编号：YW-004

青岛慧海联创信息技术有限公司

运维服务实施方案

目录

一、运维实施体系

1.1 运维服务对象

青岛慧海联创信息技术有限公司通过提供技术人员到平度市民服务中心驻场服务，服务期限自招标通过之日起两年，驻场期间负责维护各业务应用系统运作基础环境，并结合用户现有的环境、网络结构、IT资源和管理流程的特点，从流程和技术方面来规划用户的网络信息系统的结构。保证用户的运行目标、业务需求与IT服务一致。

1.2 项目驻场服务人员名单

我方提供驻场运维服务人员 8 人，其中刘宁宁为负责安全管理接口的运维管理员。

序号	姓名	资格证书
1	郑永伟	ITSS IT 服务项目经理证书、信息安全保障人员认证证书、中级网路工程师
2	宫海亭	CIIP-A 证书、信息系统项目管理师
3	刘宁宁	信息安全保障人员认证证书、CIIP-A 证书

4	姜海鹏	ITSS IT 服务工程师证书、信息安全保障人员认证证书
5	常兴旺	ITSS IT 服务项目经理证书
6	张军通	ITSS IT 服务工程师证书
7	张鹏宵	ITSS IT 服务工程师证书
8	郭超	ITSS IT 服务工程师证书、三级高级技能维修电工证书

1.3 运维服务交付物

1、服务范围内设备日常巡检，包括每天三次中心机房巡检和各层弱电间巡检，检查交换机、服务器等设备工作状态，检查弱电间和机房环境，及时发现并排除隐患。
2、服务范围内设备故障处理，对服务范围内交换机、安全设备、服务器等设备出现故障时，启动应急预案，按照流程进行处理。
3、在出现紧急安全事件时，严格按照应急预案流程处理，消除安全事件对业务环境产生的不利影响。
4、准备充足的备品备件，包括但不限于运维范围内核心设备的备品备件，便于突发故障时随时进行更换。
5、提供季度、年度的运维工作报告，提供运维期间中心机房、弱电间巡检表，提供故障处理、调优、变更事件记录，向用户展示提供运维服务期间的工作内容以及服务范围内各个系统的运行情况。
6、向用户提供服务范围内各系统的优化改进意见。

