**公开招标文件**1、投标人基本资格条件：

投标人需具备《中华人民共和国政府采购法》第二十二条规定的基本资格条件，并提供以下资格证明文件：

（1）法人提交企业法人营业执照副本(或者法人登记证书)以及组织机构代码证副本复印件；

（2）依法缴纳税收和社会保险费的证明材料,各提供下列材料:

①缴纳税收证明资料:《税务登记证》复印件，或者近三个月依法缴纳税收的证明（纳税凭证复印件），或者委托他人缴纳的委托代办协议和近三个月的缴纳证明（收据复印件），或者法定征收机关出具的依法免缴税收的证明原件。

②缴纳社会保险证明资料：《社会保险登记证》复印件，或者近三个月依法缴纳社会保险的证明（缴费凭证复印件），或者委托他人缴纳的委托代办协议和近三个月的缴纳证明（收据复印件），或者法定征收机关出具的依法免缴保险费的证明原件。

（3）法人提交法定代表人身份证明原件或者法定代表人授权委托书原件并附法定代表人身份证明原件，自然人提交身份证复印件；

（4）投标人具有实行了“三证合一”登记制度改革的新证并提交的，视同为持有并提交了工商营业执照、组织机构代码证和税务登记证，符合基本资格条件的相关条款。

2、投标人特定资格条件：

（1）投标人应是《全国网络安全等级保护测评机构推荐目录》中的单位

**评审因素和标准**

|  |
| --- |
| **评标方法及标准** |
| **评审因素** | **分值** | **评分标准** |
| 价格 | 25分 | 投标人的报价得分=(评标基准价/投标报价)×100×25%满足磋商文件要求且投标价格最低的投标报价为评标基准价,其价格分为满分。 |
| 商务部分（25分） | 资质能力 | 10分 | 投标人具有全国网络等级测评推荐机构证书的计2.5分, 具有国家计算机网络应急技术处理协调中心颁发的“网络安全应急服务支撑单位证书（省级）计2.5分。（提供证书复印件并加盖公章） |
| 投标人具有ISO9001质量管理体系认证和ISO27001信息安全管理体系认证的每个计2.5分，最高计5分。（提供证书复印件并加盖公章） |
| 同类业绩 | 5分 | 投标人提供2018年以来三级医院等保测评案例，每个计1分，最多5分。（须提供加盖投标人公章的项目合同首、尾、关键页；未提供合同复印件的，不予计分） |
| 本地服务能力 | 5分 | 投标人在湖南省本地设有服务机构的计5分；承诺中标后在湖南省成立服务机构的计2分（须提供湖南省的工商注册证明文件复印件或承诺函原件）。 |
| 售后服务 | 5分 | 售后服务方案内容完整，有完善的售后服务体系，有售前、售中、售后专职协调人员与服务保障人员，能提供良好的本地化服务，服务措施具体，响应时间短，分档计分，服务方案优的计5分，良的计4分，一般的计3分，未提供的不计分。 |
| 技术部分（50分） | 等保实施方案 | 10分 | 以磋商文件的技术要求为基准，应详细描述项目实施中涉及到的各个方面，包括测评项、测评方法、测评工具、人员安排、安全域划分拓扑图、项目分工界面、现场实施工作表单，符合等保工具测试要求的接入点示意图等。分档计分：方案完整、合理的计10分，方案较完整、较合理计5分，方案一般计3分，方案差或未提供的不计分。 |
| 技术实力 | 20分 | 1. 投标人自2018年以来在全国网络安全等级保护测评机构攻防大赛上获得一等奖的计5分，二等奖计3分，三等奖计1分。（提供相关证明复印件并加盖公章否则不计分）

2、投标人具有中国网络安全审查技术与认证中心颁发信息安全服务资质认证证书（信息系统安全运维）计5分。（提供证书复印件并加盖公章）3、投标人实施人员具有高级信息安全等级测评师且通过商用密码应用安全性评估人员测评能力考核证书的,计5分，任何一项不满足的扣3分，扣满5分为止（提供证书复印件和相关人员在投标单位近三个月的社保证明）。4、投标人拟派往本项目的项目经理同时具有高级信息安全等级测评师资质的计5分。（提供证书复印件和相关人员在投标单位近三个月的社保证明材料，并加盖投标人公章，否则不计分） |
|  | 安全运维 | 20分 | 1、安全巡检服务方案 有完善的安全巡检方案，且保障每年4次以上现场巡检计5分，任何一项不满足的扣3分，扣满5分为止2、安全加固服务方案 有完善的安全加固方案，且有专门技术人员对甲方设备进行安全加固计5分，任何一项不满足的扣3分，扣满5分为止3、应急响应服务方案有完善的安全响应服务方案，且安排有专人全天候应急处置计5分，且能任何一项不满足的扣3分，扣满5分为止4、安全培训方案 有完善的安全培训方案且能提供院级培训和信息科专业培训的计5分，任何一项不满足的扣3分，扣满5分为止 |
| 合计 | 100 |  |
|  |  |  |

**第三章项目需求**

## 一、项目名称：

项目名称一：浏阳市人民医院信息系统安全等级保护测评服务项目

项目预算：人民币万元，超预算投标为无效投标。

项目名称二：浏阳市人民医院安全运维项目

项目预算：人民币万元，超预算投标为无效投标。

## 二、项目概述：

根据《中华人民共和国网络安全法》的要求，国家实行网络安全等级保护制度，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合转发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）强调了开展信息安全等级保护工作的重要意义，规定了实施信息安全等级保护制度的原则、内容、基本要求和实施规划。卫生部《湖南省卫生行业信息系统信息安全等级保护实施方案 》（湘卫办发[2012]28号）、《关于印发<长沙市卫生计生行业信息系统安全等级保护工作实施方案>的通知》（长卫发【2018】27号）等文件对卫生行业做出了具体的要求。

