

附件一 运维服务标准

1.1. 系统运维

1.1.1. 运维组织架构

按照统一监控，统一调度，分层运维的模式，构建如下运维组织：

岗位职责	职责
运维总负责	全面负责运维管理服务目标的达成。 负责组建运维团队组织。 全面负责运维管理服务过程中检查、敦促、指导工作。 全面负责监督和改进运维管理的工作质量。
运维管理组	负责整体运维方案的制定:包括运维组织职责、运维流程及运维制度。 负责定期的方案流程回顾与优化。
运维执行经理	负责日常运维管理工作执行和分配。 负责协调和推动运维管理例外的事项的解决。 作为运维服务客户经理与客户建立专属沟通渠道。
运维技术经理	负责运维管理服务过程中的技术管理工作。 负责从技术角度保证和改进运维工作质量。 负责与客户建立专属技术沟通渠道。
客户服务与监控组	承担服务台职责，7*24 小时负责用户报障和服务请求的统一受理， 包括记录、初步支持、派单和进展跟踪。 负责云平台日常监控管理和一线支持。

虚拟层维护组	<p>负责云产品虚拟资源的资源调度及管理工作。</p> <p>负责云管理平台的维护、紧急事件处理工作。</p> <p>负责虚拟层面的例行安全防护工作。</p>
业务平台维护组	<p>负责中间件、数据库、应用系统等维护工作。</p> <p>负责虚拟机系统的日常维护、紧急事件处理工作，确保其能够正常工作。</p> <p>负责应用层面的例行安全防护工作。</p>

1.1.2. 运维服务内容

1.1.2.1. 服务范围

针对本项目提供远程的全面保障及运维服务，运维管理对象仅包括：本项目所涉及的乙方独立开发的软件产品。硬件产品或第三方产品以厂家运维方案为准。

1.1.2.2. 质保期限

双方签署项目运维协议，针对本项目系统使用期内免费运维，保修费用已计入总价。

1.1.2.3. 服务响应水平

为最终用户提供技术服务热线(7*24 小时)，负责解答用户在云平台使用中遇到的问题，并及时提出解决问题的建议和操作方法；

在服务期内，提供 7*24 小时的技术支持服务，对请求 10 分钟内响应。

在服务期内，提供 7*24 小时运行维护工作，配备不少于 5 人的远程运维服

务团队，运维团队人员有明确的岗位分工。

1.1.3. 运维管理流程

为了保障项目的服务质量，需基于 ITIL 运维管理最佳实践，定义运维管理流程，包括事件/故障管理流程、变更管理流程、资源管理流程、监控与告警管理流程。

1.1.3.1. 事件/故障管理

(1) 流程目的

事件管理流程的主要目的是尽快解决运维中出现的事件与故障，尽快恢复业务，保障运维服务达到服务水平协议。

通过对事件进行登记、分类、分级、状态跟踪、关闭确认等手段建立一个事件管理流程的闭环，从而对事件的处理过程进行监控和优化。

定期对事件信息进行统计和分析，了解事件与服务请求的分布和发展趋势，降低事件响应时间和解决时间。

(2) 流程原则

1) 管理原则

所有本项目维护范围内发生的事件，都应该记录在事件管理工具中，记录的信息应足够详细，包括事件处理交互过程，详细的解决方案和相应的附件。

所有支持人员对优先级为紧急和高的事件所采取的服务恢复行动，在比对其它行动的时候，将拥有优先处理级别。

2) 责任人原则

所有权原则用来确保每个事件在任何时段都有适当的人员负责。由用户申报

的事件单，服务台是该事件的责任人，必须确保事件得到有效跟踪与解决，并负责事件单的关闭。当事件单被分派后，接单的事件处理员作为此事件当前责任人，负责对事件进行处理。