2 常规使用流程

2.1 巡检流程

2.1.1 巡检流程适用范围

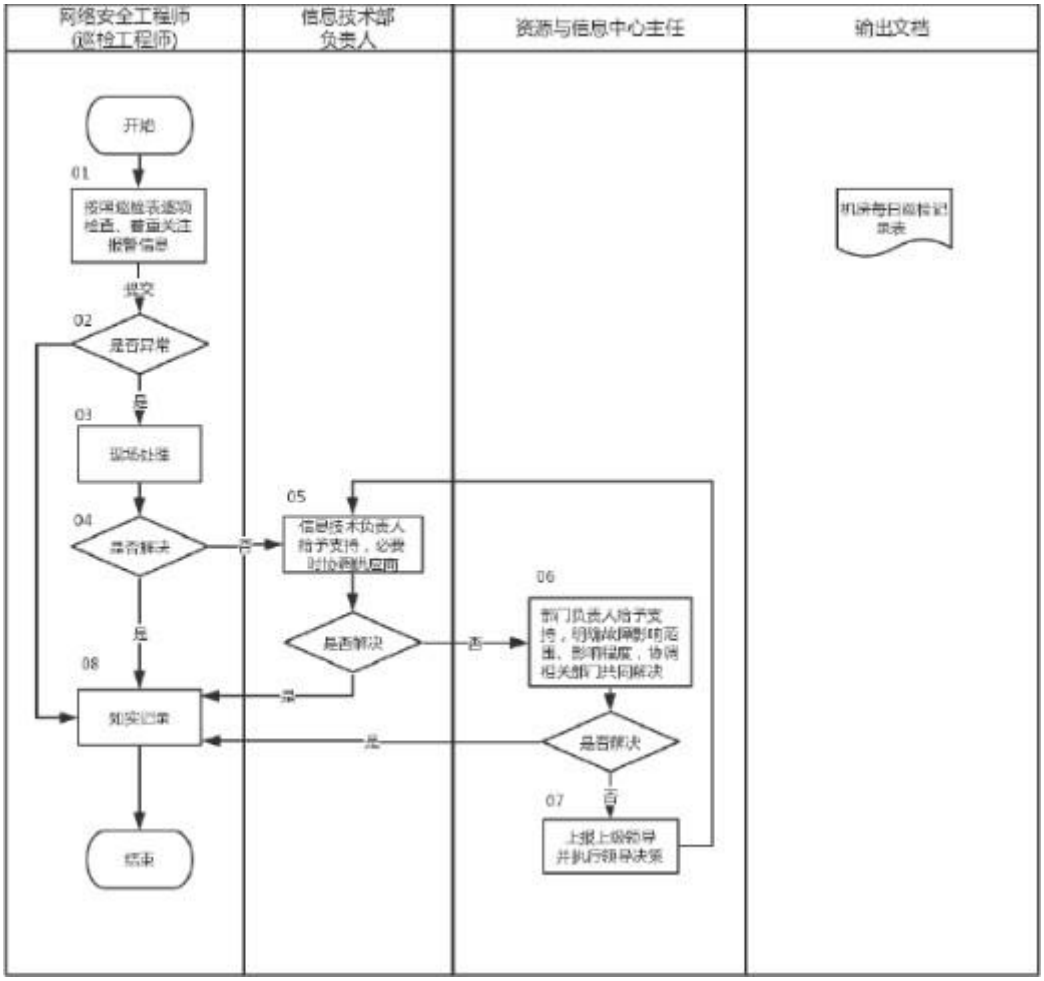
2.1.2 日常巡检时间

巡检时间	
早上	8:00
下午	14:00
晚上	20:00

2.1.3 日常巡检作业顺序

序号	作业顺序	作业要求
1	弱电间环境	检查大门、室内卫生、照明、桥架等
2	机柜	检查交换机、配线架、网线、光纤等
3	消防设备	检查灭火器

2.1.4 机房巡检流程



1) 我方提交巡检方案给用户；

2) 用户通知巡检；

3) 我方工程师进入现场巡检；

4) 巡检完毕后，收拾好现场并于五个工作日内提交巡检报告给用户。

2.1.5 中心机房巡检细则

一、定期巡检

1. 机房实行定期巡检制度。

2. 维护人员必须保证每天对机房巡检两次，确保上班时和下班之后机房设备运行正常。

3. 按要求认真填写《机房巡检记录表》，并进行妥善保存。

4. 上班时间要集中精力，坚守岗位，不得借故离岗。

二、机房巡检

1. 认真履行岗位职责，按照《日常巡检内容》进行巡检。

2. 实时监测网络运行状态，发现异常情况，应及时处理，并及时上报相关领导或者负责人。

3. 上班时间内发现故障，应及时快速地予以处理，并填报故障记录；情况比较严重的，应及时上报相关领导或领导人。

4. 未经相关领导批准，不得任意改变系统设备工作状态或关闭设备，不得随意切断用户网络线路。

5. 如遇电源变化，气候恶劣等情况时，应加强巡检，发现异常情况及时与相关人员联系。

6. 发生故障时，维护人员应立即用电话通知相关业务部门，把故障情况和初步检查结果告诉对方，并请对方协助检

7. 维护人员必须及时、准确、完整地填写巡检记录和故障处理记录。

8. 严格遵守机房巡检制度和安全保密的相关制度。

三、检查项目要求：

1. 电源、UPS：检查机房供电状况，UPS 工作情况、指示状态。

2. 服务器：检查服务器是否当机，服务器（磁盘阵列）硬盘灯指示是否正常。

3. 机房环境：检查机房空调工作状态，机房温度。

4. 网络设备：检查网络设备，包括交换机、路由器、防火墙等及其属设备。检查设备工作状态。

5. 网络通道：检查内外网络通道状态。

四、情况记录

各检查项目如无异常情况，在正常或异常栏中打“√”，如有异常情况，做好详细情况说明并及时上报信息中心领导。

五、其他要求

一周打扫一次机房。

2.1.5.1 整体机房环境

检查项	结论	情况摘要	检查项	结论	情况摘要
温度	□ 正常 □异常	℃	湿度	□正常 □异常	%
痕迹	□ 正常 □		清洁	□正常 □	

	异常			异常	
异响	□有 □无		异味	□有 □无	

注：痕迹检查地面、墙壁、天花是否有裂痕、水渍，机房内是否有鼠患、蚁患、蟑螂活动的痕迹，正常室温：20~25℃

2.1.5.2 机房运行设备

平度市市民服务中心机房运行设备有：光纤收发器、防火墙、 上网行为管理系统、服务器、交换机、网关等。

2.1.6 弱电间巡检细则

1.巡检维护人员须有高度的责任心，并按规定的时间、要求进行巡检维护。巡检时须带好必备的工具和相关巡检记录，巡检时应注意人身与设备的安全，发现重大问题立即报告。

2.所有弱电间及其他前置设备每月巡检一次，巡检维护内容；运行状态、环境卫生、箱内外积尘清除、连接导线的螺丝紧固，前端装置设备运行情况 等。

3.所有烟感、温感、水流批示器、报警按钮、联动装置，每年由物业公司组织检验一次。