为落实上述国家与卫生主管部门的政策要求，本项目拟对浏阳市人民医院 4个医院业务系统开展一次网络安全等级保护测评工作，通过全面深入的等级保护测评，进一步了解我院医院业务系统安全等级保护工作的现状，明确这批系统当前的等级保护差距和系统所存在的安全风险，并针对存在的差距与问题及时进行安全整改建设，通过测评与整改提高相关业务系统的信息安全保障能力，并取得长沙市公安行政主管部门核发的等级保护备案证明。

**三、项目采购内容一**

本次采购项目拟选定一家从事信息安全测评工作的专业机构对浏阳市人民医院5个医院业务系统提供全面深入的网络安全等级保护测评工作，根据测评中发现的等级保护差距和安全问题，提出安全整改建议方案，对安全整改过程提供咨询服务，并帮助我院最终取得当地公安行政主管部门的信息系统安全等级保护备案证明。

**1．测评对象：**

本项目信息安全等级保护测评服务对象如下表所列：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 信息系统名称 | 第一级 | 第二级 | 第三级 | 第四级 | 第五级 |
| 1、医院信息系统 |  |  | ■ |  |  |
| 2、医学影像信息系统 |  |  | ■ |  |  |
| 3、电子病历系统 |  |  | ■ |  |  |
| 4、互联网医院 |  |  | ■ |  |  |
| 信息系统数量 | 0个 | 0个 | 4个 | 0 个 | 0个 |
| 信息系统总数 | 4个 |

**2．测评内容及要求：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务****类别** | **服务子项** | **服务要点** | **交付****成果** | **备注** |
| 1、等级保护系统注册 | 协助等级保护定级备案 | 基于国家信息系统安全等级保护相关文件的要求，结合浏阳市人民医院的组织架构、业务要求、信息系统的实际情况，协助进行信息系统的等级评定。严格来讲共分为定级准备、摸底调查、初步定级、评审和审批、协助备案、定级总结等环节。 | 备案表、定级报告、专家评审意见表 | 各系统备案表与定级报告等材料送公安备案并获取备案证明扫描件 |
| 2、等级保护差距分析 | 对每个系统开展等级保护差距分析 | 一是单元测评：包含的内容包括信息系统安全技术（物理安全、网络安全、系统安全、应用安全、数据安全）和安全管理（安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理）十个方面的各个安全控制措施，涉及到71个单元测评，212个测评要求项。 | 信息系统等级保护问题清单或等级保护整改建议方案 |  |
| 二是整体测评：主要包括安全控制间、层面间和区域间相互作用的安全测评以及系统结构的安全测评等，主要是结合系统业务数据流分析不同区域和不同边界与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范是否恰当合理。 |
|  | 三是撰写系统等级测评报告：完成现场差距分析之后，整改项目组归纳整理、分析现场记录，找出目前信息系统与等级保护安全要求之间的差距，并进一步根据风险分析的结果进行调整，去掉不适用项，增加不能满足客户信息系统需求的安全要求，明确不符合项，生成《等级保护等保测评报告》。 |  |
| 等级保护整改咨询 | 整改方案设计和指导等级保护整改工作 | 依据上述等保差距分析与测评的结果，明确等级保护整改工作的工作目标，提出等级保护整改建议方案。开展安全建设整改实施方案的评审、产品选型等咨询工作。 | 评审意见、管理制度模板等咨询文档 |  |
| 指导业主、运维方或开发方进行技术和管理两方面的整改工作，包括指导系统安全加固，指导安全管理制度修订，对加固效果进行检验。 |
| 等级保护测评 | 等级保护回归测试 | 在提供等级保护整改建议方案后的半年内可负责对安全整改加固建设是否达到等保要求进行回归测试，并出具等级保护回归测试报告。 | 信息系统等级测评报告 | 每个系统出具一份等级测评报告。 |
| 等级保护备案 | 协助备案与迎检 | 协助客户完善等级保护主管部门备案所需要的文档和资料，并协助客户完成信息安全等级保护备案，配合迎接当地公安的系统备案现场检查，协助最终取得等级保护备案证明。 | 各个系统备案资料、等级保护备案证明 |  |

# 项目采购内容二：安全运维服务方案

## 资产梳理

### 资产调研

调查并纪录服务范围内各设备和系统的种类、型号、功能、物理位置、端口对应情况、部署情况等资产详细信息。

本次通过安全服务专业工具和工现场调研，输出《资产调研表》。

### 基础资料建档

利用资产调查的数据进行物理设备建档，绘制网络拓扑，统计信息点分布以及各硬件设备和软件系统的数量、拓扑位置、用途等信息。项目启动后有专业人员现场整理后，建立基础资料档案库。

**示例如下表：（包含但不限于此表格内容）**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备类型** | **设备名称** | **数量** | **部署位置** | **管理地址** | **备注** |
| 1 | 网络设备 | 路由器 |  | 出口 |  |  |
| 交换机 |  | 核心 |  |  |
| 2 | 安全设备 | 防火墙 |  | 出口 |  |  |
| IPS |  | 出口 |  |  |
| 3 | 计算设备 | 服务器 |  | 服务器区 |  |  |
| 小机 |  | 服务器区 |  |  |
| 4 | 存储设备 | 存储设备 |  | 数据存储区 |  |  |
| 备份设备 |  | 备份区 |  |  |

