华润集团采购交易平台运维管理指引

第一章　总则

第一条 为保证华润集团采购交易平台（以下简称“守正平台”）长期、稳定、持续运行，规范运维管理工作，降低系统运维风险，指导运维团队在正确的流程下开展运维工作，依据相关管理要求，结合华润守正招标有限公司（以下简称“守正公司”或“公司”）实际情况和需要，制定本指引。

第二条 本指引适用于守正平台为管理、指导与考核信息系统运维工作。

第三条 下列术语和定义适用于本指引：

（一）守正平台：指由守正公司运营管理的包括但不限于润汇采、润汇采（国际版）、润汇拍、华润 E 购、润汇融及前述系统的关联子模块等业务信息系统，及与前述系统相关的合同管理中台系统、数据分析系统、供应商评价系统、客服系统等业务辅助信息系统。

（二）平台运营管理部门：指守正公司具有守正平台信息系统管理职能的部门。

（三）外包公司：指为守正平台提供软硬件资源或服务的第三方，包括基础设施外包公司、应用系统运维外包公司和客服外包公司。

（四）事件：指导致守正平台服务中断或服务质量降低，并给用户使用造成实际影响的任何事项。

（五）问题：指守正平台用户在处理业务或使用平台时提出的各类疑问或诉求。

（六）变更：指守正平台用户提出的，需要对生产系统进行变更才能实现的功能优化、Bug 修复等需求。

（七）服务台：指为解决用户问题的服务渠道、服务媒介即服务人员的统称。

第四条 平台运营管理部门是守正平台信息系统运维的主责部门，主要负责守正平台运维管理指引的制定及修订、日常运维工作的管理、运维事件处理解决方案的跟进、产品功能迭代优化方案的跟进、产品全生命周期的管理、外包团队及个人的考核、统筹和协调公司相关部门人员参加评审等会议及需求进度跟进（包含确定方案、组织相关 UAT 测试等）。

第五条 公司各部门应配合参加平台运营管理部门组织的评审会议等，并就评审议题提供业务/专业领域意见；配合完成需求验证，并反馈验证结果；协助服务台答复业务咨询类问题。

第六条 供应链服务管理部门统筹管理客户服务工作，包括服务台管理、服务渠道管理和知识库管理等工作，并对客服外包公司进行管理、监督和资源协调。

第七条 各外包公司应依据所签订的合同提供符合要求的资源及服务，并接受守正公司对运维工作的监督、检查与考核。

第二章　基础设施运维管理

第八条 基础设施运维管理主要针对守正平台运行所需各类基础设施资源的运维管理。基础设施资源包括租用的计

算设备、存储设备、网络和自购设备（含托管及自管）。

第九条 平台运营管理部门明确所需租用的计算设备、存储设备和网络的数量和技术要求、明确设备重要等级、明确托管设备的管理标准，并据此编制和更新基础设施资源清册、拓扑图，对基础设施资源进行统筹管理；

第十条 基础设施外包公司应提供高可用、高扩展性的基础设施资源；为托管设备提供良好的机房环境及可靠电源；提供资源日常运维、网络运维和安全防护等服务。工作内容及管理细则详见附录 1 基础设施资源运维管理要求。

第十一条 操作系统系统补丁修复原则：先修复测试系统，测试系统运行情况正常后，再修复生产系统。

第十二条 对于租用的计算机存储设备，其操作系统补丁需更新时，Linux 操作系统补丁由基础设施外包单位统一评估安装；Windows 操作系统补丁经平台运营管理部门评估通过后，由应用系统运维外包公司安装。

第十三条 对于托管设备，操作系统由云雾外包单位负责。应用系统外包运维公司负责使用的设备的应用安装、部署、测试及运维工作；

第十四条 对于自管设备，平台运营管理部门负责硬件、系统层面的运维（含补丁修复）；应用系统外包运维公司负责使用的设备的应用安装、部署、测试及运维工作。

第三章 守正平台运维管理及机制

第一节 运维基本工作管理

第十五条 守正平台各业务及业务辅助信息系统的运维

服务内容包含应用系统及其运行环境，运维服务根据其工作内容分为以下六大类：

（一）服务器相关运维工作包括服务器清单梳理、资源申请、调整及回收、巡检、防火墙等网络策略梳理、系统用户及口令管理等内容。

（二）应用系统相关运维工作包括应用程序安装部署、版本升级、巡查巡检、日志、故障排查、系统漏洞评估及修复、应急处理、功能优化、Bug 处理、数据修复等变更管理及系统程序更新、代码发布、代码管理、版本控制等发布管理。

（三）应用系统接口相关运维工作包括接口规范制定、接口开发、接口发布、接口升级、日志巡检、故障排查、传输协议、加密方式等内容。

（四）应用系统性能相关运维工作包括系统性能的监控与优化，系统日常运行状态的监控等内容。

（五）数据备份相关运维工作包括数据备份策略制定、文件备份策略制定、备份执行与恢复等备份管理。

（六）数据库相关运维工作包括数据库日常巡检、维护及性能优化等内容。

第十六条 各应用系统之间、与集团内部应用，原则上优先通过 ECSB 实现对接，必须通过表、视图、第三方直连等特殊场景除外；对于事件触发的数据交互，原则上由业务上游触发后交付业务下游系统；对于定期扫描的数据交互，原则上由下游业务系统定时向上游系统取数。

第十七条 对于各应用系统，遵循“谁开发、谁运维”的原则执行，另行安排移交调整的除外。

第十八条 平台运营管理部门应建立运维团队人员通讯录，并及时更新，确保与负责人、项目组成员及时取得联系。

第十九条 各应用系统运维外包公司开展日常运维工作时，须依据附录 2 应用系统运维管理要求执行。

第二节 日常巡检机制

第二十条 守正平台正常运行时所用到的服务器、存储设备、数据库及应用的状态在监控系统中进行实时监控，同时定期对巡检项进行巡检。在巡检机制中明确如下巡检项：

（一）基础设施资源主机类巡检项应能反应主机的 CPU、内存、磁盘、网卡及线程等信息，如总的 CPU 使用率、内存使用率、分区磁盘使用率、磁盘读\写速率、网卡状态及主机线程数等巡检项目。

（二）存储类巡检项应能反应存储读写速率、存储设备使用情况等信息，如存储读\写 iops、存储卷大小及存储卷使用量等巡检项目。

（三）MySQL 数据库和 Oracle 数据库应分别设定对应的巡检项，巡检项应能反应数据库的运行状态及性能，如 mysql 版本、mysql 状态、mysql BufferPool 实例个数、mysql BufferPool 容量、mysql BufferPool 逻辑读速率、mysql Masterbinlog 信息、mysql 慢查询语句等关于 MySQL 数据库的巡检项目；Oracle 实例名称、Oracle 版本、表空间状况、物理读前 10、逻辑读前 10、执行次数前

10、消耗时间前 10 等关于 Oracle 数据库的巡检项。

（四）守正平台应用系统巡检范围应涵盖服务、接口、中间件、云平台等的运行情况，如 Docker 容器状态、Tomcat 最大处理时间、Tomcat 进\出流量、Tomcat 每秒请求数、访问页面、系统登录、文件下载等巡检项目。

第二十一条　针对守正平台设定的通用巡检项，应记录在《检查项说明表格》（附件 5）中。不同系统模块如涉个性巡检项，应额外制定并记录。

第二十二条　守正平台所涉的服务器、存储、数据库及相关应用，应按照约定的巡检频率进行巡检。巡检执行时，巡检结果应同时记录至《日常巡检机制检查表格》中（附件 6）。每月对当月巡检情况进行总结，形成月度巡检报告（附件 7）。平台运营管理部门每月对巡检情况及报告进行检查及确认。

第二十三条　在守正平台所用的监控系统中设置的监控点和监控阀值应合理、有效，项目组应保证监控系统的有效性，确保告警通知及时发出。

第二十四条　对于发出的告警通知，平台运营管理部门要及时判断告警性质，并依据问题\事件处理机制进行处理。运维项目组要对告警日志进行分析及研判，明确告警原因，降低告警频率。

