

合同编号：

温州市档案馆中心机房核心设备维保项目合同

项目名称：温州市档案馆中心机房核心设备维保项目

委托方（甲方）：温州市档案馆

受托方（乙方）：浙江索思科技有限公司

签订时间：2024 年 8 月

签订地点：温州市档案馆

有效期限：2024 年 8 月 13 日 至 2025 年 8 月 12 日

使用说明

第一，本《合同》供温州市档案馆中心机房核心设备维保项目合同双方参照使用；

第二，有关空格的数字、百分比及内容，由合同双方根据实际情况填写，双方也可根据实际需要，对有关条款进行修改、增补或者删减；

第三，在使用本《合同》时应当结合具体情况正确选择文本中所提供的相关内容；

第四，应当注意保持合同的完整性，在正文中不能表述清楚的内容可以附件的形式进行表述；

第五，在订立重大的或者内容复杂的合同时，应当向法律专家咨询；

目 录

- 一、维护环境及对象
- 二、服务期限与服务地点
- 三、服务内容、方式和要求
- 四、维护确认与验收
- 五、价格与付款方式
- 六、义务与责任
- 七、所有权、知识产权和使用权
- 八、保密
- 九、服务变更
- 十、不可抗力
- 十一、违约责任
- 十二、争议解决
- 十三、合同的生效
- 十四、名词解释
- 十五、其他
- 十六、项目合同签章
- 附件一、维护清单
- 附件二、项目维护小组

系统设备维保项目合同

本合同甲方委托乙方就温州市档案馆中心机房核心设备维保项目进行技术支持维护服务，并支付相应的技术服务报酬。双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

一、维护环境及对象

详细的维护对象清单见附件一。

二、服务期限与服务地点

1. 服务期限

本合同约定的维护服务期为1年，从2024年8月13日起至2025年8月12日止。

2. 服务地点

本合同约定的维护服务地点为：温州市档案馆机房。

三、服务内容、方式和要求

本维护项目包含以下几类：

1. 日常运行管理（设备检查、系统日常巡检、客户端操作支持）
2. 硬件设备维护（故障排除、设备修复、配件支持）
3. 产品软件维护（更新升级、安装调试、系统恢复）
4. 网络设备维护（网络诊断、故障排除、参数设置、性能优化）
5. 业务应用系统维护（修正错误、完善功能、扩展功能）

维保服务范围

运维外包服务的对象主要包括以下几内容：信息资产管理统计、网络配置、Weblogic 中间件、ORACLE 运维服务(含数据备份)、系统审计、WEB 应用安全扫描（含网络、系统与应用安全管理）、自助售后服务、核心业务保障服务、信息安全服务、虚拟化运维服务、机房卫生及线路整理（含机房环境，UPS，布线）、应急响应、定期巡检、一年专人常驻服务、楼层接入交换机和汇聚机房管理、虚拟主机管理、其他常规系统的支撑保障服务。

提供设备清单中所有设备及其相关设备的 7X24 小时(特别指定为 5×9 小时的除外) 硬件运维服务。提供附件清单中所有设备系统软件 7X24 小时技术支持服务（特别指定为 5×9 小时的除外）。提供 7X24（特别指定为 5×9 小时的除外）电话技术支持服务。在维护服务期内由于设备出现硬件问题，投标人须负责修理或更换，费用包含在本次报价中。

1、信息资产统计及管理服务

此项服务详细调查并记录服务范围内的各个设备的种类、型号、功能、物理位置、端口对应情况、部署情况等资产信息，然后录入管理系统。在服务有效期内，关注数据中心内的资产变更情况，并及时录入系统，可纵览整个数据中心的资产使用情况。

在管理硬件资产的同时，对 IP 地址、虚拟化资源、配置文件等进行管理。通过图形化的界面，准确知道 IP、应用、服务器（物理或虚拟）、机柜、网络接口、业务负责人之间的一一对应关系。

在 IP 地址管理上，同时提供 IPV4 及 IPV6 地址空间的管理，能帮助准确的了解网络内 IP 地址的使用及分配情况。

2、网络配置文件管理

此项服务为主要提供网络设备的自动配置文件管理功能，减少人工文件管理带来的复杂性，提供配置合规性管理、批量配置部署等功能。

在服务有效期内，对数据中心内的设备配置进行自动定时备份，在设备因为意外原因导致配置文件丢失时，及时恢复到指定时间点的配置。

3. 硬件运维基本服务

负责对运维设备所有硬件做故障诊断及系统性能维护。有充足的备机备件，保障核心设备出现故障后，可无偿提供备用设备服务，对所有运维设备的故障件均给予技术支持，提供维修服务，维修前须能提供备品备件的能力。提供对扩容设备进行安装调试。确保发生故障的情况下能迅速提供备机并且备机系统能够正常接管生产机的工作，保证业务不停止。