3) 优先级原则

事件的优先级表明了该事件对用户的业务影响和紧急程度。它是评定事件或服务请求处理优先顺序、解决时限的一个重要指标，优先级决定处理事件的顺序及所需的资源。

4) 目标解决时间原则

为了更好地控制事件的解决过程，事件管理流程被分解成几个阶段。每个阶段都设定相应目标时间。

5) 升级原则

事件的升级方式为技术升级和管理升级。技术升级是基于时限要求或技术能力要求而将事件受理转移给更高级别支持小组的操作。例如，一线转二线。管理升级是指在当前层级无法处理事件时，需要通知管理层，利于资源的投入。

1.1.3.2. 变更管理

(1) 流程目的

变更管理主要目的是规范生产环境变更活动，确保所有变更行为能按时完成，并且不会导致服务意外中断，降低风险，保证生产环境的稳定性、可靠性、安全性，并最大化地提升系统可用性。

(2) 流程原则

1) 管理原则

所有涉及运行环境的变更都必须严格遵循变更管理流程; 所有变更过程信息都应被记录并可追踪。

2) 审批原则

在变更管理流程中应充分考虑“风险”和“效率”的平衡, 通过对变更的充分评估和审核控制变更的风险, 但对不同类型的变更在流程或审批路径上区别对待, 以达到高效的目标。

3) 变更窗口原则

变更窗口原则用于确定变更实施的日程。变更窗口通常选择对业务影响最小的时间周期, 在规定的变更冻结期内, 原则上禁止变更。变更窗口机制应当形成书面文件并公布, 供所有参与变更人员使用。

4) 前导时间原则

前导时间是指从提交变更到变更实施之前所需要进行评估、审核等准备活动的最少时间。前导时间是基于变更影响度而定的。实施变更需要适当的前导时间进行评估和制定计划。

5) 回退原则

当变更实施失败或者无法在规定的时间内完成, 则需要进行回退。任何回退的变更将作为变更失败而关闭, 在下一次实施前, 变更请求者必须重新提交新的变更请求单(RFC), 以便重新进行审批。

6) 关闭原则

变更实施完毕并且得到确认后, 将由变更申请人关闭请求单。变更之后如果引发了其他问题, 将更新变更单的信息。

1.1.3.3. 资源配置管理

(1) 流程目的

事件管理流程的主要目的是尽快解决运维中出现的事件与故障，尽快恢复业务，保障运维服务达到服务水平协议。

通过对事件进行登记、分类、分级、状态跟踪、关闭确认等手段建立一个事件管理流程的闭环，从而对事件的处理过程进行监控和优化。

定期对事件信息进行统计和分析，了解事件与服务请求的分布和发展趋势，降低事件响应时间和解决时间。

(2) 流程原则

1) 管理原则

资源管理流程通过对 IT 基础设施资源的调配进行申请、审批、登记、部署、状态跟踪和关闭确认等活动建立了一个管理闭环，从而确保资源合理分配和使用；同时，定期对资源使用情况进行统计和分析，了解资源的分布和增长趋势，为 IT 基础设施资源池的容量管理和业务产品 IT 基础设施成本投入决策提供数据支撑。具体管理原则如下：

- a、资源管理流程是对 IT 基础资源占用的唯一入口；
- b、完整、准确地记录所有资源申请、审批、部署、使用、调整、回收等过程，以确保资源使用信息与物理环境一致；
- c、定期生成各业务资源使用情况和 IT 资源池容量管理报表；
- d、定期对资源管理流程进行回顾和优化改进。

2) 责任人原则

所有权原则用来确保每个事件在任何时段都有适当的人员负责。由用户申报

的事件单，服务台是该事件的责任人，必须确保事件得到有效跟踪与解决，并负责事件单的关闭。当事件单被分派后，接单的事件处理员作为此事件当前责任人，负责对事件进行处理。

1.1.3.4. 监控与告警管理

监控管理总体要求如下：

（1）针对网络、计算、存储和虚拟层等各系统的不同特点，制定详细完整的常规巡检制度及检查 / 监控规程，确保高可用性。

（2）告警出现时立即通知相应系统的后台值班人员，由后台值班人员负责故障的排除及判断是否升级故障；

（3）支持邮件或者短信方式的主动告警。对于监控系统所产生的告警，值班工作人员应按照事件处理流程，做统一记录，并进行故障处理；

（4）监控系统应确保安全管理，操作人员严格按照规定执行登录记录、数据备份、系统软件备份齐全；

针对各种维护操作制定相应的岗位职责及管理制度，并通过事后的监督审核确保各项操作得到可靠的执行。对于未能及时对监控系统告警进行处理的行为按照考核制度执行，对于造成严重影响的行为，追究其责任。