5.所有应用软件应做好备份，每年应审核一次备份的有效性，做过数据修改或应用软件有应运的应另作备份。

6.每年对弱电的各个系统的运行功能做一次全面的抽样测试。

7.巡检时，发现一般问题应立即解决，发现复杂总是应向项目经理请示，因故没有处理的应及时报告。

8. 详细做相关巡视记录。

2.1.7 常见异常现象及处理方法

1、服务器常见故障及现象

有关服务器无法启动的主要原因 ：

①市电或电源线故障(断电或接触不良)

②电源或电源模组故障

③内存故障(一般伴有报警声)

④CPU 故障(一般也会有报警声)

⑤主板故障

⑥其它插卡造成中断冲突

2、服务器无法启动

①检查电源线和各种 I/O 接线是否连接正常。

②检查连接电源线后主板是否加电。

③将服务器设为最小配置(只接单颗 cpu，最少的内存，只连接显示器和键盘)直接短接主板开关跳线，看看是否能够启动。

④检查电源，将所有的电源接口拔下，将电源的主板供电口的绿线和黑线短接，看看电源是否启动。

⑤如果判断电源正常，则需要用替换法来排除故障，替换法是在最小化配置下先由最容易替换的配件开始替换(内存、cpu、主板)。

3、系统频繁重启

造成系统频繁重启的原因：

①电源故障(替换法判断解决)

②内存故障(可从BIOS 错误报告中查出)

③网络端口数据流量过大(工作压力过大)

④软件故障(更新或重装操作系统解决)

4、服务器死机故障判断处理

服务器死机故障比较难以判断，一般分为软件和硬件两个方面。

1、第一方面-软件故障

①首先检查操作系统的系统日志，可以通过系统日志来判断部分造成死机的原因。

②电脑病毒的原因。

③系统软件的 bug 或漏洞造成的死机，这种故障需要在判断硬件无故障后做出，而且需要软件提供商提供帮助。

④软件使用不当或系统工作压力过大，可以请客户适当降低服务器的工作压力来看看是否能够解决。

2、第二方面-硬件故障

①硬件冲突

②电源故障或电源供电不足，可以通过对比计算服务器电源所有的负载功率的值来作出判断。

③硬盘故障(通过扫描硬盘表面来检查是否有坏道)

④内存故障(可以通过主板 BIOS 中的错误报告和操作系统的报错信息来判断)

⑤主板故障(使用替换法来判断)

⑥CPU 故障(使用替换法)

⑦板卡故障(一般是SCSI/RAID 卡或其他pci 设备也有可能造成系统死机，可用替换法判断处理)

注意：系统死机故障需要在处理完后需要在一段时间内进行一定压力的拷机测试来尽一步检查故障是否彻底解决。

5、安装操作系统时提示找不到硬盘

故障原因：

① 无物理硬盘设备。

② 硬盘线缆连接问题。

③ 没有安装硬盘控制器驱动或驱动不相符。

6、如何获得驱动程序

使用随机光盘制作相应驱动。

7、用正确的驱动仍然无法加载硬盘控制器驱动

查看是否启用了 hostraid 功能。

8、新购硬盘，安装到机器后，机器自检无法通过

①将新的硬盘取下，机器是否可以自检通过;

②检查新增加的硬盘的 ID 号是否与原来的硬盘的 ID 号相同，如果硬盘的 ID 号相同的话，自检将无法通过。

9、如何格式化 SCSI 硬盘

1、有操作系统的情况：使用磁盘管理工具格式化;

2、无操作系统的情况：在 SCSI 管理控制界面格式化;

3、以 ADAPTEC Raid 卡为例：开机-出现 CTRL+A 信息时，按 CTRL+A 进入

①选中通道 A;

②选中SCSI UTILITY-将检测到硬盘-选中要检测的硬盘;

③选中FORMAT 可对硬盘进行全面格式化;