第三节　变更管理机制

第二十五条　守正平台各系统的生产环境、生产系统功能新增、修改或删除以及缺陷修复的发布，包含程序和脚本

变更的发布，均通过变更机制进行管理。

第二十六条　平台变更纳入运维计划中，要确保系统资源、应用环境、操作技能可满足系统安全、可靠运行的要求。

第二十七条　用户需求等级主要由需求重要度及影响范围两个因素共同决定：

（一）需求重要度指需求所涉及的功能模块对守正平台的重要程度，分为“核心”、“非核心”两个级别。

（二）影响范围指需求所影响用户数量、范围及所影响的业务、是否有替代方案来判断。

第二十八条　需求优先级分为五个等级，从高到低分别是 P0（致命）、P1（紧急）、P2（高）、P3（中）、P4（低）。

第二十九条　预计工作量是项目组在了解用户需求后，评估所得的预计解决该需求的工作量，至少包括需求理解、评审、开发、测试发版等过程，用以辅助确定需求处理方式，共分为少、中、多三个级别：

（一）如预计工作量在 5 人天及以下，运维资源可应对，属于较少工作量。

（二）如预计工作量在 5-30 人天及以下，此时需统筹运维资源，属于中等工作量；

（三）如预计工作量超过 30 天，除统筹运维资源外，还可能需要进一步协调增加运维资源，属于较多工作量。

第三十条 需求处理方式是指工单系统变更申请流程中，业务审批人员所需执行的操作，包括直接发起会签、组织小规模需求评审会、组织大规模需求评审会三类：

（一）直接发起会签是指业务审批人员将该工单在系统上直接发给相关人员进行审批的过程。

（二）小规模需求评审会是指业务审批人员组织的，由合规管理部门领导或代表、需求提出人、运维项目组相关负责人参加的对需求进行评审的会议；

（三）大规模需求评审会是指业务审批人员组织的，公司管理团队、相关部门领导或代表、需求提出人、运维项目组相关负责人参加的对需求或方案进行评审的会议。

第三十一条 依据用户需求优先级结合预计工作量，守正平台需求处理方式标准如下表：

需求重要度	**影响范围**	**需求优先级**	**预计工作量**	**需求处理方式**
核心	功能不可用且大面积影响用户，且无替代方案影响业务运行	P0	-	直接业务会签
核心	功能不可用，影响部分用户，且无替代方案影响业务运行	P1	-	直接业务会签
核心	功能存在缺陷，导致体验问题，大面积影响用户或影响到高层	P1	-	直接业务会签
核心	功能不可用，影响部分用户，但有替代方案不影响业务运行	P2	少	直接业务会签
			中	组织小规模需求评审会
			多	组织大规模需求评审会

需求 重要度	影响范围	需求 优先级	预计 工作量	需求处理方式
核心	功能存在体验问题，影响少数客户	P2	少	直接业务会签
			中	组织小规模需求评审会
			多	组织大规模需求评审会
非核心	功能存在缺陷，影响大面积用户，但不影响业务运行	P2	少	直接业务会签
			中	组织小规模需求评审会
			多	组织大规模需求评审会
非核心	功能存在缺陷，影响少数用户，但不影响业务运行	P3	少、中	直接业务会签
			多	组织小规模需求评审会
非核心	功能存在体验问题，大面积影响用户	P3	少、中	直接业务会签
			多	组织小规模需求评审会
非核心	功能存在体验问题，仅影响少数用户	P4	少、中	直接业务会签
			多	组织小规模需求评审会

第三十二条　需求应按照附件 3 需求处理流程进行处理，

平台变更管理相关工作内容及流程，应参照公司《变更管理工作指引》的规定严格执行。

第四节　问题管理机制

第三十三条　用户在使用守正平台过程中遇到的各类问题，由服务台客服进行解答、指导、工单录入、反馈跟踪及知识库更新。

第三十四条　根据用户咨询内容，将问题分为系统操作、业务咨询、故障、需求、投诉建议 5 类：

（一）系统操作：指用户对守正平台系统操作不熟练导致的问题，如：如何解密。

（二）业务咨询：指用户关于业务规则、处理进展等问题的咨询，如：如保证金如何退还、退还进度等；

（三）故障：指用户使用守正平台过程中，由于系统报错，导致业务中断或部分中断，无法进行下一步处理。

（四）需求：指用户对守正平台提出新功能、优化功能的需求等。

（五）投诉建议：指用户对守正平台提供的服务、方式等不满意，或有新的想法希望守正平台采用所引发的问题（业务投诉通过系统流程处理）。

第三十五条　根据与用户接触程度和问题来源，公司将服务台服务人员分为一线、二线、三线，具体指：

（一）一线：直接面对用户，解决用户系统操作类、业务咨询类和形成知识库的故障\需求类问题,如实记录投诉建议类问题并行成工单。

（二）二线：承接一线无法解答的业务咨询类、系统操作类问题及故障\需求类问题；同时更新知识库、操作手册，组织一线操作培训、功能培训，针对新开发的功能，编写功能简介等内容。

（三）三线：承接需要通过系统变更或技术处理等方式解决故障\需求类问题。

第三十六条　服务台客服应尽量引导用户优先通过人工智能机器人解决问题，其次选择在线客服、客服电话、邮箱等渠道，以便于记录及跟踪问题，形成有效的知识积累及传递，提高服务质量。

第三十七条　对于不能即时关闭的问题，应遵循“谁接收、谁关闭”的处理原则进行闭环管理，即用户反馈的问题服务台前台如无法即时处理，可通过工单方式向服务台后台寻求支持，待问题处理完成后，由问题接收人将处理结果反馈至对应用户。

第三十八条　所有问题都应被完整准确记录，记录人应保证记录的信息详细、准确。

第三十九条　所有问题都应按照附件 1 问题处理流程进行处理，重大问题可升级为事件，并按事件管理机制进行处理。

第五节　事件管理机制

第四十条 系统时间等级由重要度、影响程度、影响时间三个因素共同确定：

（一）重要度：指信息系统或基础设施对企业的重要程

度，分为“核心”、“重要”、“一般”三个级别。守正平台中润汇采、润汇采（国际版）、润汇拍及华润 E 购为核心系统，润汇融、合同管理中台系统、数据分析系统、供应商评价系统、客服系统为重要系统，其他系统为一般系统。

（二）影响程度：指影响用户的数量、范围以及所影响的业务、服务的多少。

（三）影响时间：指以用户受影响的时间为开始，以服务恢复后时间为结束。

第四十一条　系统事件分为四个等级，从高到低分别是 L1（重大）、L2（严重）、L3（较大）、L4（一般），具体标准如下：

系统重要度	事件影响程度	事件影响时间	事件级别
-	守正平台全部业务和服务无法办理，且无法采取临时补救措施处理	达到半小时以上	L1
核心	系统半数以上用户，所有业务和服务无法办理，且无法采取临时补救措施处理	达到 3 小时以上	L2
核心	系统半数以上用户，部分业务和服务无法办理，且无法采取临时补救措施处理	达到 6 小时以上	L2
重要	系统半数以上用户，所有业务和服务无法办理，且无法采取临时补救措施处理	达到 12 小时以上	L2
重要	系统半数以上用户，部分业务和服务无法办理，且无法采取临时补救措施处理	达到 24 小时以上	L2
核心	系统半数以上用户，所有业务和服务无法办理，且无法采取临时补救措施处理	超过半小时，未达 3 小时	L3
核心	系统半数以上用户，部分业务和服务无法办理，且无法采取临时补救措施处理	超过 3 小时，未达 6 小时	L3
核心	系统少量（10%以内）用户，所有业务和服务无法办理，且无法采取临时补救措施处理	达到 3 小时以上	L3
核心	系统少量（10%以内）用户，部分业务和服务无法办理，且无法采取临时补救措施处理	达到 6 小时以上	L3
重要	系统半数以上用户，所有业务和服务无法办理，且无法采取临时补救措施处理	超过 3 小时，未达 12 小时	L3
重要	系统半数以上用户，部分业务和服务无法办理，且无法采取临时补救措施处理	超过 12 小时，未达 24 小时	L3

