杀毒软件与网络安全服务项目合同

合同编号：

签订地点：陕西省森林工业职工医院

甲方：陕西省森林工业职工医院

乙方：成都华软技术工程有限公司

招标时间：　年　月　日

由陕西省森林工业职工医院组织采购的项目名称：陕西省森林工业职工医院杀毒软件及网络安全服务项目的项目，采购编号为：SXWZ2026ZB-SGYY-156，由评标委员会评定并经甲方确认成都华软技术工程有限公司为成交供应商。依据《中华人民共和国民法典》的规定，甲乙双方一致同意按以下条款订立《杀毒软件与网络安全服务项目合同》（以下简称“本合同”）。

第一条　服务范围

经甲乙双方友好协商，按本合同之约定由乙方向甲方提供网络安全相关服务。服务范围具体详见附件一：《服务清单》。

第二条　合同金额及期限

1、服务期:

①杀毒软件授权及升级服务期 3 年，3 年服务费共计 195000 元；

②网络安全服务服务期 3 年，合同一年一签，分 3 期签订，每期价格为：183700 元（其中网络安全服务 143700 元，设备特征库升级 40000 元）；每期届满根据甲方需要，同时经甲方考核良好后，方可与续签下一年度合同，续签次数最多不超过两次，累计服务期限不超过三年。

2、本期合同包含杀毒软件授权及升级服务期 3 年；网络安全服务服务期 1 年，设备特征库升级服务期 1 年，维护服务期以双方合同签订之日起算；本合同总金额为￥378700 元（人民币大写叁拾柒万捌仟柒佰元整）

第三条　付款方式

1、乙方杀毒软件授权及网络安全服务中设备特征库更新升级完成后，支付合同总金额的 30.00%。

2、项目整体通过医院组织的验收后，支付合同总金额的 65.00%。

3、自项目验收之日起三年服务期满后，乙方不存在未处理的违约行为或未整改的

质量问题的，甲方支付合同总金额的 5%。

4、甲方有权在本合同项下任何一笔应付费用中，直接抵扣乙方根据本合同约定应向甲方支付的违约金、赔偿金等款项。

5、乙方账户信息如下：

开户名称：成都华软技术工程有限公司

开户银行：中国工商银行股份有限公司成都浆洗街支行

银行帐号：4402262009100040170

第四条　服务内容及乙方责任

乙方保障杀毒软件的正常运行并提供合同约定的各类网络安全服务，对软件中存在的缺陷进行升级和优化，确保软件的正常使用。未经甲方书面同意，乙方不得将本合同项下的全部或部分服务转包或分包给任何第三方。甲方向乙方提供的有关数据资料均视为甲方的商业秘密，乙方不得向任何第三方泄露。本合同所界定的服务是指乙方在上述维护期限内提供给甲方的软件应用的支持和培训服务，包括远程电话支持、用户培训、故障维护等，具体说明如下：

（1）远程电话支持：电话 7×24 小时远程支持或软件技术问题解决与分发。

（2）故障维护：乙方配合甲方解决系统运行过程中由于网络、服务器、计算机、操作系统等原因所产生的软件无法正常运行的情况，保障系统的正常运行，并在完成故障处理后出具产品维护报告，包含问题的原因、解决办法及建议。

（3）定时巡检：经甲方许可，乙方每年度进行定期现场巡检（具体根据甲方要求），对甲方应用软件的软硬件环境进行检查，发现系统稳定运行的隐患因素并及时排除。乙方向甲方出具系统巡检报告，内容包含巡检范围、结果及巡检建议。

（4）服务响应承诺：在维保期内，如软件系统发生故障，乙方需在接到甲方通知后【30】分钟内予以响应，并提供远程支持。若远程支持无法解决问题，乙方应保证工程师在【4】小时内到达甲方指定现场。工程师到达现场后，应保证在【4】小时内排除故障或提供明确的解决方案及完成时间表，并须经甲方书面确认。

