A包需求书

一、需求规模

运维需求范围如下：

机房运维；

软硬件设备运维；

应用系统运维；

其他运维服务。

1.机房运维

对机房UPS、配套柴油发电机组、视频监控等设备运维。

2.软硬件设备运维

网络设备、安全设备、主机设备、存储设备、操作系统、数据库软件及中间件软件等运维。

3.应用系统运维

对海南省应急管理厅的应用系统进行运维。

4.其他运维服务

人员派驻；

安全服务；

特种车辆运维以及卫星通信服务费购买；

气象局数据服务。

二、建设内容

1.总体目标：

1.1 保障各相关应用系统正常运行及系统客户服务；

1.2 保障硬件设备资源及配套网络安全环境的正常运行；

1.3 保障与本项目涉及信息系统相关各项工作正常开展。

1.4 完成本项目涉及信息系统的一次网络安全攻防演练和一次渗透测试、两次50人以上的网络安全培训。

2. 具体目标：

2.1 确保全年的系统可用率达到 99%以上；

2.2 运维服务及时率超过 95%；

2.3 系统用户满意度超过 95%。

三、需求分析

（一）机房及配套工程运维需求分析

本项目机房设备清单如下：

序号	运维对象		品牌型号	基本技术参数	单位	数量	用途	备注
1	空调系统运维	格力 柜式空调	格力 柜式空调		台	8	空调系统	
2		OMARA 智能空调控制器	OMARA 智能空调控制器		台	8	空调系统	
3	配电系统运维	UPS	UPS	山特 C10KS 额定功率：10KVA 后备时间：1 小时输入配线：单相二线+地线含后备 1 小时	台	2	配电系统	
4		油罐	油罐	2000L 油罐(含电缆、加油泵、防火、防雷、防静电等)	个	1	配电系统	
5		低压配电柜	低压配电柜	ATS 国产 空开施耐德	台	2	配电系统	
6		24U 机柜	24U 机柜		台	2	配电系统	
7	机房基础环境	柴油发电机组	康明斯 200KW 柴油发电机		台	1	机房基础环境	
8		灭火器		手提式 IG02 气体灭火器	个	11	机房基础环境	
9		灭火器		柜式七氟丙烷灭火器（设备间）	个	2	机房基础环境	
10		灭火器		柜式七氟丙烷灭火器（设备间）	个	2	机房基础环境	

本项目机房及配套设备运维需求见下表：

序号	服务模块	内容描述
1	机房值班值守	机房 7×24 小时技术人员值班值守，保证操作系统正常运转，需提供技术驻场服务。
2	机房定期现场巡检	对机房设备进行定期全面巡检，最大可能地发现机房设备存在的隐患，保障设备稳定运行。
3	现场故障处理	按服务级别：7×24 小时故障处理。
4	问题管理并记录	对遇到的问题进行汇总和报告。

（二）软硬件基础设施运维需求分析

本项目软硬件基础设施清单如下：

序号	设备名称	运维对象	品牌型号	基本技术参数	单位	数量
1	视频监控、卫星设备	视频监控平台服务器	海康威视 DS-VE2208C-BBC 视频监控平台服务器	E5-2620 V3（6 核 2.4Hz）*1/16GB DDR4/1TB SATA*2/热插拔/SAS3008/DVD/1GbE*4/冗电/导轨/2U Windows Server 2008 R2 简体中文激活码 1、电源：高效能 550W 铂金冗余电源；2、电源电压 200-240V/50Hz	台	1
2		流媒体服务器	海康威视 DS-VE2208C-BBC 流媒体服务器	E5-2630 V3（8 核 2.4Hz）*1/16GB DDR4*2/1TB SATA*2/热插拔/SAS3008/DVD/1GbE*4/冗电/导轨/2U Windows Server 2008 R2 简体中文激活码 1、电源：高效能 550W 铂金冗余电源；2、电源电压 200-240V/50Hz	台	1
3		C 波段双向天线	C 波段双向天线	其他网络设备	台	1
4		卫星终端（含功放、LNB）	卫星终端（含功放、LNB）	其他网络设备	台	1
5		电缆线	电缆线	其他网络设备	台	1
6		海事卫星便携卫星设备	海事卫星便携卫星设备	其他网络设备	台	2
7	交换机、网关	视频设备接入网关	海康威视 DS-68VAG000 视频设备接入网关	支持 GB/T28181 标准协议实现平台间联网；支持协议网关与媒体网关分离的工作模式，能将国际码流实现无损转发；性能参数：千兆网络环境下单台联网网关可同时提供 800M 码流转发；	台	1
8		视频联网网关	海康威视 DS-68NCG000 视频联网网关	支持 GB/T28181 标准协议实现平台间联网；支持协议网关与媒体网关分离的工作模式，能将国际码流实现无损转发；性能参数：千兆网络环境下单台联网网关可同时提供 800M 码流转发；	台	1
9		核心交换机	H3C 1s-5130-30s-hi 核心交换机	24 个千兆电口，4 个万兆 SFP+口 2 个 QSFP+ 堆叠口（配单摸光模块），冗余电源，支持虚拟化功能，交换容量 598Gbps，转发率 216Mpps。三年原厂保修服务	台	1

10	视频会议存储	、终端海康威视 DS-A80216S 视频存储	海康威视 DS-A80216S 视频存储	16 盘位磁盘阵列；192Mbps 接入带宽，2 个千兆网口；支持视频流和图片进行混合直写存储；支持 SMART IPC 接入，支持存储只能信息，实现只能事件检索功能，精确定位重点事件，并可通过平台进行智能浓缩播放，有效节省客户时间	台	1
11		Polycom Group550 主会场高清视频终端	Polycom Group550 主会场高清视频终端	包含主机一台、高清摄像机一个、全向数字麦克风 1 个，原厂 3 年质保	台	1
12		Polycom Group300 分会场高清视频终端	Polycom Group300 分会场高清视频终端	包含主机一台、高清摄像机一个、全向数字麦克风 1 个，原厂 3 年质保	台	20
13		Polycom RMX 200 高清多点控制单元	Polycom RMX 200 高清多点控制单元	支持 30 路高清会场接入，原厂 3 年质保	台	1
14		单屏支架	单屏支架	定制支持一台 12 寸至 55 寸范围内 PDP、LCD、LED 显示屏安装；钢结构主体，底座万向轮安装，可灵活移动，尺寸（宽*深*高）920mm*600mm*1470mm（约）	套	21
15		紫荆 HD800 便携箱式移动视频应急指挥终端	紫荆 HD800 便携箱式移动视频应急指挥终端	室内系统	台	2
16		飞利蒙 VGA 信号延长器	飞利蒙 VGA 信号延长器	其他视频	台	1
17	视频综合平台	海康威视 DS-B20-S05—A 视频综合平台	海康威视 DS-B20-S05—A 视频综合平台	8U 标准机箱，满足各种规模的监控需求；标准机架式设计，运营级 ATCA 机箱系统；插拔式模块化设计，可根据需求灵活扩展；5 槽位机箱，双电源适配器，单主控板；业务模块支持热插拔、双电源冗余、只能风扇自动调温，确保系统稳定可靠；双高速无阻塞背板设计，满足大容量视频数据高速交换的需求	台	1
18		海康威视 DS-6532HD-B20D 解码输出版（H.265）	海康威视 DS-6532HD-B20D 解码输出版（H.265）	8 路视频输出，DVI 接口	块	2