重要	系统少量（10%以内）用户，所有业务和服务无法办理，且无法采取临时补救措施处理	达到 12 小时以上	L3
重要	系统少量（10%以内）用户，部分业务和服务无法办理，且无法采取临时补救措施处理	达到 24 小时以上	L3
一般	全部用户业务和服务无法办理，且无法采取临时补救措施处理	达到 24 小时以上	L3
-	对企业业务、服务产生一定影响，且影响时间达到半小时以上、但未达到以上标准的事件。		L4

第四十二条　若系统事件导致不良社会影响、诉讼等恶性结果时，可按以上定级标准重新定级。

第四十三条　事件处理流程依据事件等级，按照事件发现、处理、整改提高（如有）三个阶段进行处理，具体过程遵照附件 2 事件处理流程执行。

第四十四条　事件影响用户使用时，平台运营管理部门应在 15 分钟内将当前情况通知公司相关部门负责人，以便及时将情况告知用户，做好解释工作。若事件导致守正平台系统半数以上用户受到影响，平台运营管理部门应在 60 分钟内网站上进行公告。

第六节　安全与应急管理机制

第四十五条　在运维管理过程中，平台运营管理部门应确保信息资产免受各种威胁造成的损害，最小化信息系统安全风险，既要保证业务逻辑安全，又要保证应用系统及其相关数据库\中间件的使用安全，还要保证业务数据的保密性。

第四十六条　在业务层面，公司各部门需要从业务合规和风险控制的角度，对业务规则、业务流程和控制阈值设置等进行评审，从而确保业务逻辑的安全性。

第四十七条　在应用层面，守正平台应通过身份鉴别、访问控制、日志审计、剩余信息保护、通信完整性、通信保

密性、抗抵赖、软件容错、资源控制、应用监控、客户端安全防护、防敏感信息泄露、Web 攻击防范等方式保证应用层面的安全性。

第四十八条　守正平台应通过安全配置加固、数据库\中间件访问控制、数据库权限控制、数据库\中间件高可用性、敏感数据据脱敏等方式保证数据库\中间件的安全性。

第四十九条　守正平台应及时对数据、文件及日志进行存储及备份，保证数据的安全性。

第五十条　守正平台应通过安全配置加固、系统访问控制、系统权限控制、系统高可用性、入侵防范、恶意代码防范、系统备份等方式保证主机\操作系统的安全性。

第五十一条　对于守正平台系统发生的各种突发事件，应在最短时间内快速反应，采取有效措施，消除突发事件对业务应用的负面影响，并积极开展事后分析，总结经验，不断完善应急预案体系。

第四章　运维指标及考核管理

第五十二条　平台运营管理部门应对运维管理工作制定量化指标，并按季度对项目团队及个人进行考核。

第五十三条　系统运维指标

指标名称	计算方式	指标描述与度量
系统可用性	全年可用时长比例	全年可用时长比例不低于99.95%
定期检查合格率	所有定期检查合格次数/所有定期检查*100%	日检合格率应在97%以上 月度巡检合格率应为100%
漏洞修复完成率	所有已完成修复的漏洞数量/所有已发现漏洞数量*100%	指定时间段内，修复完成率应在90%以上
异常主动发现率	所有主动发现的异常数量/所有已发生异常数量*100%	指定时间段内，异常主动发现率应在80%以上

系统服务恢复时间目标（RTO）	从平台服务异常导致业务停顿开始到平台恢复至正常时结束此两点之间的时间间隔	2小时
系统数据恢复点目标（RPO）	容灾系统能把数据恢复到灾难发生前的时间点,即数据丢失和前一次备份之间的时间间隔。	1小时

第五十四条 系统优化指标

指标名称	计算方式	指标描述与度量
系统优化完成率	所有已完成的系统优化的数量/所有受理的优化数量*100%	指定时间段内，优化完成率应在90%以上
系统优化及时率	按计划完成的数量/所有完成的数量*100%	指定时间段内，优化及时完成率应在90%以上
二次bug率	二次Bug数量/发生Bug数量*100%	指定时间段内，二次bug率应低于5%
功能设计一次通过率	一次评审通过的功能设计文档的数量/所有功能设计文档的数量*100%	指定时间段内，功能设计评审一次通过率在95%以上

第五十五条 事件管理指标

指标名称	计算方式	指标描述与度量
事件解决率	指定时间段内，所有成功解决的事件/所有受理的事件*100%	指定时间段内，事件解决率应在90%以上
事件平均解决时间	指定时间段内，所有事件解决时间/事件总数	事件平均解决时间应该在60分钟内
事件总数	指定时间段内发生的所有事件的数量	
重大事件数量	指定时间段内发生的L2及以上或核心系统影响半数以上用户的L3事件数量	指定时间段内重大事件次数不超过3次

第五十六条 项目团队评价方式如下:

评分组成	权重%	评分人	评分对象	评分依据
平台稳定运行	40	甲方项目管理人员	乙方	评价周期内： 平台可用率不低于 99.95%； 短周期优化完成率不低于 85%；年度优化完成率不低于 95%；

评分组成	权重%	评分人	评分对象	评分依据
				按时完成应用系统日检，日检率不低于97%； 按时完成服务器月度巡检并提交巡检记录及报告，月度巡检率应为100%； RTO≤2小时；RPO≤1小时；
运维服务质量（业务口径）	30	业务人员	乙方	服务评价：针对每个工单，由业务用户在客服一体化平台中进行评分。 全年有效投诉次数≤10次；
运维服务质量（技术及管理口径）	30	甲方项目管理人员	乙方	服务质量：二次bug率≤5%；工单一次性解决率≥98%； 服务能力：包括沟通能力、技术能力及资源支持能力； 沟通能力：问题描述及问题理解能力； 技术能力：功能设计文档涉及场景是否考虑全面，功能设计评审一次通过率≥95%； 资源支持能力：人员离职或有新资源需求时，新资源到位时间应小于3天；
合计	100分			

第五十七条 业务口径评分为针对每个工单，在客服一体化平台中由业务用户进行评分，平台运营管理部门定期从客服一体化平台中导出相关数据进行统计。

第五十八条 个人评价方式如下：

评分组成	权重%	评分人	评分对象	评分依据
项目团队评价得分	50	甲方项目管理人员	乙方运维人员	项目团队综合得分

评分组成	权重%	评分人	评分对象	评分依据
员工个人评价得分（通用）	20	甲方项目管理人员	乙方运维人员	保证服务时间，按时打卡，不迟到、不早退； 上班期间树立良好个人形象，严禁穿短裤、短裙、拖鞋及奇装异服； 注意办公区信息安全，严格遵守信息保密原则，打印完毕后需及时取走打印物品； 人员入场、离场应办理相关手续； 办公区域严禁吸烟。
员工个人评价得分	30	甲方项目管理人员	乙方运维人员	**技术客服评价内容：** 技术客服电话接通率≥90%； 问题回复率≥98%； 全年有效投诉次数≤10 次； **实施、交付人员服务评价内容：** 代码注释详细，遵守华润源代码管理办法； 功能设计文档涉及场景是否考虑全面，功能设计评审一次通过率≥95%； 二次 bug 率≤5%。
合计	100 分			