若乙方未能遵守上述任一承诺，每发生一次，应向甲方支付合同总额【1%】的违约金；若因此给甲方造成损失的，乙方还应赔偿全部实际损失。

第五条　甲方责任

负责本合同范围内维护服务工作的组织、协调，确保做好配合工作，具体内容如下：

（1）提供维保清单（包括设备名称、型号、数量等）。

（2）甲方分管部门安排专人负责和协调售后维护的相关工作，以确保维护过程的

顺利进行。

（3）涉及到甲方现有其他系统及数据时，甲方应有人员全程陪同，涉及操作时，应由甲方工作人员进行陪同。

（4）业务科室派专人负责系统的日常运行和故障报修，并在乙方进行现场售后维护时提供必要的支持与配合。

第五条　保密与数据安全

5.1 保密信息的定义

本合同所称"保密信息"是指甲方在合同履行过程中向乙方披露或乙方接触到的、与甲方相关的所有信息，包括但不限于：

（1）患者个人信息、健康医疗数据、诊疗记录、病历资料等一切医疗相关数据；

（2）甲方信息系统的系统架构、源代码、数据库结构、接口文档、系统账号及口令等技术信息-；

（3）甲方的业务流程、管理数据、经营信息、财务数据等商业信息；

（4）甲方提供的所有书面或电子文档、资料、数据；甲方明确标示为"保密"或依其性质应被视为保密的信息。

5.2 保密义务

（1）乙方应对保密信息承担严格的保密义务，不得向任何第三方泄露、披露、提供或允许第三方接触保密信息。

（2）乙方仅可在履行本合同义务的必要范围内使用保密信息，不得将保密信息用于任何其他目的-。

（3）乙方应采取不低于保护自身同等重要保密信息的谨慎程度（且在任何情况下不得低于合理注意程度）的保护措施，确保保密信息的安全-。

5.3 数据安全特别约定

（1）甲方系统产生的全部业务数据、管理数据及日志信息的所有权归甲方所有。乙方不得借服务工作之便非法获取、使用、篡改、泄露或买卖甲方数据。

（2）乙方在服务期间接触到的甲方数据应在甲方指定的系统环境中处理，未经甲方书面同意，不得将数据复制、转移至乙方或其他第三方的存储设备或系统中。

（3）乙方应严格遵守《数据安全法》《个人信息保护法》等法律法规，遵守甲方信息安全管理各项规章制度-。

5.4 人员管理

（1）乙方应对其工作人员进行保密教育和培训，确保其了解并遵守本合同的保密义务。

（2）乙方应建立人员访问权限管理制度，仅授予工作人员履行职务所必需的最小权限。

5.5 数据存储与跨境传输

双方在项目建设、运行、维护过程中收集和产生的保密信息应在中华人民共和国境内存储；未经甲方书面同意和依法合规评估，乙方不得向境外提供任何保密信息-。

5.6 本合同终止或解除后，乙方应立即停止使用所有保密信息；并将所持有的所有保密信息载体（包括原件、复制件、电子版等）全部归还甲方，或根据甲方的要求予以销毁；

5.7 保密期限

本条约定的保密义务永久有效，不因本合同的变更、解除或终止而失效。

第六条　违约责任

（1）任何一方违反本协议导致本协议无法继续履行的，违约方需赔偿守约方违约金，该违约金不足以弥补守约方实际损失的，违约方应赔偿守约方所有实际损失，项目实施过程中甲方一旦发现实施内容与招标文件要求及投标文件响应情况不一致，甲方有权书面通知乙方进行整改，经整改后仍不符合投标响应文件的，甲方有权解除合同，并且乙方需要承担违约责任，乙方需支付合同总额的20%作为违约金且返还甲方已经支付但未履行部分的款项。

（2）甲方认可本合同中乙方软件是乙方的重要财产，如甲方违反本合同知识产权条款的约定，乙方有权立即单方解除本合同，并要求甲方赔偿合同总额的10%作为违约金。

（3）任一方违反本条保密义务的，守约方有权单方解除本合同。违约方支付合同总额的10%作为违约金，并赔偿守约方因此遭受的全部损失（包括但不限于直接损失、间接损失、声誉损失、行政罚款、诉讼费、律师费等）。