19		海康威视 DS-6408HFH-B20VD 视频输入板	海康威视 DS-6408HFH-B20VD 视频输入板	4 个 VGA 输入接口；接入 VGA 模拟信号，4 个 DVI 输入接口；接入 DVI 数字信号	块	2
20		海康威视 DS-1600K 网络键盘	海康威视 DS-1600K 网络键盘	10.1 英寸电容触摸屏	台	1
21	通用软件	双机热备软件	双机热备软件	北京微彩华创 ServHA Cluster v3.5 for Windows	套	1
22		控制软件	控制软件	DLS 大屏智能控制软件 V3.0	套	1
23		应用服务器操作系统	微软 Windows server 2008 R2 标准版	（支持 1-4CPU，1 个虚拟机，5 个用户访问授权许可）	套	4
24		数据库软件	微软 SQL Svr 2014 简体中文标准版 15 客户端		套	1
25	办公业务系统软件	办公系统维护费			套	1
26		手机办公维护费			套	1
27		平板签批系统服务费			套	1
28	防火墙	天融信防火墙软件升级			套	1

1. 网络与安全系统运维需求

根据系统的现状，所需的运维服务包括：技术人员值守、定期现场巡检、设备保修与现场备件安装、现场软件升级、现场故障处理、问题管理并记录、运行分析及建议。

从网络的连通性、网络的性能、网络的监控管理三个方面实现对网络系统的运维管理。基本服务内容应包括：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证网络的实时连通和可用，保障接入交换机、汇聚交换机和核心交换机的正常运转。并提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对设备及网络进行全面检查，通过该工作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。
3	设备保修及现场	在故障情况下，负责对故障设备进行维修或原厂返修，对需要

	备件安装	备件顶替的进行现场安装调试。
4	现场软件升级	分析软件升级的必要性和风险，并软件升级。
5	现场故障处理	按服务级别：7×24 小时。
6	问题管理并记录	对遇到的问题进行汇总和报告。
7	运行分析及建议	通过对网络运行状况、安全问题进行周期性检查、分析，全面了解历史故障情况，并提出故障预防建议，最大程度减少网络及安全故障隐患，更高效的进行网络及安全管理。

2. 服务器与存储系统运维需求分析

所需的运维服务包括：

技术人员值守、定期现场巡检、设备保修与现场备件安装、补丁服务、升级服务、现场故障处理、问题管理并记录、系统优化。

服务器与存储系统运维的基本服务内容应包括：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证主机、存储的连通和可用，提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对主机、存储设备进行全面检查的服务项目，通过该工作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。
3	设备保修及现场备件安装	在故障情况下，负责对故障设备进行维修或原厂返修，对需要备件顶替的对备件进行现场安装调试。
4	补丁服务	消除软件漏洞给系统带来的安全隐患，并对安装补丁所引起的系统连锁反应进行合理的平衡。
5	升级服务	对系统进行软件或硬件的升级，以改进、完善现有系统或消除现有系统的漏洞。
6	现场故障处理	按服务级别：7×24 小时。
7	问题管理并记录	对遇到的问题进行汇总和报告。
8	系统优化	对客户系统的主机、存储设备、操作系统、提供优化服务。

3. 系统与工具软件运维需求分析

3.1 操作系统运维

操作系统运行维护服务是包括主动操作系统版本及补丁管理、性能资源监控等工作。通过管理可了解当前操作系统日常运行状态，识别问题发生在什么地方，有针对性地进行性能优化。同时，密切注意运行变化，主动地预防可能发生的问题。

操作系统运行维护的基本内容应包括：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证操作系统正常运转，并提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对操作系统进行全面检查，通过该工作获得运行的第一手资料，最大可能地发现存在的隐患，保障稳定运行。
3	操作系统补丁升级	根据操作系统厂商提供的补丁，分析当前系统环境升级的必要性和风险，进行补丁升级。
4	现场故障处理	按服务级别：7×24 小时。
5	问题管理并记录	对遇到的问题进行汇总和报告。

3.2 数据库运维

数据库是多数应用系统稳定运行及数据安全保管的核心环节，数据库运行维护服务是包括主动数据库性能管理和数据备份管理，数据库的主动性能管理对系统运维非常重要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。数据库数据备份管理是对数据库中正在运行的业务及相关数据，按建设方案设定的备份策略进行及时备份，备份数据的管理，以及当出现系统故障时，通过备份数据进行数据的恢复等工作。

具体数据库运行维护监控的基本服务内容应包括：

序号	服务模块	内容描述
1	数据库支持服务	每周 7 天，每天 24 小时驻场支持，以满足业务发展的需要。根据问题的严重程度，将优先解决客户认为是关键而紧急的任务。对客户提出的一般性问题进行技术咨询、指导。定期的客户管理报告，避免问题再度发生。
2	数据库现场服务响应	数据库宕机； 数据坏块； 影响业务不能进行的数据库问题。
3	数据库健康检查	对数据库的配置及运作框架提出建议，降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张； 检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患； 检查数据库系统是否需要应用最新的补丁集； 检查数据库空间的使用情况； 监控数据库性能，确认系统的资源需求。

序号	服务模块	内容描述
4	数据库产品性能调优	分析应用类型和用户行为，并以此评价并修改数据库的参数设置； 评价应用对硬件和系统的使用情况，并提出建议 通过改善系统环境的稳定性来降低潜在的系统宕机时间。
5	数据备份检查及数据恢复	依据系统建设方案的数据备份策略，检查数据库备份的安全可用； 系统故障时进行数据备份的恢复； 定期进行备份数据的恢复演练。

4. 应用系统运维需求分析

业务应用软件是整体系统运维的最高层面，也是最终用户使用的界面，上述硬件及系统软件的运行情况，都会在应用软件中得到体现。应用软件运维涉及的工作内容较多，除了正常的系统监测检查外，面向最终用户的使用培训及基于用户需求的应用调整也是必须要考虑的内容。应用系统运维所需服务包括：

运行监控、数据处理、定期巡检、故障处理、数据备份协助、日常技术支持等，本项目无系统优化开发的内容。

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证应用系统的可用，提供 7×24 小时的驻场技术支持服务，根据用户的问题，进行用户故障分析，并分配给相关人员处理。
2	用户使用指导	基于应用系统最终用户的使用情况，通过电话、微信群、应用系统公告等方式，对用户系统使用过程中对系统应用不熟练或疑问的地方进行解答，并指导用户正常使用。 该项服务应区分于应用系统部署上线的批量集中培训。 按服务级别：7×24 小时。
3	系统错误修改	基于用户的反馈，及时判断并发现应用系统本身的错误，并及时进行修改。 按错误级别：程序错误 24 小时； 数据错误 8 小时； 配置错误 4 小时。
4	系统功能优化	基于应用系统最终用户的使用情况，对确实影响用户操作的功能缺陷进行修补优化。 该项服务应区分于基于业务需求的应用系统升级服务。原则上单次修改工作量不超过 3（人天）在用户反馈后 3 个工作日内响应，并按与用户商定时间内完成修改。
5	问题管理并记录	对遇到的用户请求，包括使用问题、系统故障等进行汇总

序号	服务模块	内容描述
		和报告。
6	优化升级建议	根据应用系统的用户使用情况，以及用户的业务发展趋势，评估当前应用的功能及性能，并提出优化升级建议。

5.其他运维服务需求分析

5.1 人员派驻服务

由于规划科技信息处技术人员编制和运维经费的限制，规划科技信息处运维能力较为薄弱。需要根据信息系统实际使用情况和运行状况，要求运维服务提供商在平时安排 8 人进行驻点维护。对信息化系统设备进行日常的维护，服务内容包括上述各项服务中能够现场解决的部分内容，现场派驻人员不能提供的服务由运维服务提供商安排其他资源提供；当战时的时候需要运维服务提供商提供更多的具有专业性质的人员进行现场系统的维护以保障系统的正常运行，同时需要运维服务提供商提供专业的人员对下面市县的运维设备进行每个季度的巡检。