第五十九条 个人综合得分=项目团队评价得分*50%+员工个人评价得分(通用)*20%+员工个人评价得分(个性)*30%。

第六十条 如出现重大事故（数据删除、信息泄漏、代码丢失等）或导致系统停运时间超过 4 小时，本季度评分为 0 分。

第五章 附则

第六十一条 法律法规、监管规定或政策文件另有规定

的，从其规定。

第六十二条 本指引为守正公司三级制度。

第六十三条 本指引由守正公司平台运营部负责制订、修订和解释。

第六十四条 本指引自发布之日起生效。守正平台于2021 年 9 月 28 日颁布的《华润集团守正电子招标采购平台运维管理工作指引》同时废止。

附件

附件 1：问题处理流程图

附件 2：事件处理流程图

附件 3：需求处理流程图

附件 4：资源清册表格

附件 5：检查项说明表格

附件 6：日常巡检机制检查表格

附件 7：月度巡检报告模板

附件 8：接口汇总表格

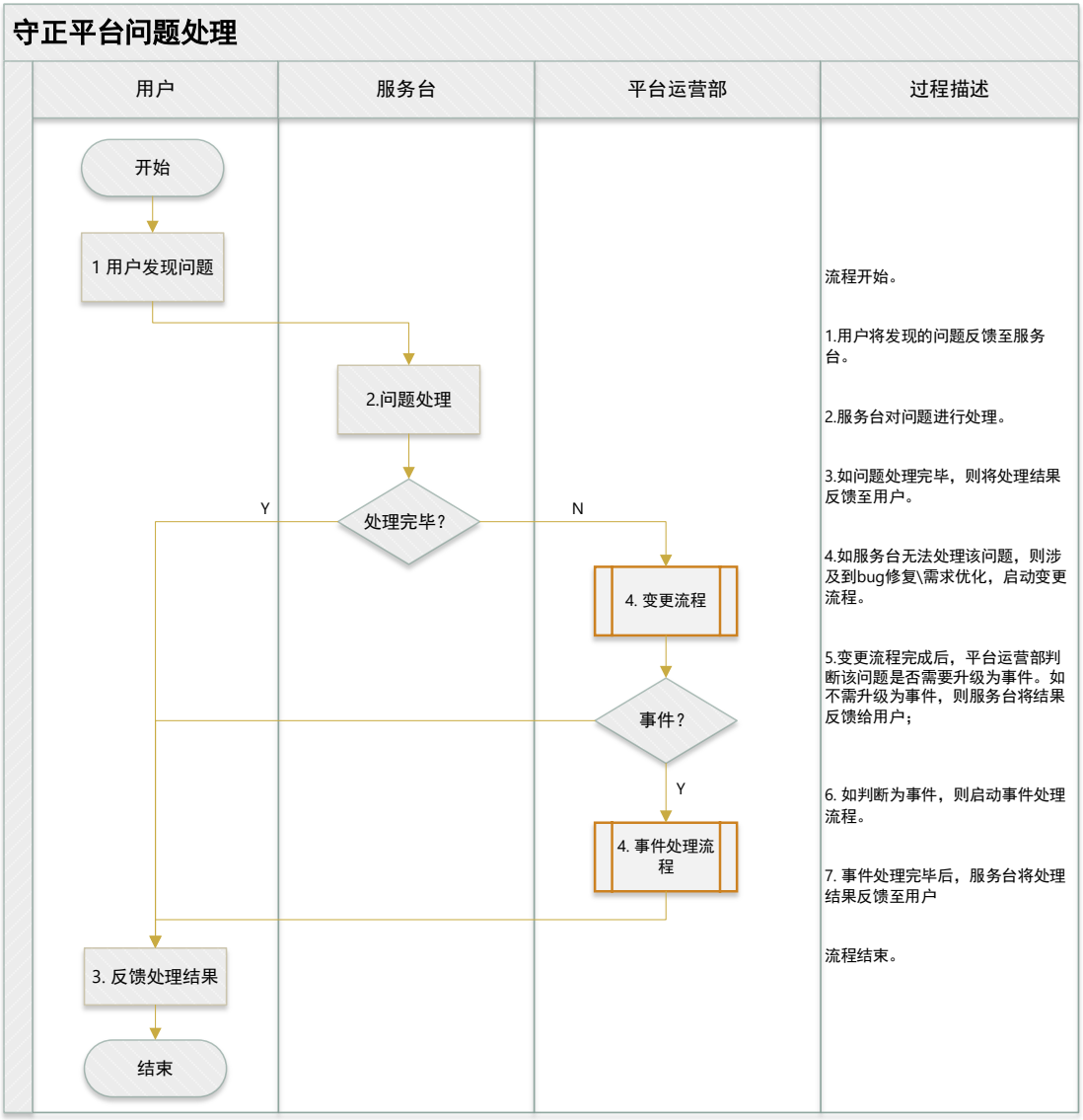
附件 9：数据备份策略表格

附录

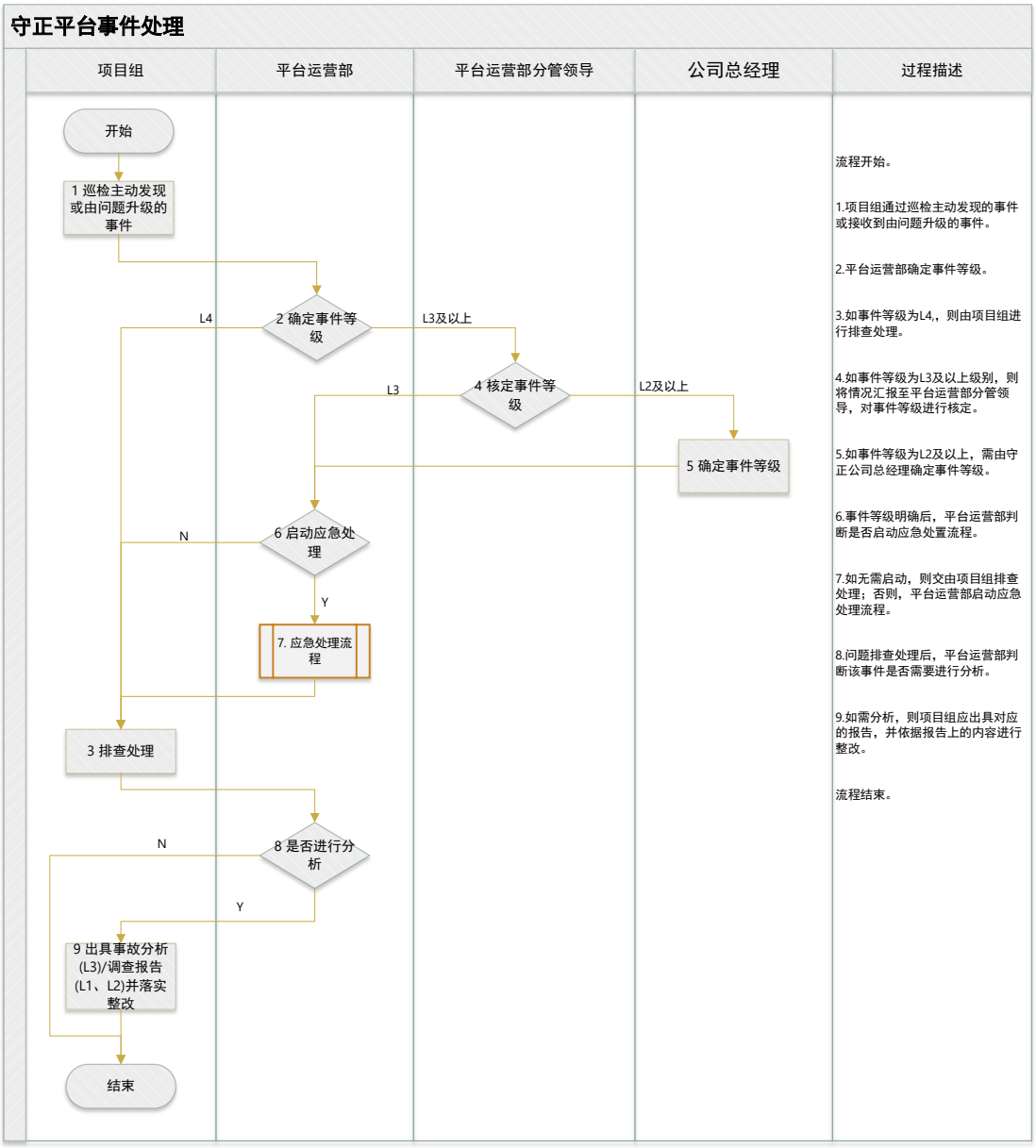
附录 1: 基础设施资源运维管理要求

附录 2: 应用系统运维管理要求

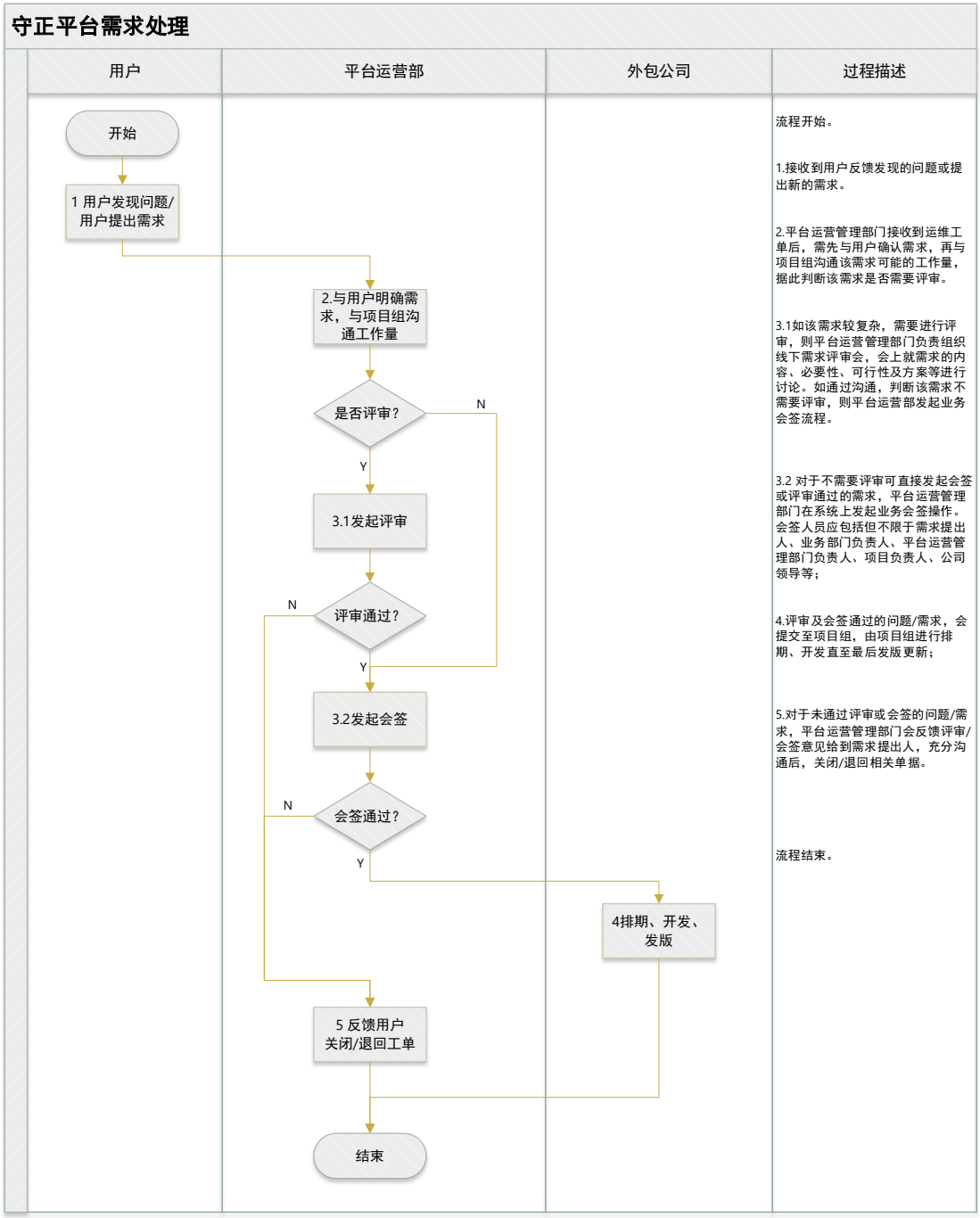
附件 1:问题处理流程图


守正平台问题处理
用户
服务台
平台运营部
过程描述
开始
1 用户发现问题
2.问题处理
处理完毕?
Y
N
4. 变更流程
事件?
Y
4. 事件处理流程
3. 反馈处理结果
结束
流程开始。
1.用户将发现的问题反馈至服务台。
2.服务台对问题进行处理。
3.如问题处理完毕，则将处理结果反馈至用户。
4.如服务台无法处理该问题，则涉及到bug修复\需求优化，启动变更流程。
5.变更流程完成后，平台运营部判断该问题是否需要升级为事件。如不需升级为事件，则服务台将结果反馈给用户；
6. 如判断为事件，则启动事件处理流程。
7. 事件处理完毕后，服务台将处理结果反馈至用户
流程结束。

附件 2：事件处理流程图


守正平台事件处理
项目组
平台运营部
平台运营部分管领导
公司总经理
过程描述
开始
1 巡检主动发现或由问题升级的事件
2 确定事件等级
L4
L3及以上
4 核定事件等级
L3
L2及以上
5 确定事件等级
6 启动应急处理
N
Y
7. 应急处理流程
3 排查处理
8 是否进行分析
N
Y
9 出具事故分析(L3)/调查报告(L1、L2)并落实整改
结束
流程开始。
1.项目组通过巡检主动发现的事件或接收到由问题升级的事件。
2.平台运营部确定事件等级。
3.如事件等级为L4，则由项目组进行排查处理。
4.如事件等级为L3及以上级别，则将情况汇报至平台运营部分管领导，对事件等级进行核定。
5.如事件等级为L2及以上，需由守正公司总经理确定事件等级。
6.事件等级明确后，平台运营部判断是否启动应急处置流程。
7.如无需启动，则交由项目组排查处理；否则，平台运营部启动应急处理流程。