### 软件配置建档

利用资产调查的数据进行软件配置建档，记录软件系统的版本、用途、组件、配置、更新情况等信息，实现配置管理，建立软件安装媒介档案，建立服务器软件和升级包配置档案；

项目启动后有专业人员现场整理后，建立软件配置档案库。

### 资产赋值

识别和列出信息安全管理范围内被评估的业务环境、业务运营和信息相关的所有的资产，定义一个价值尺度并为每一项资产分配价值（机密性、完整性和可用性的价值）。输出《资产赋值表》。

### 服务流程

1）确定资产调研范围。

2）根据范围进行人工调研。

### 资产梳理交付物

输出《资产调研表》、建立硬软件资源档案库、《资产赋值表》。

## 安全巡检服务方案

### 巡检对象

信息系统安全巡检的对象主要包括服务器、数据库、中间件和应用。

操作系统（Windows类、Linux类、Unix类）；

数据库（包含但不限于SQL Server、MySQL、db2、Sybase、Oracle）；

中间件（包含但不限于IIS、tomcat、httpd、JBOSS、webloigc、webSphere）；

网络设备（包含但不限于交换机、路由器）。

各类应用服务账户（FTP、MySQL、MSSQL、NNTP、IMAP、RDP、Redis、PcAnywhere、rlogin、SMB、SMTP、SNMP、POP3、SSH、Telnet、VNC）等。应用软件。

### 巡检内容

巡检内容包括机房安全检查、网络架构安全检查、服务器异常情况检查、服务器病毒木马及webshell查杀、非法外联情况检查、安全设备日志分析、安全配置检查（包括服务器安全配置和网络设备安全配置）、漏洞扫描和渗透测试。

|  |  |  |
| --- | --- | --- |
| **工作内容** | **发现问题** | **工作描述** |
| 异常情况巡检 | 安全事件 | 按日常安全巡检表对重要对外服务器、网络设备、安全设备运行情况和异常情况进行日常巡检，对巡检中发现的安全问题进行加固。包括异常进程、异常帐号、异常流量、异常服务、异常端口、异常文件、异样启动项等。 |
| 安全日志分析 | 安全事件 | 随着网络规模的增长，用户网络中防火墙、防病毒软件、IDS、VPN等信息安全设备不断增加，庞大的日志数据令用户无从下手。各类系统产生的安全日志实现全面、有效的集中收集、管理、审计服务。查看安全设备日志，利用安全日志分析工具对服务器、网络设备、安全设备、应用系统日志进行统一分析。 |
| 服务器webshell查杀 | webshell | 使用工具对所有服务器进行webshell、木马病毒查杀。webshell是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。 |
| 安全漏洞扫描 | 安全漏洞 | 安全漏洞扫描是使用专门的漏洞扫描工具对被测信息系统进行全面的安全漏洞扫描。漏洞扫描是脆弱性识别的重要手段，能够发现信息系统中存在的严重漏洞，针对扫描结果并结合人工验证，将发现的应用系统漏洞、主机操作系统漏洞、数据库漏洞、逻辑缺陷、弱口令、信息泄露等脆弱性问题，形成漏洞扫描报告，通过对漏洞的修补完善，避免对信息系统造成严重影响。 |
| 弱口令扫描 | 弱口令 | 利用弱口令扫描工具对服务器、网络设备、安全设备、应用系统、终端进行弱口令扫描，形成弱口令扫描报告。 |
| 安全配置核查 | 安全配置脆弱性 | 通常都是由于人为的疏忽造成，主要包括了账号、口令、授权、日志、IP通信等方面内容，反映了系统自身的安全脆弱性。按照上线安全基本要求，检测配置是否符合要求。 |
| 渗透测试 | 安全漏洞和业务逻辑安全问题 | 利用各种业内安全扫描器和富有经验的安全测试工程师的人工经验对客户的网站及提交的相关服务器等设备进行非破坏性质的模拟入侵者攻击，目的是侵入系统并获取机密信息并将入侵的过程和细节产生报告给用户。渗透测试和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率，不能发现高层次、复杂的安全问题；渗透测试需要对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业机能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。渗透内容包括不限于：WEB渗透：SQL注入、跨站脚本攻击、跨站请求伪造、目录遍历、错误信息泄露、命令执行、反序列化等漏洞、webshell木马上传、目录可写信息枚举、源代码泄露。系统渗透：远程命令执行、远程账户新建、账户提权、账户克隆、虚拟机逃逸测试、杀毒软件免杀测试。数据库渗透：端口扫描、版本信息获取、哈希值枚举、webshell写入。 |

### 巡检方法

巡检方法是指巡检人员依据技术标准在实施安全巡检时采取操作的方法，巡检方法包括现场访谈、文档审查、配置检查、工具检查和实地察看5种，每年提供不少于4次的现场巡检。这5种安全巡检方法的具体描述如下表：

|  |  |  |
| --- | --- | --- |
| **序号** | **巡检方法** | **任务描述** |
| 1 | 查阅文档 | 通过查阅设计资料、管理文档、运行日志、登记资料或其他相关文档，检查信息系统安全技术要素的安全技术功能、策略和机制的设置和实际运行情况或安全管理要素的安全管理策略和措施的设置和执行情况； |
| 2 | 人员访谈 | 通过对相关人员进行访谈，了解和获取信息系统安全技术要素的安全技术功能、策略和机制的设置及其实际运行情况或安全管理要素的安全管理策略、措施的设置和执行情况； |
| 3 | 实地察看 | 通过实地察看，了解信息系统被检查安全技术要素的安全技术功能、策略和机制的设置情况； |
| 4 | 配置检查 | 通过系统所提供操作界面，对运行中的信息系统被检查安全技术要素的安全技术功能或安全管理要素的安全管理措施进行实际使用操作，考察被检查安全技术功能或安全管理措施的实际作用； |
| 5 | 工具检查 | 通过采用专业工具，对信息系统被检查安全技术要素的安全技术功能技术参数进行检测、漏洞扫描等。 |