产品升级更新服务：对于网络安全产品，中标供应商必需提供安全产品的软件及安全库的更新升级服务，如因设备停产、停止更新、停止服务等原因无法更新升级，需出具原厂书面证明，得到招标方确认后，可以不提供更新升级服务。

备品备件要求：

- a. 有充足的备品备件；
- b. 设备故障无法在短时间内修复时，投标人必须 12 小时内提供备件到现场；

4. 系统软件维护基本内容

提供对工具类系统,包括备份系统、虚拟化系统、日志系统及所有 ORACLE 版本升级（或安装新版本）、故障维护及性能优化调整，如果不能在 4 小时之内解决系统软件问题，采购方将有权请第三方技术人员上门维护，费用由中标方承担。

(1) 故障响应及处理：

- a. 对系统性能严重损坏，接到支持需求必须立即做出回应；

b. 对系统运行正常，仅受到有限的影响或未受到严重影响，接到支持需求必须在 30 分钟内做出回应；

(2) 服务工程师：技术维保工程师应具备上述维保对象的硬件系统、软件系统、管理及操作系统等方面的知识，具备相应的技术资格认证，并有 3 年以上从业经验；

(3) 产品升级：提供产品升级评估和升级服务。

5. 数据库系统维护基本内容

提供 ORACLE 数据库系统 7X24 小时电话技术支持服务。当用户遇到紧急事故，或者系统迁移、安装等重大问题，通过前期电话沟通后，在最短的时间内派出具有 ORACLE 认证的现场技术支持工程师（OCP 认证级别及以上）在 30 分钟内到达用户现场，为用户提供现场技术服务。

(1) 系统安装、优化服务

为用户提供 ORACLE 数据库软件的安装、配置服务，在系统环境满足 ORACLE 安装需求的前提下，保证数据库系统能够正确安装、配置，直至能够交付用户正常使用。

根据用户需要，为用户指定的 ORACLE 数据库服务平台，进行系统级和数据库级的调优工作：专业技术人员根据系统环境（硬件配置、操作系统、数据库系统），以及多年的系统和 ORACLE 的实践经验进行调优工作。

(2) 系统检查服务

每季度指定具有 ORACLE 认证的专业技术人员到用户现场进行对 ORACLE 数据库系统进行检查（例如：ORACLE 表空间使用状态、ORACLE 警告日志、数据备份执行情况…等等）。同时巡检工程师负责向客户提供现场咨询服务，咨询范畴包括硬件配置、应用软件性能分析/合理化建议等。

(3) ORACLE 数据库升级服务

在厂商必要的补丁或升级产品推出后，为用户提供升级资讯。在接到用户 ORACLE 数据库升级需求后，派出具有 ORACLE 认证的现场技术支持工程师将用户的 ORACLE 数据库软件升级至最佳版本。

(4) 数据迁移服务

根据用户的数据迁移需求，派出具有 ORACLE 认证的现场技术支持工程师，将原系统的数据移植到新系统上的 ORACLE 数据库之中，并保证数据的完整性和可用性。

(5) 数据库备份与恢复服务

在用户数据库系统第一次安装完毕时，在现场为用户制定备份策略、搭建数据备份系统；在用户数据库系统遇到重大问题时，30 分钟内到达用户现场进行系统恢复；

(6) 数据库故障应急服务

当用户的数据库系统出现各种意外情况(如系统崩溃、硬件损坏、电源掉电等)造成数据库不能正常使用情况,在接到用户故障电话后 30 分钟内,派出具有 ORACLE 认证的专业技术工程师将到达用户现场,进行故障的分析、排查,并最终保证其恢复可用(在用户严格按照既定的备份策略执行的前提下,保证数据不丢失)。

6. 定期现场巡检服务

每季度对数据中心进行全面检查的服务项目,通过该服务可使客户获得设备运行的第一手资料,最大可能地发现存在的隐患,保障设备稳定运行。同时,有针对性地提出预警及解决建议,能够提早预防,最大限度降低运营风险。

巡检包括但不限于以下内容:

机房环境内容巡检,定期对机房的温湿度监控设备、UPS 监控设备、消防监控设备等机房环境监控设备的温湿度、电压、电流、烟雾等关键工作指标进行例行监控,当发生异常情况时,及时进行跟踪和处理。

机房设备硬件情况巡检,机房网络情况巡检,对整个网络健康状态进行分析,定期对各网络安全设备的 CPU 利用率、内存利用率、磁盘利用率、端口流量、报警信息等关键工作指标进行例行监控,当发生异常情况时,及时进行跟踪和处理;网络及安全设备配置管理、网络系统流量分析、网络及安全设备日志分析、软件升级。