5.2 海南省应急管理厅办公系统维护服务

序号	服务项目	说明
1	办公系统维护费	服务内容：（1）提供该应用系统 5×8 小时的技术支持和技术咨询服务，重大故障请求 2 小时给予响应；（2）提供 4 次巡检服务：系统检查和补丁更新、运行状态监控、系统日志清理，以及以上问题的应急响应。
2	手机办公维护费	服务内容：（1）提供该应用系统 5×8 小时的技术支持和技术咨询服务，重大故障请求 2 小时给予响应；（2）系统检查和补丁更新、运行状态监控、系统日志清理，以及以上问题的应急响应。
3	平板签批系统服务费	服务内容：（1）提供该应用系统 5×8 小时的技术支持和技术咨询服务，重大故障请求 2 小时给予响应；（2）系统检查和补丁更新、运行状态监控、系统日志清理，以及以上问题的应急响应。

5.3 特种车辆基础设备运维

本项目含一台特种车辆运维，包括车载基础设备日常维修、维护费、通信费及车辆燃油费。

5.4 气象数据服务费

实现全岛常规气象要素格点化精细预报，针对应急管理需要，升级短时临近气象业务系统，构建基于气象观测分析的自然灾害预警业务应用，建立与应急厅

信息共享、协同联动的气象服务渠道。

序号	服务项目	功能	数量
1	数据总线传输维护	前置服务器、网络、数据推送的维护。	1 年
2	实况监测格点类产品	全省降水量、温度、湿度、风场的实况格点产品制作。	1 年
3	雷达卫星数据产品	包含雷达卫星资料收集、处理、校验以及产品制作。	1 年
4	格点预报数据产品	包含资料分析、预报分析以及 1*1km 预报产品制作。	1 年
5	其他各类接口数据接口维护	自动观测数据、预警信号等传输的接口维护。	1 年

（三）安全技术需求

1.物理环境安全需求

物理和环境安全主要是指由于网络运行环境和系统的物理特性引起的网络设备和线路的不可使用，从而会造成网络系统的不可使用，甚至导致整个网络的瘫痪。它是整个网络系统安全的前提和基础，只有保证了物理层的可用性，才能使得整个网络的可用性，进而提高整个网络的抗破坏力。

物理和环境安全包括机房选址、机房建设、设备设施的防盗防破坏、防火、防水、电力供应、电磁防护等，需要在数据中心机房的建设过程中严格按照国家相关标准进行机房建设、综合布线、安防建设，并经过相关部门的检测和验收。

2.通信网络安全需求

网络整体架构和传输线路的可靠性、稳定性和保密性是业务系统安全的基础，通信网络的安全主要包括：网络架构安全、通信传输安全、边界安全、防入侵、网络安全审计和网络安全的集中管控等方面。

2.1 网络架构安全

网络架构是否合理直接影响着是否能够有效的承载业务需要。因此网络结构需要具备一定的冗余性；带宽能够满足业务高峰时期数据交换需求；并合理的划分网段和 VLAN。

2.2 通信完整性与保密性

由于网络协议及文件格式均具有标准、开发、公开的特征，因此数据在网上

存储和传输过程中，不仅仅面临信息丢失、信息重复或信息传送的自身错误，而且会遭遇信息攻击或欺诈行为，导致最终信息收发的差异性。因此，在信息传输和存储过程中，必须要确保信息内容在发送、接收及保存的一致性；并在信息遭受篡改攻击的情况下，应提供有效的察觉与发现机制，实现通信的完整性。

而数据在传输过程中，为能够抵御不良企图者采取的各种攻击，防止遭到窃取，应采用加密措施保证数据的机密性。

3. 区域边界安全需求

3.1 边界隔离与访问控制

边界安全包括对接入网络和外联的双重安全管控要求，随着移动办公的发展，网络范围不断延展，无线网络的使用相对传统办公而言，对网络边界的有效管控更是严峻的考验；对于一个不断发展的网络而言，为方便办公，在网络设计时保留大量的接入端口，这对于随时随地快速接入到业务网络进行办公是非常便捷的，但同时也引入了安全风险，一旦外来用户不加阻拦的接入到网络中来，就有可能破坏网络的安全边界，使得外来用户具备对网络进行破坏的条件，由此而引入诸如蠕虫扩散、文件泄密等安全问题。因此需要对非法客户端实现禁入，同时，需要能够对内部用户非授权联到外部网络的行为进行限制或检查；并对无线网络的使用进行管控。

3.2 防入侵和防病毒

现今，病毒的发展呈现出以下趋势:病毒与黑客程序相结合、蠕虫病毒更加泛滥，目前计算机病毒的传播途径与过去相比已经发生了很大的变化，更多的以网络形态进行传播，并且，一旦病毒通过网络边界传入局域网内部，就已经对信息系统造成了破坏，因此，病毒防护手段需要在系统边界进行部署，在网络层进行病毒查杀，防止感染系统内部主机。

此外，来自互联网、其他非可信网络的各类网络攻击也需要通过安全措施实现主动阻断针对信息系统的各种攻击，如病毒、木马、间谍软件、可疑代码、端口扫描、DoS/DDoS 等，实现对网络层以及业务系统的安全防护，保护核心信息资产的免受攻击危害。

3.3 网络安全审计

安全技术措施并不可能万无一失，一旦发生网络安全事件，需要进行事件的追踪与分析，针对网络的攻击行为和非授权访问等行为，需要在网络边界、重要网络节点上进行流量的采集和检测，并进行基于网络行为的审计分析，从而及时发现异常行为，规范正常的网络应用行为。

4. 计算环境安全需求

信息设备存储和处理大量的业务信息，也是攻击者的最终目标，主机系统自身的漏洞一旦被攻击者利用，获取系统权限，将直接导致信息系统被破坏或数据泄露。此外，应用和数据是安全保护的对象，应用系统在开发过程中由于技术的局限性和开发管理的漏洞，总是存在一些安全漏洞，在系统上线后，被恶意攻击者利用，进而给单位的经济利益、业务、甚至声誉带来影响。

计算环境安全需求包括对主机和应用系统用户进行身份鉴别和访问控制、安全审计、对主机和各类终端的入侵防范和恶意代码防护、数据保密性和完整性保护、数据备份与恢复、剩余信息和个人信息保护。具体包括：

4.1 主机身份鉴别

主机操作系统登录均必须进行身份验证。过于简单的标识符和口令容易被穷举攻击破解。同时非法用户可以通过网络进行窃听，从而获得管理员权限，可以对任何资源非法访问及越权操作。因此必须提高用户名/口令的复杂度，并定期进行更换，或者，采取更可靠的身份鉴别措施。

4.2 主机访问控制

主机访问控制主要为了保证用户对主机资源的合法使用。非法用户可能企图假冒合法用户的身份进入系统，低权限的合法用户也可能企图执行高权限用户的操作，这些行为将给主机系统带来了很大的安全风险。用户必须拥有合法的用户标识符，在制定好的访问控制策略下进行操作，杜绝越权非法操作。

4.3 系统审计

对于登陆主机后的操作行为则需要进行主机审计。对于服务器和重要主机需要进行严格的行为控制，对用户的行为、使用的命令等进行必要的记录审计，便于日后的分析、调查、取证，规范主机使用行为。

4.4 恶意代码防范

病毒、蠕虫等恶意代码是对计算环境造成危害最大的隐患，当前病毒威胁非常严峻，特别是蠕虫病毒的爆发，会立刻向其他子网迅速蔓延，发动网络攻击和数据窃密。大量占据正常业务十分有限的带宽，造成网络性能严重下降、服务器崩溃甚至网络通信中断，信息损坏或泄漏。严重影响正常业务开展。因此除了在网络层采取必要的病毒防范措施外，必须在主机部署恶意代码防范软件进行监测与查杀，同时保持恶意代码库的及时更新。

4.5 应用系统安全功能开发

应用系统在开发过程中需同步考虑安全功能的实现，包括系统用户管理、身份认证、访问控制和应用安全审计等相关功能，并在应用系统开发过程中通过采用密码技术实现数据的完整性和保密性保护。

需要实现对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；对于重要信息系统需要采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现；