④选中VERIFY 可对硬盘进行检测，检查是否有坏道;

注意：在格式化硬盘时不能中断或停电，不然会损坏磁盘。

10、在Aisino 系列中有RAID 卡机器，当其中一个硬盘不能正常工作 RAID 报警，但系统能正常运行，怎么办

1、用一个新硬盘，确保容量大于或等于不能正常工作的硬盘，最好用相同型号的硬盘替换即可。

2、RAID 卡相关常见故障

第一类：RAID 卡本身有问题

①经常表现为 RAID 信息丢失，硬盘经常掉线，不能做 REBUILD，开机自检时检测不到硬盘或时间长。

典型故障A：作完 RAID1，安装操作系统，一切正常，但第二次重启系统时，发出报警声，经检查发现一块硬盘掉线，REBUILD 后，又恢复正常，但重启后又掉线。怀疑为硬盘故障，校验硬盘后均无问题。最后更换 RAID 卡，故障解决。

典型故障B：机器经常死机，且有时候启动速度非常慢。观察系统日志，发现在系统启动时有这样一个错误提示：设备/devices/scsi/port0 在传输等待的时间内没有响应。更换 RAID 卡后，恢复正常。

第二类：硬盘本身问题

①表现为硬盘掉线，在 RAID 阵列中的状态为 DEAD，或者在作REBUILD时，作到某一进度就不能继续。

典型故障：硬盘掉线后，做 REBUILD 时，作到 20%时出现错误提示无法继续进行。在确认掉线硬盘，硬盘盒及 SCSI 电缆都能正常工作后，对在线硬盘进行校验，发现有坏道，修复硬盘，重做 REBUILD，恢复正常。

第三类：硬盘盒或模组的接触问题

①此类问题经常表现为RAID 卡根本检测不到硬盘，此类问题比较简单，但在处理硬盘盒相关机器时，需要注意一些问题。

典型故障：RIAD 卡中检测不到硬盘，把 SCSI 电缆接到主板的 ULTRA160 接口上，故障依旧，拔出硬盘盒(不包括硬盘盒后面的托架)更换，故障依旧，更换硬盘，还是不行。最后卸下硬盘盒后面的托架(非热插拔部分)，发现后托架上 80PIN 接口上的一根针弯曲，校直弯针，恢复正常。

11、在服务器上使用的 SCSI 硬盘，为什么硬盘的 ID 号不能设置为 7

SCSI 控制器中，默认将 ID=7 设置为硬盘控制器占，所以硬盘的 ID 号不能设置为 7。

12、为什么开机自检无法通过

解决方法：

①机器切断电源，将机箱打开，用“COMS CLEAR”跳线的跳线帽将“COMS

CLEAR”跳线的另外两个针短接(跳线参看主板说明书)。

②机器加电，自检，等机器自检完闭，报 CMOS 已被清除，然后将机器电源关掉，把跳线复原即可。

③机器重新开机。

13、物理内存插槽报错

解决方法：

开机-按 F2 进入“SETUP”-“ADVANCED”--“MEMORY CONFIGURATION”回车-“CLEAR DIMM ERRORS”直接回车。

2.2 事件处理流程

2.2.1 事件处理适用范围

适用于平度市市民服务中心项目管理、系统监测、运行维护、培训服务、集成服务等应对活动。

2.2.2 技术服务支持流程

我公司提供为期 1 年运维服务项目。

在运维服务期内，我方提供及时周到的服务，现场运维值班人员实行 7*24 小时值班制。重要会议、节假日、恶劣天气夜间提供双岗值班。

对于服务请求，电话铃响两声内及时拿起电话回应，受（授）电话要语言明确、口齿清晰、语音适中，使用普通话，态度和蔼，用语文明，应先问对方“您好”达到 100%的用户响应度。接到客户的报修电话，应在《电话接听记录表》中详细记录来电人的单位、姓名、联系电话及服务要求，并及时反馈至当日值班技术主管处。