机房主机安全巡检,利用现有的漏洞扫描设备全网扫描、分析上述系统的安全漏洞,及时发现安全隐患,备份系统日常维护,状态检查,故障处理等。

服务器操作系统、应用系统、数据库安全巡检,存储及磁带库数据安全巡检。

机房信息变动情况收集整理、文档更新。

7. 信息安全服务

包括以下五个方面: 1) 根据浙江省和温州市信息安全工作要求对温州市档案局管辖的包括业务系统、服务器、网络设备、安全设备等所有信息系统资产在内的信息系统进行信息安全风险评估;

2) 对温州市档案馆的信息系统进行全面梳理,协助温州市档案馆依据信息系统的现状完成等级保护相关工作; 3) 定期提供业务系统服务器漏洞扫描、对外服务网站应用层漏洞扫描、网页防篡改状态检查、互联网安全保护技术状态检查、业务系统服务器恶意代码防范工具状态检查、个人终端漏洞扫描测试,并协助温州市档案馆对发现的问题和漏洞进行修复; 4) 对温州市档案馆提供安全防范技术措施落实情况核查与优化、应急预案建设与演练、公众服务系统安全检测、安全培训等安全服务; 5) 完成上级主管部门信息安全检查所需要的相关工作。

项目内容明细及要求

安全目标

根据温州市档案馆信息系统网络、应用及数据等方面安全需求，针对保护目标及结合等级保护基本要求，通过安全评估、安全巡检、协助加固、应急响应等服务，针对服务实施前与实施后防护效果进行打分，能够直观地、具体量化地展现安全服务效果和服务价值，有效降低网络安全和数据库安全风险。

安全服务内容

7.1 信息系统安全风险评估

通过人工安全评估服务从多角度审查，全面模拟黑客的方式评估信息系统的安全状况，识别安全威胁与脆弱性，分析与监管要求的差距，出具分析报告和改善方案。评估范围包括组织范围，比如某些部门；物理范围，比如机房、办公区域等；系统范围，比如主机、数据库、中间件、网络设备、安全设备、重要信息系统、相关管理制度等。安全评估内容应包含网络架构安全评估、主机系统安全评估、数据安全评估、应用安全评估及整体安全策略评估五大块内容。

具体要求包括：

网络架构安全评估：包括结构安全与网段划分评估、网络访问控制评估、接入访问控制评估、网络安全审计评估、边界完整性检查评估、网络入侵防范评估、恶意代码防范评估、网络设备自身防护评估。

主机系统安全评估：包括身份鉴别、自主访问控制、安全审计、系统保护、剩余信息保护、恶意代码防范、资源控制等方面评估。

数据安全评估：包括数据保护评估、数据完整性评估、数据保密性评估、安全备份评估。

应用安全评估：包括身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、软件容错、资源控制、代码安全等方面。

整体安全策略评估：依据物理安全、网络安全、主机安全、应用安全、数据安全等五个方面评估结果，同时考虑在信息安全管理体系统等其他互补因素，然后进行全面的整体安全策略有效性评估。评估结果作为后期加固依据。

服务频率：1年1次

交付物：《xx系统风险评估报告》

7.2 漏洞扫描服务

采用扫描工具结合人工验证对本项目的信息系统进行脆弱性评估，获得应用、数据库、系统、设备等漏洞对应及分布情况，并提供可操作的安全建议，并进行安全加固。

漏洞扫描所采用的工具须满足以下条件：

具有计算机软件著作权登记证书；

具有兼容性资质证书；

软件产品登记证书；

涉密资质产品检测证书；

服务周期：一年，4次。

交付物：《xx系统漏洞扫描报告》。

7.3 安全检查服务

人工结合工具对服务范围的网络设备、主机设备、操作系统、数据库、应用中间件等进行设备安全配置、主机配置、数据库配置、应用配置等方面的安全基线检查。根据检查结果提出整改建议，协助运维管理人员开展整改工作。

服务周期：一年，1次。

交付物：《xx安全检查报告》。

7.4 7*24小时日志分析服务

定期对内网全网日志中的高级别日志进行分析，对安全事件进行溯源、满足《网络安全法》日志存储不少于6个月的要求，并出具分析报告。结合人工方式，利用综合日志审计平台、设备、系统自身的日志数据进行综合分析，判断网络、操作系统、应用中间件、网络安全设备等资产的整体运行情况、安全状况等，直观展现上述内容给用户，提出整改意见，帮助整改。

