华能海南昌江核电有限公司

智能安全移动办公平台采购技术规格书

**批准： 日期：**

**会签： 日期：**

**审核： 日期：**

**编制： 日期：**

**华能海南昌江核电有限公司**

**2021年10月**

**1.项目概述**

## **1.1项目背景**

华能海南昌江核电有限公司（以下简称“采购方”）位于海南省昌江黎族自治县海尾镇塘兴村，负责昌江核电二期工程项目建设和运营，昌江核电二期工程规划建设两台120万千瓦核电机组，采用具有我国自主知识产权的“华龙一号”技术方案，昌江核电二期工程于2021年3月31日正式开工建设。

为了满足昌江核电二期工程项目管理信息化需求，目前采购方已建立了一套比较完整的内网应用系统，包括OA系统、邮件系统、综合管理系统、核电ERP系统、网上报销系统、核电一体化辅助系统、法务系统、物资管理系统、风险管理系统和内网统一门户系统，并建立了内网统一门户系统与各应用系统的单点集成，实现了各业务系统工作任务的统一管理。

根据昌江核电二期工程项目建设管理的特点，采购方各级管理人员经常出差或在外网办公，需要从互联网访问内网业务，对移动办公具有紧迫的现实需求，采购方需要建设一套智能安全移动办公平台，满足项目管理人员安全高效移动办公需求。

## **1.2移动办公需求**

目前采购方按照集团公司双网隔离的安全政策要求，建立了内网与外网隔离的“双网”架构。从互联网访问内网业务系统将增加内网业务暴露在互联网的风险，因此，需要建立一套安全高效的通过互联网访问内网的移动办公系统。

经过对目前市场上技术路线比较前沿和成熟的移动办公技术和解决方案进行调研和测试，拟采用“PC沙箱+零信任安全网关”一体化技术方案，建立移动办公平台，能够全面解决移动办公过程中的各类安全问题。

通过PC沙箱技术构建安全工作空间，提供安全可控的数据隔离和控制方案，确保内网应用产生的所有数据将会被加密保存在PC端沙箱内，无实际数据落地到个人终端。针对移动办公的操作行为进行限制，可对沙箱内的应用进行操作控制，如水印控制、截屏控制、网络控制、打印控制、数据隔离、双因子身份认证、传输隧道加密、操作审计等，防止终端上的数据泄露。通过以零信任接入技术，提供数据传输隧道加密，对移动办公业务应用数据流转的全链路进行有效管控，降低敏感应用数据在通信传输环节发生泄露的风险。

## **1.3标准与偏差**

实施方需执行本规范书所列要求、标准，本规范书未提及的内容，则应满足或优于相关国家标准、电力行业标准等，有矛盾时，按较高标准执行。所有标准都会被修订，实施方应执行最新版本。

实施方如对本规范书有偏差（无论多少）都必须清楚地表示在“差异表”中，否则采购方认为实施方完全接受和同意本规范书的要求。实施方如有优于本规范书基本要求的条款，也应在投标文件中特殊说明。

**2.采购范围**

## **2.1采购范围**

本项目采购一套智能安全移动办公平台所需要的服务器和软件产品及安装部署实施服务，采购内容如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购项目** | **规格** | **数量** | **备注** |
| 1 | PC沙箱软件 | 参考“技术要求”描述 | 1套 |  |
| 2 | 零信任安全网关软件 | 参考“技术要求”描述 | 1套 |  |
| 3 | 授权许可 | PC沙箱及零信任安全网关软件授权许可 | 300个 |  |
| 4 | 服务器 | 参考“技术要求”描述 | 2台 | 用于部署PC沙箱管理平台和零信任安全网关 |