附件：<<电话接听记录表>>

序号	来电时间	来电单位/姓名	来电号码	来电事由	处理人员/时间	处理结果	备注
1							
2							
3							
4							

5							

出现故障后，20 分钟内协助用户排除故障，达到 98%以上的故障解决率。

回访用户平均满意度不低于 98%。

紧急、特殊的服务要求应立即提供服务至解决问题为止。

未能及时完成服务请求的，应向用户提出书面解释。

现场人员不能排除故障，我方技术支持人员在 30 分钟内到达现场维修。

总结周、月、季度的主要工作、完成情况、存在问题及处理办法，通过报表形式汇报给招标方。

以全年主要工作内容为主，总结存在的问题和不足，提出改进办法以报表的形式汇报给招标方。

对于 38 个数据中心机房、信息机房和网络接入间，每日早 8:00，中午 14:00，夜间 20：00 按时进行三次巡检工作，（特殊天气提前 30 分钟巡检，并增加应急人员）巡检人员每次到达巡检点后用巡更机采集信息源信息。巡检记录每天收集汇总存入计算机。管理人员用巡检管理软件汇总后的数据进行统计分析，以考核人员的工作情况。发生故障时，10 分钟内到达现场，30 分钟内完成维修更换工作，在故障解决过程中，随时保持与客户进行情况汇报。

3 变更流程

3.1 变更流程适用范围

适用于我公司为平度市市民服务中心提供的基础环境运维服务、硬件运维服务、软件运维服务。

3.2 变更注意事项

1、变更的风险评估按照质量风险管理标准执行，变更前风险评估由变更部门在起草打分完成后与变更申请表一并上交，由变更风险评估小组来审核批准风险评估内容并以此制定行动计划。变更各项活动完成后，变更后风险评估由变更部门起草打分完成后由变更评估小组来审核批准，关于变更的风险评估请注意以下几点：

1）变更前后风险评估应运用失败模式效果分析（FMEA）工具，不再使用文字性描述的形式进行风险评估。

2）变更前风险评估起草审核批准时间与变更申请表的变更申请时间为同一天；变更后风险评估起草审核批准时间与变更批准表的变更批准时间为同一天。

3）变更风险评估报告应有评估小组人员的会签表，风险评估报告审核批准人员应与变更申请批准表中评估小组人员对应一致。

4）变更涉及的风险评估报告版本为 01 版。

5）变更风险评估中应评估对产品的具体风险，以及对关键质量属性的风险，特别是主要变更。

6）使用 FEMA 工具进行风险评估时，严重性（S）/可能性（P）/可检测性（D）的分值保留小数点后一位，并按照只进不舍的原则确定；RPN 的分值按照只进不舍取整的原则确定。

7）变更部门在进行风险评估打分时，一定注意打分的合理性，现在此项内容是外部检查的一个重点。

2、变更类别应依据定义进行判定，不能将高级别的判定成了低级别的。

3、注意时间的逻辑顺序：

1）变更行动计划的预计完成日期最好与实际完成日期不要差太多，每一项行动计划的预计完成日期应体现出先后顺序，不能为同一天。

2）对于新增设备，应当先进行文件修订、人员培训后，再进行验证。

3）变更设计的工艺规程、SOP 等文件修订的完成时间，应为文件的最

终批准时间。

4）文件修订后人员培训的完成时间，应为培训效果评估的最终完成时间。

5）变更涉及验证的完成时间，应为验证报告的最终批准时间。

6）变更涉及的 SOP 修订后生效日期应在变更批准之后。

7）变更实施日期应在变更涉及的 SOP 修订生效日期之后等。

4、变更前后情况及原因等事项内容必须描述完整和准确，行动计划内容应详细说明具体的行动。

5、变更行动计划由 QA 签字确认，QA 在签字时必须明确需要执行的内容，以便对行动的完成情况进行追踪确认。如果发现实际执行措施与计划内容不一致，QA 及时进行反馈。

6、对于次要变更，将变更实施后一周内涉及本次变更的具体生产活动内容写入变更实施追踪表；对于主要变更，将变更实施后涉及本次变更的具体生产活动写入变更实施追踪表，在进行变更效果评估时，变更实施追踪时间应为开始追踪时间，变更效果评估时间应为完成追踪时间。

7、变更批准时，变更涉及的验证报告及修订后的文件必须再支持性的文件内容中列出，变更后的支持性文件除 SOP、验证方案报告、图纸外，对于新增设备还应当包括设备预防性维护等相关材料。