服务周期：一年，2次。

交付物：《全网日志分析报告》

7.5 协助安全加固服务

根据各类安全评估结果的具体情况，制定服务目标的整改加固建议。针对不同类型的目标系统，协助进行安全加固处理，合理加强服务目标的安全性。完成整改后开展复查工作。

服务周期：一年，2次。

交付物：《xxx加固方案》、《xxx加固报告》。

7.6 应急预案与应急演练

依据实际情况为作为温州市档案馆信息系统建立网络安全应急预案，组织网络安全事件应急相关人员在有计划及受控制的情况下，依据预先制定的网络安全应急预案执行可预见的减少信息系统停顿、失败或灾难影响的预案措施。使相关人员熟悉应急响应、处置过程，尽可能消除信息系统所出现的中断，保护系统免受重大故障或灾难的影响，

缩短系统中断的恢复时间。

服务周期：至少一年 1 次。

交付物：《XX 网络安全应急预案》、《XX 网络安全应急演练报告》。

7.7 应急响应服务

网络没有绝对的安全，在确保安全设备合理部署及安全服务保障情况下，具备 365*24 小时的应急响应服务。如单位网络管理员或系统管理员根据初步判断认为和安全事件相关，通过电话咨询服务商安全专家，安全专家再根据安全事件级别进行应急响应，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。安全事件包括但不限于：病毒和蠕虫事件、黑客入侵事件、内容篡改事件、信息泄漏事件等。

服务时间：365*24 小时。

交付物：《应急事件处理报告》。

7.8 安全培训服务

为协助温州市档案馆提高内部人员的安全意识、安全技术能力及安全管理能力等，针对管理和技术两个层面制定阶梯性人员能力培训计划，通过安全培训使相关人员的安全能力有明显提升。培训讲师需具有至少一项信息安全专业资质，如 CISSP、CISP、ISO 27001 LA、等级保护测评师认证资质。

服务周期：2 次。

交付物：《xx 培训大纲》、xxx 培训 PPT。

7.9 新系统上线测试

提供新业务系统上线安全测评服务，识别新系统主机、中间件、数据库、应用等潜在安全风险，针对发现的安全隐患制定有效处置方案，降低新业务系统风险系数，建立一体化新业务安全检测体系，检测数据成果作为新上线安全建设参考依据。

新系统上线安全检测具体要求：

对新业务系统系统进行主机漏洞扫描，以发现目标新业务系统系统的全弱点为目标。

对新业务系统中指定网页范围进行新业务系统高危脚本漏洞挖掘验证，包括 SQL 注入、XSS 攻击、恶意执行逻辑错误等典型脚本漏洞信息。

对新业务系统进行网络安全脆弱性检测。

对新业务系统进行渗透测试。

服务频率：按照实际客户需求，不超过 2 次

交付物：《新上线系统安全评估报告》

7.10 重要时刻值守服务

在重大节假日、重大活动期间，提前进行信息系统安全专项检测，并提交检测报告。当用户认为必要时，重大割接或其它任何客户认为可能对其业务运营产生重大影响时刻，提供 7*24 小时的现场值守服务。

7.11 安全服务的要求

- 1、提供 7*24 小时的技术支持（包括电话咨询与现场服务）。
- 2、在接到电话后，必须在 10 分钟内响应，30 分钟内必须到达温州市档案馆现场。
- 3、每次对系统进行安全评估、安全扫描、渗透测试、安全加固之前必须先提供相应的技术方案与业主方技术人员充分沟通，以确保系统的安全运行。

- 4、实施过程中应尽可能小的影响系统和网络的正常运行，做好备份和应急措施，不能对温州市档案馆系统内的应用系统的正常运行产生影响，包括系统性能明显下降、网络拥塞、服务中断等，如无法避免出现这些情况应先停止项目实施，并向业主方书面详细描述。

- 5、所使用的信息安全类工具软件（包括 web 应用安全评估系统、数据库安全评估软件系统、远程安全检查工具、大数据分析平台等）必须为正版产品，并进行详细说明。

- 6、项目服务过程的数据和结果数据严格保密，未经业主方授权，任何机构和个人不得泄露给其它单位和个人。

- 7、协助业主方完成各项年度安全检查工作。

- 8、服务提供商必须签订保密协议，做好相关信息数据保密工作，承担保密责任。不得对外透露与用户相关的设备、网络和系统信息，不得复制与用户相关的数据和信息，不得以任何方式和渠道向外界传递、泄露、披露任何信息数据。