## **2.2向采购方提供的技术支持**

|  |  |
| --- | --- |
| **序号** | **技术支持内容** |
| 1 | 技术咨询服务。项目实施前由项目总监组织与采购方交流同类的移动办公系统开展与实施经验，并给出咨询意见，优化出更适合采购方的项目实施方案。不定期与采购方开展技术交流，为后期的系统改进优化提供支持服务。 |
| 2 | 提供现场安装、开发、测试、上线的全程跟踪服务； |
| 3 | 验收合格后提供维保及功能完善； |
| 4 | 指定专门的富有经验的技术人员和业务专家提供售后服务，并随时保持联系； |
| 5 | 公司提供7X24小时技术支持服务 |
| 6 | 对于产品和系统完善性需求，由经验丰富的技术人员和业务专家现场支持； |
| 7 | 系统框架模块内的功能及流程调整，软件故障排除，软件重装，软件的后门和漏洞进行补丁安装，以及相应的版本升级维护服务； |
| 8 | 系统上线后因系统本身不稳定需要进行升级改造的，免费及时进行解决；如因系统问题造成客户损失的，实施方承担全部责任； |
| 9 | 系统迁移时现场技术支持； |
| 10 | 提供服务器软件升级技术服务，根据新版本服务器软件的功能和稳定性，对是否采用新版本提出建议，并配合实施； |
| 11 | 服务报告的编制和递交。 |
| 12 | 与采购方商讨符合的应急计划，编写《应急操作手册》,满足及时应对重大故障时的应急保障需求，确保IT服务连贯性，制定应急保障方案 |

**3.标准/规范**

本项目采购和实施过程中，需满足国家及华能集团公司信息化建设管理相关规定。国家相关法规和技术标准包括但不限于：

GB/T 35282-2017 《电子政务移动办公系统安全技术规范》

GB/T 28448-2019 《网络安全等级保护测评要求》

GB/T 25070-2019 《网络安全等级保护安全设计技术要求》

GB/T 22239-2019 《网络安全等级保护基本要求》

GB-9385-2008 《计算机软件需求规格说明规范》

GB/T12504 《计算机软件质量保证计划规范》

GB8567-88 《计算机软件产品开发文件编制指南》

**4.资质要求**

实施方应具有以下资质：

1)具有ISO9000 系列质量保证体系认证证书。

2)近五年内具有安全移动办公类业绩或电力行业网络安全项目业绩，并提供相应的证明（截止投标时间，以合同签订日期为准，须至少提供合同封面、签字盖章页及合同内容页的复印件）。

3）提供PC沙箱+零信任安全网关产品厂商授权书和售后服务承诺函。

**5.技术要求**

## **5.1总体要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **总体要求** |
| 1 | PC沙箱 | 实现对PC应用的DLP保护，提供数据隔离、数据加密、应用控制、网络拦截、水印技术、截屏监控、打印控制等安全能力，支持应用安全策略、访问安全策略、数据隔离加密等防护。 质保期：一年质保。 |
| 2 | 零信任安全网关 | 支持实现零信任安全接入、隧道加密、访问管理、安全管理等零信任网关能力。 质保期：一年质保。 |
| 3 | 服务器 | 满足部署PC沙箱管理平台和零信任安全网关相关技术要求。  质保期：三年质保 |

## **5.2 PC沙箱技术要求**

1. Windows操作系统兼容：支持Win7 x64和Win10 x64操作系统。
2. ★办公应用兼容支持:PC沙箱集成零信任接入能力，兼容支持B/S应用。在不对现有业务系统做任何业务逻辑、网络架构、访问配置更改的前提下，可通过新采购的PC沙箱，在原有内/外网防火墙、内外网隔离网闸等安全设备的协同配合下，无缝实现仅允许应用于互联网和华能外网网络环境中的现有业务系统通过PC沙箱保障安全运行、并在受保护的情况下受控访问位于华能内网的系统服务端，严格禁止现有业务系统在PC沙箱外的非安全环境中进行使用。
3. ★安全沙箱隔离:在终端本地操作系统建立独立工作域，与本地文件系统隔离。
4. 应用控制策略配置:针对每个工作域可运行应用支持白名单配置管理，白名单之外的应用禁止在工作域内运行。
5. 终端工作域应用导入:终端本地操作系统已安装应用，可通过拖拽方式导入工作域，不需要二次安装。
6. 终端环境检测:对终端操作系统环境进行策略检查，不符合策略要求的环境，限制登录使用工作域。
7. 工作域数据防泄漏:支持全屏或沙箱应用水印，水印内容格式支持自定义。
8. 工作域操作限制：工作域可限制用户进行截屏/录屏操作；策略允许用户进行截屏/录屏操作时,能够进行操作审计；可支持配置策略，禁止向同级/更低级别域通过剪切板交换数据；工作域对工作域内的文件提供透明加解密，对用户无感知；工作域可以禁止用户打印操作；如果允许打印操作，打印内容显示水印。
9. 域间文件交换策略:支持多级工作域的定义和使用，缺省仅支持从低级别域到高级别域的文件单向流入策略。

