云南腾电科技有限公司

服务可用性和连续性管理程序

（YNTD-ITSS-0608）

编制人:谢广胜　　编制时间:2025.01.07

审核人:赵建中　　编制时间:2025.01.07

批准人:陆涛　　审批时间:2025.01.07

1. 目的

本制度依据ITSS《信息技术服务 运行维护 第1部分：通用要求》（GB/T 28827.1-2022）及公司《信息安全管理程序》，旨在建立规范的服务可用性与连续性管理机制，实现以下目标：

1. 确保运维服务可用性达到服务级别协议（SLA）约定标准，保障客户业务稳定运行；
2. 识别服务中断风险，制定预防与恢复措施，将服务中断造成的损失降至最低；
3. 满足ITSS运维服务管理体系认证要求，提升公司运维服务规范化水平与市场竞争力。

2. 范围

本制度适用于公司所有运维服务项目的可用性管理、连续性规划、应急响应及恢复全过程，涵盖以下内容：

运维服务涉及的网络设备、服务器、存储系统、应用系统等IT资产；

服务可用性指标监测、分析与优化活动；

服务连续性计划的制定、演练、评审与更新；

服务中断事件的应急处置与恢复工作。

本制度约束对象包括运维部、研发部、质量部、人力部及所有参与运维服务的人员。

3. 术语与定义

术语	定义
服务可用性	在约定时间内，运维服务满足客户业务需求的能力，通常以“服务可用时间/约定服务时间×100%”计算
服务连续性	面对服务中断事件时，通过预防、应急响应与恢复措施，保障服务在规定时间内恢复的能力
RTO（恢复时间目标）	服务中断后，从故障发生到服务恢复至可接受水平

	的最长允许时间
RPO（恢复点目标）	服务中断后，恢复数据时允许丢失的最大数据量对应的时间点
应急响应	服务中断发生后，为控制事态扩大、减少损失而采取的即时处置措施

4. 职责与权限

4.1. 运维部

作为制度执行主体，负责服务可用性指标的日常监测、统计与分析；
牵头制定服务连续性计划及专项应急方案，组织应急演练；
服务中断时，启动应急响应，主导故障排查与服务恢复工作；
定期汇总可用性数据与连续性管理情况，形成改进报告。