8. 虚拟化运维服务

此项服务主要涵盖故障排除、日常巡检、性能检查及优化、数据安全保护、产品培训等多个方面。

日常巡检及检查优化方面，结合用户历史数据及原厂商工具，预测分析用户虚拟化平台未来的业务增长情况，及时发现潜在问题，避免资源过度使用及不足等情况的发生。

数据安全保护主要为用户提供虚拟化平台的集中备份与恢复方案、协助用户进行数据迁移及应急预案的制定。

网络安全上帮助用户解决虚拟化平台上虚拟机之间流量互通带来的安全威胁，进行端口隔离，实施基于主机的虚拟防火墙，对访问流量进行控制。

9. 备品备件服务

提供备品备件服务，服务器、存储、交换机、安全设备等核心硬件产品备件，当设

备故障可提供备品备件以保障应用稳定运行。对所有运维设备的故障件均给予技术支持，维修前须提供备品备件。在发生故障的情况下能迅速提供备机并且备机系统能够正常接管生产机的工作，保证业务不停止。

10. 容灾演练

服务期内不少于一次核心系统灾难备份及恢复的应急演练

11. 设备租赁服务

11.1 安全感知平台 1 套

在重大节假日、重大活动期间、信息系统安全专项检测期间或用户认为必要时提供 1 套集检测、可视、响应处置于一体的大数据安全分析平台，让安全可感知、易运营。产品以大数据分析为核心，结合了威胁情报、UEBA、机器学习、失陷主机检测、大数据关联分析、NTA 流量分析、可视化等技术，对全网安全进行可视，帮助用户看清业务、看到威胁、看懂风险，并辅助用户决策。

四、维护确认与验收

1. 维护人员

甲乙双方指派专人组成本合同维护项目的管理小组，管理和实施本项目。管理小组成员名单和通讯方式见附件 2。双方可以根据具体情况更换本方管理小组的成员，但应当以书面方式通知另一方；如乙方重新指定的小组成员涉及到本项目的重要方面，应当事先征得甲方的同意。双方应当在合理和维护双方利益的基础上讨论人员更换事宜。参与项目的所有人员都应当受本合同第八条款的约束。

2. 维护确认

(1) 维护确认一般每月或者每季度进行一次。维护确认前，乙方应当根据附件中的检验规格和标准，对维护项目进行功能和运行检验。乙方应当在每次维护确认前 2 个工作日内，以书面方式提请甲方按照合同及其附件所约定的内容进行维护确认。重大维护内容发生后，乙方可以及时以书面方式提请甲方进行维护确认。提请对应用软件维护项目进行维护确认的，乙方还应当提交相应的软件维护文档，所提交的文档应当包括纸质版和电子版各一份。

(2) 甲方应当在接到乙方书面材料的 2 个工作日内进行维护确认。如甲方无正当理由而不进行维护确认，则视为甲方已经确认。双方对此另有约定的除外。维护确认的内容包括系统故障现象、原因、故障排除过程、更换配件情况、恢复状况等。

3. 验收

(1) 维护项目按合同规定完成后，甲方应当及时进行验收。乙方应当以书面方式向甲方递交维护项目验收通知书，甲方在收到验收通知书后的 3 个工作日内，确定具

体日期，由双方按照本合同规定的验收标准完成验收，验收标准见附件。甲方有权委托第三方机构进行验收，对此乙方应当配合。

(2) 如属于乙方原因致使维护项目未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长5个工作日，直至符合验收标准。

(3) 如由于甲方的原因致使维护项目未能通过验收，甲方应当在5个工作日内排除故障，之后7日内再次进行验收。

五、价格与付款方式

1. 价格

本维护项目的总价为 737000 元，大写：人民币柒拾叁万柒仟元整。

2. 付款方式

(1) 合同签订并具备实施条件后 7 个工作日内，甲方向乙方支付合同总价的 50% 作为预付款；完成全部维保服务内容并通过验收后 7 个工作日内支付合同总金额 50% 的合同尾款。

(2) 甲方付款前，乙方应向甲方开具等额有效的增值税发票，甲方未收到发票的，有权不予支付相应款项直至乙方提供合格发票，并不承担延迟付款责任。发票认证通过是付款的必要前提之一。

六、义务与责任

1. 甲方

(1) 甲方应当向乙方提供必要的工作条件，包括必要的技术资料、技术准备，协助乙方做好维护服务。

(2) 甲方应当保证其要求乙方维护的软件、硬件以及相关的文档未侵犯第三方知识产权。

2. 乙方

(1) 乙方保证维护工作的过程未侵犯第三方合法权益。

(2) 经乙方维护更新后的软件，其任何部分如被依法认定为侵犯第三方合法权利，或者任何由乙方授予的权利被认定为侵权，乙方应当承担相应的责任，并尽力用同等功能的合法软件替换该软件，或者取得相关授权，以使甲方能够继续享有本合同所规定的各项权利，并且乙方应当赔偿甲方由此而造成的损失。

