**项目需求**

**一、项目基本情况**

1、项目名称：机房运维服务项目。

2、项目内容：机房运维服务主要包含：（1）医院机房内现有网络设备、安全设备、服务器、存储、备份等设备（机房设备维保内容包括合同履行期内采购人新增及超过售后期的设备）进行维护，确保设备正常运作；（2）结合HIS等级保护测评报告，针对不满足项开展中山市坦洲人民医院网络信息安全加固建设，包含物理安全、系统安全、数据安全、访问控制、安全管理和监督等方面的整改修复，实现中山市坦洲人民医院信息系统达到等保三级标准。（3）根据中山市卫生健康局《关于印发<2024年中山市医疗卫生机构网络数据安全绩效考核指标>的通知》要求，完成相关安全服务的考核指标。

3、项合同履行期：自合同约定生效之日起1年。

4、报价：项目采购预算（最高限价）：￥230000.00元

二、服务要求

1. 机房运维

1.1 中山市坦洲人民医院机房内现有网络设备、安全设备、服务器、存储、备份等设备（机房设备维保内容包括合同履行期内采购人新增及超过售后期的设备）。

本项目合同履行期内对中山市坦洲人民医院中心机房设备进行运行维护，响应供应商投标报价包括但不限于报修、运输、重要数据恢复等相关费用（厂家保修范围内的设备，需提供协助服务），含合同实施过程中的应预见或不可预见等一切费用及合理的企业利润，保证在合同履行期内机房设备正常运行。（备注：设备列表只提供参考，维护数量以实际情况为准，供应商在报价前可以到医院进行实地考察或电话咨询。）