8、审核好变更记录中的变更编号和受控流水号。

9、变更评估小组人员签名后日期未签，应由小组成员中最后一人签字，为避免此类问题的发生，请变更签名人员上交变更时进行复核。

10、变更证明材料必须按照要求附全，变更风险评估报告上交原件，其余证明材料上交复印件。

11、最终上交的变更请注意将用铅笔填写的内容擦除。

12、注意空格部分的划线签名并标注日期。

13、存档部门和变更部门均应建立相应的变更登记表，以便对变更进行统计、分析及其他管理工作的进行。

4 安全事件判断和应急预案

4.1 安全事件判断

4.1.1 安全事件级别定义

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

4.1.2 安全事件分级标准

安全事件分类	安全事件子类	等级	信息泄漏（Confidentia	
			核心商密	普通商密
有害程序事件（MI）	计算机病毒事件（CVI）	三级		
		二级		
		一级		
	蠕虫事件（WI）	三级		
		二级		
		一级		
	木马事件（THI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	僵尸网络事件（BI）	三级		
		二级		
		一级		
	混合攻击程序代码（BAI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	网页内嵌恶意代码事件（WBPI）	三级		
		二级		
		一级		
	其他有害程序事件（OMI）			
网络攻击事件（NAI）	拒绝服务攻击事件（DOSAI）	三级		
		二级		
		一级		
	后门攻击事件（BDAI）	三级		
		二级		
		一级		
	漏洞攻击事件（VAI）	三级		
		二级		
		一级		
	网络扫描窃听事件（NSEI）	三级		
		二级		
		一级		
	网络钓鱼事件（PI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	干扰事件（II）	三级		
		二级		
		一级		
	访问流量异常事件（TEI）			
	其他网络攻击事件（ONAI）			
	篡改事件（IAI）	三级		>=1个

信息破坏事件（IDI）	篡改事件（IAI）	二级	>=1个	>=300个
		一级	>=100个	>=1000个
	信息假冒事件（IMI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	信息泄露事件（ILEI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	信息窃取事件（III）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	信息丢失事件（ILOI）	三级		
		二级		>=1个
		一级	>=1个	>=100个
	其他信息破坏事件（OIDI）			
运维风险管控事件（OMRCI）	系统操作审计事件（SOAI）	三级		
		二级		
		一级		
	访问互联网行为事件（AIBI）	三级		
		二级		
		一级		
	账号异常事件（AEI）	三级		
		二级		
		一级		
	其他操作风险事件（OORI）			
信息内容安全事件（ICSI）	违反宪法和法律、行政法规的信息安全事件	三级		
		二级		
		一级		
	针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事	三级		
		二级		
		一级		
	组织串联、煽动集会游行的信息安全事件	三级		
		二级		
		一级		
	其他信息内容安全事件			
	软硬件自身故障（SHF）	三级		
		二级		
		一级		
		三级		
其他信息安全事件（OI）	不能归为以上类别的信息安全事件			
	人为破坏事故（MDA）	二级		
		一级		
	其他设备设施故障（IF-OT）	三级		
		二级		
		一级		
灾害性事件（DI）	灾害性事件（DI）			

4.1.3 安全事件解决流程

1、单位网络与信息系统技术人员一旦发现发生安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位主管领导及计算机网络中心协助处理。

2、计算机网络中心接到上级有关部门安全事件通报或自主发现单位信息系统发生安全事件后，第一时间以口头方式将相关情况通报相关单位主管领导，相关单位主管领导接到通知后，应立即组织技术人员赶赴现场进行紧急处置。随后计算机网络中心以书面形式，将安全事件详情、要求整改内容及时限通报给有关单位。

3、单位主管领导、计算机网络中心根据发生安全事件的信息系统重要程度、损失情况以及对工作和社会造成的影响判定安全事件等级。安全事件划分为四个等级：特别重大事件（I 级，如特殊敏感时期网页被篡改）、重大事件（Ⅱ级，如网页被篡改、重要应用系统瘫痪）、较大事件（Ⅲ级，如上级有关部门通报的安全事件）和一般事件（Ⅳ级，如自主发现系统漏洞、但尚未被利用）。对重大事件和特别重大事件，应及时上报网络安全工作领导小组，对涉及人为故意破坏事件应同时报告公安机关。

4、事件处置过程中要及时掌握损失情况，查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为故意破坏应积极配合公安机关开展调查。

5、事后整改报告应在安全事件处置完毕后 2 个工作日内以书面形式报送计算机网络中心。相关责任单位应进一步总结事件教训，研判安全现状、排查安全隐患，加强制度建设、安全设施建设，全面提升安全防护能力。