(3) 乙方所承担的维护项目的质量标准应当符合国家标准、行业标准或者制造企业的标准。若无国家标准、行业标准或者制造企业的标准的，以符合合同目的的其他标准作为质量标准。除此之外还应当符合温州市有关安全、环保、卫生等有关规定。

(4) 乙方不得将本合同项目的部分或者全部维护工作转包给第三方承担。

七、所有权、知识产权和使用权

1. 所有权

本合同中所列硬件设备，不论维护前还是维护后，其所有权均归甲方所有。

2. 知识产权

合同中所列应用软件的知识产权归甲方所有，另一方非经对方同意，不得以任何方式向第三方披露、转让，除本项目维护需要外，不得以任何方式进行商业性利用。

3. 使用权

甲方拥有合同中所列产品软件的正版使用权，乙方仅可在与项目有关的维护工作中使用，任何情况下不得以复制或者其他方法供自己使用或者提供给第三方。

甲方使用乙方提供的第三方软件，应当依照乙方与第三方对该软件使用的约定进行。乙方应当将该约定的书面文件的原件交甲方核对，复印件交甲方存档。

八、保密

1. 信息传递

在本合同的履行期内，任何一方可以获得与本项目相关的对方的保密信息，对此双方皆应谨慎接受并不得向第三方披露。

2. 信息披露

获取对方保密信息的一方仅可将该信息用于履行其在本合同项下的义务，且只能由相关的工程技术人员使用。获取对方保密信息的一方应当采取适当有效的方式保护所获取的信息，未经授权不得使用、传播或者公开。除非有对方的书面许可，或者该信息已被拥有方认为不再是保密信息，或者已在社会上公开，该信息不得对外披露。如因乙方原因导致甲方数据泄露，给甲方造成不良影响或损失，将依法追究乙方的法律责任。

3. 保密措施

甲乙双方同意采取相应的安全措施，遵守和履行上述约定。经双方协商，一方可以检查对方所采取的安全措施是否符合上述约定。

九、服务变更

1. 甲方如提出部分维护项目的变更建议，应当以书面形式提交给乙方。乙方应当在5个工作日内，对该变更后合同价格、服务内容、系统性能、技术参数等可能发生的变化作出预估，并书面回复甲方。

2. 甲方在收到乙方回复后，应当在5个工作日内，以书面方式通知乙方是否接受乙方回复。如甲方接受乙方回复，则双方可对该变更以书面形式予以确认，并按变更后的约定继续履行本合同。

3. 乙方如提出部分维护项目的变更建议，应当对该变更后合同价格、服务内容、系

统性能、技术参数等可能发生的变化作出预估，并以书面形式提交给甲方。

4. 甲方在收到乙方的变更建议后，应当在5个工作日内，以书面方式通知乙方是否接受乙方的变更建议。如甲方接受乙方的变更建议，则双方可对该变更以书面形式予以确认，并按变更后的约定继续履行本合同。如甲方不同意乙方的变更建议，则乙方应当按原合同执行，但由此产生的信息系统的风险以及其他相关风险由甲方承担。

十、不可抗力

1. 由于台风、水灾、火灾、地震等不可抗力因素，直接影响本合同的履行或者不能按照合同的约定履行时，可以免除遇有不可抗力的一方的相关合同责任。但遇有不可抗力的一方应当及时通知对方，并在15日之内提供不可抗力的详细情况及合同不能履行或者部分不能履行或者需要延期履行的理由和有效的证明文件。甲乙双方根据不可抗力因素对合同履行的影响程度，协商决定是否解除合同，或者部分免除履行合同的义务，或者延期履行合同。

2. 遇有不可抗力的一方，应当尽可能地采取必要的措施减轻不可抗力对本合同的履行所造成的影响。由于未采取适当措施致使另一方损失扩大的，不得就扩大损失的部分要求免除本方责任；由于未采取适当措施致使本方损失扩大的，也不得向对方要求赔偿。

十一、违约责任

1. 如乙方未按合同约定完成维护项目，除依照以下约定支付违约金外，甲方有权要求乙方赔偿损失：

(1) 定期维护每延期5日，乙方应当向甲方支付合同总价0.5%的违约金，但违约金的总数不超过合同总价的5%；

(2) 定期维护延期超过10日或者延误维护确认10次，甲方有权解除合同，并要求乙方赔偿损失。

2. 如甲方未按合同约定的期限付款，每延期15日，甲方应当向乙方支付合同总价0.5%的违约金，但违约金的总额不超过合同总价的5%；如延期付款超过30日，乙方有权解除合同，并要求甲方赔偿损失。

