
（7）安全应急服务；
（8）个人信息和重要数据保护；
（9）落实国家法律法规；
（10）配合做好信息安全检查
（11）其他要求。</td></tr>
<tr><td rowspan="2"></td><td>验收分项</td><td>验收情况</td><td>是否通过</td><td>备注</td></tr>
<tr><td>1.网络及主机服务器安全服务</td><td>按合同要求完成安全服务</td><td>☑是 □否</td><td></td></tr>
</table>

验收记录	2. 网站安全服务	按合同要求完成安全服务	☑是 ☐否	
	3. 信息安全服务	按合同要求完成安全服务	☑是 ☐否	
	4. 安全风险评估服务	按合同要求完成安全服务	☑是 ☐否	
	5. 安全风险评估服务	按合同要求完成安全服务	☑是 ☐否	
	6. 开展渗透测试服务	按合同要求完成安全服务	☑是 ☐否	
	7. 安全应急服务	按合同要求完成安全服务	☑是 ☐否	
	8. 个人信息和重要数据保护服务	按合同要求完成安全服务	☑是 ☐否	
	9. 落实国家法律法规	按合同要求完成安全服务	☑是 ☐否	
	10. 配合做好信息安全检查	按合同要求完成安全服务	☑是 ☐否	
	11. 其他要求	按合同要求完成安全服务	☑是 ☐否	
验收结论	验收结论性意见: 2023 年 3 月 1 日至 2024 年 2 月 29 日乙方已按合同要求完成网络安全和信息安全服务，服务质量符合此次服务要求，履约验收合格。			
	有异议的意见和相关说明（如有）: 无。 提出异议人员签字:			
参与验收人员签字/盖章	采购单位验收小组成员签字（单位公章）: 组长: 组员: 2024年3月13日			
	中标/成交供应商参与人员签字（单位公章）: 2024年3月13日			

项目履约情况评价表

采购单位名称：深圳市福田区民意速办和智慧城市建设中心　　联系人及电话：吕振华，82918699

<table>
<tr><td colspan="3">采购项目名称</td><td>福田区政府计算机网络安全和信息安全服务续签合同（2023-2024年）</td><td>项目编号（如有）</td><td></td></tr>
<tr><td colspan="3">中标/成交供应商</td><td>深圳市安络科技有限公司</td><td>供应商联系人及电话</td><td>周智广 18565659133</td></tr>
<tr><td colspan="3">中标/成交金额</td><td>￥2,996,000.00</td><td>合同履约时间</td><td>自2023年3月1日至2024年2月29日</td></tr>
<tr><td rowspan="8">履约情况评价</td><td colspan="2">总体评价</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td rowspan="6">分项评价</td><td>质量方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>价格方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>服务方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>时间方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>环境保护</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>其他</td><td colspan="3">评价内容为：乙方在服务期很好的完成了福田区政府计算机网络安全和信息安全服务项目。
评价等级为：☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td colspan="3">具体情况说明</td><td colspan="3">合同的服务内容：
一、安全服务的主要内容：
1、总体服务要求：
在福田区政府政务网络安全系统集成防护的情况下，保障在线运行的信息系统安全，实现计算机网络主干不因安全原因而瘫痪，重要数据不被非法窃取，区政府网站页面不被篡改，保障互联网网站及信息系统的安全运行，信息系统安全管理有序进行的安全服务目标。
2、具体工作内容：
（1）网络及主机服务器安全服务；
（2）网站安全服务；
（3）信息安全服务；
（4）安全风险评估服务；
（5）安全等级保护服务；
（6）开展渗透测试服务；
（7）安全应急服务；</td></tr>
</table>