6、责任单位应指定专人负责每日定时对网站、应用系统的运行情况进

行检查，做到安全事件早发现、早报告、早控制、早解决。

4.1.4 响应与处理时间

系统发生故障，用户可在第一时间内与我公司驻场工程师取得联系，说明客户单位、故障机型，尽可能说明故障现象以及可能的故障原因。

用户也可与我公司服务中心直接联系，服务中心调度长在第一时间内与我公司项目经理取得联系，服务中心的 SMS 系统会全程跟踪本次服务。

我公司驻场工程师会立即在响应时间内与客户现场工程师取得联系，取得详细的故障信息，做出相应的判断，首先排除因系统参数设定、使用中的软性故障，如果未能排除故障则驻场工程师立即准备赴现场服务。

服务工程师携带相应备件赴用户现场进行维修。首先进行现场诊断，分析锁定故障部件，更换部件或调整参数，数据恢复，直至系统恢复正常运行。

每次现场服务完成后，由我公司工程师填写《故障处理服务单》，由客户方代表确认并签署意见后交公司存档。

如第一次现场服务不能解决故障，则立即启动应急预案。

4.2 应急预案

4.2.1 网站、网页出现非法言论时的应急预案

1、网站内容由具体负责人员密切监视，每天不少于一小时。发现网上出现非法信息时，应立即向单位网络安全分管领导报告情况；情况紧急的应先及时采取删除等处理措施，再按程序报告。

2、单位网络安全分管领导接到报告后，应于二十分钟内核实情况，并协调技术人员做好清理非法信息、作好必要的记录，强化安全防范措施等工作。

3、网站维护员工作人员应立即追查非法信息来源，并妥善保存有关记录及日志。

4、网络安全分管领导召开安全相关会议，如认为情况严重，4小时内

向有关上级机关和公安部门报警。

4.2.2 黑客攻击或软件系统遭破坏性攻击时的应急预案

1、如网页内容被篡改时，应立即向单位分管网络安全分管领导通报情况。

2、网络安全分管领导接到报告后，应于十分钟内核实情况，并协调技术人员网络安全员开展应对工作，网络安全员应在十分钟内首先应将被攻击的服务器等设备从网络中隔离出来，并保护好现场。

3、网络管理员协同有关部门共同追查非法信息来源。

4、网络管理员应协助网站开发单位做好网站的恢复工作。

5、网络安全分管领导召开安全相关会议，如认为情况严重，则立即向公安部门或上级机关报警。

4.2.3 数据库发生故障时的应急预案

1、各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

2、一旦数据库崩溃，应立即向网络安全分管领导报告，数据库安全员应试图排查问题，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

4.2.4 设备安全发生故障时的应急预案

1、服务器等关键设备损坏后，有关人员应立即向网络管理员通报。

2、网络管理员应立即查明原因。

3、如果能够自行恢复，应立即用备件替换受损部件。

4、如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

4.2.5 内部局域网故障中断时的应急预案

1、局域网中断后，网络管理员应立即判断故障节点，查明故障原因，并向网络安全分管领导汇报。

2、如属线路故障，应重新安装线路。

3、如属路由器、交换机等网络设备故障，应立即与设备提供商联系更换设备，并调试畅通。

4、如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试畅通。如遇无法解决的技术问题，立即向上级单位或有关厂商请求支援。

4.2.6 广域网外部线路中断时的应急预案

1、广域网中断后，有关人员应立即启动备用线路接续工作，同时向网络管理员报告。

2、网络管理员接到报告后，应迅速判断故障节点，查明故障原因。

3、如属我方管辖范围，网络管理员要立即予以恢复。如遇无法恢复情况，立即向有关厂商请求支援。

4、如属电信部门管辖范围，立即与电信维护部门联系，请求修复。

4.2.7 外部电中断后的应急预案

发生外部电力供应中断后，应立即向值班经理汇报。如预先接到停电通知，应立即将相关通知报送值班经理，设备维保部部通知公司内各部门，做好准备工作。

已接到通知的电力中断：

1）停电当天，应在中心显眼地方竖立停电通知并写清楚停电原因；

2）使用紧急照明，保证各主要公共区域及通道的照明。

突发性电力中断：

1）事故发生后，安全管理人员应立即与维保部核实停电原因、停电时间长度，要求立即派遣专业电工，到现场排查事故原因，同时，将信息反馈给值班经理；

2）接到汇报后，值班经理立即启动应急预案，通知市民服务中心所有员工，解释停电原因，提示保管好个人财物、原地等待进一步通知。如已确定短时间内无法恢复的，应启动消防疏散应急预案，疏散员工，并在中心显眼地方竖立停电通知；