1. **信息类设备明细表**

|  |  |  |
| --- | --- | --- |
| 设备名称 | 机房 | 备注 |
| san存储 | 中心机房 | san |
| 服务器存储 | 中心机房 | his服务器存储 |
| 服务器 | 中心机房 | 儿童肿瘤接口、不良事件系统 |
| 服务器 | 中心机房 | 合理用药 |
| 服务器 | 中心机房 | 院感系统 |
| 服务器 | 中心机房 | his系统dg数据库 |
| 服务器 | 中心机房 | PACS |
| 服务器 | 中心机房 | LIS、体检 |
| 服务器 | 中心机房 | 新HIS01 |
| 服务器 | 中心机房 | 新HIS02 |
| 服务器 | 中心机房 | 群集 |
| 服务器 | 中心机房 | 杀毒服务器 |
| 服务器 | 中心机房 | 病案妇幼计免 |
| 服务器 | 中心机房 | MSTDC |
| 服务器 | 中心机房 | 合理用药 |
| 服务器 | 中心机房 | 离线查询 |
| 服务器 | 中心机房 | 域服务2 |
| 服务器 | 备用机房 | 财务 |
| 服务器 | 中心机房 | 中山市区域平台 |
| 服务器 | 备用机房 | OA、重症监护系统数据采集程序、不良事件、移动查房的网站 |
| 服务器 | 中心机房 | 院内感染自动抽取程序、银医通数据库 |
| 服务器 | 中心机房 | 备份控制 |
| 服务器 | 备用机房 | 影像图片备份 |
| 服务器 | 中心机房 | 病案归档数据服务器、供应室 |
| 服务器 | 中心机房 | 病历归档转换服务、不良事件AdverseEvent、重症监护单icu、体检服务、会诊服务 |
| 服务器 | 中心机房 | 通用报表管理、阳光用药、绩效考核病历首页数据采集接口 |
| 服务器 | 中心机房 | 中公网-社保实时审核、物资管理系统 |
| 服务器 | 中心机房 | 微信公众号 |
| 服务器 | 中心机房 | 区域平台PACS前置机 |
| 服务器 | 中心机房 | 票据打印云服务 |
| 服务器 | 中心机房 | 互联网医院 |
| 服务器 | 中心机房 | 疫苗预约服务器 |
| 服务器 | 中心机房 | 电子票据服务器 |
| 服务器 | 中心机房 | 电子票据CA服务器 |
| 服务器 | 中心机房 | LIS服务上传 |
| 服务器 | 中心机房 | 心电网络服务器 |
| 服务器 | 中心机房 | hp磁带机备份服务器 |
| 服务器 | 中心机房 | 传染病前置服务器 |
| 服务器 | 中心机房 | 发热门诊售药机 |
| 服务器 | 中心机房 | 国药控股耗材管理服务器1 |
| 服务器 | 中心机房 | 国药控股耗材管理服务器2 |
| 服务器 | 中心机房 | 银医通服务器 |
| 服务器 | 中心机房 | 医博医保审核 |
| 服务器 | 中心机房 | SPD服务器 |
| 服务器 | 中心机房 | 单病种服务器 |
| 服务器 | 中心机房 | 广东省药品不良反应上报 |
| 服务器 | 中心机房 | 传染病前置机 |
| 服务器 | 中心机房 | HR人事管理系统 |
| 服务器 | 中心机房 | 食源性服务 |
| 路由器 | 中心机房 | 社会区域路由 |
| 深信服 | 中心机房 | 云桌面 |
| 防火墙 | 中心机房 | 防火墙 |
| 防火墙 | 中心机房 | 下一代防火墙 |
| 防火墙 | 中心机房 | 防火墙 |
| 防火墙 | 中心机房 | 网关 |
| 路由器 | 中心机房 | 连卫生局网关 |
| 服务器 | 中心机房 | 社保前置机 |
| 服务器 | 中心机房 | 卫生局SV |
| 网络及安全设备 | 中心机房 | 下一代防火墙-AF |
| 网络及安全设备 | 中心机房 | 上网行为管理-AC |
| 网络及安全设备 | 中心机房 | 负责均衡AD |
| 网络及安全设备 | 中心机房 | 深信服超融合 |
| 网络及安全设备 | 中心机房 | 集群IP |
| 网络及安全设备 | 中心机房 | HCI1 |
| 网络及安全设备 | 中心机房 | HCI2 |
| 网络及安全设备 | 中心机房 | 深信服超融合交换机（桌面云） |
| 网络及安全设备 | 中心机房 | 深信服超融合交换机1 |
| 网络及安全设备 | 中心机房 | 深信服超融合存储交换机管理口（直连） |
| 网络及安全设备 | 中心机房 | 深信服VDC |
| 网络及安全设备 | 中心机房 | 深信服VMP |
| 网络及安全设备 | 中心机房 | 数据中心交换机地址（接服务器） |
| 网络及安全设备 | 中心机房 | 核心交换机 |
| 网络及安全设备 | 中心机房 | 中心机房政务网交换机 |
| 网络及安全设备 | 中心机房 | 无线查房管理地址 |
| 网络及安全设备 | 中心机房 | 无线查房WIFI信号 |
| 网络及安全设备 | 中心机房 | 新HIS系统光交换机san配置 |
| 网络及安全设备 | 中心机房 | 应用交付-AD |
| 网络及安全设备 | 中心机房 | 堡垒机-OSM |
| 网络及安全设备 | 中心机房 | 零信任访问控制系统-aTrust |
| 网络及安全设备 | 中心机房 | 数据中心交换机 |

本项目成交人必须提供1名或以上精通软硬件的维保技术人员驻场，驻场工作时间为每天上午8：00-12：00，下午14：30-17：30（双休制），在采购人单位提供现场服务，其他时间根据采购人要求安排现场或电话值班，随时接受医院合理的加班要求。

驻场人员要严格遵守医院制度，坚守岗位，随时留意设备有无异常情况，若发现异常情况或 接到障碍申告，需马上前往处理，如属于重大故障，立即按照重大故障流程上报采购人及成交人， 随后立即启动应急服务响应。驻场人员统一执行采购人工作人员的各项规章制度，遵守采购人制 定的值班规定和文明准则。成交人的驻场人员在上岗前需与采购人签署保密协议书，应严格遵守 保密要求，不得将采购人的设备数据和相关用户资料提供给任何第三方，除本项目外，不得以其 他任何方式使用本项目的有关数据。成交人一般情况不得更换项目组人员，如需更换提前1个月 书面报告采购人，征得采购人同意情况下才能更换；如果成交人项目组人员存在工作态度、责任 心、技术能力、协调能力等方面之一的问题时，采购人有权要求成交人更换项目组人员，并且成 交人在收到采购人书面通知之日起5个工作日内更换。否则，采购人有权解除合同。