需要提供访问控制功能，对登录的用户分配账号和权限；授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。

需要提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

需要提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；在故障发生时，应自动保存易失性数据和所有状态，保证系统能够进行恢复。

需要提供剩余信息保护功能，保证释放内存或磁盘空间前，上一个用户的登录信息和访问记录被完全清除或被覆盖。

4.6 数据完整性与保密性

数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。具体包括：

需要采用校验码技术或密码技术保证重要数据在传输和存储过程中的完整

性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

采用密码技术保证重要数据在传输和存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

4.7 数据备份和恢复

对于关键数据应建立数据的备份机制，而对于网络的关键设备、线路均需进行冗余配置，备份与恢复是应对突发事件的必要措施。

四、运维方案

（一）基本思路

按社会化分工，通过公开招标方式，引入有经验和有技术实力的企业，提供专业化和高质量的运维外包服务，降低管理成本和非专业化自行运维可能出现的技术风险。

（二）基本原则

1.科学性原则

运行维护内容制定是在遵循国家和部相关标准规范的基础上，结合海南省应急管理厅信息化运维工作的要求和特点，科学划分运维业务分类、定额科目和成本单元，以及各成本单元的工作量与相应的业务经费。

2.可操作性原则

运行维护服务既要体现当前技术条件下信息化基础设施、应用支撑平台、应用系统等运行维护管理工作的内容，又要考虑信息技术飞速发展的特点和与相关业务的衔接与协调，并具有针对性和可操作性、易于使用和管理。

3.经济性原则

运行维护经费严格按财政经费预算和使用要求进行计算，并充分考虑可能的升级更新需求，坚持勤俭办事，以现行开支标准与实际情况为基础，兼顾当前与长远，讲究效率与效益。

（三）运维方案

1.机房及配套工程运维方案

从机房的空调系统、电源系统、配电系统、消防系统以及机房的环境监控系统对机房进行运维并且需要按照业主方要求对设备制定巡检方案。

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证操作系统正常运转。并提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对机房各设备进行全面检查，通过该工作获得运行的第一手资料，最大可能地发现存在的隐患，保障稳定运行。
3	现场故障处理	按服务级别：7×24 小时。
4	问题管理并记录	对遇到的问题进行汇总和报告。

2. 软硬件基础设施运维方案

2.1 网络与安全系统运维方案

从网络的连通性、网络的性能、网络的监控管理三个方面提供对网络系统的运维服务并且定期检查设备的日志文件，保证日志文件的保存期在六个月以上。

网络、安全系统运维的基本服务内容如下表：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证网络的实时连通和可用，保障接入交换机、路由器、网关和应用流量管理系统的正常运转。 并提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对设备及网络进行全面检查，通过该工作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。
3	设备保修及现场备件安装	在故障情况下，负责对故障设备进行维修或原厂返修，对需要备件顶替的进行现场安装调试。
4	现场软件升级	分析软件升级的必要性和风险，并软件升级。
5	现场故障处理	按服务级别：7×24 小时； 5×8 小时。
6	问题管理并记录	对遇到的问题进行汇总和报告。
7	运行分析及建议	通过对网络运行状况、安全问题进行周期性检查、分析，全面了解历史故障情况，并提出故障预防建议，最大程度减少网络及安全故障隐患，更高效的进行网络及安全管理。

2.2 服务器与存储系统运维方案

服务器与存储系统的运维服务包括主机、存储设备的日常监控，设备的运行状态监控，故障处理及补丁升级等内容并且定期检查设备的日志文件，保证日志

文件的保存期在六个月以上。

服务器与存储系统运维的基本服务内容如下表：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证主机、存储的连通和可用，提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对主机、存储设备进行全面检查的服务项目，通过该工作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。
3	设备保修及现场备件安装	在故障情况下，负责对故障设备进行维修或原厂返修，对需要备件顶替的对备件进行现场安装调试。
4	补丁服务	消除软件漏洞给系统带来的安全隐患，并对安装补丁所引起的系统连锁反应进行合理的平衡。
5	升级服务	对系统进行软件或硬件的升级，以改进、完善现有系统或消除现有系统的漏洞。
6	现场故障处理	按服务级别：7×24 小时。
7	问题管理并记录	对遇到的问题进行汇总和报告。
8	系统优化	对客户系统的主机、存储设备、操作系统、提供优化服务。

2.3 系统软件与其他工具软件运维方案

系统与工具软件的运维服务包括对操作系统运维、数据库运维等内容。

2.3.1 操作系统运维方案

操作系统运行维护服务是包括主动操作系统版本及补丁管理、性能资源监控等工作。通过管理可了解当前操作系统日常运行状态，识别问题发生在什么地方，有针对性地进行性能优化。同时，密切注意运行变化，主动地预防可能发生的问题。

操作系统运行维护的基本内容如下表：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证操作系统正常运转；并提供 7×24 小时的驻场技术支持服务。
2	定期现场巡检	对操作系统进行全面检查，通过该工作获得运行的第一手资料，最大可能地发现存在的隐患，保障稳定运行。
3	操作系统补丁升级	根据操作系统厂商提供的补丁，分析当前系统环境升级的必要性和风险，进行补丁升级
4	现场故障处理	按服务级别：7×24 小时。
5	问题管理并记录	对遇到的问题进行汇总和报告。

2.3.2 数据库运维方案

数据库运行维护服务包括主动数据库性能管理和数据备份管理，数据库的主动性能管理对系统运维非常重要。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。数据库数据备份管理是对数据库中正在运行的业务及相关数据，按建设方案设定的备份策略进行及时备份，备份数据的管理，以及当出现系统故障时，通过备份数据进行数据的恢复等工作。

具体数据库运行维护监控的基本服务内容如下表：

序号	服务模块	内容描述
1	数据库支持服务	每周 7 天，每天 24 小时驻场技术支持，以满足业务发展的需要。根据问题的严重程度，将优先解决客户认为是关键而紧急的任务。对客户提出的一般性问题进行技术咨询、指导。 定期的客户管理报告，避免问题再度发生。
2	数据库现场服务响应	数据库宕机； 数据坏块； 影响业务不能进行的数据库问题。
3	数据库健康检查	对数据库的配置及运作框架提出建议，降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张； 检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患； 检查数据库系统是否需要应用最新的补丁集； 检查数据库空间的使用情况； 监控数据库性能，确认系统的资源需求。
4	数据库产品性能调优	分析应用类型和用户行为，并以此评价并修改数据库的参数设置； 评价应用对硬件和系统的使用情况，并提出建议； 通过改善系统环境的稳定性来降低潜在的系统宕机时间。
5	数据备份检查及数据恢复	依据系统建设方案的数据备份策略，检查数据库备份的安全可用； 系统故障是进行数据备份的恢复； 定期进行备份数据的恢复演练。

2.4 应用系统运维方案

应用系统运维服务的方案及内容如下表：

序号	服务模块	内容描述
1	技术人员值守	长期的技术人员值守，保证应用系统的可用，提供 7×24 小时的驻场技术支持服务，根据用户的问题，进行用户故障分析，并分配给相关人员处理。
2	用户使用指导	基于应用系统最终用户的使用情况，通过电话、微信群、应用系统公告等方式，对用户系统使用过程中对系统应用不熟练或疑问的地方进行解答，并指导用户正常使用。 该项服务应区分于应用系统部署上线的批量集中培训。 按服务级别：7×24 小时； 5×8 小时。
3	系统错误修改	基于用户的反馈，及时判断并发现应用系统本身的错误，并及时进行修改； 按错误级别：程序错误 24 小时； 数据错误 8 小时； 配置错误 4 小时。
4	系统功能优化	基于应用系统最终用户的使用情况，对确实影响用户操作的功能缺陷进行修补优化； 该项服务应区分于基于业务需求的应用系统升级服务。原则上单次修改工作量不超过 3 人天在用户反馈后 3 个工作日内响应，并按与用户商定时间内完成修改。
5	问题管理并记录	对遇到的用户请求，包括使用问题、系统故障等进行汇总和报告。
6	优化升级建议	根据应用系统的用户使用情况，以及用户的业务发展趋势，评估当前应用的功能及性能，并提出优化升级建议。

