云南腾电科技有限公司

服务数据管理制度

（YNTD-ITSS-0806）

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

文件编制和变更履历

版本	编制/更改		发布		实施		更改记录
	作者	日期	审核	日期	批准	日期	
V1.0	谢广胜	2025.1.7	赵建中	2025.1.7	陆涛	2025.1.7	首次发布

目录

1. 目的

为满足IT服务管理体系（ITSS）认证要求，建立标准化的服务数据管理机制，规范公司服务数据的全生命周期管控，确保服务数据的完整性、准确性、安全性和可用性。通过有效管理服务数据，支撑IT服务优化决策、提升服务质量与效率，同时保障数据使用符合法律法规、客户协议及公司保密要求，为公司IT服务运营与持续改进提供可靠数据支撑，特制定本制度。

本制度旨在实现服务数据“一数一源、一源多用”的管理目标，推动数据资源整合共享，挖掘数据价值，强化数据安全保障，提升公司IT服务管理的科学化水平。

2. 适用范围

本制度适用于公司所有IT服务相关数据（以下简称“服务数据”）的采集、存储、处理、传输、使用、销毁等全生命周期管理活动，涵盖数据管理的技术支撑、流程执行及人员操作等各个环节。

服务数据涉及的范围包括但不限于：IT运维服务数据（故障记录、巡检数据、变更记录等）、客户服务数据（客户基本信息、服务请求、满意度数据等）、服务绩效数据（KPI指标数据、服务成本数据等）、配置管理数据（配置项信息、关系数据等）及其他与IT服务相关的数据。

公司各部门及全体员工，在涉及服务数据相关操作时，均需严格遵守本制度规定。

3. 术语与定义

1. 服务数据

指公司在IT服务运营过程中产生、采集或获取的，与IT服务提供、管理、优化相关的各类结构化、半结构化及非结构化数据，是支撑IT服务决策的核心资源。

2. 数据生命周期

指服务数据从产生或采集开始，经过存储、处理、传输、使用，直至最终销毁的完整过程，每个阶段均需遵循相应的管理规范。

3. 数据分类

根据服务数据的来源、用途及属性，将其划分为不同类别，实现数据的差异化管理。

4. 数据分级

根据服务数据的敏感程度、泄露风险及影响范围，将其划分为不同安全级别，实施分级保护。

5. 数据质量

指服务数据满足规定需求的程度，主要包括准确性、完整性、一致性、时效性及可用性等指标。

6. 数据脱敏

指通过一定技术手段（如加密、替换、删除等）对敏感服务数据进行处理，在保留数据使用价值的同时，防止敏感信息泄露的技术措施。

4. 角色与职责

角色	职责部门/人员	核心职责	具体工作内容
数据管理员	运维部	服务数据的日常管理与运维	1. 负责数据管理平台的部署、维护及故障处理； 2. 执行服务数据的采集、存储、备份及清理操作； 3. 建立并维护服务数据台账，确保数据可追溯； 4. 监控数据质量，协助处理数据质量问题； 5. 配合开展数据安全防护及审计工作。
数据审核人	运维部经理	服务数据管理的审核与决策	1. 审核服务数据分类分级标准及管理规范； 2. 审批数据采集、使用、销毁等重要操作申请； 3. 监督数据管理流程的执行情况，确保合规性；

			4. 协调解决数据管理中的重大问题及跨部门争议。
数据采集人	各运维相关部门指定人员	服务数据的规范采集与提交	1. 按照数据采集标准收集本部门相关服务数据，确保数据真实、完整； 2. 及时提交采集数据至数据管理平台，标注数据类别及级别； 3. 配合数据管理员进行数据质量校验，修改完善不合格数据。
数据使用人	各运维相关部门指定人员	服务数据的合规使用与反馈	1. 在授权范围内使用服务数据，不得擅自扩大使用范围或泄露数据； 2. 按照规定流程申请敏感数据的使用权限，使用后及时归档或销毁相关数据副本； 3. 发现数据质量问题或安全隐患时，及时向数据管理员反馈。
安全负责人	运维部	服务数据的安全与保密管控	1. 制定数据安全防护策略及应急处置预案； 2. 实施数据加密、访问控制等安全措施，定期开展安全检查； 3. 调查处理数据安全事件，追溯责任并提出整改建议； 4. 组织数据安全培训，提升员工安全意识。
审计监督人	质量部	服务数据管理的审计与监督	1. 定期对数据管理流程执行情况、数据质量及安全合规性进行审计； 2. 核查数据台账与实际数据的一致性，评估数据管理成效； 3. 针对审计发现的问题，督促相关部门限期整改，形成审计报告。