	（8）个人信息和重要数据保护； （9）落实国家法律法规； （10）配合做好信息安全检查； （11）其他要求。 二、网络及主机服务器安全服务的要求： 1、服务要求： （1）在服务期内对福田区政府的信息系统每年进行一次安全风险自评估。 （2）对福田区政务网络的和交换机的端口和配置进行安全设置；对福田区政务网络机房的主机服务器的操作系统、数据库系统等进行不定期的安全防护和系统漏洞补丁升级。 （3）定期对福田区政务网络、主机服务器及所有客户端电脑进行防病毒情况的分析。 （4）定期对福田区政务网络的防火墙与网络入侵检测设备进行安全设置及联动，防范网络黑客的攻击行为。 （5）定期对所有主机服务器的端口、配置进行定期的安全检查、对操作系统级和数据库级的系统安全漏洞进行安全处理和补丁升级。 （6）定期对福田区政务网络重要的网络交换机和主机服务器进行安全巡检和安全评估，对管理和使用中出现的安全问题及时地弥补处理。 （7）每3个月对福田区政务网络和主机系统进行一次全面的信息安全检测（含所有端口、配置、系统设置、安全日志等的对照审查和分析等），并向甲方提交书面的评估报告等。 （8）定期对区机关各单位的网站和信息系统进行应用层扫描工作。 （9）担任甲方计算机网络和主机系统的安全顾问，在网络和主机系统进行升级、扩建时，提供安全风险评估，并提供安全修补建议。 （10）制定网络安全应急服务预案，每年实演至少1次。 2、具体工作内容： （1）在服务期间，需每3个月对福田区政务网络及其主机系统(包括政务网络内的所有交换机等网络设备、服务器、防火墙及其管理器，入侵检测设备及其管理器、UPS设备的管理器以及网管工作站等，下同)进行安全评估，修补安全漏洞。乙方须向甲方提交安全漏洞评估审计报告和修补方案、修补方法、修补过程等文档资料，提供补丁程序的官方下载网址并将修补用的补丁程序制作成光盘提交给甲方保存。 （2）乙方应及时向甲方通报已发现的、公开或尚未公开的安全漏洞及其修补方法，可采用书面或电子邮件等方式，每月提供安全通报不少于2次。 （3）乙方应及时向甲方通报最近流行的网络病毒类型、传播途径和传播方法，及时通报最近网上流行的安全陷阱类型（如通过邮件、聊天软件、网络下载等途径传播病毒、安装木马程序等）及其识别和防范方法。 （4）乙方每月至少1次检查甲方的政务网络及其主机系统，安装

	新的补丁程序，进行漏洞修补，并提供相应情况的报告。 （5）乙方每月至少对甲方的政务网络进行1次安全检测。侦测内容为危害网络的病毒或持续的黑客攻击活动，追踪传播病毒或黑客发动攻击设备的地址，协助甲方采取措施清除病毒或阻止黑客对网络环境的破坏。分析甲方的网络环境，指导甲方做好病毒和黑客攻击的防护工作。 （6）乙方需提供7×24小时服务，甲方的政务网络及其主机系统发现有安全问题时，乙方应立即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。对于每次安全服务，乙方应保存现场资料，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。乙方将保存的现场资料和有关文档资料提交给甲方。 （7）对福田区机关各单位所有网站和信息系统(现数量约200个，今后根据建设情况还会增加)每年开展至少1次的安全扫描，扫描结果发现存在高中风险漏洞的，提供漏洞修补建议，指导网站和信息系统建设单位进行漏洞修补和系统加固，提交系统安全扫描报告。 （8）乙方协助甲方制定安全管理制度，保证福田区政务网络及其主机系统安全稳定运行。 （9）乙方为甲方安全管理员提供必要的安全管理、维护培训和甲方工作人员的安全使用培训，每年至少制作一期信息安全视频培训教材，采用网上培训的方式对采购人所有联网终端用户进行培训。 （10）做好迎接市信息安全主管部门对福田区主机服务器和数据库服务器安全检查的准备工作。 3、需安全维护的服务器范围: 对福田区所有服务器进行信息安全维护，其中大部分为虚拟机，服务器总数现约为700台，今后根据建设情况还会增加。 三、网站安全服务 1、提出网站安全防护措施，制定网站安全应急服务预案，每年实演1次。 2、福田区政府所有网站和信息系统日常安全防护，目前数量约150个，今后根据建设情况还会增加。 3、在网站或信息系统被攻击或页面被篡改时提供应急响应服务，应急响应时间在1小时以内。分析网站被攻击的原因，提交书面分析报告，并协助甲方和市公安局网监分局做好对攻击者的追查工作。 4、做好迎接市信息安全主管部门对福田区网站信息安全检查的准备工作。 四、信息安全服务 1、制定对全区性的信息化生产系统的应急服务预案，每季度实演至少1次。 2、对重要信息化业务系统、数据库等信息安全进行日常的维护服务。 3、对规划或新建业务应用系统的信息安全提出专业意见或建议。 4、分析出现的信息安全疑难问题，并给出专业的解决建议和意见。