2.5 其他运维服务方案

2.5.1 人员派驻服务

根据信息系统实际使用情况和运行状况，要求运维服务提供商安排 8 人（其中 3 人为技术人员，5 人为机房值班人员）进行 7*24 小时驻点维护，驻场人员需提供技术资质证书、当地社保记录，其中驻场技术人员需根据业主方要求派驻相关技术人员。对信息化系统设备进行日常的维护，服务内容包括上述各项服务中能够现场解决的部分内容，现场派驻人员不能提供的服务由运维服务提供商安排其他资源提供；同时需要运维服务提供商提供专业的人员对下面市县的运维设备进行每个季度的巡检；在战时，需要运维服务提供商提供更多的具有专业性质的人员进行现场系统的维护以保障系统的正常运行 以保障应急指挥的正常工作。

现场派驻人员需完成的主要工作包括：

项目相关软硬件的日常维护服务；

日常安全状态监控服务及故障处理（网络设备、服务器、存储设备、应用软

件、数据库的故障处理及日常巡检）；

病毒及网络安全防护维护、安全日志收集分析、系统升级、优化等安全加固服务；

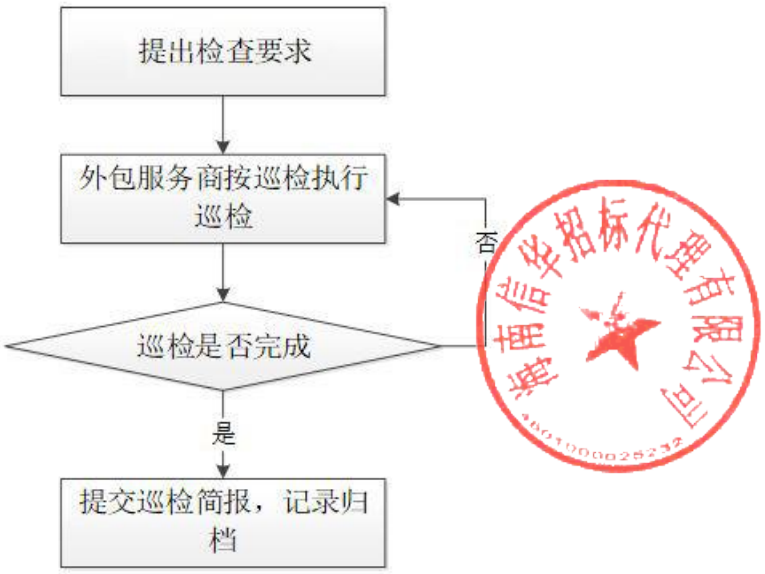
网络应急响应处理服务。

2.5.2 关键服务说明

系统维护是以预防为主，运维服务商安排工程师对清单中的设备定期检查机房环境，供电系统，设备软硬件运行情况、系统性能和物理连接等指标，及早发现故障隐患，减少系统宕机的机会，优化运行环境，延长设备寿命。

2.5.2.1 定期巡检服务

每次巡检结束，运维服务商现场工程师填写“定期巡检表”， 规划科技信息处的技术人员确认后签字。“定期巡检表”一式两份，规划科技信息处和运维服务商各存一份，最终出具正式的巡检总结报告，运维服务商应按以下流程制定严格的定期健康检查流程：



2.5.2.2 现场故障处理服务

服务内容主要包括：

●对于清单上的设备，根据故障现象，提供现场故障诊断，快速定位故障原因；

●进行 7×24 小时不间断故障处理，直至业务恢复；

●在设备出现硬件故障，需要更换时，运维服务商需提供备件保修服务；

●必要时触发故障升级管理流程；

●故障处理过程中，由服务热线通知故障申告人处理进展和状态；

●故障处理完毕后，由服务热线通知故障申告人确认，并做满意度调查，闭环管理。

故障等级划分如下表：

序号	故障等级	故障现象
1	P1 级	系统宕机或者不可用，不能保存进行中的工作，或者导致数据丢失等，导致对应的业务服务停止。
2	P2 级	系统严重告警或性能明显下降，业务系统不正常使用，导致对应的业务服务受到影响等。
3	P3 级	系统出现一般告警，或性能有所下降，对应的业务服务能够提供。

故障管理要求：

运维服务商应与设备和服务提供商需建立密切的合作和沟通关系，必要时可组织各方面的专家，共同解决复杂疑难故障。如果需要，运维服务商管理层需直接参与设备的维护服务，调度及整合更多资源，快速制定解决方案、监督解决过程，使故障得以快速、妥善地解决。

2.5.3 问题管理与记录服务

资料管理是维护工作的基石，运维服务商需在规划科技信息处许可的情况下，建立服务维护档案，以便在需要时可以快捷准确的查询。

服务内容如下：

●设备档案：建立清单中设备的资料库，内容包括厂家，型号，系列号，硬件配置，软件配置，地址配置，更换、升级记录等。

●服务记录：将提供服务记录和服务简报，包括热线服务记录，现场故障服务记录，专项服务记录，备件服务记录等，各项记录一式两份；定期向采购人提供服务简报，包括月度、半年和年度服务简报，将服务工作和维护建议定期向采购人汇报。

●分析报告服务:在每次故障处理结束后，都会向采购人提供故障分析报告服务；在我中心有需求时，提供系统性能分析报告、优化建议报告，变更分析报告等服务。负责对各种报告分类归档管理，方便查阅。

●服务结束后，提交年度运行维护服务报告，将一年来的日常巡检记录、各种故障处理情况、设备运行情况、设备健康状况详细记录，并根据我中心业务实

际情况对各级系统进行全面的评估，并提出优化和未来发展建议。

（四）运维制度与规范

1.服务制度方案

运维服务制度主要包括服务时间管理制度、服务行为规范制度和服务问题记录制度。具体内容如下：

1.1 服务时间管理制度

1.1.1 接收服务请求和咨询：在 5*8 小时工作时间内设置由专人值守的热线电话。

1.1.2 在非工作时间设置有专人 7*24 小时接听的移动电话热线，用于解决内部的技术问题以及接听 7*24 小时机房监控人员的机房突发情况汇报。

1.2.服务响应时间

序号	服务级别	响应时间	故障解决时间
1	I 级：属于紧急问题；其具体现象为：系统崩溃导致业务停止、数据丢失。	30 分钟，2 小时内提交处理方案。	12 小时以内
2	II 级：属于严重问题；其具体现象为：出现部分部件失效、系统性能下降但能正常运行，不影响正常业务运作。	30 分钟，2 小时内提交处理方案。	24 小时以内
3	III 级：属于较严重问题；其具体现象为：出现系统报错或警告，但业务系统能继续运行且性能不受影响。	30 分钟，2 小时内提交处理方案。	48 小时以内
4	IV 级：属于普通问题；其具体现象为：系统技术功能、安装或配置咨询，或其他显然不影响业务的预约服务。	30 分钟，2 小时内提交处理方案。	5 天内

技术支持人员在解决故障时，会最大限度保护好数据，做好故障恢复的文档，力争恢复到故障点前的业务状态。对于“系统瘫痪，业务系统不能运转”的故障级别，如果不能于 12 小时内解决故障，应在 16 小时内提出应急方案，确保业务系统的运行。故障解决后 24 小时内，提交故障处理报告。说明故障种类、故障原因、故障解决中使用的方法及故障损失等情况。