5. 服务数据分类与分级

5.1. 数据分类

为实现服务数据的精准管理，根据数据来源及用途，将服务数据划分为以下类别，各类数据需在管理平台中明确标识：

数据类别	涵盖范围	管理责任部门
运维服务数据	故障记录、事件处理日志、巡检报告、变更请求、配置项变更记录、性能监控数据等	运维部
客户服务数据	客户基本信息、服务合同、服务请求、满意度调查结果、投诉处理记录等	服务台
绩效数据	KPI指标完成情况、服务成本数据、人员绩效记录、服务质量评估报告等	质量部
配置管理数据	IT基础架构配置项信息、配置项关系、配置基线、配置审计记录等	运维部
其他服务数据	服务相关的规章制度、培训记录、知识库关联数据等	各相关部门

5.2. 数据分级

根据服务数据的敏感程度及泄露后的影响范围，将其划分为三级，实施分级保护：

1. 一级（公开级）：无敏感信息，可在公司内部公开共享的数据，如服务流程规范、公开的服务案例、非涉密的绩效统计数据等。此类数据仅需进行基本的格式规范管理。
2. 二级（内部级）：涉及公司内部运营信息，不宜对外公开的数据，如普通运维记录、内部服务请求、非核心绩效数据等。此类数据需进行访问权限控制，仅限授权人员使用。

3. 三级（敏感级）：涉及客户隐私、公司核心业务信息及重大利益，泄露后将造成严重影响的数据，如客户身份证号、联系方式、服务合同核心条款、核心配置信息、财务数据等。此类数据需实施加密存储、严格权限管控及使用审计。
4. 数据分级需由数据采集人初步判定，经部门负责人及数据审核人复核确认后，在数据管理平台中标记存档。数据级别可根据实际情况变化进行调整，调整流程需经运维部批准。

6. 服务数据全生命周期管理

6.1. 数据采集

1. 采集原则：遵循“按需采集、最小必要、真实准确”的原则，仅采集与IT服务管理相关的数据，避免数据冗余；确保采集的数据真实反映实际情况，严禁伪造或篡改数据。
2. 采集标准：各数据类别需制定统一的采集标准，明确数据字段、数据格式、计量单位、提交频率及责任主体。例如：故障记录需包含故障发生时间、地点、现象、处理过程、解决结果等字段，提交频率为故障处理完成后2小时内。
3. 采集方式：优先采用自动化采集方式（如通过监控工具、服务管理系统自动抓取数据）；确需人工采集的，需通过标准化表单（电子或纸质）提交，确保数据规范。
4. 采集审核：数据采集人提交数据后，数据管理员需在1个工作日内完成数据质量初步校验，校验不合格的退回采集人修改；敏感级数据需经数据审核人二次审核确认后，方可纳入数据管理平台。

6.2. 数据存储

存储载体：服务数据需存储在公司指定的专用服务器、数据仓库或云存储平台中，严禁存储在个人设备或非授权外部存储介质中。存储设备需具备高可用性、高可靠性及安全防护能力。

存储分类：按照数据类别及级别进行分类存储，敏感级数据需单独存储并实施加密处理（加密算法需符合国家相关标准）；不同级别的数据需设置独立的存储区域及访问控制策略。

存储期限：根据数据类别及相关法规要求，明确数据存储期限：

一级数据：存储期限不少于1年；

二级数据：存储期限不少于3年；

三级数据：存储期限不少于5年，涉及客户隐私及合同纠纷的数据需永久存储（或按法规要求延长存储期限）。

备份策略：采用“本地+异地”双重备份策略，确保数据安全。一级、二级数据每周备份一次，三级数据每日备份一次；备份数据需进行加密存储，并定期（每月）验证备份数据的有效性，确保可正常恢复。

6.3. 数据处理

1. 处理目的：通过数据清洗、整合、脱敏等处理，提升数据质量，挖掘数据价值，为服务决策提供支持。
2. 处理流程：

   数据清洗：去除重复数据、修正错误数据、补充缺失数据，确保数据准确性；
3. 数据整合：将分散在不同系统中的数据进行关联整合，形成统一的数据视图；
4. 数据脱敏：对敏感级数据进行脱敏处理，如客户身份证号替换为“XXXXXX****XXXX”，处理后的数据需保留必要的使用价值；
5. 数据标准化：将处理后的数据转换为统一格式，便于查询、统计及分析。
6. 处理权限：数据处理操作需由授权的数据管理员执行，敏感级数据的处理需经数据审核人批准，并全程记录操作日志；严禁未经授权对数据进行修改、删除等处理。

6.4. 数据传输

1. 传输安全：服务数据传输需采用加密传输协议（如SSL/TLS、VPN等），确保数据在传输过程中不被窃取或篡改；严禁通过非加密邮件、即时通讯工具（如普通微信、QQ）传输敏感级数据。

2. 传输范围：数据传输需限定在公司内部授权系统或经批准的外部合作方系统范围内；向外部传输数据（如向客户提供服务报告）需经数据审核人及分管副总双重批准，并签订数据保密协议。
3. 传输记录：所有数据传输操作需自动记录传输日志，包括传输时间、传输内容、发送方、接收方、传输状态等信息，日志存储期限不少于1年，便于追溯。