	5、做好迎接信息安全主管部门对福田区信息安全检查的准备工作。 五、安全风险评估服务 承担福田区数据管理中心的“福田区政府信息安全风险评估工作”。制定安全风险评估的日常工作制度；帮助甲方按照风险评估制度要求，将安全管理落实到日常安全工作中；承担起草年度《福田区信息安全风险评估工作报告》工作，协助甲方做好迎接市信息安全主管部门对福田区安全风险评估检查的准备工作。 六、安全等级保护服务 根据国务院信息化工作办公室颁布的《电子政务信息安全等级保护实施指南（试行）》和国家保密局颁布的《涉及国家秘密的信息系统分级保护管理办法》，协助甲方进行安全和保密等级划分以及相应的系统保护和系统监管。其中安全等级保护工作，按照国家《信息安全等级保护管理办法》和《信息系统安全等级保护定级指南》，对应用系统进行等级定级，根据应用系统的性质对其进行安全保护的等级定级，每年对该类应用系统及网站进行信息安全风险测评。做好迎接市信息安全主管部门对福田区信息系统安全等级保护检查的准备工作。 七、开展渗透测试服务 针对福田区至少100个信息系统、网站进行渗透测试，主要内容包括：（一）对所有系统进行一次应用层风险扫描，出具扫描报告；（二）模拟黑客的攻击方法对福田区信息系统进行非破坏性的攻击测试，找出存在的安全漏洞及风险，取得网站和业务系统的权限，并提供渗透报告。 八、安全应急服务 针对福田区网络安全、网站安全、各应用系统安全（含移动应用）、数据库安全和数据备份系统安全等，协助甲方制定和修订各类系统应急预案，制定应急演练方案，评估演练可能出现的问题，模拟真实应急场景的灾难恢复，提高信息化部门的应急应变能力。在国家法定节假日期间，乙方需安排人员值班，遇到信息安全突发事件，应协调组织安全专家及时赶赴现场提供应急安全服务。 九、个人信息和重要数据保护 针对福田区信息系统情况，按照《信息安全技术个人信息安全规范》规定，完成福田区个人信息和重要数据在组织管理、制度建设、人员管理、技术保障、规范操作等方面的工作。 十、落实国家法律法规； 配合甲方落实《网络安全法》、《数据安全法》、《深圳市电子政务信息安全管理试行办法》等规定。 十一、配合做好信息安全检查； 1、配合甲方做好迎接上级主管部门信息安全检查：协助甲方做好每年上级信息安全和保密安全检查及培训工作，以及做好迎接市信息安全主管部门对福田区信息系统安全检查的准备工作。 2、配合甲方对福田区党政机关单位信息安全检查和绩效评估：协

	助甲方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。
采购单位意见（公章）	乙方在服务期很好的完成了福田区政府计算机网络安全和信息安全服务项目，履约评价等级为优。 日期：2024年3月13日

备注：采购人可根据项目实际情况增减分项内容。本表必须在合同履行完毕后 30 日内反馈。