（4）乙方因未能如期提供服务或因其他违约行为，甲方有权单方解除合同，要求乙方赔偿合同总额的10%作为违约金并赔偿甲方因此遭受的全部损失（包括但不限于直接损失、间接损失、声誉损失、行政罚款、诉讼费、律师费等）。

第七条　监管考核

（1）巡检与资料交付：乙方按合同约定定期开展系统巡检、安全核查，按时提交巡检报告、隐患清单。漏检、报告迟交、内容不实，每次扣除当期维保款5%；发现重大隐患隐瞒不报，每次扣除当期维保款 10%。

（2）人员与重大保障：乙方固定维保对接人，更换主要技术人员须提前告知甲方信息科并完成交接。节假日、等级评审、大型医疗保障等关键时段，乙方须保持 7×24 小

时应急联络畅通，联络失效、保障缺位的，每次扣除当期维保款 5%。

（3）隐患整改管理：甲方信息科提出系统缺陷、安全隐患整改要求并出具整改通知的，乙方须在规定时限内整改完毕并反馈结果。逾期整改、整改不到位或虚假整改，每次扣除当期维保款 5%。

（4） 责任约定：因乙方操作失误、维保疏漏导致系统中断、影响临床业务、造成数据异常或信息泄露的，乙方承担全部赔偿责任；造成严重影响的，甲方有权单方解除合同并追偿损失。

（5） 履约管控：乙方多次发生上述违约情形，甲方可暂缓支付维保款项，直至问题整改到位；拒不整改或履约持续不达标的，甲方有权解除维保合同。

第八条 争议解决

双方将本着长期友好合作的精神，协商解决维护服务过程中的问题及纠纷。双方一致同意：

(1)违约及责任承担：甲方或乙方未履行本合同的约定条款，视为违约，并承担因违约给守约方造成的全部实际损失。。

(2)不可抗力：如发生不可抗力，使一方受不可抗拒力影响，未能履约，应在事件发生 15 个工作日内通知另一方，在获得对方谅解后，可免除全部或部分责任。如得不到另一方谅解，受不可抗拒力影响一方，在出具公证机关的不能履行或不能部分履行合同义务的证明后，可据此免除全部或部分责任。

(3)争议解决：有关本合同的一切争议，双方首先通过友好协商解决，协商不能解决时，任何一方均可向甲方所在地的人民法院诉讼解决。在解决争议期间，与争议无关的合同条款继续有效。