## **5.3零信任安全网关技术要求**

1. ★业务服务端端口隐藏：现有业务系统和新增零信任网关均无需对外暴露任何TCP端口（不需在现有华能外网互联网防火墙或VPN网关增加映射TCP端口到互联网）。使用UDP单包授权(SPA)技术，仅允许认证后的用户才能通过SDP零信任网关正常访问业务，从而减少互联网暴露面，降低恶意攻击和入侵风险。在现有华能外网互联网防火墙上映射SDP网关端口时，仅需对外映射风险性低的UDP端口，而无需对外映射TCP端口。
2. ★客户端形态：支持以下三种形态：（1）支持单客户端形态，可支持以SDP客户端独立运行的形态使用；（2）可定制化开发支持与PC沙箱融合，依附于PC沙箱、移动端沙箱运行，在端侧仅需进行一次登录操作；（3）SDK形态，支持以SDK形态与门户系统进行集成使用。
3. ★操作系统兼容（单SDP客户端形态）：当以单独的客户端存在时，支持鸿蒙、Android 7.0-11.x、iOS 11.0-14.x、Windows 7 32/64bit、Windows 10 32/64bit、MacOS 10.12以上等终端的接入。
4. 连续认证失败锁定：连续认证失败超过指定次数后，在指定时间内不允许再次登录。
5. 设备健康度检测：移动设备支持检测是否root/越狱、是否开启锁屏密码、是否开启指纹/面容解锁、是否运行在模拟器中、是否开启全盘加密、是否打开调试模式等。
6. 接入设备数量限制：支持针对移动端和PC端分别设置同时允许登录的设备数量。
7. 隧道协议：网关传输通道使用UDP协议，网关UDP端口对没有通过认证的用户不可见。
8. 最小化授权管理：可根据用户状态、时间、位置、网络、设备类型、IP地址等信息综合评估定义访问权限，根据评估结果可基于虚拟组、组织架构、用户做最小化授权。

## **5.4服务器技术要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **指 标** | **技术参数** |
| 1 | ★外观 | 2U机架式机箱，含上架导轨。 |
| 2 | ★处理器 | 配置2颗英特尔至强银牌4210 (10核2.2GHz /13.75MB/85W)处理器。 |
| 3 | ★内存 | 配置2条16GB DDR4 ECC 内存；标配24个内存插槽。 |
| 4 | ★硬盘 | 配置4块2.4TB 10K SAS硬盘；配置SR430C-M 1GB缓存（支持RAID 0/1/5/6/10/50/60）。 |
| 5 | ★网卡控制器 | 板载2\*GE+2\*10GE（不含光模块)。 |
| 6 | 显卡控制器 | 集成 |
| 7 | 光驱 | 无 |
| 8 | ★电源 | 配置2个900W交流电源（1+1冗余）。 |
| 9 | ★管理功能 | 配置4个冗余热插拔风扇，4个USB 3.0接口，集成BMC管理模块，板载iBMC管理模块，支持IPMI、SOL、KVM Over IP、虚拟媒体等管理特性，对外提供1个10/100Mbps RJ45管理网口。 |
| 10 | 保修服务 | 原厂三年保修服务 |