工作基本要求如下：

(1)维保人员需熟悉现场设备的位置；熟悉现场设备的安装、调试、维修方法。

(2)熟悉各设备的操作。尤其要熟悉集成系统、历史数据的查看方法；能处理现场的常见问题处理。

(3)维保人员应按计划对设备进行巡检。

(4)维修要及时，必须做到当天发现的问题，当天现场检查维修。

(5)维修记录需在电脑中记录保存。

(6)维保人员发现意外情况应及时准确地向采购人相关管理人员报告。

(7)要熟记采购人常用电话与人名、职务，保持工作沟通。

(8)妥善保存维修备件，待修件、完好件分区存放。

(9)除工程师工作站外，其他电脑禁止安装任何软件，禁止文件拷入/拷出操作。禁止非本班值班 人员操作值班设备。未经许可不得以采购人工作人员的身份接受新闻媒体采访，不得对外泄漏医院内部信息。

(10)为更好地管理维保服务工作，本项目成交人应对维修设备进行逐个检查，登记设备的硬件使用情况、存在的问题，按每个设备建立独立的设备档案资料，以便于日后开展设备维修保养工作。

(11)在维保过程中，通过记录每个设备的维修备件替换情况、故障问题等情况，不断地完善设备 档案资料，提高设备维护效率，节省维修时间，从而使得医院医疗日常工作能更顺利地进行。

1.3.属于原厂商维护保养期内的设备出现故障时，由成交人联系原厂商对设备进行免费维修，并在设备维修好后安装回原处，产生的一切费用包含于本项目成交总金额中。

1.4.驻场工程师需对机房所涉及的设备、操作系统进行充分熟悉学习并熟练掌握安装配置维护技术，当设备出现问题时，能及时发现并协助相关技术人员解决故障。

1.5.网络维护工作包括机房核心交换设备、服务器、存储设备、备份设备等故障的排除和维修，保障设备的稳定运行。

1.6.在维护期内，医院的数据中心机房业务系统服务器因维护维修硬件时，如因数据迁移服务等产生费用，均包含于本项目成交总金额中。

1.7.驻场人员接到采购人报障后先初步排除设备故障，能现场解决的现场处理，需要更换配件的及时和采购人相关人员沟通。

1.8.驻场工程师在对院内设备操作过程中，提前和采购人充分沟通其所修设备数据目录，提 前做好相关数据备份，终端设备由于维修维护导致的数据丢失由成交人负责（设备正常使用损坏所造成的数据丢失不在范围内）。

1.9.保障措施

1.9.1.充足备品备件

要求备有符合采购人使用的常用设备的备品备件，解决设备故障时可在最短时间内使用备品备件应急替换。同时，针对本项目的实际情况，成交人应提供一定数量的备用设备存放在采购人单位，方便在出现紧急故障时进行及时有效的处理，备用设备需放置在采购人指定位置，并根据医院设备实际运行情况而调整备用设备数量，维护期满后备品备件归还成交人。常规备件包括备用服务器、硬盘、光驱、内存条、网卡、网线、硬盘线、数据线、水晶头、电源线等。

设备因配件年久老化，无法进行维修使用的情况下，按规定上报采购人，采购人对设备进行 确认无法修复后作报废处理，再由采购人酌情进行更换。

1.9.2.现场巡检保养服务

为能更及时详细地了解机房设备的运行情况，成交人驻场人员应在日常工作过程中随时对设备进行现场巡检，了解设备的运行状况，并及时解决问题。同时，还可根据使用者的需要，及时提出对应的优化建议与措施，更高效地满足使用者需求。通过日常的巡检工作，可对系统进行预防性维护，包括检查系统状态、设备清洁、系统备份等。