第九条 其他

“本合同”一式陆份，“甲方”执肆份，“乙方”执贰份，具有相同的法律效力。自“双方”代表签字加盖合同章（或公章）之日起生效。

第十条 附件条款

合同附件为合同不可分割的组成部分，与合同正文具有同等法律效力。

附件一：服务清单

附件二：公司营业执照、委托书、受托人身份证复印件

附件三：产品承诺书

附件四：分项报价表

（以下无正文）

甲方：陕西省森林工业职工医院（盖章）

开户行：中国农业银行鄠邑区营业厅

账号：　26160101040008544

地址：陕西省西安市鄠邑区画展将 9 号

邮政编码：

电话：

法定代表人（授权代表）：

签约日期：2026 年 10 月 19 日

乙方：成都华软技术工程有限公司（盖章）

开户行：中国工商银行股份有限公司成都浆洗街支行

账号：4402262009100040170

地址：成都市武侯区玉林北街 1 号 1 栋 3 单元 21 层 2103 号

邮政编码：610041

电话：028-85350922

法定代表人（授权代表）：

签约日期：2026 年 10 月 19 日

附件一：《服务清单》

序号	服务名称		服务范围	服务时间	数量
1	杀毒软件授权及升级服务		提供650个终端杀毒软件产品授权和3年软件版本及特征库免费升级服务License授权可同时支持普通PC操作系统和服务器Server操作系统。	3年	650点
2	网络安全服务	互联网暴露面梳理	1、对单位暴露在互联网端的域名、IP、端口等网络资产进行排查。通过与现有资产清单进行对比梳理，发现未知资产和风险端口，形成准确的互联网资产清单，梳理出互联网攻击面。 2、基于单位互联网出口IP地址、域名、备案信息、关键词等信息，结合攻防人员信息收集能力，利用搜索引擎、网络空间资产搜索平台等，对单位系统暴露在互联网的关联资产进行排查。 3、对互联网链路出口IP地址段进行全面探测，发现资产存活状态、设备指纹信息、开放服务端口信息等；基于已知域名，对根域进行爆破，挖掘暴露在互联网的子域名。 4、输出成果：《陕西省森林工业职工医院互联网暴露资产清单》	1年	1次
3		渗透测试	1、提供渗透测试服务，模拟黑客使用的漏洞发现技术和攻击手段，对目标网络、系统、主机应用的安全性进行深入探测，发现系统最脆弱环节，出具相应的测试与分析报告，并提出相应的整改建议及措施。 2、渗透测试内容至少包括：信息收集类、配置管理类（HTTP/HTTPS方法测试、应用中间件测试、信息泄露、异常错误等）、认证类（用户枚举、密码猜解、密码重置、密码策略测试等）、会话类（cookie测试、session会话测试等）、授权类（越权访问、路径遍历、任意文件下载、逻辑缺陷测试等）、数据验证类（SQL注入、 跨站脚本、代码注入、URL跳转、文件上传测试等、输入输出校验绕过、数据篡改）、系统应用漏洞等。 3、按照采购人要求，对被测系统进行模拟攻击测试工作。 4、交付成果：《陕西省森林工业职工医院信息系统渗透测试报告》		4次
4		漏洞扫描	1、季度对所有服务器、网络、安全设备、数据库、中间件等进行全面漏洞扫描工作，并将扫描结果进行系统化管理，清晰掌握信息系统上的漏洞信息。 2、扫描完成出具详细《漏洞扫描报告》。		4次
5		应急演练服务	1、网络安全应急预案：服务过程中针对可能发生的安全事件，为应急准备、事件报告、事件处理、灾难恢复的各个方面所预先制定的科学有效的行动规范和工作流程，在发生		1次

			信息安全事件时，及时开展有序和有效的应急响应工作。 2、网络安全应急演练：制定应急预案演练工作计划，并模拟在网络及重要设备出现故障等紧急情况下，依据前期制定的应急预案进行处理，其中至少包括事件的发现、上报、处理等环节。提高对安全事件的响应能力；同时验证预案的正确性和适用性，进行总结分析，并根据需要对应急预案进行修订。 3、交付成果：《陕西省森林工业职工医院网络安全应急预案》、《网络安全应急演练方案》 、《陕西省森林工业职工医院网络安全应急演练脚本》、《陕西省森工医院网络安全应急演练报告》		
6		攻防演练服务	1、供应商组织攻击团队与防守团队进行模拟对抗，攻击团队对靶机进行攻击演练，防护团队对攻击进行检测、响应、处置，通过进行攻防演练，医院可以及时发现并修复安全漏洞，提高员工的安全意识和应急响应能力，从而更有效地保护患者数据和医疗服务的安全。 2、交付成果：《陕西省森林工业职工医院攻防演练成果报告》		1 次
7		安全巡检	1、每季度对项目服务范围内的所有网络安全等设备进行一次全面的现场巡检，至少包括：检查设备硬件指示灯状态、风扇运转状况、电源模块负载、设备健康状态，系统运行状态，并记录设备运行日志中的异常告警信息。 2、配合对支持特征库升级的各类安全设备特征库进行检查与更新，确保其防护能力及时有效。 3、建立巡检发现问题的闭环管理机制，对巡检中发现的潜在故障隐患，在下次巡检时进行复核验证，确保问题得到有效解决或风险处于受控状态。 4、交付成果：《陕西省森林工业职工医院安全巡检报告》。		4 次
8		应急响应服务	1、遇到重大或突发网络安全事件后按照要求的服务响应级别采取相关的措施和行动。正确应对安全事件，降低安全事件带来的损失和影响，并将业务以及网络恢复到正常状态；应急响应至少包含以下几类安全事件：WEB 安全事件、恶意程序事件、网络攻击事件、信息破坏事件等。 2、服务标准：为服务范围内所有设备及系统提供 5×8 小时的现场技术支持服务与 7×24 小时的在线技术支持服务。 3、安全事件专项处理：针对信息安全事件，在确保系统恢复的同时，采取技术手段跟踪和锁定入侵来源，并完整获取、保存与事件相关的日志、数据等入侵证据。 4、报告与归档：应急事件处置完毕后 3 个工作日内，提交正式的《应急事件处置工作报告》双方共同备案留档。 5、汇报总结：应急响应工作完成后向采购人进行专题汇报，阐明故障的发生原因、解决过程、解决结果和今后的预防方法。		按需