### 巡检流程

整个安全巡检流程共分四个阶段：准备阶段、编制实施方案阶段、现场安全巡检阶段、编制报告及项目总结阶段。

一、**准备阶段**的主要工作任务为项目启动、收集及分析信息。项目启动主要是通过合同或工作部署单位的授权来开展，确定巡检实施小组成员名单，以及双方所承担的义务；而工作任务收集及分析信息，是通过收集巡检过程所需材料并分析、整理成表。

二、**编制实施方案阶段**的主要工作任务是确定巡检对象、确定巡检内容、开发作业指导书、编制实施方案。对用户信息分析，确定巡检对象及巡检内容；并根据巡检内容及相关的技术资料进行作业指导书的开发；以此为依据编写实施方案。

**三、现场安全巡检阶段**的主要工作任务由现场安全准备、现场安全巡检、巡检报告编制三部分组成。现场安全准备的工作主要为现场安全巡检做前期的准备工作，而现场安全巡检则依据作业指导书及工具操作手册对巡检对象按照安全巡检内容进行现场安全巡检（包含手工巡检及工具巡检）；巡检报告编制是对现场安全巡检的结果进行人工分析及工具分析，找出信息系统存在的安全问题或系统漏洞，并依据巡检结果分析的数据进行编写安全巡检报告，并提出适合的安全建议

**四、项目总结阶段**的主要工作任务是在巡检结束后对巡检项目进行总结，对巡检结果进行汇总分析，并向用户单位进行汇报。

### 安全巡检服务交付物

《安全巡检报告》：

列出安全巡检所发现的问题，并给出整改方法和建议。

## 安全加固服务方案

### 安全加固概述

随着网络技术的飞速发展，网络安全逐渐成为影响信息系统业务发展的关键问题。由于信息系统拥有各种网络设备、操作系统、数据库和应用系统，存在大量的安全漏洞，对其进行安全加固增加其安全性是十分必要的。

安全加固是指参考国内国际权威的系统安全配置标准，并结合用户信息系统实际情况，对信息系统涉及的主机、网络设备、应用及数据库的脆弱性进行分析并修补，包括安全配置加固和漏洞修补，增强用户信息系统抗攻击能力，有效减轻系统总体安全风险，提升信息系统安全防范水平，可以建立起一套适应性更强的安全保障基线，有效构建起信息系统安全堤坝。

### 安全加固内容

安全加固是参考国内国际权威的系统安全配置标准，并结合用户信息系统实际情况，在用户允许的前提下，对重要服务器的操作系统和应用服务进行适度安全配置加固和系统安全优化，包括打补丁、停止不必要的服务、升级或更换程序、修改配置及权限等，包括操作系统安全加固和优化、应用软件安全加固和优化、网络设备安全加固和优化，加固服务内容包括基线加固、漏洞修复和安全设备调优。

#### 基线加固

* **主机加固**

针对目前使用的操作系统，如Windows、Linux、AIX等进行加固。

Windows设备安全加固内容：账号、口令、授权、日志配置操作、日志保护配置、共享文件夹及访问权限、Windows服务、防病毒管理、自动播放、屏幕保护、远程登录控制、补丁管理、IP协议安全配置操作、时间同步服务。

Linux操作系统安全加固内容：账号、口令、文件权限、IP协议安全、日志审计、关闭不必要的服务、资源控制。

AIX操作系统安全加固内容：账号、口令、授权、日志配置、IP协议安全、路由协议安全、补丁管理、内核调整、服务进程和启动、AIX可被利用的漏洞。

* **数据库加固**

针对不同数据库类型的数据库如Oracle、SQL Server、MySQL等进行加固，加固服务的内容包括：身份鉴别、访问控制、安全审计、资源控制等安全项加固。加固方法包括：对数据库安全策略、服务等进行安全加固；加强对敏感存储过程的管理，尤其是能执行操作系统命令的存储过程。

Oracle数据库安全加固内容：账号、口令、授权、日志审计、远程操作连接。

Linux版MySQL数据库安全加固内容：认证授权（以非root用户启动MySQL、口令策略、共享帐号、最小权限、IP地址限制、删除无关帐号）、日志审计、安全文件权限配置、连接数限制。

Windows版MySQL安全加固内容：认证授权（以普通用户权限运行MySQL、口令策略、共享帐号、最小权限、IP地址限制、删除无关帐号）、日志审计、安全文件权限配置、连接数限制。

SQL Server数据库安全加固内容：账号、口令、授权、日志审计、通信协议、补丁、停用不必要的存储过程。

* **中间件程序加固**

针对不同中间件类型如IIS、Tomcat、Weblogic、Apache等进行加固，加固内容包括中间件程序安全策略、服务等。

IIS中间件安全加固内容：账号、口令、授权、日志配置操作、日志保护配置、文件系统及访问权限、IIS服务组件、隐藏IIS版本号及敏感信息、版本和补丁管理、IP协议安全配置操作、连接数限制。

Linux版Apache安全加固内容:认证授权设置、以非root用户启动Apache、目录安全配置、限制IP地址访问、日志审计设置、配置错误日志、配置访问日志、其他安全设置、隐藏Apache版本号、关闭目录浏览功能（必选）、禁用Apache的执行功能、防御拒绝服务攻击、自定义错误页面、升级使用最新版Apache。

Windows版Apache安全加固内容：认证授权设置、以普通用户权限运行Apache、目录安全配置、限制IP地址访问、日志审计设置、配置错误日志、配置访问日志、其他安全设置、隐藏Apache版本号、关闭目录浏览功能（必选）、禁用Apache的执行功能、防御拒绝服务攻击、自定义错误页面。