8.问题排查处理后，平台运营部判断该事件是否需要进行分析。
9.如需分析，则项目组应出具对应的报告，并依据报告上的内容进行整改。
流程结束。

附件 3：需求处理流程图


守正平台需求处理
用户
平台运营部
外包公司
过程描述
开始
1 用户发现问题/用户提出需求
2.与用户明确需求，与项目组沟通工作量
是否评审？
N
Y
3.1发起评审
评审通过？
N
Y
3.2发起会签
会签通过？
N
Y
4排期、开发、发版
5 反馈用户关闭/退回工单
结束
流程开始。
1.接收到用户反馈发现的问题或提出新的需求。
2.平台运营管理部门接收到运维工单后，需先与用户确认需求，再与项目组沟通该需求可能的工作量，据此判断该需求是否需要评审。
3.1如该需求较复杂，需要进行评审，则平台运营管理部门负责组织线下需求评审会，会上就需求的内容、必要性、可行性及方案等进行讨论。如通过沟通，判断该需求不需要评审，则平台运营部发起业务会签流程。
3.2 对于不需要评审可直接发起会签或评审通过的需求，平台运营管理部门在系统上发起业务会签操作。会签人员应包括但不限于需求提出人、业务部门负责人、平台运营管理部门负责人、项目负责人、公司领导等；
4.评审及会签通过的问题/需求，会提交至项目组，由项目组进行排期、开发直至最后发版更新；
5.对于未通过评审或会签的问题/需求，平台运营管理部门会反馈评审/会签意见给到需求提出人，充分沟通后，关闭/退回相关单据。
流程结束。

附件 4：资源清册表格

服务器用表

序号	管理模式	设备类型	所属项目	所属应用\模块	用途	主机名	IP 地址	操作系统	状态	责任人	备注

物理设备用表

序号	设备归属	所属项目	所属应用\模块	用途	设备名称	设备品牌及型号	主机名	IP 地址	操作系统	S/N 号	质保状态	安装位置	资产编号

附件:5：检查项说明表格

序号	所属系统	所属应用\模块	检查类别	IP 地址	检查频率	检查类别	检查项	检查项说明	检查项异常值

附件 6：日常巡检机制检查表格

序号	所属项目	所属应用\模块	IP 地址	状态	巡检项一	巡检项二	巡检项三	……	巡检时间	巡检人员	巡检状态	备注

附件 7：月度巡检报告模板

巡检系统：XXXXXXXXXXX　　巡检周期：XXXX 年 XX 月　　巡检人：XXXXX

生产环境			
巡检类别	**巡检机器数量**	**是否有异常**	**异常发现日期**
主机类		是□　否□	
存储类		是□　否□	
数据库类		是□　否□	
应用类		是□　否□	
测试环境			
巡检类别	**巡检机器数量**	**是否有异常**	**异常发现日期**
主机类		是□　否□	
存储类		是□　否□	
数据库类		是□　否□	
应用类		是□　否□	
本周期巡检异常情况详细说明（如异常情况复杂，处理难度大，应另附说明报告）			
异常设备 IP	功能模块	异常情况详细说明	解决方法
本周期其它告警处理情况			
1. 2. 3. 4. 5.			