（注：以上标注★相关内容为重要技术参数和要求，其中服务器参考华为2288H V5相关技术指标。）

**6.进度要求**

合同签订的15天内完成系统部署、本地安装、测试、并完成相应的集成开发等工作。

|  |  |  |
| --- | --- | --- |
| **项目内容** | **天数** | **备注** |
| 合同签订 | 开始 |  |
| 网络调研规划设计服务 | 2天 |  |
| 服务器环境及资源准备 | 1天 |  |
| 系统部署安装 | 3天 |  |
| 客户环境调测适配（含测试） | 6天 |  |
| 项目验收（含培训） | 3天 |  |
| 项目试运行 | 30天 |  |

**7.质量保证要求**

1. 系统终验合格后进入系统质量保证期，自双方代表在系统终验合格单上签字之日起计算，有效期为1年。
2. 实施方提供1年免费维护服务和技术支持服务，为本项目提供完善周到的技术支持和售后服务，指派技术人员、协调厂商提供技术服务。
3. 质量保证期内，提供优质的服务和技术保障。系统试运行期间，安排专人指导需求方使用人员的操作，排除系统试运行过程中出现的故障；系统出现故障（致使系统无法正常运行）时，技术人员将即时进行响应，提出解决方案和措施，并做好问题记录，确保问题解决。
4. 质量保证期内，协助采购方做好项目管理工作。尤其是在其他系统变更、调整等过程中提供相关服务，使各系统能正常运行。
5. 服务内容包括：技术咨询、软件优化升级、状态报告和故障检测、优化系统、扩容与改造建议、用户满意度调查等。
6. 技术咨询：提供平台产品相关的免费技术咨询服务，服务方式包括热线电话、电子邮件（7×24）、传真等方式。
7. 软件优化升级：优化升级服务包括基础产品运维、软件系统运维、系统软件升级、业务功能完善。
8. 软件系统运维：保障本项目建设的应用软件系统安装、调试、运行正常。

**8.培训要求**

实施方提供不少于3天不少于5人次的厂商认证的工程师安装配置等实操培训课程。

培训工具包括：

1. 文档资料：包括产品说明书、用户使用手册、产品管理手册及其他培训资料。
2. 培训器材：笔记本电脑，投影仪及扩音话筒等，如有条件可以采用多媒体会议室，效果更佳。
3. 实际操作测试环境

培训方式为：

1. 人工授课：使用多媒体资料（PPT或其他）对相关用户进行全方面的使用讲解。
2. 实际环境模拟（UAT环境）：培训师借助于UAT环境对被培训者进行实际操作的跟踪指导，以确保正式使用时被培训者能正确操作和熟练使用。
3. 培训效果考核：通过制定培训内容相关的试卷或培训师对被培训者实际操作的水准进行考核，以对培训效果进行检查，并将结果反馈给相关负责人。

**9.文件要求**

在项目准备阶段，部署实施阶段，测试阶段，上线准备和最终上线阶段。提供全套详细文档资料，包括但不限于：需求分析说明书、系统设计文档、系统架构文档、系统部署文档、系统功能测试文档、操作手册、技术维护手册、操作人员培训手册、常见问题处理手册等各类文档。

**10.验收要求**

实施方完成系统部署后开始上线进入试运行阶段，试运阶段持续时间为1个月，试运期间，系统应稳定运行并对系统存在问题进行消缺。试运期间的要求：

（1）功能和技术指标满足各技术规格书要求。

（2）在试运行期间由于实施方案的原因，本系统所涉及到的所有软件有一条或多条达不到规定的技术性能时，实施方应在试运行期内采取有效措施，使其完全达到规定的技术要求，并且试运行期将重新开始计算直到试运行期满，在此期间的一切费用由实施方承担。

试运结束后，系统正式上线运行并组织项目验收。

项目验收：合同要求范围内系统功能上线后，符合技术方案要求，由采购方组织项目验收工作。验收的内容为系统所有功能、性能以及稳定性的测试，系统的所有功能和技术性能达到合格。

最终验收前，实施方填写《华能海南昌江核电有限公司信息化项目竣工验收申请表》及《华能海南昌江核电有限公司信息化项目竣工验收表》，经双方确认后作为验收的依据。

**11.附件**

投标方将与规格书的差异汇集成下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 规格书章节号 | 规格书要求 | 实际供货差异描述 |
|  |  |  |  |