Tomcat中间件安全加固内容：账号、口令、授权、日志配置操作、定时登出、错误页面处理、目录列表访问限制。

Weblogic中间件安全加固内容：账号、口令、授权、日志、审计、其他安全配置、定时登出、错误页面处理、禁用Send Server header。

* **网络设备加固**

对二层交换设备、三层交换设备、路由器、防火墙等网络设备进行加固，加固服务的内容包括：访问控制、安全审计、网络设备防护等安全项加固。

CISCO网络设备安全加固内容：账号、口令、密码复杂度、加固CON端口的登录、加固AUX端口的管理、对网络设备的管理员登录地址进行限制、HTTP登录安全加固、设置登录超时时间、用户权限分配、限制具备管理员权限的用户远程登录、日志配置、日志安全要求、远程日志功能、防止地址欺骗、SNMP服务器配置、使用ssh加密传输、禁用空闲端口、端口级的访问控制策略。

HUAWEI网络设备安全加固内容：用户帐号分配、限制具备管理员权限的用户远程登录、无效账户清理、静态口令复杂度、静态口令加密、密码重试、加固CON端口的登录、加固AUX端口的管理、对网络设备的管理员登录地址进行限制、远程登录加密传输、设置登录超时时间、用户权限分配、配置日志功能、对用户操作进行记录、对用户登录进行记录、开启NTP服务保证记录的时间的准确性、远程日志功能、ACL配置、防止地址欺骗、SNMP服务器配置、配置SNMPV2或以上版本、修改SNMP的Community默认通行字、动态路由协议口令要求配置MD5加密、禁止发布或接收不安全的路由信息、MPLS安全、禁用空闲端口、关闭不必要的服务。

H3C网络设备安全加固内容：账号、设备特权口令、密码复杂度、设置特权口令(推荐)、关闭未使用的端口、账号口令、Console口密码保护、禁止无关账号、日志配置操作、审核登录、VTY端口防护策略、远程主机IP地址段限制、远程管理通信安全、更改SNMP 服务读写权限管理、修改SNMP默认的Community字符串、Community字符串加密、IP/MAC地址绑定、ARP攻击防御、ARP防止IP报文攻击、关闭设备FTP服务、防源地址欺骗攻击、端口隔离、启用端口安全功能。

## 应急响应服务方案

### 应急响应服务内容

安全应急服务是指当企业发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件、需要紧急解决问题，当用户提出应急响应请求时，安全专家第一时间赶到事件现场或者采取远程应急方式，快速对事件进行处置，使企业的网络信息系统在最短时间内恢复正常工作，帮助企业查找入侵来源，给出入侵事故过程报告，同时给出解决方案和防范报告，为企业挽回或减少损失。并协助用户相关人员进行事件调查、保存证据、查找后门、追查来源等，同时提供事件处理报告以及后续的安全状况跟踪。

提供应急响应服务内容包括但不限于以下方面：

1. 事件调查分析：根据事件识别所发生事件的情况，对需要进一步分析的事件直接进行到相关的安全设备、网络设备、服务器、数据库等分析事件的细节情况，进行细致的精确分析；
2. 事件取证：对确定有问题的严重事件进行调查后取证，将实际证据保存下来，形成文档提供给用户；
3. 事件解决方案和恢复：根据事件发生的实际情况调整网络设备、安全设备、服务器等的安全策略，解决和恢复事件造成的影响；
4. 书写事件总结报告：针对发生的事件前因后果书写总结报告；
5. 提出整改建议：对影响面大，后续可能还会发生的事件提出全面整改建议。
6. 减少损失和负面影响：利用自身的资源协调能力降低或减少事件对中心的负面影响，减少中心的整体损失。

安全事件应急响应的目标通常包括：

1. 采取紧急措施，恢复业务到正常服务状态；
2. 调查安全事件发生的原因，避免同类安全事件再次发生；
3. 为事件取证提供参考。

### 应急响应事件

本方案所指事件均为网络安全事件，是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。包括但不限于以下事件类型：

**（一）有害程序事件**

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件。有害程序是指插入到信息系统中的一段程序，有害程序危害系统中数据、应用程序或操作系统的保密性、完整性或可用性，或影响信息系统的正常运行。

有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件等7个子类。

**（二）网络攻击事件**

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的事件。

网络攻击事件包括拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件等7个子类。

**（三）信息破坏事件**

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它信息破坏事件等6个子类。

### 应急响应时间

应急响应服务是指客户遇到安全事件时，通过电话、微信、QQ或邮件寻求技术支持和帮助，在确认客户的服务请求后，我方派工程师进行应急响应。

|  |  |
| --- | --- |
| **服务时间** | 7×24小时，电话支持、远程支持和现场支持 |
| **响应时间** | 客户以电话、微信、QQ或邮件等方式提出服务申请，我方在收到客户申请后30分钟内进行回应，并由技术人员确定技术响应方式。如通过电话及远程方式能解决，如条件允许则即刻进行远程支持处理；如电话及远程方式无法解决，则根据故障等级协调技术人员赴现场进行技术支持。 |
| **处置时间** | 根据安全事件等级不同，决定现场响应：**严重安全事件：**造成系统重大故障或成功入侵事件，如勒索、挖矿、挂马、域名劫持、网页篡改等，市内1小时到达现场，4小时内解决，其它地市需加上车程时间，根据距离和交通便利性有差异。**一般安全事件：**网络一般异常，但不影响设备业务的正常使用，市内4小时到达现场，24小时内解决，其它地市需加上车程时间，根据距离和交通便利性有差异。 |
| **应急响应报告出具时间** | 系统恢复正常状态后，结束应急处理。我方在24小时内提供包含安全事件现象和处理过程的报告。 |