4.2. 研发部

提供技术支撑，协助排查复杂技术故障，制定系统优化方案；
负责IT资产的定期维护与巡检，减少硬件故障导致的服务中断；
参与服务连续性计划制定，提供技术可行性评估。

4.3. 应急管理部

结合《信息安全管理程序》，识别服务中断相关的安全风险；
监督应急响应过程中的信息安全措施落实，防止数据泄露；
参与服务连续性计划评审，提出安全改进建议。

4.4. 服务台

负责与客户沟通，明确SLA中可用性指标及RTO、RPO要求；
服务中断时，及时向客户通报故障情况及恢复进展；
收集客户对服务可用性的反馈，协助运维部优化服务。

4.5. 总经理

审批服务可用性目标、服务连续性计划及应急方案；

保障服务可用性与连续性管理所需的资源（人员、资金、技术工具）；

评审服务可用性与连续性管理工作成效，推动持续改进。

5. 服务可用性管理

5.1. 可用性目标确定

服务台与客户对接，结合业务重要程度及行业标准，在SLA中明确以下可用性要求，经双方签字确认后生效：

核心业务系统可用性目标：通常不低于99.9%（允许年中断时间≤8.76小时）；

一般业务系统可用性目标：通常不低于99.5%（允许年中断时间≤43.8小时）；

特殊场景（如节假日、业务高峰期）的可用性保障要求。

运维部需将SLA中的可用性目标分解为具体的IT组件（如服务器、网络设备）可用性指标，确保目标可监测、可落地。

5.2. 可用性监测与统计

5.2.1. 监测范围与工具

运维部部署网络管理系统（NMS）、服务器监控系统、应用性能监控工具，对以下内容进行实时监测：

网络设备：带宽利用率、端口状态、丢包率、延迟；

服务器：CPU利用率、内存占用、磁盘空间、进程状态；

应用系统：响应时间、并发用户数、交易成功率；

存储系统：存储利用率、IOPS、数据同步状态。

5.2.2. 监测数据管理

监测数据需实时采集、自动存储，存储周期不少于1年，内容包括：

常规监测数据：每5分钟采集一次关键指标，每小时生成基础监测报告；

故障相关数据：故障发生时间、故障类型、影响范围、处理过程、恢复时间。

5.2.3. 可用性计算

运维部每月按以下公式计算服务可用性，形成《服务可用性统计报告》：

服务可用性=（约定服务时间-服务中断时间）/约定服务时间×100%

注：服务中断时间指因运维责任导致的服务不可用时间，不包含客户授权的计划性停机时间及不可抗力导致的中断时间。

5.3. 可用性分析与优化

运维部每月召开可用性分析会议，结合统计数据开展以下工作：

对比实际可用性与SLA目标，分析未达标的原因（如硬件故障、配置不合理、攻击事件）；

识别可用性瓶颈，如网络带宽不足、服务器性能过载等，制定优化方案；

对高频故障点进行根因分析，通过硬件升级、软件补丁、配置优化等措施减少故障发生。

优化方案需明确责任人和完成时限，实施后需跟踪验证优化效果，确保可用性持续提升。

6. 服务连续性管理

6.1. 风险识别与评估

运维部联合应急管理部，每半年开展一次服务中断风险评估，参考《信息安全管理程序》中的风险评估方法，识别以下风险：

技术风险：硬件故障、软件漏洞、网络攻击、数据丢失；

环境风险：机房断电、火灾、洪水、自然灾害；

管理风险：人为误操作、人员流失、应急响应不当。

风险评估需形成《服务中断风险评估报告》，明确风险等级、影响范围及

潜在损失，为连续性计划制定提供依据。

6.2. 服务连续性计划制定

6.2.1. 计划核心内容

运维部依据风险评估结果及SLA中的RTO、RPO要求，制定《服务连续性计划》，内容包括：

应急指挥小组、技术处置小组、客户沟通小组的组成及职责；

RTO与RPO明确：按业务优先级划分核心业务（RTO≤1小时，RPO≤15分钟）、一般业务（RTO≤4小时，RPO≤1小时）；

预防措施：硬件冗余、数据备份、漏洞修复、异地容灾等；

应急响应流程：故障上报、应急启动、故障排查、服务恢复步骤；

资源保障：应急设备、备用网络、技术文档、联系方式清单。

6.2.2. 专项应急方案

针对高频风险，需制定专项应急方案，包括但不限于：

服务器故障应急方案：明确备用服务器切换流程及数据恢复方法；

网络中断应急方案：制定备用网络链路切换步骤；

数据丢失应急方案：规定数据恢复的操作流程及验证标准；

机房灾难应急方案：明确异地容灾中心启动条件及业务切换流程。

6.2.3. 计划审批与发布

《服务连续性计划》及专项应急方案需经研发部、应急管理部审核，报管理层批准后发布，确保所有相关人员可随时获取最新版本。

6.3. 预防措施实施

6.3.1. 硬件与网络冗余

核心服务器采用双机热备模式，确保单台服务器故障时自动切换；

网络设备（路由器、交换机）采用冗余配置，关键链路实现双线备份；

机房配备UPS不间断电源及柴油发电机，保障断电后核心设备运行≥4小时。

6.3.2. 数据备份与恢复

严格执行数据备份策略，确保数据可恢复，具体要求如下：

数据类型	备份频率	备份方式	存储位置	恢复验证周期
核心业务数据	实时增量+每日全量	加密备份	本地+异地容灾中心	每周1次
一般业务数据	每日增量+每周全量	加密备份	本地存储	每月1次

6.3.3. 日常维护与巡检

技术支持部按以下要求开展日常维护，减少服务中断风险：

每日巡检：核心设备运行状态、备份任务执行情况；

每周巡检：网络拓扑稳定性、软件补丁更新情况；

每月巡检：硬件健康状态、容灾系统可用性。

6.4. 应急响应与恢复

6.4.1. 故障上报与分级

服务中断发生后，发现人需立即通过电话、应急平台等方式上报，运维部根据故障影响范围及RTO要求，将故障分为四级：

故障等级	判定标准	响应时限
一级（特别重大）	核心业务中断，影响所有客户，RTO≤1小时	5分钟内响应，应急指挥小组立即启动
二级（重大）	核心业务部分中断，影响重要客户，RTO≤2小时	10分钟内响应，技术处置小组立即介入
三级（较大）	一般业务中断，影响部分客户，RTO≤4小时	30分钟内响应，运维工程师现场处置
四级（一般）	单台设备故障，不影响业务运行	1小时内响应，安排计划性

		修复

6.4.2. 应急处置流程

故障隔离：采取措施隔离故障源，防止故障扩散，如断开故障设备、关闭异常进程；

应急恢复：根据专项应急方案启动恢复措施，如切换至备用服务器、恢复数据、启用备用网络；

客户沟通：服务台按“首报、续报、终报”原则向客户通报情况，首报不超过30分钟，续报间隔不超过1小时；

故障排查：服务恢复后，深入排查故障根因，避免同类问题重复发生；

总结报告：应急处置结束后24小时内，运维部形成《服务中断应急处置报告》，记录处置过程、原因分析及改进措施。

6.5. 计划演练与评审

6.5.1. 应急演练

运维部每年至少组织一次应急演练，每年覆盖所有专项应急方案，演练要求如下：

演练形式：桌面推演与实战演练相结合，核心业务系统需开展实战演练；

参与人员：运维相关部门经理和相关职位运维工程师等；

演练评估：演练结束后，组织评估会议，分析演练过程中存在的问题，形成《应急演练评估报告》。

6.5.2. 计划评审与更新

运维部每年对《服务连续性计划》进行一次全面评审，出现以下情况时需及时更新：

1. SLA变更或客户业务需求调整；
2. IT系统架构升级或核心设备更换；
3. 应急演练或实际应急处置中发现计划缺陷；
4. 相关法律法规或ITSS标准更新。

7. 考核与改进

7.1. 考核指标

公司将服务可用性与连续性管理纳入运维部绩效考核，核心指标如下：

指标名称	计算公式	目标值	考核周期
服务可用性	（约定服务时间-服务中断时间）/约定服务时间×100%	99%	年度
服务中断次数	次数，统计服务中断次数	≤2	年度

7.2. 持续改进

运维部每月汇总可用性数据、应急处置情况，每季度组织服务可用性与连续性管理评审会议，针对以下内容制定改进措施：

可用性未达标的根因及优化方案；

应急处置过程中暴露的流程或技术问题；

客户反馈的服务可用性相关意见；

ITSS标准更新带来的管理要求变化。

改进措施需明确责任部门、完成时限及验证方法，确保改进效果可量化、可追溯。

8. 相关文件与记录

8.1. 相关文件

《信息安全管理程序》

《服务级别协议管理规范》

GB/T 28827.1-2022《信息技术服务 运行维护 第1部分：通用要求》

8.2. 相关记录

《服务可用性统计报告》

《服务中断风险评估报告》

《服务连续性计划》

《专项应急方案》

《服务中断应急处置报告》

《应急演练评估报告》

《服务可用性与连续性管理评审报告》

9. 附则

本制度由公司运维部负责解释与修订，自发布之日起施行。