巡检工作主要包括：

(1) 对服务器系统的运行状态，对系统CPU、内存、I/O状态、进程等进行检查；

(2) 外部设备运行状态，对磁盘阵列、磁带机等的状态、设置进行检查；对风扇、后备电池、磁盘、磁带、键盘等敏感部件进行重点检查，如有故障征兆则可提前进行更换；

(3) 连接件检查，对连接插头、电缆、电源插座等进行检查；

(4) 新接入设备，按采购人信息中心要求设置指定的IP地址，记录主机MAC地址及物理位置；

(5) 系统优化，协助客户对OS进行系统性能调整和系统优化，提高系统效率；进行相关的安全性进程检查；

(6) 远程技术支持服务

要求设有客户服务热线，提供全天候无间断的产品技术咨询、故障申报、硬件维修、培训需 求受理、以及服务政策咨询等服务内容。可提供服务内容：

①售后技术咨询、故障申报、远程故障受理；

②产品技术咨询、设备硬件更换/维修、培训请求；

③服务产品咨询以及服务投诉与建议；

④最新版本获取、产品配套的用户配置手册；

⑤在线技术支持、在线咨询答疑。

1.9.3.服务响应时间

（1）30分钟响应方式

在接到维护服务信息后，30分钟内安排驻场技术人员到达故障现场，处理系统故障。

（2）2小时响应方式

经技术人员检修，如预计设备故障在2小时内无法排除的情况，将在设备故障时间起计2小时内提供不低于故障设备档次及性能的备用设备供采购人使用，直至故障设备修复。

（3)24小时响应方式

提供24小时响应服务，全天24小时服务热线电话，2小时内提供备件更换服务等。

1.9.4.沟通机制

（1）为保证项目进度与质量，需接受医院合理的加班要求。

（2）项目经理需对本项目的整体工作负责，随时与采购人沟通，指导和监督团队其他人员每天的工作计划，跟踪项目进度，及时处理项目中碰到的问题。

（3）针对此项目，成立监察小组，定期对项目内日常工作记录进行检查，确保项目在一个良性的机制下高质量、高效率的进行。

（4）严格按照进度要求监督项目进度。对可能影响进度的情况，提前做好准备工作。

（5）保证有充足的后备与应急人员，以应付突发的大量临时性指定任务，确保项目进度。

（6）成交人需配备多名后备工程师作为本项目现场及远程技术支持，协助解决疑难技术问题。

（7）项目团队成员需具有与项目相匹配的专业技术能力。

1.9.5.监督机制

要求成交人设有专门的服务监督机构，由成交人的主要负责人全面负责。服务监督机构不定 期以各种方式向采购人各使用科室征询对成交人服务的意见和建议。

1.9.6.应急服务

应急情况一般是指：系统宕机且未能确定故障原因、因突发事件并发而造成不能提供有效备 件、第一次现场服务故障未排除、因自然灾害等不可抗力造成设备损坏等情况。

以下情况虽然不属于成交人责任范围，但成交人要尽全力予以配合：因地震、雷击、战争等 不可抗拒力造成设备损坏；因供电系统、火灾等造成设备损坏。

1.9.6.1.应急响应时间

法定节假日期间，如发生重大故障，成交人应在5分钟内响应，在半小时内由驻点人员赶赴现场。同时以最快速度与采购人共同讨论，在20分钟内成立应急事件处理小组，组织后备专业技 术团队，制定应急预案，与驻点技术人员一同以最快速度进行故障处理，直至问题解决。

1.9.6.2.应急措施

在突发应急情况时，将迅速派出高层管理人员赶赴现场，会同采购人领导共同协商，调度指挥各方面有效资源完成抢修工作。针对不同情况，将单独或同时采取以下几种应急措施：

1.9.6.2.1.紧急备机替换

当服务器设备出现故障且无法快速恢复时，成交人需提供备用机给，以保障采购人业务系统在最短的时间内恢复运行。

1.9.6.2.2.紧急调用工程师

要求成交人提供服务工程师及技术顾问队伍，如实际工作中有需要，成交人须在1小时内调动后备工程师紧急赶赴医院现场完成相关工作。

当第一次紧急调用现场的工程师仍不足时，成交人仍可继续按实际情况增派后备工程师赶赴 现场协助。

1.9.6.2.3.紧急调用第三方资源

要求成交人与采购人现有设备厂家建立良好合作关系，可以获得各厂商优先的技术支持和备 件服务。在十分紧急情况下，可借助第三方后备厂商资源，包括备件、技术资源、技术工程师等。

1.9.6.2.4.重大故障书面报告

在重大设备故障解决之后，成交人应对重大故障事件形成书面报告给医院，将事故发生原因、 处理方式以及如何避免再次发生的方法等内容进行详细记录，并归入设备档案库中，在项目服务 期结束后统一交还医院，以便作为日后借鉴依据。