9		重大活动安全保障服务	1、针对全年重大会议、敏感时间段、节假日、上级开展网络安全攻防演练等特殊时期内开展重大活动专项保障，安排专业服务人员 7*24 小时值守，保障网络安全，具体要求如下： （1）监测预警：将日常安全运维升级为 7×24 小时重点监控，安排人员轮班值守，重点监测单位的各类业务系统，做好攻击监测、响应、处置、溯源分析、记录及事件报告等工作，并提供应急响应技术支持，发现网络系统安全隐患时及时启动应急预案。 （2）分析研判：针对监测到的网络安全事件，通过主机日志、安全设备日志、系统日志等信息对攻击行为进行分析研判，每个保障期结束后提供安全保障报告并提出后续安全防护整改建议。 （3）应急处置：根据研判分析结果和网络安全应急预案，对网络安全事件进行处置。 （4）追踪溯源：根据安全防护设备、安全监测设备产生的告警信息、样本信息等，结合各种情 报系统对攻击事件进行溯源分析。 （5）交付成果：《安全保障总结报告》（含攻击监测记录、事件处置情况、溯源分析结果、安全防护整改建议等）。		按需
10	设备特征库升级	外网防火墙	华为 USG6625E： IPS 特征库升级、AV 特征库升级包含：①产品特征库升级服务；②远程支持服务；		1 年	/
11		入侵防御	天融信 IPS-LIC-1Y-TI-A3110：	一、升级授权及实施要求：原厂提供升级服务。 二、技术支持服务要求：提供 7×24 小时远程支持（含电话、在线客服、远程桌面等渠道），并建立专属技术支持通道，快速响应技术咨询与故障处置；远程无法解决的问题提供现场支持。 三、软件系统保修要求：服务期内，免费修复系统自身缺陷及兼容性问题。 四、重大变更现场技术支持服务：针对系统升级、网络拓扑调整、防护策略重构等重大变更场景，提供全流程现场技术支持。变更前制定详细实施方案，明确风险防控措施并组织技术交底；实施过程中安排专业人员现场指导，严格把控风险、降低业务影响。		/
12		上网行为管理	天融信 BUNDLE-LIC-1Y-ACM-B2504			/
13		入侵检测	绿盟 V5.6R10F02SP07：包含：①产品系统升级；②远程支持服务；③产品保修服务；④软、硬件故障。若远程无法解决提供上门服务。			/

附件二：公司营业执照、委托书、受托人身份证复印件

1、营业执照



统一社会信用代码

91510107794919 43X2

营业执照

（副 本） 副本编号：1-1

名 称 成都华软技术工程有限公司

类 型 有限责任公司(自然人投资或控股)

法定代表人 庞先志

经营范围 一般项目：信息系统集成服务；信息系统运行维护服务；信息技术咨询服务；大数据服务；物联网技术服务；计算机软硬件及辅助设备批发；计算机软硬件及辅助设备零售；网络与信息安全软件开发；软件开发；软件外包服务；信息咨询服务（不含许可类信息咨询服务）；日用百货销售；家用电器销售；建筑材料销售；五金产品批发；广播影视设备销售；金属制品销售；办公设备销售；电子元器件批发；消防器材销售；电线、电缆经营；家具零配件销售；家用视听设备销售；日用家电零售；五金产品零售；通信设备销售；建筑装饰材料销售；电子元器件零售；租赁服务（不含许可类租赁服务）；计算机及办公设备维修；通讯设备修理；日用电器修理。（除依法须经批准的项目外，凭营业执照依法自主开展经营活动）