附件 8:接口汇总表格

序号	* 系统	对侧系统	* 接口名称	* 接口地址	Service ID	接口方向	* 接口功能描述	* 端口号	* 技术类型	* 通讯方式	编码\加密方式	* 接口上线时间	* 接口状态	* 对侧单位	* 对侧接口负责人	系统负责人

附件 9：数据备份策略表格

资源类型	备份类型	备份频率	备份时间	保留周期	责任人	对侧负责人	备注

附录 1: 基础设施资源运维管理要求

1　机房运维管理要求

1.1　电源管理

应定期对机房供电电压，电流稳定性进行监控，每天检查设备电源线、插头及列头柜的工作状态；管理员应定期对 UPS 设备进行充放电测试，有条件可进行负载测试，保证 UPS 每天的备电时间在 30 分钟以上；管理员应保证柴油发电机处于待命状态，定期对备用发电机进行空载测试。当突然停电时，应采取应急措施及时处理。

1.2　防雷管理

管理员应每季度对避雷装置、防雷保安器、交流电源地线等进行检查，对异常情况进行及时处理。

1.3　防火管理

管理员应每季度对气体灭火设备和自动报警系统进行检查，对异常情况进行及时处理；应每年进行一次消防演练；禁止在机房内堆放易燃易爆物品。

1.4　防水管理

机房应保持清洁干燥，管理员应在巡检中，检查机房环境监控系统中有无漏水（如空调管道、天花板、墙壁、窗户等），如发生漏水或渗水情况，应及时进行处理。

1.5　电磁防护管理

内外部人员在机房内作业时应佩戴静电环。

1.6　温湿度控制管理

场地值守人员应在每天巡检中，检查机房环境监控系统中的温湿度数据及告警信息，温度应介于 23±2℃之间；湿度应介于 40%-70%之间以及对超标情况进行及时处理。

1.7　线缆安全管理

管理员每年应定期对机房线缆的铺设情况进行检查，对异常情况进行处理。

1.8　应具有防范台风、暴雨等自然灾害的应对措施；

1.9　防鼠虫管理

管理员应为机房配备防鼠防蟑设施设备 (如防鼠板、蟑螂屋) 并定期更换。

1.10　机房访问控制与设备安全：

1.10.1　需进入机房的来访人员应经过申请和审批流程，管理员根据申请和审判记录对来访人员身份进行鉴别，填写《机房来访人员登记表》，对来访人员的姓名、证件号码、单位、进出时间、事由、联系方式等进行记录，记录保留三年。

1.10.2　应限制和监控来访人员的活动范围，并对其活动进行全程或全责陪同。

1.10.3　应配置电子门禁系统，控制鉴别和记录进入的人员；门禁系统日志应保留一年，每月对日志进行定期检查。

1.10.4　原则上禁止携带电脑或移动介质进出机房，紧急情况下，经批准或授权后，方可带入或带出。

1.10.5　当发生人员岗位变动时，需同时调整门禁权限，及时删除离职人员的授权。

1.10.6　应将设备或主要部件进行固定，并设置明显的不易除去的标记。

1.10.7　应对介质分类标识，存储在具备一定物理安全条件的介质库或档案室中，如应将磁带保存在具备防火、防水、防酸、防电磁的环境中。

1.10.8　任何人不得将食物和饮料带入机房，禁止在机房内饮食。

1.10.9　任何人不得破坏机房内的设备。

2　计算及存储设备管理要求

2.1　可用性及可靠性要求

计算及存储设备应具备 99.99%的可用性，拥有 7*24 小时持续运行能力，物理主机及核心网络设备应支持热备；确保硬件设备完整清洁、保证其电气特性、机械特性及准确率等各项指标符合要求。

2.2　扩展性要求

设备应具备良好的扩展性，对于设备运行瓶颈能够通过扩展增加资源，确保设备文档运行。

2.3　性能要求

系统主要硬件的容量和性能指标（包括内存容量、处理器主频、硬盘容量、通信网带宽）应能适应整个系统处理能力、通信传输量、数据存储量和业务实际需求等各方面的要求。

2.4　设备监控要求

应具备在线监控、告警功能，并能及时通知责任人进行处理。

2.5　日常巡检要求

硬件设备应定期巡检，对设备运行状态、故障情况监控及反馈，在设备发生故障时，提供 7*24 小时备件更换服务。

2.6　升级更新要求

系统软件发布软件版本或补丁版本时，根据系统运行情况和安全管控要求，提供软件升级方案，完成系统软件的升级工作。

2.7　应急响应要求

具备应急响应、处理能力，并有相应的应急预案。灾备应急预案至少包括：系统运行的现状描述、可能发生的灾难预计、系统的备份策略、系统应急解决方案、系统回退方案。

2.8　合理化建议要求

对硬件设备资源利用及性能情况进行监控，发现系统性能的瓶颈，并提出针对系统瓶颈的解决建议。

3　网络基本要求

3.1　网络可靠性、稳定性要求

3.1.1　负责通过网络及通信设备合理配置、网络资源的分配使用、日常检测等方式，保证网络畅通，可用性应达到99.99%，并定期报告网络及通信设备使用情况。

3.1.2　负责对网络及通信设备的实时监控，定时侦听网络线路的流量及阻塞情况、数据流向、线路通信能力的占用比率，如发现问题，应及时解决。

3.1.3　负责备份网络日志文件，分析运行情况并反馈至平台运营管理部门。

3.2　带宽及质量要求

3.2.1　带宽按照业务需求进行确定，实行弹性带宽，按实际使用结算，但最低带宽不低于 200Mbps。

3.2.2　网络延迟<10ms,网络抖动<10ms,丢包率<1%,网络可用性达到 99.8%以上。

4　安全管理要求

4.1　机房安全管理要求

4.1.1　建立运维服务体系，严格监督与检查、应急预案演练等措施，确保 IT 设备和机房场地设施的稳定运行。

4.1.2　需定期作好各类设备的安全性能检查，使各项指标符合标准；需定期检查备用设备的状况，在主用设备发生故障时，备用设备能够立即投入使用。

4.1.3　机房应具备灭火器、温度、火情、烟雾告警装置和安全防护用具，并有专人负责，定期检修，每个维护人员应熟悉消防器材的一般使用方法。机房还应具备自动灭火或切断电源的手段。

4.1.4　要防治鼠害虫害，确保各种布线完好和各种设备不受损害。

4.1.5　定期向相关人员传授安全知识，增强相关人员的安全防范意识。

4.2　虚拟服务器安全管理要求

4.2.1　服务器必须安装防病毒软件、统一的操作系统和补丁版本。

4.2.2　服务器资源必须通过堡垒机远程管理。

4.2.3　统一遵守集团的 DMZ 和防火墙安全策略。

4.2.4　定期进行安全检查，整改发现的高危安全漏洞。

4.2.5　对各类主机的管理和对用户、文件系统分配、访问权限进行安全设置。

4.3　操作系统安全管理要求

4.3.1　系统访问控制要求

对于重要的系统主机，应考虑采用系统管理员操作行为审计系统（SAO）对管理员的操作行为进行审计。

4.3.2　系统高可用性要求

根据业务需求，设计操作系统的高可用性方案，如 HA、集群、负载均衡、热备等。

4.3.3　入侵防范、恶意代码防范要求

通过网络层面的 IDS\IPS、防病毒网关实现对操作系统的入侵防范、恶意代码防范，按需部署专业木马监控系统、APT 攻击检测系统。

4.3.4　系统备份要求

设计操作系统备份方案，包括备份频率、备份介质、数据恢复测试等。

4.3.5　日常运维过程中，应执行好系统安全加固、账号权限管理、操作系统升级和补丁管理、防病毒、日志管理、备份与恢复、变更管理等安全管理要求。

4.4　漏洞安全管理要求

4.4.1　针对 web 漏洞，加强安全编码规范，对输入、输出内容过滤及校验；部署 web 防火墙，防范跨站脚本、注入等攻击，清除能够被直接或者间接对系统攻击的漏洞。