1.2 服务行为规范制度

●遵守最终用户的各项规章制度，严格按用户相应的规章制度办事。

●与其他部门和环节协同工作，密切配合，共同开展技术支持工作。

●出现疑难技术、业务问题和重大紧急情况时，及时向负责人报告。

●技术支持时要文明礼貌，语言清晰明了，语气和善。

●遵守保密原则。对被支持单位的网络、主机、系统软件、应用软件等的密码、核心参数、业务数据等负有保密责任，不得随意复制和传播。

1.3 服务问题记录制度

根据使用人员提出问题的类别，将问题分为咨询类问题和系统缺陷类问题二类：咨询类问题是指通过服务热线或现场解疑等方式能够当场解决用户提出的问题，具有问题解答直接、快速和实时的特点，该问题到现场支持人员处即可中止，对于该类问题的记录可使用咨询类问题记录模版进行记录。系统缺陷类问题是指使用人员提出的问题涉及到系统相应环节的确认修改，需要经过逐级提交、诊断、确认、处理和回复等环节，问题有解决方案后，将解决方案反馈给最终用户。具体提交流程如下：

●问题提交。应用信息系统的应用用户发现属于系统缺陷类的问题时，填写系统缺陷类问题提交单，提交服务支持单位。

●问题分析。服务单位接到用户提交的问题单，要组织相应人员对问题单中描述的问题进行分析研判，确定问题的类型(技术问题、业务问题或者操作问题)。属于技术问题，提交采购人对存在的问题提出具体的处理意见和建议；属于业务问题，提交服务中心业务人员进行处理；属于操作问题，可安排相关人员对问题提出人进行解释，并将系统缺陷类问题提交单转为系统咨询类问题提交单。

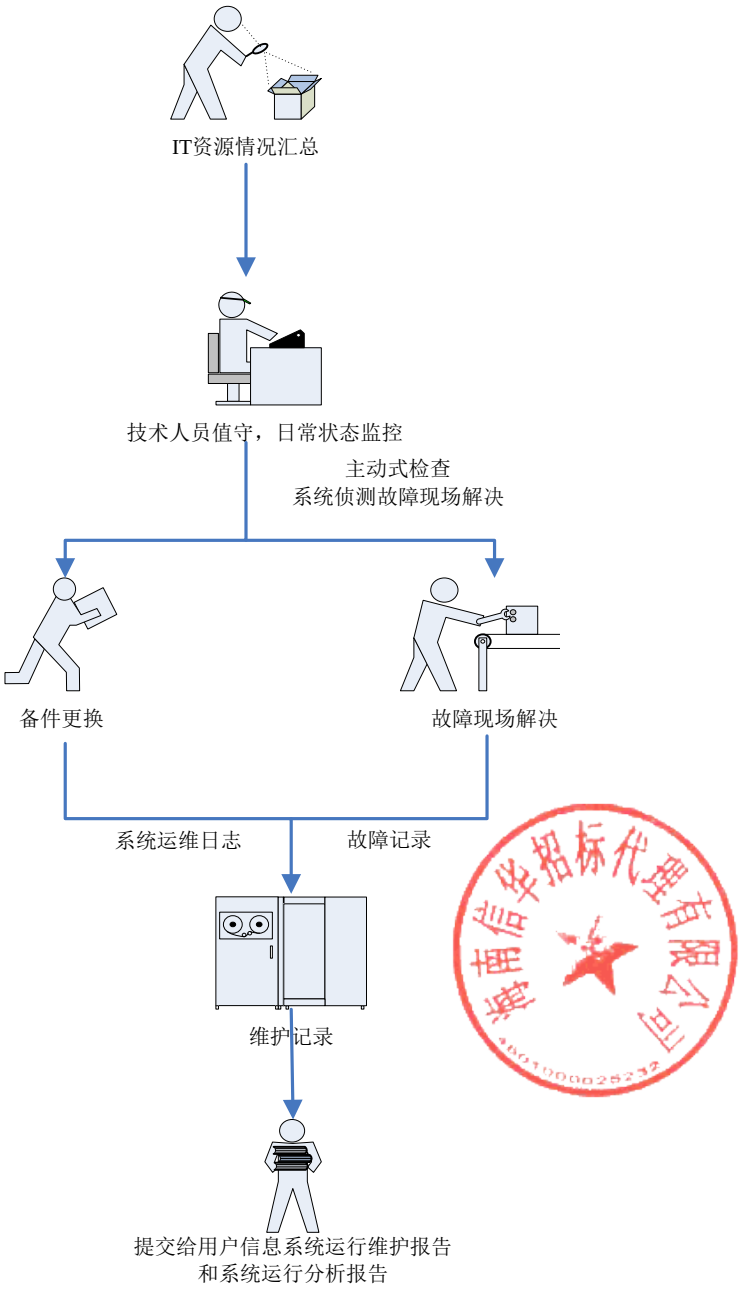
●问题确认、解决。采购人的技术人员和业务人员收到系统缺陷类问题提交单后，对提交的问题进行归类汇总和分析、确认。可以解决的，明确问题解决的具体处理建议和措施，经主管领导签字同意后，交实施人员进行解决方案的实施。服务人员确认是否解决，并将解决方法附在系统缺陷类问题提交单上反馈给问题提出人员。

●问题回复。服务中心根据提交的问题进行分析，制定解决方案并进行实施解决，同时做好变更记录。将解决方案汇总后及时向问题提交单位或问题交办单位做出回复，并将分析过程和问题产生原因一并提交。