3）安全管理人员启动紧急照明保证各主要公共区域及通道照明。同时，警戒组准备好手电筒或其他照明工具，到公司各主要出入口维持秩序，做好警戒工作，严防有人制造混乱，浑水摸鱼；

4）值班经理、安全管理人员协同排查事故原因，组织电力抢修；

5）当供电恢复正常时，值班经理、安全管理人员应检查公司内所有用电设备的正常运作情况，如有损坏，须立即报告上级领导，安排处理。

4.2.8 发生火灾时的应急预案

（1）发生火灾时，应迅速判断火情，立即报告值班经理、项目经理，组织、指挥灭火。

（2）局部轻微着火，不危及人员安全，可以马上扑灭的要立即采取相应措施或使用灭火器材予以扑灭。

（3）火势较大并有蔓延可能时，立即拨打消防报警电话“119”，报告火灾发生的单位、详细地址、火灾情况、联系人及联系电话等信息。在消防人员到来之前，组织人员灭火，延缓火势蔓延。

（4）紧急疏散员工到安全地带。组织员工撤离时，让员工沿安全通道

有序逃离，远离玻璃门窗、吊灯等，保护好头部，切忌拥挤，防止摔倒踩伤。如遇浓烟叮嘱员工用湿毛巾捂住口鼻，尽可能以最低的姿势蹲行或爬行逃离。

（5）在保证人员安全撤离的条件下，尽可能切断电源，撤出易燃易爆物品，积极抢救贵重物品、设备及重要资料。

（6）火灾扑灭后：迅速查看员工受伤情况，对摔伤、砸伤、烧伤的员工迅速送往医院救治;清点火灾中损失的财、物；写出火灾发生的情况报告，上报相关部门。

5 服务管理

5.1 服务质量管理

5.1.1 行为规范

在岗期间标准着装，统一黑色或藏青色西服、西裤及皮鞋，浅色系衬衣。文件架统一摆放于桌面左上角，架内书本按左高右低依次排列整齐。桌面除笔、本、手机、杯子、充电器、绿植、电脑等办公用品外，不得摆放其他杂物。

接听电话时语气温和，以“您好，运维办公室”开始，询问对方所属单位、所在房间以及具体需求，然后进行登记并指派服务人员处理。

5.1.2 服务提供

申请单必须由服务台详细填写位置及故障后，交由技术人员携带处理故障。

技术人员务必立即响应服务请求，无故不得推迟。若无法独自处理，需先请示主管。

不允许两人同时去处理故障，如故障需两人处理的，需经主管同意。

5.1.3 服务环境

当日及次日值班人员应于每日早 8:30-8:45 清理地面卫生及垃圾桶杂物。

5.2 服务沟通机制

5.2.1 内部沟通

建立健全规范公司会议系统,使公司各种指令、计划信息能上传下达,相互协调，围绕企业各项指标的完成统筹执行。通过月会、周例会、调度会、座谈会、班前班后会等形式，快速地将信息进行有效的传递，使大家按计划有条不紊进行,步调一致，向目标明确，提高工作效率和效能,使目标完成得到保障。

欢迎各级层员工进来沟通谈话，了解各级层员工的需求动态，尽可能满足他们,正实现以人为本,提高员工满意度,把员工当作绩效伙伴而非打工者,形成命运共同体,而非单纯利益共同体。

5.2.2 外部沟通

随时与客户保持密切沟通，了解客户反馈的意见和需求，安排相关人员处理，需要客户提供资源的，积极与客户沟通。处理完成后，向客户反馈处理结果，了解是否满足客户要求。

5.3 服务风险管理

提高风险管理意识，既要有长期计划，也要有短期安排。制定应急预案，人员、设备皆有备份，应对突发情况。

采用规范化的管理模式，制定规范化的规章制度、岗位责任制，根据项目自身特点，对涉及风险的工作内容，制定较为细致的、有针对性的实施细则和风险管理计划，从而使企业的所有项目均能按统一规定的工作程序、要求、标准去做好实施工作，正确履行运维服务的各种责任，从而达到降低风险的目的。

建立较为完善的监督检查机制，进行动态管理。企业的管理层经常到项目中进行检查与指导，并加强与客户的沟通，听取客户的意见，及时把各种新的法律法规、内外形势变化、企业和客户的要求等传达到项目人员，并针对项目存在的风险隐患，及时加以处理，使其消失于萌芽状态，避免风险事故的发生。