注册资本 (人民币)壹仟万元整

成立日期 2006 年 11 月 20 日

住 所 成都市武侯区玉林北街 1 号 1 栋 3 单元 21 层 2103 号

登记机关 2025 年 12 月 09 日

国家企业信用信息公示系统网址：http://www.gsxt.gov.cn

市场主体应当于每年 1 月 1 日至 6 月 30 日通过国家企业信用信息公示系统报送公示年度报告

国家市场监督管理总局监制

2、法定代表人授权书

法定代表人授权书

陕西省森林工业职工医院：

本授权委托书声明：我 庞先志（法定代表人姓名） 系注册于 成都市武侯区玉林北街1号1栋3单元21层2103号（供应商地址） 的成都华软技术工程有限公司 （供应商名称） 的法定代表人，现代表公司授权下面签字的 岳莹、商务（被授权人的姓名、职务） 为我公司合法代理人，代表本公司参加 杀毒软件及网络安全服务项目 （项目名称） 采购项目编号为 SXWZ2026ZB-SGYY-156 的采购活动。以我方名义全权处理该项目有关投标、签订合同以及执行合同等一切事宜。

本授权书有效期自投标文件递交截止之日起 90 日历天，特此声明。

供应商（单位名称及公章）： 成都华软技术工程有限公司

法定代表人（签字或盖章）：

被授权人（签字或盖章）： 性别： 女 职务： 商务

被授权人身份证号码： 511902199710126980

联系地址： 成都市武侯区玉林北街1号1栋3单元21层2103号

联系电话： 18384128396

法定代表人及被授权人身份证复印件

法定代表人身份证复印件（正/反面）

中华人民共和国
居民身份证

签发机关　成都市公安局锦江分局
有效期限　2021.06.28-2041.06.28

姓名　庞先志
性别　男　民族　汉
出生　1984 年 8 月 23 日
住址　成都市锦江区观音桥街55号3栋2单元31楼3号



公民身份号码　511902198408239410

被授权人身份证复印件（正/反面）

中华人民共和国
居民身份证

签发机关　巴中市公安局巴州分局
有效期限　2026.08.14-2046.08.14

姓名　岳莹
性别　女　民族　汉
出生　1997 年 10 月 12 日
住址　四川省巴中市巴州区平梁镇枣儿塘村8组1号



公民身份号码　511902199710126980

附件三：产品承诺书

kaspersky

产品服务承诺函

致：陕西省森林工业职工医院

卡巴斯基技术开发（北京）有限公司作为卡巴斯基®安全解决方案系列产品的制造和生产厂家，主要营业地点设在北京市东城区青龙胡同 1 号歌华大厦 B 座 1219 室。谨对成都华软技术工程有限公司，主要营业地点设在成都市武侯区玉林北街 1 号 1 栋 3 单元 21 层 2103 号参与陕西省关于杀毒软件及网络安全服务项目，项目编号：SXWZ2026ZB-SGYY-156 投标做出如下承诺：

在产品叁年授权有效期内，提供如下服务：服务内容

1. 新病毒信息发布和预警

服务方式	网上发布
服务次数	有重大病毒发现时
服务内容	重大病毒信息发布及预警
服务结果	技术文档发送

2. 用户回访

服务方式	电话
服务次数	平均每半年一次
服务内容	公司产品的使用情况、用户对产品的意见及建议、解决用户使用产品中的各种问题
服务结果	收集用户意见和建议，并及时解决用户问题

3. 病毒库更新

服务方式	自动升级、网站离线更新包下载
服务次数	自动更新平均每小时更新一次、提供离线更新工具

卡巴斯基技术开发（北京）有限公司
北京市东城区青龙胡同 1 号歌华大厦 B 座 1219 室
邮编：100007

服务内容	提供病毒库的升级文件，供卡巴斯基用户升级病毒库。
服务结果	病毒库升级成功

4. **软件升级**

服务方式	自动升级、Email、邮寄或网上下载
服务次数	根据版本发布情况以及用户使用情况
服务内容	修改产品不足，完善和增加产品性能后的软件进行升级
服务结果	完成软件升级