6.5. 数据使用

1. 使用权限：实行“权限最小化”原则，根据岗位需求为员工分配相应的数据使用权限：

   一级数据：全体员工可查询使用；
2. 二级数据：相关业务部门员工经部门负责人批准后可查询使用；
3. 三级数据：仅核心岗位人员经数据审核人批准后可查询使用，且需明确使用范围及期限。
4. 使用规范：数据使用需严格遵循申请用途，不得超出授权范围使用数据；严禁将服务数据用于个人目的或未经批准的商业用途；使用敏感级数据时，需对使用过程进行记录，使用完毕后及时清理临时数据副本。
5. 数据共享：内部数据共享需通过授权的数据管理平台进行，严禁私自拷贝或转发数据；外部数据共享（如向客户、合作方提供数据）需签订数据共享协议，明确共享范围、用途及保密责任，并经数据审核人及法务部门批准。
6. 数据发布：对外发布服务数据（如服务白皮书、公开绩效报告）需经数据审核人及公司管理层批准，发布前需对数据进行脱敏处理，确保不包含敏感信息。

6.6. 数据销毁

1. 销毁条件：达到规定存储期限且无保留必要的数据，或因业务调整不再需要的数据，可申请销毁；涉及客户隐私及法律纠纷的数据，需在满足法规要求后再进行销毁。

2. 销毁流程：数据使用部门提交《服务数据销毁申请表》，说明销毁数据的类别、级别、数量及原因，经部门负责人、数据审核人批准后，由数据管理员执行销毁操作；敏感级数据的销毁需由审计监督人现场监督。
3. 销毁方式：

电子数据：采用专业的数据销毁工具（如多次覆写、物理销毁存储介质），确保数据无法恢复；
4. 纸质数据：采用粉碎、焚烧等方式销毁，严禁随意丢弃。
5. 销毁记录：数据销毁后，数据管理员需填写《服务数据销毁记录表》，详细记录销毁数据信息、销毁方式、时间、执行人及监督人等信息，记录表需归档保存不少于3年。

7. 数据安全与保密管理

1. 访问控制：数据管理平台需建立严格的身份认证及权限管理机制，员工需通过账号密码（定期更换）、短信验证等多因素认证方式登录；权限分配遵循“岗责匹配”原则，员工离职或岗位调整时，需在1个工作日内注销或调整其数据访问权限。
2. 安全防护：数据存储及传输设备需安装防火墙、杀毒软件、入侵检测系统等安全防护工具，定期（每月）进行漏洞扫描及病毒查杀；敏感级数据需采用加密存储、加密传输双重保护措施，密钥由安全负责人统一管理。
3. 保密要求：全体员工需遵守数据保密规定，严禁泄露、出售或非法提供服务数据；未经批准，严禁将存储有服务数据的设备带出公司；参加外部会议或交流时，不得擅自披露敏感数据。
4. 应急处置：安全负责人需制定《服务数据安全应急处置预案》，明确数据泄露、丢失、损坏等安全事件的应急响应流程；定期（每半年）组织应急演练，提升应急处置能力。发生安全事件时，需立即启动预案，采取隔离、止损措施，并及时向管理层汇报。
5. 员工培训：人力部需将数据安全与保密知识纳入新员工入职培训及在职员工定期培训内容，每年培训不少于2次；培训后需进行考核，确保员工掌握数据管理规范及安全防护技能。

8. 数据质量管控

1. 质量监控：数据管理员每日对新增数据进行质量抽检，每周形成《服务数据质量周报》；数据管理平台需具备质量监控功能，对数据异常情况（如格式错误、字段缺失）进行自动预警。
2. 问题整改：发现数据质量问题后，数据管理员需在2个工作日内通知相关责任部门及人员，明确整改要求及期限；责任部门需在规定期限内完成整改，数据管理员负责复核验收。
3. 持续改进：每月由数据审核人组织召开数据质量分析会，总结质量问题产生的原因，制定改进措施（如优化采集表单、加强培训等），并跟踪改进效果。

9. 审计与监督

1. 定期审计：审计监督人每季度联合运维部对服务数据管理情况进行全面审计，审计内容包括：数据分类分级准确性、流程执行合规性、数据质量达标情况、安全防护措施落实情况及权限管理合理性等，审计结果形成《服务数据管理审计报告》，上报公司管理层。
2. 专项审计：发生数据安全事件、重大数据质量问题或ITSS认证检查前，需开展专项审计，重点核查相关环节的管理情况，明确责任主体，提出整改建议。
3. 整改跟踪：审计发现的问题需明确整改责任人、整改措施及整改期限，由审计监督人跟踪整改落实情况；整改完成后，需进行复核验收，确保问题闭环管理。对违反本制度的部门或个人，按照公司奖惩规定进行处理；造成严重后果的，追究相关法律责任。

10. KPI指标

指标名称	计算方式	目标值	考核频次
分析利用次数	次数，分析利用次数	≥2次	季度