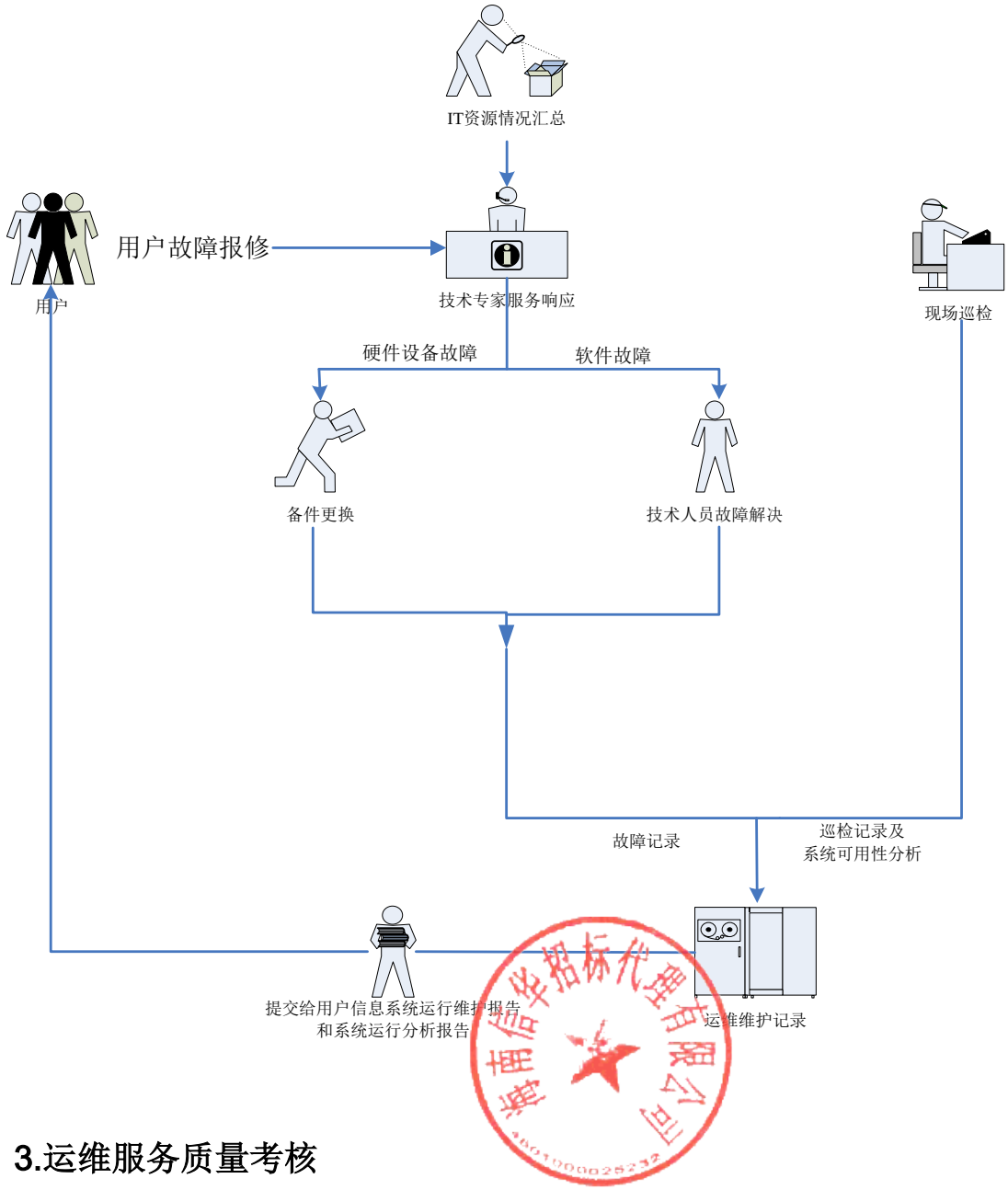
2. 服务流程方案

运维服务主要包括两个流程：一是为技术人员值守服务；二是定期巡检结合故障现场服务。

2.1 技术人员值守运行维护服务的基本操作流程如下图所示：



2.2 定期巡检结合故障现场运行维护服务的基本操作流程如下图所示：



3.运维服务质量考核

根据系统特性，要求运维服务商须接受以下指标管理要求。7×24（含节假日）小时响应并处理，不符合故障处理要求扣除相应的考评分数，若年终服务考评分低于 90 分，将相应扣减服务费用。

3.1 故障响应时间

序号	故障等级	故障响应时间	考评分值
1	最高	5 分钟	未按时响应扣 5 分。
2	高	10 分钟	未按时响应扣 3 分。
3	中	15 分钟	未按时响应扣 2 分。
4	低	30 分钟	未按时响应扣 1 分。

3.2 业务恢复时间

序号	故障等级	最后解决时限	考评分值
1	最高	4 小时	未在承诺的时间内完成扣 5 分。
2	高	8 个小时	未在承诺的时间内完成扣 3 分。
3	中	12 个小时	未在承诺的时间内完成扣 2 分。
4	低	24 个小时	未在承诺的时间内完成扣 1 分。

3.3 事件分析时间

序号	优先级代码	最后解决时限	考评分值
1	最高	8 小时	未在承诺的时间内完成扣 5 分。
2	高	16 个小时	未在承诺的时间内完成扣 3 分。
3	中	24 个小时	未在承诺的时间内完成扣 2 分。
4	低	48 个小时	未在承诺的时间内完成扣 1 分。

3.4 故障升级报告机制

序号	优先级别	通告路径(通知)
1	最高	登记 → 事件经理 离最终期限 2 小时 → 事件处理人、事件经理，甲方项目经理 已超时 → 事件处理人、事件经理、甲方项目经理、甲方主管部长 → 甲方主管领导。
2	高	离最终期限 4 小时 → 事件处理人、甲方项目经理 已超时 → 事件处理人、事件经理、甲方项目经理、甲方主管部长。
3	中	离最终期限 6 小时 → 事件处理人 已超时 → 事件处理人、事件经理、甲方具体负责人。
4	低	离最终期限 12 小时 → 事件处理人 已超时 → 事件处理人、事件经理、甲方具体负责人。

3.5 服务时间指标中各项参数说明表

序号	参数	定　义
1	响应时间	从服务台转入或其他系统转入或直接申告故障到得到响应的时间。
2	到现场时间	需现场服务时，从申告故障到工程师到达分行现场的时间。
3	业务恢复时间	从申告故障，到工程师彻底或临时解决故障、恢复业务的时间间隔。
4	事件分析时间	从故障临时解决/恢复业务到工程师提供事件情况分析报告的时间。
5	升级时间	从申告故障，到故障被升级到更高一级管理人员的时间间隔。

（五）项目服务要求

1. 项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准，在项目实施中投标人

须做到：

●提供完整的系统实施方案和项目实施管理办法；

●项目实施完成后提供可靠的后期技术服务工作；

●严格按照双方确定的计划进度保质保量完成工作；

●规范项目实施过程中的文档管理。

2.项目验收要求

项目验收须按照《海南省大数据管理局关于印发<海南省政务信息化项目建设管理实施细则（暂行）>的通知》要求，中标人提供详细的项目验收方案，经采购人审核通过后，由采购人组织，中标人及相关信息化项目验收专家人员组成的验收小组，对项目进行全面的验收。

B 包需求书

一、项目要求

通过委托专业网络安全等级测评服务机构，根据《中华人民共和国网络安全法》、《网络安全等级保护条例》、网络安全等级保护 2.0 标准等相关文件及标准要求，对采购人信息系统进行网络安全等级保护测评，并出具《网络安全等级保护测评报告》和《网络安全等级保护整改方案》，明细如下：

序号	信息系统/服务项目	备案级别	重要程度
1	海南省应急管理厅门户网站测评	三级	非常重要
2	海南省应急管理厅办公系统（OA）测评	三级	非常重要
3	应急管理“一张图”系统测评	三级	非常重要
4	遥感灾情辅助决策系统测评	三级	非常重要
5	海南省应急管理“一张图”测评	三级	非常重要
6	信息接入与会商决策系统测评	二级	非常重要
7	应急通讯融合系统测评	二级	非常重要
8	整改指导	测评结束后，按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，针对测评报告进行解读，并将技术措施和管理措施有机结合，建立网络安全综合防护体系，提供整改方案，协助指导整改，以达到提高网络整体安全保护能力。	
9	结果输出	一、《网络安全等级保护测评报告》 二、《网络安全等级保护整改方案》	

二、项目目标

通过网络安全等级保护测评服务，对采购人的信息系统开展符合性测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。找出问题，针对性的制定整改措施，推进网络安全防护体系不断完善。

三、测评依据

1.《中华人民共和国网络安全法》

2.《网络安全等级保护条例》

3.GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》

4.GBT 22240-2020 《信息安全技术网络安全等级保护定级指南》

5.GB/T 25058-2010《信息安全技术信息系统安全等级保护实施指南》

6.GB/T25070-2019《信息安全技术网络安全等级保护安全设计技术要求》

7.GB/T28448-2019《信息安全技术网络安全等级保护测评要求》

8.GB/T28449-2019《信息安全技术网络安全等级保护测评过程指南》

9.网络安全等级保护测评报告模板（2021 版）

四、服务人员要求

实施测评工作的技术人员必须具备公安部信息安全等级保护评估中心颁发的《网络安全等级测评师证书》。

五、服务内容

服务期内，测评机构须向采购人提供以下服务。

1.等级保护培训咨询服务

1.1 等级保护政策/标准咨询

随着国家信息安全等级保护的推进工作，信息安全等级保护政策、法律法规和标准体系也会相应的发布和更新，测评机构应针对本项目设立信息安全等级保护咨询平台，明确较为固定的咨询服务人员，并根据咨询要求提供正式的答复资料和文档。咨询内容包括但不限于信息安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

1.2 信息系统等级变更咨询

在信息系统出现等级变更时，测评机构须协助采购人对信息系统进行分析，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

1.3 等级保护建设整改咨询

按照信息系统安全总体方案要求，测评机构须结合信息系统安全建设项目计划，根据信息安全等级保护相关标准和规定，对采购人等级保护建设整改工作提供全面的安全方案的详细设计咨询，结合采购人的实际情况，协助采购人进行分