5. **应急通告**

服务方式	Email 或 网站公告
服务次数	重大病毒事件发生时
服务内容	重大病毒事件处理等
服务结果	重大事件通知

6. **新病毒检测服务**

服务方式	Email
服务次数	00：00～24：00
服务内容	病毒样本检测
服务结果	对用户提供的病毒样本进行检测并说明（仅限样本是否是恶意程序）

响应速度与应急措施

对提交的可疑文件（包括新病毒），卡巴斯基技术开发（北京）有限公司在接到可疑文件的24 小时内给予答复。

A：紧急情况下，如果可疑病毒开始在系统内大量扩散，卡巴斯基技术开发（北京）有限公司会在收到可疑程序后的 3 小时内向企业提供紧急应对方法。

卡巴斯基技术开发（北京）有限公司
北京市东城区青龙胡同 1 号新华大厦 B 座 12 层
邮编：100007
T：8610 8418 6111
F：8610 8418 6222
www.kaspersky.com.cn
www.securelist.com

B：在接到用户提出的问题后，卡巴斯基技术开发（北京）有限公司将根据问题的种类和紧急程度以及先后顺序，保证在规定时间内向企业做出响应和提供相应的支持。问题种类和响应级别参照下表。

产品故障反应及解决时限表

编号	级别	描　　述	反应时间	解决时间
A	最高级 Critical	软件死锁、没有反应。 病毒爆发、大量扩散。	30 分钟	3 小时内
B	紧急 Urgent	系统主要功能无法执行。 系统性能突然严重降低。	2 小时	1 个工作日
C	重要	系统出现错误，不过有变通方法可以暂时运作。	1 个工作日	3 个工作日
D	普通 Normal	索取产品更新（非电子数据方式）。 索取一般信息。	1 个工作日	3～5 个工作日

如遇不可抗拒原因致使人员无法按时完成，有关责任将予以免除。

产品故障级别划分说明

A：最高级

在运转期间，大量软件死锁、没有反应，病毒爆发、大量扩散，以致影响并中断网络正常服务功能。

B：紧急

在运转期间，且可以短暂容忍的情况下，产品部分主要功能失效，以至影响网络用户的关键应用及维护人员操作。

C：重要

在运转期间，在可以容忍而没有严重影响的情况下，产品部分非主要功能失效，影响网络用户及维护人员操作。

kaspersky

D：普通

在运转期间，有某些功能不会使用或者由于操作上的问题造成轻微故障，不影响用户的业务。

应急措施

发生紧急事件（病毒爆发）时，用户应立即通知卡巴斯基服务中心， 卡巴斯基服务中心会启动紧急救援服务体系，提供安全专家紧急响应服务，同时了解病毒爆发状况，如病毒爆发地点、病毒感染现象等，确定参与紧急事件响应技术人员和响应方式。

本服务承诺函有效期为自签发之日起六个月，在此期间，若本公司发布本服务承诺函所列产品的升级版本，则上述产品自动替换为相应升级版本。

卡巴斯基技术开发（北京）有限公司

2025 年 09 月 21 日

卡巴斯基技术开发（北京）有限公司
北京市丰城区南京胡同 号新华大厦 B 座 1 层
邮编 100007

T +86 10 8418 6211
F +86 10 8418 6222
www.kaspersky.com.cn
www.securelist.com

附件 4：分项报价表

序号	服务名称		单价	数量	总价	合计
1	杀毒软件授权及升级服务		300.00	650 点	195000.00	195000.00
2	网络安全服务	互联网暴露面梳理	6000.00	1 次	6000.00	143700.00
3		渗透测试	8500.00	4 次	34000.00	
4		漏洞扫描	2800.00	4 次	11200.00	
5		应急演练服务	6500.00	1 次	6500.00	
6		攻防演练服务	30000.00	1 次	30000.00	
7		安全巡检	2000.00	4 次	8000.00	
8		应急响应服务	24000.00	按需	24000.00	
9		重大活动安全保障服务	24000.00	按需	24000.00	
10	设备特征库升级	外网防火墙	17200.00	/	17200.00	40000.00
11		入侵防御	5500.00	/	5500.00	
12		上网行为管理	3500.00	/	3500.00	
13		入侵检测	13800.00	/	13800.00	