### 应急响应实施流程

应急响应流程如下：



#### 准备阶段

目标：在事件真正发生前为应急响应做好预备性的工作。

内容：根据不同角色准备不同的内容。

输出：《准备工具清单》、《事件初步报告表》、《实施人员工作清单》

#### 检测阶段

目标：接到事故报警后在服务对象的配合下对异常的系统进行初步分析，确认其是否真正发生了信息安全事件，制定进一步的响应策略，并保留证据。

内容：

检测范围及对象的确定；

检测方案的确定；

检测方案的实施；

检测结果的处理。

输出：《检测结果记录》

#### 抑制阶段

目标：及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏，同时要确保封锁方法对涉及相关业务影响最小。

内容：

抑制方案的确定；

抑制方案的认可；

抑制方案的实施；

抑制效果的判定；

输出：《抑制处理记录表》

#### 根除阶段

目标：对事件进行抑制之后，通过对有关事件或行为的分析结果，找出事件根源，明确相应的补救措施并彻底清除。

内容：

根除方案的确定；

根除方案的认可；

根除方案的实施；

根除效果的判定；

输出：《根除处理记录表》

#### 恢复阶段

目标：恢复安全事件所涉及到得系统，并还原到正常状态，使业务能够正常进行，恢复工作应避免出现误操作导致数据的丢失。

内容：

恢复方案的确定；

恢复信息系统；

输出：《恢复处理记录表》

#### 总结阶段

目标：通过以上各个阶段的记录表格，回顾安全事件处理的全过程，整理与事件相关的各种信息，进行总结，并尽可能的把所有信息记录到文档中。

内容：

1、事故总结；

2、事故报告；

输出：《应急响应报告表》

## 信息安全培训

### 网络安全培训体系设计

湖南金盾培训课程主要依据国家信息安全法律、法规、相关标准，结合湖南金盾等级保护的实施和网络攻防经验设计。培训内容分为四大模块，包括网络安全意识模块、网络安全法律法规模块、网络安全等级保护模块、网络安全攻防模块，通过循序渐进的方式，从浅显的网络安全基础知识到网络安全的实战经验，使学员能够更容易的由浅入深掌握网络安全的相关内容。可对信息安全管理人员、信息安全技术人员、单位全员针对性的提供所需掌握网络安全知识和技能的培训方案。

### 网络安全培训方案

#### 网络安全意识培训

##### 培训概述

世界头号黑客Kevin Mitnick 曾说过“人是最薄弱的环节。你可能拥有最好的技术、防火墙、入侵检测系统、生物鉴别设备，可只要有人给毫无戒心的员工打个电话……”技术无法保护每一个人远离每一种可能存在的安全风险，信息安全管理人员要教会员工安全思考的方式。投资员工，让他们建立起保持数据正确的责任感，是企业面对安全威胁的最佳方式。

实际上一个企业的整体安全水平不仅要看专职的安全管理与技术人员的能力，还要看全体员工的安全意识是否到位，这与持续的安全意识教育与培训是密不可分的。提高和维持所有员工的信息安全意识和技能，对员工理解信息安全对单位的意义，开展信息安全工作，在单位 内逐步建立和融入信息安全的文化，提高整体安全水平是非常重要的。当然，这可能是一个漫长而艰难的过程。

##### 培训目标

信息安全意识培训的目标是提高员工的信息安全意识，加深对信息安全的认识，加强识别信息安全风险的能力和信息安全风险防范技能。

##### 培训对象

该课程的培训对象适用单位全员(针对医院职工和信息中心技术人员培训各一场)。

##### 培训形式

本项培训课程以PPT+讲解+视频+现场演示+答疑形式组成。

安全意识培训还可搭配通过网络钓鱼的方式进行一次全员的网络安全意识测试。

##### 培训内容

| **序号** | **主要内容** | **时长** | **具体内容** |
| --- | --- | --- | --- |
| 1 | 网络安全概述 | 20分钟 | 课程目标介绍、课程内容介绍、通过一些通俗易懂的解释使全体员工了解信息安全的内含：介绍什么是信息、什么是信息安全、信息安全的CIA、信息安全目标、信息安全环节、信息安全实质 |
| 2 | 信息安全形势 | 20分钟 | 通过一些具体数据和例子，使全体员工了解目前国际国内在不同领域的信息安全相关形势，以及信息安全对于企业的重要意义：安全事件、安全漏洞、恶意代码、垃圾邮件、WEB安全、移动威胁、网络犯罪、数据泄露、攻击源、外部监管 |
| 3 | 身边的信息安全问题 | 60分钟 | 通过调查数据、相关案例、动画、视频等生动形象的方式来加深普通员工的理解和印象：口令、电子邮件、浏览器、即时通讯工具、社交网站、移动存储介质、手机安全、网络钓鱼、网络盗窃、电脑安全、信息资产、物理安全、第三方安全、企业信息泄露、个人信息泄露、业务连续、社会工程学、信息安全事件等 |

**三、测评依据与标准：**

对信息系统及网络进行独立、公正、权威的等保测评，测评主要依据以下标准：

* 《关于信息安全等级保护工作的实施意见》（公通字[2004]66）；
* 《信息安全等级保护管理办法》（公通字 [2007]43号）；
* 《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）；
* 《信息安全技术 信息系统安全等级保护基本要求》-GB/T22239-2019；
* 《信息安全技术 网络安全等级保护定级指南》-GA/T 1389-2017；
* 《信息安全技术 网络安全等级保护测评过程指南》-GB/T 28449-2018；
* 《信息安全技术 网络安全等级保护测评要求》-GB/T 28448-2019；
* 《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 网络安全等级保护安全设计技术要求》-GB/T 25070-2019
* 《信息安全技术 网络安全等级保护测试评估技术指南》GB/T36627-2018
* 《湖南省卫生行业信息系统信息安全等级保护实施方案》（湘卫办发[2012]28号）
* 《关于印发<长沙市卫生计生行业信息系统安全等级保护工作实施方案>的通知》（长卫发【2018】27号）