1.9.7.漏洞修复

对于发现的服务器操作系统及操作系统附带软件的中高危漏洞，成交人需在漏洞发现时3个工作日内完成修复。

1.10.在维护期内，中标人需提供网络监控管理平台，

（1）支持IPMI硬件、网络、服务器操作系统、Oracle数据库等监控功能。

（2）支持监控网络中的终端和IOT设备的资产状态，设备类型包括服务器、门禁、打印机、扫描仪、信号灯等。

（3）支持流量检测和异常监控统计分析，包括攻击通信TOP5、异常通信TOP5等。流量检测趋势图，包括：接口速率统计、协议数据统计、应用层数据统计、网络层数据统计。

（4）支持通过检测、阻断、限流、审计报警等防御手段，对蠕虫、后门、木马间谍软件、Web攻击、拒绝服务等攻击进行有效防御。

1.11.弱电线路整理服务

成交人需负责对采购人机房内弱电线路进行归类整理，并使用标签进行标注，保证各类设备接入线路的整洁、美观、查找方便。

**2. 三级等保整改**

2.1 按照网络安全等级保护2.0国家标准要求，根据行业标准、技术标准及医院业务需求，同时结合HIS等级保护测评报告，针对不满足项开展中山市坦洲镇人民医院网络安全加固建设，包含物理安全、系统安全、数据安全、访问控制、安全管理和监督等方面的整改修复，实现中山市坦洲镇人民医院信息系统达到等保三级标准。 2.2 合同履行期限： 自合同签订之日起90个日历天内；项目完工日期以网警出具三级等保证书当天为完工日期。