4.4.2　针对应用程序及第三方中间件漏洞，定期对应用程序执行应用层面的安全性测试，发掘并解决应用层面的代码漏洞和配置缺陷，定期升级应用程序版本。

4.4.3　针对操作系统及数据库漏洞，应及时与供应厂商联络，获得最新的安全补丁及修复建议。

4.4.4　漏洞修复应根据漏洞严重等级排序，优先完成高危漏洞修复工作。

4.5　网络安全管理要求

4.5.1　制定专项访问控制策略，包括入网访问控制、网络权限控制、目录安全控制、属性安全控制、网络服务器安全控制、监控控制、端口和节点安全控制、防火墙安全控制。

4.5.2　所有系统和应用必须有访问控制登记表，由系统负责人明确定义访问控制规则、用户和用户组的权限以及控制访问机制，访问控制登记表应该进行周期性的检查以保证授权正确。

4.5.3　访问权限必须根据工作完成的最小需求来定，应遵循“工作所需，权限最小”原则，不能超过工作实际所需的范围。

4.5.4　对外连接的区域（如互联网出口），须配置防火墙功能的设备，进行内外网络隔离，公司内网环境之外要访问内网必须通过 VPN 接入。

4.5.5　生产服务器安全区与测试安全区需进行策略隔离，禁止互相访问，公司外部与内网之间建立 DMZ 区用于作为代理。

4.5.6　各安全区域内可以通过设置主机防火墙增加 ACL 隔离措施，从不同网络协议层次增强对主机系统的保护，包括基于 IP 和端口的主机网络访问控制、基于应用程序路径和名称的主机应用程序网络访问控制等。

4.5.7　对网络及通信设备进行合理配置、网络资源的分配使用，根据业务需求或其他特殊情况，网络访问控制策略需要变更调整时，应做好更新调整记录，形成更新记录报告。

5　守正平台网络拓扑图

附录 2: 应用系统运维管理要求

1　网络安全运维管理

1.1　防火墙管理

1.1.1　防火墙申请

应用部署环境划分生产环境、测试环境和灾备环境，每个应用环境有明确的 IP 地址范围分区，原则上跨环境之间的防火墙不允许互相开通(根据实际需要)，根据 IP 添加访问规则，各服务器之间网络端口的访问必须开启防火墙策略。防火墙策略开通应由应用系统外包单位发送防火墙策略开通申请邮件，经平台运营管理部门系统负责人确认，抄送部门领导或分管领导审批，审批通过后，由平台运营管理部门系统负责人在 ITSM 系统提单申请开通对应防火墙策略。

1.1.2　防火墙策略梳理

针对平台润汇采、润汇采（国际版）、润汇拍、华润 E 购及数据分析系统，应用系统外包单位需定期整理服务器防火墙开通策略清单，提供平台运营管理部门系统负责人存档，清单内容应包括但不限于环境类型、部署应用、策略用途、源 IP、目的 IP、端口等信息。

1.2　堡垒机管理

通过办公内网或慧盾访问服务器资源、数据库时，必须通过堡垒机。堡垒机的账号权限应根据各子系统服务器资源申请开通。堡垒机增加服务器资源时，应用系统外包单位发送堡垒机资源申请邮件，经平台运营管理部门系统负责人确认，

抄送部门领导或分管领导审批，审批通过后，平台运营管理部门系统负责人在 ITSM 系统提单申请增加服务器资源。

2　服务器资源运维管理

2.1　服务器资源申请\变更

根据项目建设及运维需要，应用系统外包单位提供硬件搭建方案初稿，经平台运营管理部门技术负责人评估通过后，由应用系统外包单位发送服务器资源申请邮件，经平台运营管理部门部门领导或分管领导审批通过，平台运营管理部门系统负责人在 ITSM\华润云系统中提单申请增加服务器资源。

2.2　服务器资源扩容

在服务器 CPU、内存、存储等资源不能满足实际业务需要时，应用系统外包单位发送扩容申请邮件，经平台运营管理部门系统负责人评估，部门领导审批通过后，平台运营管理部门系统负责人在 ITSM 系统提单申请扩容。

2.3　服务器资源回收

针对生产环境、测试环境和灾备环境的空闲资源，应用系统外包单位确认未在空闲资源上部署应用程序后，可通过邮件通知平台运营管理部门系统负责人，经平台运营管理部门系统负责人评估，部门领导审批通过后，平台运营管理部门系统负责人在 ITSM 系统中提单申请资源回收。

2.4　服务器资源梳理

针对守正平台招标系统、非招系统、智能客服系统、数据分析系统，应用系统外包单位需定期梳理并更新资源清册并提供至平台运营管理部门系统负责人存档，清册内容应包含管

理模式、设备类型、所属项目、所属应用\模块、用途、主机名、IP 地址、操作系统、状态、责任人等相关信息。

2.5　服务器巡检

为保证应用系统稳定运行，应用系统外包单位需定期组织对应用系统所使用的服务器进行巡检，详细巡检项见附件 5《检查项说明表格》，巡检结果应据实填写至附件 6《日常巡检机制检查表》。平台运营管理部门对巡检情况不定期进行核查。

2.6　操作系统版本

操作系统版本由集团数据中心或华润云统一安装维护，为满足守正平台部署要求，应同时满足以下要求：

（1）服务器安装 Linux 操作系统时，应按最小化安装，安装版本为 7.3 或以上，服务器安装的 Windows 操作系统，版本应为 2012 或以上。

（2）操作系统版本升级时，需整理服务器部署的应用程序清单，并编写升级实施方案，方案内容包括但不限于升级的方式、升级的范围、升级的内容及关联程序影响、升级的备份及还原措施等。

（3）平台运营管理部门负责组织评估评审会议，由平台运营管理部门分管领导、部门领导、各系统负责人、应用系统外包单位项目经理及技术负责人，共同评估版本升级的可行性及风险性，会议最终形成版本升级方案。

（4）操作系统版本原则，先升级测试系统，观察测试系统运行情况正常后，再升级生产系统。

（5）版本升级完成后，完整验证业务系统，确保升级不影响业务使用。

3　应用程序安装部署与版本控制管理

3.1　按照平台运营管理部门的要求，应用系统外包单位需完成应用程序、中间件、数据库、第三方控件等的安装、部署及测试，协助平台运营管理部门对应用程序版本进行升级，同时对系统程序更新、代码发布、代码管理、版本控制等工作进行管理。

3.1.1　应用系统版本升级管理

（1）针对日常更新迭代需求，应用系统外包单位应整理当周\月版本计划及需求列表、整理计划升级的功能点的发布信息、完成相关代码打包、升级前的代码备份及版本回退策略等。

（2）平台运营管理部门负责组织评审会议，由平台运营管理部门分管领导、部门领导、各系统负责人、外包单位项目经理及技术负责人，共同评估版本升级的可行性及风险性，会议最终形成版本升级方案。

（3）程序版本升级原则，先升级测试系统，观察测试系统运行情况正常后，再升级生产系统。

（4）版本升级完成后，完整验证业务系统，确保升级不影响业务使用。

3.1.2　中间件、第三方插件、数据库等产品版本升级管理

（1）中间件、第三方插件、数据库等产品在进行版本升级时，首先各项目组需汇总所涉应用程序清单，编写升级实施方案，

方案内容包括但不限于升级的方式、升级的范围、升级的内容及关联程序影响、升级的备份及还原措施等。

（2）平台运营管理部门负责组织评估评审会议，由平台运营管理部门分管领导、部门领导、各系统负责人、应用系统外包单位项目经理及技术负责人，共同评估版本升级的可行性及风险性，会议最终形成版本升级方案。