布或分期地落实安全技术与管理措施，并根据预期实现的安全目标，全程提供在建安全设备和系统的测试、验收工作等咨询服务。

1.4 信息系统安全检查咨询

在我厅开展信息系统安全检查时，全程提供咨询服务，包括检查范围、检查方法、检查结果分析以及整改措施制定等。

1.5 等级保护测评咨询

测评过程中，测评机构应协助用户单位参照《网络安全等级保护测评要求》中评估内容和方法，对测评过程中所涉及到的评估项及测评过程中所编制相关表格、填写项提供全程咨询服务，确保测评工作的顺利开展。

1.6 相关政策、法规、技术标准的培训。

测评机构应向甲方提供完整的培训方案，对信息安全等级保护相关政策、法规、技术标准进行全面培训。

2. 等级保护测评服务

依据《中华人民共和国网络安全法》、网络安全等级保护 2.0 标准等相关文件及标准要求，对采购人信息系统的安全技术体系和安全管理体系等进行合规性检查，出具《网络安全等级保护测评报告》，并提出具有针对性的整改建议。

2.1 测评内容

对采购人的信息系统进行摸底、分析和梳理，提出详细的等保测评方案。

对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

●安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评。

●安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

●完成测评工作后，提出整改建议；最后出具符合公安部门要求的信息系统安全保护等级测评报告，并在后期整改实施过程中提供全程咨询服务。

2.2 测评实施

网络安全测评项目过程需按照《网络安全等级保护测评过程指南》开展工作，

等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

2.2.1 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

序号	项目内容	工作内容	成果输出
1	项目启动	1.组建测评项目组； 2.编制《项目计划书》； 3.确定采购人应提供的资料。	向用户提交 《项目计划书》 《提供资料清单》。
2	信息收集分析	1.整理调查表单； 2.发放调查表单给采购人； 3.协助采购人填写调查表； 4.收回调查结果； 5.分析调查结查。	《系统基本情况分析报告》。
3	工具和表单准备	1.调试测评工具； 2.模拟被测系统搭建测评环境； 3.模拟测评； 4.准备打印表单。	确定测评工具（测评工具清单） 《现场测评授权书》 《测评结果记录表》 《文档交接单》。

2.2.2 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。详细要求见下表：

序号	工作内容	工作详细任务	输出成果
1	测评对象确认	识别被测系统等级； 识别被测系统的整体结构； 识别被测系统的边界； 识别被测系统的网络区域； 识别被测系统的重要节点和业务应用； 确定测评对象。	《测评方案》的测评对象部分。
2	测评指标确定	识别被测系统业务信息和系统服务安全保护等级； 选择对应等级的 ASG 三类安全要求作为测评指标； 就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标。	《测评方案》的测评指标部分。
3	工具测试点确定	确定工具测试的测评对象； 选择测试路径； 确定测试工具的接入点。	《测评方案》的测试工具接入点部分。
4	测试内容确	识别每个测评对象对象的测评指标；	《测评方案》的

	定	识别每个测评对象对应的每个测试指标的测试方法。	单项测评实施和系统测评实施部分。
5	测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册； 针对没有现成测评指导书的测评对象，开发新的测评指导书。	《测评方案》的测评实施手册部分。
6	测评方案编制	描述测评项目基本情况和工作依据； 描述被测系统的整体结构、边界和网络区域； 描述被测系统的重要节点和业务应用； 描述测评指标； 描述测评对象； 描述测评内容和方法。	向用户提交《测评方案》。

2.2.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。详细要求见下表：

序号	工作内容	工作详细任务	输出
1	现场测评准备	现场测评授权书签署； 召开现场测评启动会； 双方确认测评方案； 双方确认配合人员、环境等资源； 确认信息系统已经备份； 测评方案、结构记录表格等资料更新。	会议记录、确认的授权委托书、更新后的测评计划和测评方案。
2	现场测评和结构记录	依据测评指导书实施测评； 记录测评获取的证据、资料等信息； 汇总测评记录，如果需要，实施补充测评。	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果：技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果：技术安全测评的物理安全和
3	结果确认和资料归还	召开现场测评结束会； 测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可； 测评人员归还借阅的各种资料。	

			管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件。

2.2.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。详细要求见下表：

序号	工作内容	工作详细任务	工作依据（模版）
1	单项测评结果判定	分析测评项所对抗威胁的存在情况；	等级测评报告的单项测评结果部分。
		分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较；	
		综合判定单个测评项的测评结果。	
2	单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果；	等级测评报告的单项测评结果汇总分析部分。
		判定每个测评对象的单元测评结果。	
3	整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况；	等级测评报告的系统整体测评分析部分。
		分析被测系统整体结构的安全性对结果的影响情况。	
4	风险分析	整体测评后的单项测评结果再次汇总；	等级测评报告的风险分析部分。
		分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性；	
		分析威胁利用安全问题后造成的影响程度；	
		为被测系统面临的风险进行赋值；	
		评价风险分析结果。	
5	等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数；	等级测评报告的等级测评结论部分。
		形成等级测评结论。	
6	测评报告编制	概述测评项目情况；	等级测评报告提交用户。
		描述被测系统情况；	
		描述测评范围和方法；	

		描述整体测评情况；	
		汇总测评结果；	
		描述风险情况；	
		给出等级测评结论和整改建议。	

六、服务要求

1. 调研和评估

测评机构须给出采购人在进行调查和评估时所需要提供的信息列表，并经采购人确认。采购人有权利不提供信息列表以外的任何信息。

安全评估必须按照分层的原则，包括但不限于以下对象：物理环境、网络结构、网络服务、主机系统、数据、应用系统、安全系统、安全相关人员、处理流程、安全管理制度、安全策略等。

在评估前，测评机构应详细描述安全调查和评估的组织方式，包括组成的人员及分工、评估的过程组织、实施时间安排、评估方式所遵循的标准等。测评机构需要描述调查和评估过程的步骤，每一步骤的具体内容、时间安排、详细实施过程、可能对网络及主机造成的影响等等。

安全调查和评估的过程中，测评机构如需采购人配合，测评机构需要详细描述需要配合的内容。如需要采购人协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由测评机构给出具体示例。采购人有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由测评机构负完全责任。

安全调查和评估过程中，如需使用安全工具，请详细描述所使用的安全工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求等。所使用的安全工具必须具备公安部颁发的《计算机安全产品销售许可证》。

测评机构应向采购人提供详细的评估的原始材料、各种表单及结果报告。

测评机构需要详细描述本次评估采用的评估方式及标准。

2. 信息系统安全等级保护符合性测评

按照公安部制订的网络安全等级测评报告格式编制等级测评报告，报告中必须明确相应信息系统是否满足等级保护要求。

●符合省级以上公安部门提出的网络安全等级保护测评相关要求。

●测评过程中应确保符合国家标准规范；

●测评过程中应确保软硬件环境的稳定性、运行正常；

3. 整改方案编制

测评机构需根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合采购人实际情况，且能够切实解决问题。

整改建议方案应明确设计依据、整改内容、整改方案、能够解决的问题、投资概算以及风险评估。

在整改实施过程中，测评机构应全力支持，负责技术把关、整改验收以及其他咨询工作。

4. 交付成果和报告

测评机构需在合同签订之日起 90 天内交付成果和报告，包括上述 7 个待测评系统的《网络安全等级保护测评报告》和《系统网络安全整改建设方案》，以及测评过程材料，包括调研表、技术测评记录、会议纪要等。

5. 服务验收标准

5.1 服务验收须满足以下所有条件：

符合信息系统等保测评验收文档要求，文档要求齐全、规范、准确、详细：

●完成网络安全的测评工作，并出具《测评报告》；

●针对性的制定整改方案，并出具《整改建议方案》；

●提交调研表、技术测评记录、会议纪要等服务过程材料；

5.2 售后服务要求

对于现状测评过程中发现的安全问题，中标人应先出具问题汇总报告，并给采购人预留三十天的整改时间，整改完成后中标人提供一次全面问题复查，并出具《网络安全等级保护测评报告》。同时招标针对本次测评范围内的问题提供一年期的技术咨询服务。