2.3 整改依据及标准

本项目依据最新的网络安全等级保护相关要求，即等保 2.0。主要参考以下标准：

《中华人民共和国计算机信息系统安全保护条例 》（国务院 147 号令）

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）

《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

《关于开展信息系统安全等级保护基础调查工作的通知》（公信安［2005］1431号）

《信息安全等级保护管理办法》（公通字[2007]43 号）

《关于开展全国重要信息系统安全等级保护定级工作的通知》（ 公信安[2007]861 号）

《关于开展信息安全等级保护安全建设整改工作的指导意见( 公信安[2009]1429 号)》

《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）

《全国人民代表大会常务委员会关于加强网络信息保护的决定》

《中华人民共和国网络安全法》

《信息技术 安全技术 信息安全管理体系要求》（ISO/IEC 27001:2013）

《信息技术 安全技术 信息安全控制实用规则》（ISO/IEC 27002：2013）

《计算机信息系统安全保护等级划分准则》（GB 17859-1999）

《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

《信息安全技术 网络安全等级保护基本要求 第 1 部分：安全通用要求》（GB/T 22239.1-2019）

《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240－2008）

《信息安全技术 网络安全等级保护设计技术要求 第 1 部分：通用设计要求》（GB/T 25070.1-2019）

《信息安全技术 信息系统安全等级保护实施指南》（GB-T 25058-2010）

《信息安全技术 网络安全等级保护测评要求 第 1 部分：安全通用要求》（GB-T 28448.1-2012）

信息安全技术 网络安全等级保护测评过程指南（GB-T 28449-2012）

**3. 2025年中山市坦洲人民医院数据安全安全服务**

3.1 根据中山市卫生健康局《关于印发<2024年中山市医疗卫生机构网络数据安全绩效考核指标>的通知》要求，本单位需对以下安全服务项目进行采购：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 2024年中山市医疗卫生机构网络数据安全绩效考核相关安全服务明细表 | | | | | |
| 序号 | 服务项目 | 服务描述 | 数量 | 单位 | 备注 |
| 1 | 信息安全制度建设 | 建立并完善机房管理制度、网络安全设备管理制度、数据安全管理制度、维护厂商(供应商)保密协议、数据安全保密协议、个人信息和重要数据存储制度等 | 1 | 次/年 | 交付资料：相关制度文档 |
| 2 | 系统风险评估 | 通过对重要资产的分级、安全威胁发生的可能性及严重性分析、对系统物理环境、硬件设备、网络平台、基础系统平台、业务应用系统、安全管理、运行措施等方面的安全脆弱性的分析，并通过对已有安全控制措施的确认，借助定量、定性分许的方法，推断出用户关心的重要资产当前的安全风险，并根据风险的严重级别制定风险处置计划，确定下一步的安全需求方向，提出有针对性的抵御威胁的防护对策和整改措施，并为防范和化解信息安全风险，或者将风险控制在可接受的水平，从而为最大限度地保障网络和信息安全提供科学依据。 | 4 | 次/年 | 服务对象：HIS/LIS/PACS/微信公众号 交付资料：《风险评估报告》 |
| 3 | 漏洞扫描 | 基于漏洞数据库，通过扫描等手段对指定的系统、设备、应用的脆弱性进行自动化检测，发现可利用漏洞；帮助企业或者组织来侦测、扫描和改善其信息系统面临的风险隐患；侦测某个特定设备的系统配置、系统结构和属性；执行安全评估和漏洞检测；提供漏洞修补方案和补丁管理建议； | 4 | 次/年 | 服务对象：机房设备及业务系统 服务交付物：《漏洞扫描报告》 |
| 4 | 渗透测试 | 通过渗透测试进行非破坏性质的模拟入侵者攻击，获取系统信息并将入侵的过程和细节总结编写成测试报告，由此确定应用系统存在的安全威胁。开展人工渗透测试及工具渗透测试，通过工具、手工交叉方式渗透，查找信息系统存在的脆弱点和安全漏洞，输出扫描报告及修复建议，为单位后续加固、整改，提供情况分析报告。 | 4 | 次/年 | 服务对象：业务系统 服务交付物：《渗透测试报告》 |
| 5 | 弱口令扫描 | 依据单位资产台账，完成应用账户、管理员账户、系统账户的默认口令和弱口令检查，对发现的隐患口令依据口令相关策略提出整改意。 | 4 | 次/年 | 服务对象：机房设备及业务系统 服务交付物：《弱口令扫描报告》 |
| 6 | 漏扫修复及防病毒查杀 | 针对漏洞扫描、渗透测试、弱口令扫描结果 ，逐一进行漏洞修复、病毒查杀及安全加固工作。 | 4 | 次/年 | 服务交付物：《漏扫修复报告》 |
| 7 | 网络与信息安全情况通报 | 每季度通告最新的安全动态、安全技术的发展趋势，包括时效性很强的漏洞、攻击手法、病毒码的预先通知，帮助客户系统管理人员在最快的时间内了解重要的安全信息，以便提前、及时地制定安全对策。 | 4 | 次/年 | 服务交付物：《安全通报报告》 |
| 8 | 网络安全培训 | 针对单位人员进行安全意识、安全常识、web构成、常见漏洞、热点0Day事件、入侵流程、恶意软件现象和防御方法培训。针对组织决策者、管理者，工作人员、运维人员和管理员等角色从个人电脑安全、邮件安全、移动安全、日常工作生活等维度进行强化安全意识培训。 | 2 | 次/年 | 服务交付物：《网络信息安全培训报告》 |
| 9 | 攻防演练 | 红队模拟攻击者发起攻击，通过采用供应链攻击、水坑攻击、社工钓鱼、Web应用攻击、近源渗透、物理攻击、多级域渗透等攻击手段，对目标信息系统进行深度攻击测试，暴露安全防御薄弱点，验证安全防护措施有效性。并进行演练复盘，针对暴露的弱点，提出建设性整改建议，协助完成安全整改工作；蓝队专家现场安全值守，通过安全设备进行风险监测，对安全告警开展分析研判，依照应急预案与应急处理流程进行应急响应与安全处置，验证应急响应与处置流程执行与联动机制。 | 1 | 次/年 | 服务交付物：《攻防演练总结报告》 |
| 10 | 应急演练 | 根据突发网络安全事件的性质，深度切合单位所面临的实际网络安全问题。为单位提供全方位，分门别类的演练方案；突发网络安全事件演练解决方案应急演练场景可分为：有害程序事件演练，网络攻击事件演练，信息破坏事件演练，设备实施故障演练和灾害性事件演练。 | 2 | 次/年 | 服务交付物： 《应急演练处置预案》 《应急演练总结报告》 |
| 11 | 重大活动安全保障 | 在重大活动期间对客户的互联网业务做好全面的安全防护，确保客户网络具备较强的安全防护能力，建立强壮的安全堡垒，最大程度地减少在重大活动期间被攻破的概率，重大活动期间，在全面防护的同时具备全面的信息安全事件监控预警能力，实时监控安全态势，及时发现攻击行为，实现对网络攻击的实时发现、阻断与防护。在重大活动期间（如护网、两会、七一建党节、国庆节等重大节日）保障单位的网络安全，一旦发现安全事件进行应急处置。 | 不限次 | 年 | 服务交付物： 《网络安全事件处置报告》如有 |