（3）程序版本升级原则，先升级测试系统，观察测试系统运行情况正常后，再升级生产系统；

（4）版本升级完成后，完整验证业务系统，确保升级不影响业务使用。

4　应用系统维护管理

通过对应用系统的日常维护及系统监控等方式，保证守正平台应用系统的安全性、可靠性和可用性。

4.1　应用系统日常维护管理

应用系统日常维护工作包括但不限于巡查巡检、日志、故障排查、系统漏洞评估、应急处理、功能优化、Bug 处理、数据修复等。

4.1.1　巡查巡检

为保证守正平台系统稳定运行，应用系统外包单位需定期组织对守正平台所有应用系统进行巡检，详细巡检项见附件 5《检查项说明表格》，巡检结果应据实填写至附件 6《日常巡检机制检查表格》中。平台运营管理部门对巡检情况定期或不定期进行核查。

4.1.2　漏洞处理

（1）STP 系统每天定时对守正平台服务器资源漏洞扫描，扫描出的漏洞按等级分为高危、中危、低危。平台运营管理部门系统负责人每周五定期查看 STP 系统漏洞扫描情况，将导出的漏洞清单以邮件的方式发送给应用系统外包单位项目经理，组织应用系统外包单位项目经理进行系统地风险评估工作同时落实修复方案，方案评审及实施应根据《华润集团守正电子招标平台变更管理工作指引》进行。

（2）应优先修复高危漏洞，原则上高危漏洞修复时间不能超过 15 天，中低危漏洞修复时间不能超过 30 天。

（3）漏洞修复原则，先修复测试环境漏洞，观察测试系统运行情况正常后，再修复生产环境漏洞。

（4）应用系统外包单位在修复漏洞前，首先确认是否有 sudo 权限，如没有相关权限，应根据实际需要向平台运营管理部门相关负责人申请开通。

（5）漏洞修复完成后，应用系统外包单位应通过电话或邮件等方式，及时将修复情况通知平台运营管理部门相关负责人，平台运营管理部门相关负责人需在 STP 系统上再次对服务器资源扫描，确认漏洞修复是否完成。

4.1.3　系统防护

（1）针对应用系统开展安全基线的配置与核查，对账户安全策略、口令策略、登录策略、系统审计日志做好安全防范配置。

（2）守正招标平台系统登录、服务器登录、应用程序、ECSB\ESB 等密码，必须满足密码策略、复杂度要求（14 位

及以上数字、大小写字母和特殊字符的组合），每 3 个月定期修改服务器密码，禁止所有服务器使用同一个密码。

（3）部署 zabbix、运维监控平台，对服务器的 CPU、内存、存储等主机状态进行实时监控，针对监控平台邮件或短信反馈的异常信息，项目组应及时排查相关问题。

（4）针对 DMZ 主机部署 G01 主机客户端，应用主机部署青藤云病毒防护客户端，如需临时关闭的，由平台运营管理部门相关负责人向集团系统组申请关闭。

（5）禁止在服务器上增加、删除程序及其他内容；严禁私自复制、拷贝服务器上的数据及其他内容；严禁在服务器上制造、传播计算机病毒；严禁故意输入计算机病毒，危害服务器运行、网络安全和数据安全。

4.2　系统监控管理

应用系统外包供应商，应针对各自负责的应用系统的日常运行情况进行监控，对应用系统各性能瓶颈模块进行重点监控，必要时应提出有针对性的优化方案，平台运营管理部门对优化方案进行评估并组织评审，评审通过后由应用系统外包单位按审批通过的方案实施优化，从而实现应用系统性能的逐步提升。

针对监控异常事项的告警短信或邮件，应及时发送至平台运营管理部门相关负责人，并对引起异常的原因进行排查处理。

5　接口管理

5.1　接口程序的安装部署管理

各应用系统如需开发接口，原则上应通过 ECSB\ESB\SSDP 方式实现对接。接口不应对外开放，所采用的传输方式（如 https、rest、restful 等安全传输协议)应保证数据的安全性，接口间的互联，需使用 base64 等加密模式。

5.2　接口程序升级管理

在接口升级、应用系统版本升级时，存在对接口产生影响的可能性，应评估升级对接口\对外关联的系统产生的影响。在升级完成后，应进行多系统间的测试，保证升级后，接口能正常运行，系统间能正常交互。

新增或升级接口时，应用系统外包单位更新附件 8《守正平台接口汇总表格》后，方可申请新增接口，经平台运营管理部门相关负责人审核通过后，方可执行。

应用系统外包单位应定期梳理接口信息，及时更新附件 8《守正平台接口汇总表格》。

6　数据库日常维护管理

6.1　数据库日常巡检、维护及性能优化管理

（1）应用系统外包单位应依据《日常巡检机制检查表》中的数据库巡检项，按要求对数据库进行日常巡检，记录巡检结果，同时通过运维监控平台对日志、会话数、表空间、磁盘空间等主要数据库参数实时监控。

（2）归档数据库（oracle、mysql）日志备份，做到增量备份每天一次、全量备份每月两次。

（3）应用系统外包单位对数据库进行 表空间维护、权限分配、异常问题处理等运维操作，定期监控数据库异常情况，同时对潜在的异常进行分析并提出预防方案。

（4）按集团灾备演练计划要求，应用系统外包单位配合平台运营管理部门完成年度生产数据库、灾备数据库切换演练。

（5）对数据库要进行持续性的安全配置加固，安全配置加固包括但不限于账号口令、服务安全、日志审计等方面。

（6）关于数据库的安全补丁，应及时与厂商联系，获取最新的安全补丁通报、安全补丁和厂商的修复建议，据此完成数据库版本升级、一般技术性和紧急技术漏洞修复工作。

6.2　数据库性能优化管理要求

数据库优化是多方面的，原则是减少系统的瓶颈，减少资源的占用，提高系统的反应速度。通过 SQL 调优、索引调优及连接池配置等方面对数据库性能进行优化，减少数据库瓶颈点，提升数据库性能，使系统响应更快。

数据库性能优化方案由应用系统外包单位的数据库管理员制定，经平台运营管理部门相关负责人审核通过后，方可执行。

6.3　数据库安全管理要求

（1）数据库安全规定：对所有数据库的管理和对表、视图、记录和域的授权工作统一由数据库管理员执行。

（2）平台运营管理部门依据实际需求，根据不同类型数据、文件的重要性，制定相应的备份策略并记录至附件 9《数据备份策略表格》。数据备份策略文档中必须包括备份数据所

在主机名称、备份数据说明、备份频率、磁带异地存放频率和地点等各项要求和步骤流程。数据备份操作需要进行流程审批，确保操作的规范性。

（3）当服务器、交换机及其他系统主要设备配置更新变化，服务器应用系统、软件修改后均要在改动前进行备份。

（4）所有数据备份工作由应用系统外包单位的数据库管理员在业务低负载时段执行，并进行详实记录，同时由系统负责人进行检查，确保备份操作正确执行。

（5）如遇网络攻击或病毒感染等突发事件，各相关方应积极配合系统负责人进行处理，同时将情况进行详细的记录。

（6）数据备份需要定期检查，确认数据备份操作是否执行成功。

（7）需要恢复备份数据时，应记录本次数据恢复的内容，包括但不限于数据内容、恢复原因、恢复数据来源、恢复时间及恢复方案等，经平台运营管理部门相关领导审批通过后方可执行。

（8）项目组按要求编写数据库恢复操作手册，定期对备份数据进行恢复测试工作，确保备份恢复工作能顺利进行，日常备份能正确还原，并根据测试结果优化备份恢复操作步骤。

（9）平台运营管理部门制定数据、文件等备份测试的巡检项，各项目组按既定的巡检表进行巡查巡检，并仔细记录巡检结果。