十二、争议解决

本合同发生争议的，由双方协商解决，也可按下列方式解决。

依法向甲方所在地的人民法院提起诉讼。

十三、合同的生效

1. 本合同经双方各自指定的代表签字并盖章后生效。

2. 本合同一经签署，未经双方同意，任何一方不得随意更改。本合同所列的附件经双方代表签字并盖章后成为本合同的组成部分。

3. 本合同一式四份，双方各执二份，具有同等法律效力。

十四、名词解释

1. 维护

维护是指为保障信息系统的正常运行和使用，对其中软件、硬件等进行的检查、维修、备份以及改正错误、提高性能等相关工作。

2. 维护确认

维护确认是指甲方对乙方依照合同对维护工作内容进行确认的行为。

3. 业务应用系统

业务应用系统是指按甲方业务需求，由乙方或者第三方定制开发的计算机应用软件系统。

4. 产品软件

产品软件是指甲方向乙方或者第三方购置的成熟的商品化软件，包括操作系统、数据库、开发工具、中间件软件、安全软件、办公自动化软件、专业应用软件等。

5. 保密信息

保密信息是指甲乙双方各自所拥有的不为公众所知的管理信息、方式方法、产品信息、计算机源代码、技术文档和技术资料等，或者由甲乙双方在履行本合同过程中明确指明为保密的合法信息。

6. 规格

规格是指在技术或者有关维护服务任务上所设定的关于硬件和软件的技术标准、规范。

十五、其他

1. 如一方改变通讯地址，应当提前以书面方式通知另一方。

2. 本合同未尽事宜，双方可以另行协商，商定内容经双方代表签字并盖章后与本合同具有同等效力。

十六、项目合同签章

甲方：

法定（委托）代表人（签字）：

电话：

传真：

地址：温州市府西路 81 号

日期：2024年8月5日

乙方：

法定（委托）代表人（签字）：

电话：

传真：

地址：温州鹿城南汇街道惠民路 666 号

日期： 年 月 日

附件一 维护清单

数字档案馆一期					
项目	设备名称	品牌型号规格	数量	设备位置	服务期限
1	数据库服务器	HP 580G7	2	设备机房	一年
2	应用服务器	HP 380G7	3	设备机房	一年
3	磁盘阵列	HP EVA6400	1	设备机房	一年
4	SAN 交换机	HP 8/24	2	设备机房	一年
5	磁带库	昆腾 I80	1	设备机房	一年
6	数据链路安全审计网关	深信服 WOC-2050-PLC	1	设备机房	一年
7	刀片机箱	HP C3000	1	设备机房	一年
8	RFID 无线条码管理系统设备	北京汉龙	1	1 楼中控室	一年
				2 楼查阅大厅	一年
				5 楼库房	一年
数字档案馆二期					
项目	设备名称	品牌型号规格	数量	设备位置	服务期限
1	数据库服务器	HP BL680cG7	2	设备机房	一年
2	业务服务器	HP BL460G7	2	设备机房	一年
3	磁盘阵列	HP EVA6400	1	设备机房	一年
4	光纤交换模块	HP B-series 8/24c BladeSystem	1	设备机房	一年
5	网络交换模块	HP Flex-10	2	设备机房	一年
6	磁带库	HP MSL8096	1	设备机房	一年
7	防火墙	天融信 TG-5114	1	设备机房	一年
8	日志审计系统	思福迪 (主机 logbase-H530,	1	设备机房	一年
		探测器 logbase-NS1000)			一年
9	上网流控及审计系统	深信服 AC2000	1	设备机房	一年
数字档案馆三期					
项目	设备名称	品牌型号规格	数量	设备位置	服务期限
1	数据库服务器	HP DL580G7	2	设备机房	一年
2	文件存档服务器	HP DL388p	1	设备机房	一年
3	防火墙	北京网御星云 powerv426	1	设备机房	一年
4	路由器	杭州华三 RT-SR6602-X1	1	设备机房	一年
登记备份项目					
项目	设备名称	品牌型号规格	数量	设备位置	服务期限
1	登记备份数据库服务器	HP DL580	1	设备机房	一年