**四、项目成果要求**

根据收集的信息和完成的分析创建评估文档，并向用户相关人员陈述本次评估结果，提出相应的安全整改措施建议，使用户充分理解信息系统存在的等级保护差距与其安全风险，以尽早采取整改与加固措施，最终完成本次评估活动。测评后，投标人应至少提交以下成果：

1、《信息系统安全等级保护测评报告》：主体报告，描述被测评系统的信息安全现状，找出存在的安全隐患，描述系统安全防护措施与国家标准要求之间的差距，对存在的漏洞进行风险分析，最后提出整改建议。报告格式符合公安部所发《信息系统安全等级测评报告模板》的要求。

2、《等级保护整改建议方案》（或等级保护问题清单）：综合报告后的辅助报告，通过综合分析，了解了当前的安全现状，提出针对相关医院业务系统安全问题的总体安全解决建议方案。

3、协助完成等级保护备案工作，取得长沙市等保办核发的备案证明。

**五、****质量保证要求：**

1. 在本次等级测评中中标人应遵循的原则：

  （1）保密原则：对测评的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害竞争性磋商人的行为，否则采购方有权追究投标人的责任。

  （2）标准性原则：测评方案的设计与实施应依据国家等级保护的相关标准进行。

  （3）规范性原则：中标人的工作中的过程文档，具有很好的规范性，可以便于项目的跟踪和控制。

  （4）可控性原则：测评服务的进度要跟上业主对进度的要求与安排，保证采购方对于测评工作的可控性。

  （5）整体性原则：测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面。

  （6）最小影响原则：测评工作应尽可能小的影响系统和网络，并在可控范围内；测评工作不能对现有信息系统的的正常运行、业务的正常开展产生任何影响。

1. 在评估期间，评估单位应免费为用户的技术人员提供相关的技术评估服务与咨询服务。服务可通过现场、电话、电子邮件、传真等方式进行，具体方式以解决问题为准。
2. 评估单位须认真审核信息系统技术实施状况，测试信息系统安全状况，对信息系统、网络安全设备及其配置进行审查，及早预测以后可能带来的各种安全隐患与风险，并提供消减各种安全隐患与风险的解决方案。
3. 评估单位作为独立的第三方权威的技术机构，应遵循“守法、公正、公平、独立”的原则，依据国家和有关主管部门标准进行测评，能出具合格的评估报告，并给出相应的合理的整改建议方案。
4. 评估机构应当及时报告信息系统安全评估的进展与汇总情况。
5. 评估单位必须履行对用户单位的相关信息进行保密的义务。
6. 项目完成时间：合同签订并接到采购人通知后 60 个工作日完成等级保护测评及其配套服务工作，并递交测评服务成果资料。
7. 测评人员要求：本项目的测评人员需具有2 年或以上测评工作经验。投标人参与本项目的成员至少有4人，现场测评人员不得少于3人，在突发应急事件中能临时增加至4 名测评与咨询人员。须提供人员配备及管理方案，并确保人员的稳定。如更换测评人员，须由用户单位同意并签字确认。
8. 中标人的专业资质要求：具有中国信息安全测评中心授予的“国家信息安全测评授权证书”。
9. 本项目执行期间，服务团队成员应遵守甲方工作作息时间要求和工作规定。
10. 投标人应按等级保护测评要求制定测评过程中产生的文档，达到科学、规范、详尽、统一的要求

**六、****其它**

1、中标单位在签订合同时，若坚持提出附加条件和不合理要求，中标资格将被取消，该中标人对由此产生的一切后果负责。

2、未尽事宜，以相关规定、要求和相关法律法规规定为准。

# 第三章 响应文件的组成及格式

供应商的响应文件应包含以下七个部分：

**一、磋商响应声明**

附件1：法定代表人身份证明

附件2：法定代表人授权书

**二、供应商的资格证明材料**

附件3：供应商基本情况表

附件4：主要人员简历表

**三、服务方案**

附件5

**四、技术/商务响应与偏离表**

**五、报价一览表及报价文件**

附件6：报价文件(服务类项目适用)