1.1.4. 安全运维方案

1.1.4.1. 安全运维服务原则

（1）保密性原则

在安全运维服务实施过程中，将严格遵循保密原则，服务过程中涉及到的任

何用户信息均属保密信息，不得泄露给第三方单位或个人，不得利用这些信息损害用户利益。并与签订保密协议，承诺未经允许不向其他任何第三方泄露信息。

(2) 互动性原则

在整个安全运维服务实施过程之中，将强调客户的互动参与，不管是从准备阶段，还是实施阶段。每个阶段都能够及时根据客户的要求和实际情况对实施内容、方式作出相关调整，进而更好的进行运维服务工作。

(3) 最小影响原则

安全运维服务工作应尽可能小的影响系统和网络的正常运行，不能对业务的正常运行产生显著影响（包括系统性能明显下降、网络阻塞、服务中断等），如无法避免，则应对风险进行说明。

(4) 规范性原则

安全运维服务工作的实施必须由专业的信息安全服务人员依照规范的操作流程进行，对操作过程和结果要有相应的记录，提供完整的服务报告。

(5) 质量保障原则

在整个安全运维服务工作实施过程中，将特别重视项目质量管理，项目的实施将严格按照项目实施方案和流程进行，并由项目协调小组从中监督、控制项目的进度和质量。

1.1.4.2. 安全运维服务内容

1.1.4.2.1. 安全保障体系

针对本项目安全运维，我司计划通过总体规划，分步推进的方式，建立健全信息安全保障体系，并落实到实际的网络安全工作中去。

1.1.4.2.2. 日常安全运维规范制定

根据日常安全运维工作内容，制定相对应的规范、流程、表单，以供安全运维人员使用。

1.1.4.2.3. 日常监控与事件处理服务

(1) 安全监控和日志收集

对网络安全设备、服务器设备、存储设备等其他硬件设备的监控、及时发现设备存在的故障，第一时间进行响应。并对收集的日志进行分类汇总分类，包括日志产生的原因、警告级别进行分类。

对系统软件（操作系统、数据库、中间件等）进行监控，并对相关日志进行收集。

(2) 事件处理服务

对安全监控中发现的监控指标异常、设备运转异常等，第一时间进行响应，及时报修。

1.1.4.2.4. 安全事件应急响应

服务期限内，提供 7*24 小时的远程安全应急响应，接到客户安全事件通知后，立即以远程方式对安全事件进行分析、抑制、溯源，最大程度降低安全事件对客户带来的损失。

安全应急响应，包括以下服务内容。

(1) 判定安全事件类型

从网络流量、系统和 IDS 日志记录、桌面日志中判断安全事件类型。查明安

全事件原因，确定安全事件的威胁和破坏的严重程度。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。

(2) 抑制事态发展

抑制事态发展是为了将事故的损害降低到最小化。在这一步中，通常会将受影响系统和服务隔离。这一点对保持系统的可用性是非常重要的。

(3) 排除系统故障

针对发现的安全事件来源，排除潜在的隐患，消除安全威胁，彻底解决安全问题。

1.1.4.2.5. 恢复信息系统正常操作

在根除问题后，将已经被攻击设备或由于事故造成的系统损坏做恢复性工作，使网络系统能在尽可能短的时间内恢复正常的网络服务。

1.1.4.2.6. 安全态势监控

定期跟踪国内外的安全漏洞发布平台（如 CNCERT、CNVD、乌云），及时发现新近出现的安全漏洞，通过电话、邮箱等方式，及时向客户通告最新的针对业务的（或具有重大影响的）安全漏洞、安全病毒、安全攻击、安全技术等安全态势信息，并提供有参考意义的安全防护建议，保证客户信息安全工作的前瞻性和预判性。