2	登记备份应用服务器	HP DL380	3	设备机房	一年
3	在线备份前置机	HP DL380	3	公积金	一年
				设备机房	一年
				设备机房	一年
4	SAN 交换机	HP SAN Switch	2	设备机房	一年
5	主存储磁盘阵列	HP EVA6400	1	设备机房	一年
6	核心交换机	华为核心交换机 S9306	2	设备机房	一年
7	防火墙	网域星云 power v-3000	1	设备机房	一年
8	IPS	网域星云 power v-520IPS	1	设备机房	一年
9	VPN 接入、广域网加速设备	深信服 WOC-2050-W	3	公积金	一年
				设备机房	一年
				设备机房	一年
10	安全审计可信网关	深信服 SSL VPN-3050-S	1	设备机房	一年
11	漏洞扫描系统	启明星晨天镜脆弱性扫描系统	1	设备机房	一年
12	UPS	易事特 UPS- EA9960 (主机)	1	动力机房	一年
13	磁带库	HP MSL 4048	1	设备机房	一年
馆际一体化项目					
1	业务服务器	HP ProLiant BL660c Gen8	1	设备机房	一年
2	互联网业务服务器	HP DL380p Gen8	3	设备机房	一年
3	多媒体应用服务器	HP DL380p Gen8	1	设备机房	一年
4	多媒体管理服务器	HP DL380p Gen8	1	设备机房	一年
5	互联网磁盘阵列	HP MSA 2040 双控制器存储	1	设备机房	一年
6	网页防火墙 WAF	绿盟 WAFNX3-CH540 京	1	设备机房	一年
7	VPN	深信服 VPN 6050	1	设备机房	一年
8	IPS	绿盟 NIPSNX3-N1000A-C	1	设备机房	一年
9	准入控制系统	盈高 ASM4000-CS	1	设备机房	一年
信息化设备和大楼中控集成项目					
1	存储设备	OceanStor 5210 V5	1	设备机房	一年
2	数据库服务器	2288H V5	2	设备机房	一年
3	应用服务器	2288H V5	2	设备机房	一年
4	核心交换机	S7703	2	设备机房	一年
5	日志审计	LogBase-AH1000S	1	设备机房	一年
6	堡垒机	LogBase-BH1000S	1	设备机房	一年
7	大楼监控系统	海康威视 (90 个摄像头、13 个门禁及配套设备)	1	设备机房	一年
8	大楼中控系统	易事特 (主机 1 台、温湿度感	1	设备机房	一年

		应器 20 个、配套设备)			
9	音视频转码设备	TYST-5000ST	1	设备机房	一年
其它服务					
1	常驻人员服务		1		一年
可添加服务					
1	统一运维服务平台 (万国软宝 ITOSS 2000)	集成 IT 网管和机房动力环境功能, 统一界面; 支持机房动力环境、机房链路、网络设备、服务器、数据库、应用系统等监控; 使用专用硬件平台, 内置防火墙模块、数据库。100 个许可 License, 不分监测类型。	1	设备机房	一年
2	资产管理软件 (索思资产管理信息系统软件 V2.0)	提供一套信息类设备统计管理软件, 详细调查并记录服务范围内的各个设备的种类、型号、功能、物理位置、端口对应情况、部署情况等资产信息, 并能录入管理系统。在管理硬件资产的同时, 能对 IP 地址、虚拟化资源、配置文件等进行管理。通过图形化的界面, 能准确知道 IP、应用、服务器 (物理或虚拟机)、机柜、网络接口、业务负责人之间的一一对应关系。	1	设备机房	一年
3	应用管理平台 (深信服 VDC+aDesk-STD-100+虚拟机管理软件 VMS)	设备的运维和服务管理都通过这一平台, 有效杜绝非法用户直接访问, 同时可以接管“统一运维服务平台”, 有授权情况下可以查看数据中心设备的运行情况, 终端故障不影响平台正常使用。配置含 1 套控制器+2 套固定终端+配套虚拟化软件, 要求瘦终端、控制器、虚拟化软件统一平台管理, 以保证兼容性和售后服务一体化;	1	设备机房	一年
7X24 小时技术支持服务					
项目	设备名称	品牌型号规格	数量	设备位置	服务期限
1	数据库系统软件	Oracle11g 企业版	3	设备机房	一年
2	中间件系统软件	Weblogic 企业版, 1CPU 授权	1	用于软件开发	一年

3	备份软件	SYMC NETBACKUP ENTERPRISE SERVER 7.0	3	设备机房	一年
4	虚拟化软件	VMware vSphere 5.0	1	设备机房政务网刀箱服务器	一年

附件二、项目维护小组

姓名	本项目主要工作	年龄	性别	专业
陈贵之	项目管理	33	男	信息管理和信息系统
陈辉	项目管理	41	男	软件工程
彭涛	网络设备服务	28	男	计算机科学
叶东亮	网络设备服务	27	男	计算机网络技术
刘侠	网络设备服务	28	女	计算机网络技术
周科常	网络设备服务	29	男	计算机网络技术
赵汉利	网络设备服务	31	男	计算机应用
翁向高	运维服务	33	男	计算机科学
邹志远	运维服务	27	男	计算机科学
蒋建平	数据库服务	30	男	计算机网络技术
胡齐辉	数据库服务	24	男	计算机应用
李克祥	软件维护服务	29	男	自动化
金莉卷	软件维护服务	30	女	计算机科学和技术
黄俊涛	驻点服务	24	男	计算机应用