**六、供应商认为需要供的其它资料**

**七、最后报价**

1. **磋商响应声明**

致 (采购人或采购代理机构)：

我方已仔细研究了 (项目名称)的竞争性磋商文件（采购代理编号：）的全部内容，知悉参加竞争性磋商的风险，我方承诺接受磋商文件的全部条款且无任何异议。

一、我方同意在磋商文件中规定的提交首次响应文件截止时间起日内(响应文件有效期)遵守本响应文件中的承诺且在此期限期满之前均具有法律约束力。

二、我方提交响应文件正本一份和副本一式份，并保证响应文件提供的数据和资料全部内容真实、合法、准确和完整，我们对此负责，并愿承担由此引起的法律责任。

三、我方愿意向贵方提供任何与本项采购有关的数据、情况和技术资料。若贵方需要，我方愿意提供我方作出的一切承诺的证明资料。

四、我方愿意按磋商文件规定和磋商小组要求重新提交响应文件和最后报价。

五、我方承诺遵守法律规定，保证在获得成交资格后，按照磋商文件确定的事项签订采购合同，履行双方所签订的合同，并承担合同规定的责任和义务。

六、我方在此声明：

（一）我方与采购人或采购代理机构不存在隶属关系或者其他利害关系。

（二）我方与参加本项目的其他供应商不存在直接控股、管理关系，或者与其他供应商法定代表人（或者负责人）为同一人。

（三）我方未为本项目前期准备提供设计或咨询服务。

（四）我方承诺（承诺期：成立三年以上的，为提交首次响应文件截止时间前三年内；成立不足三年的，为实际时间）：

1、我方依法缴纳了各项税费及各项社会保障资金，没有偷税、漏税及欠缴行为。

2、我方在经营活动中没有存在下列重大违法记录：

(1)受到刑事处罚；

(2)受到三万元以上的罚款、责令停产停业、在一至三年内禁止参加政府采购活动、暂扣或者吊销许可证、暂扣或者吊销执照的行政处罚。

附件1：法定代表人身份证明

附件2：法定代表人授权书

供应商名称(盖单位章)：

法定代表人或其委托代理人 (签字)：

日 期：年月日

#### 附件1法定代表人身份证明

**法定代表人身份证明**

供应商名称：

注册号：

注册地址：

成立时间： 年 月 日

经营期限：

经营范围：主营： ；兼营：

姓名： 性别： 年龄： 系（供应商名称）的法定代表人。

特此证明。

附：法定代表人身份证复印件

供应商名称（盖单位章）：

日期：年月日

#### 附件2 法定代表人授权书

**法定代表人授权书**

本人（姓名、职务）系 （供应商名称）的法定代表人，现授权（姓名、职务）为我方代理人。代理人根据授权，以我方名义：(1)签署、澄清、补正、修改、撤回、提交（项目名称、磋商采购编号）响应文件；(2)签署并重新提交响应文件及最后报价；(3)退出磋商；(4)签订合同和处理有关事宜，其法律后果由我方承担。

委托期限： 。

代理人无转委托权。

本授权书于年月日签字生效，特此声明。

附：委托代理人身份证复印件及法定代表人身份证明(附件1，原件)

法定代表人（签字）：

委托代理人（签字）：

日期：年月日

**二、供应商的资格证明材料**

#### 附件3供应商基本情况表

供应商基本情况表

盖供应商单位章

|  |  |  |  |
| --- | --- | --- | --- |
| 供应商名称 |  | 法定代表人 |  |
| 组织机构代码 |  | 邮政编码 |  |
| 委托代理人 |  | 电子邮箱 |  |
| 上年营业收入 |  | 员工总人数 |  |
| 营业执照 | 注册号码 |  | 注册地址 |  |
| 发证机关 |  | 发证日期 |  |
| 营业范围（主营） |  |
| 营业范围（兼营） |  |
| 基本账户开户行及帐号 |  |
| 税务登记机关 |  |
| 资质名称 | 等级 | 发证机关 | 有效期 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 备注 | 提供营业执照和组织机构代码证(副本复印件)，其他资料按第二章要求提供。 |

#### 附件4主要人员简历表

**主要人员简历表**

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 |  | 性 别 |  |
| 职 务 |  | 职 称 |  |
| 毕业学校、专业 |  |
| 身份证号 |  | 拟在本合同任职 |  |
| 执业资格证 |  | 执业资格证书号 |  |
| 近三年承担项目情况 |
| 时间 | 类似项目名称 | 担任职务 | 项目单位名称及电话 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

说明：主要人员证书、类似项目证明资料等按第三章要求提供。

供应商名称：

法定代表人或其委托代理人(签字)：\_

日期： 年 月

**三、服务方案**

#### 附件5技术服务方案

服务类项目供应商应根据第三章规定编写服务方案或服务大纲。服务方案或服务大纲应包括：(1)服务目标、范围和任务；(2)服务方案；(3)服务团队组织安排计划；(4)工作流程；(5)进度计划及保证措施；(6)质量保证措施；(7)其他。

**四、技术/商务响应与偏离表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 竞争性磋商采购文件条目号 | 采购规格/商务条款 | 响应文件的规格/商务条款 | 响应与偏离 | 说明 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

说明：1、“响应与偏离”应注明“响应”或“偏离”。

供应商名称：

法定代表人或其委托代理人(签字)：

日 期： 年 月 日

**五、报价一览表及报价文件**

#### 附件6 报价一览表（货物、服务类适用）

|  |  |  |  |
| --- | --- | --- | --- |
| 项目名称 项目名称 |  | 磋商采购编号 |  |
| 采购代理编号 |  |
| 品目代码 |  |
| 报价 | 大写：元人民币整小写：元人民币整 |
| 合同周期 |  |
| 项目负责人 |  |
| 服务人数 | 人 |
| 备 注 |  |

说明：“品目代码”栏按**《政府采购品目分类目录》规定填写，如**C050301车辆维修和保养服务**；**

供应商（盖单位章）：

法定代表人或其委托代理人签字：

日期：年月日

分项价格表(货物、服务类适用)

**项目名称：**

**包号： 金额单位：元**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务名称 | 品目代码 | 计量单位 | 具体要求说明 | 单价 | 数量 | 合计 | 政策功能编码 | 备注 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 合计 |  |  |  |  |  |  |  |  |

报价金额合计：小写：大写：

说明：品目代码是指货物《政府采购品目分类目录》中的分类代码，应与采购文件的需求对应，否则报价有可能被拒绝。政策功能编码包括货物或服务的提供厂商为“中型企业”或者“小型、微型企业”，以及提供的产品的中国环境标志认证证书编号、节能标志认证证书号、两型产品编号。

**六、供应商认为需要提供的其它资料**

**七、最后报价**

说明：最后报价按磋商一般规定，价格不得高于第一轮报价，格式按附件6提供。