**文件编号：ITSS-08-01-06**

**版本：V1.0**

万洲奇智（青岛）信息科技有限公司

服务数据管理制度

|  |  |
| --- | --- |
| 编制人:毛彦超 | 编制时间:2025.01.08 |
| 审核人:陈姝羽 | 编制时间:2025.01.08 |
| 批准人:郭万洲 | 审批时间:2025.01.08 |

**修订记录**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 日期 | 版本 | 变更说明 | 编写人 | 审核人 | 批准人 |
| 2025.01.08 | V1.0 | 新建文档 | 毛彦超 | 陈姝羽 | 郭万洲 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

目录

[万洲奇智（青岛）信息科技有限公司 1](#_Toc32549)

[服务数据管理制度 1](#_Toc3391)

[1. 目的 5](#_Toc32588)

[2. 原则 5](#_Toc24071)

[3. 适用范围 5](#_Toc17759)

[4. 岗位职责 5](#_Toc24113)

[4.1. 运维部 5](#_Toc23263)

[4.2. 研发部 6](#_Toc13399)

[5. 服务数据管理 6](#_Toc2710)

[5.1. 服务数据全生命周期管理 6](#_Toc11344)

[5.1.1. 数据采集 6](#_Toc13421)

[5.1.2. 数据存储 7](#_Toc1060)

[5.1.3. 数据处理与转换 7](#_Toc3333)

[5.1.4. 数据使用与共享 8](#_Toc14786)

[5.1.5. 数据销毁 8](#_Toc3865)

[5.2. 数据安全与合规 9](#_Toc10076)

[5.2.1. 安全防护 9](#_Toc21745)

[5.2.2. 合规管理 9](#_Toc27528)

[5.3. 数据质量控制 10](#_Toc624)

[5.3.1. 质量指标 10](#_Toc17314)

[5.3.2. 质量监控 10](#_Toc27775)

[5.3.3. 质量改进 10](#_Toc29184)

[5.4. 数据共享与应用 11](#_Toc20707)

[5.4.1. 数据共享 11](#_Toc22259)

[5.4.2. 数据应用 11](#_Toc18888)

[5.5. 监督与审计 11](#_Toc23214)

[5.5.1. 内部监督 11](#_Toc17019)

[5.6. 制度评审与改进 12](#_Toc30601)

[5.6.1. 外部审计 12](#_Toc7983)

[5.7. 培训与宣贯 12](#_Toc28475)

[5.8. 考核指标 12](#_Toc6088)

[6. 附则 12](#_Toc19199)

[7. 附件 13](#_Toc1523)

[8. 记录 13](#_Toc1470)

目的

本制度旨在通过建立系统化的服务数据管理体系，实现服务数据的规范采集、安全存储、高效利用和合规管控，提升服务质量与效率，支撑服务过程改进和应急交付决策，保障服务数据资产的完整性与价值最大化。

原则

1. 全面性原则：

覆盖服务数据全生命周期各环节，确保无管理盲区。

1. 准确性原则：

保证服务数据真实、准确、完整，为决策提供可靠依据。

1. 安全性原则：

采取必要的技术和管理措施，保障服务数据不被泄露、篡改或滥用。

1. 合规性原则：

遵循国家相关法律法规及行业标准，规范服务数据的管理与使用。

1. 实用性原则：

服务数据管理流程应简洁高效，满足服务优化和业务发展需求。

适用范围

适用于组织内所有与服务活动相关的数据，包括但不限于服务需求数据、响应数据、执行数据、结果数据、客户反馈数据、应急交付数据等，涵盖数据从产生、流转、使用到销毁的全生命周期，涉及所有参与服务数据管理的部门及人员。

岗位职责

运维部

1. 负责服务数据管理系统的建设、维护和技术支持，保障系统安全稳定运行，提供数据存储、处理、分析等技术服务。
2. 负责制定和完善服务数据管理制度、流程和标准，组织开展数据治理工作，监督制度的执行情况.
3. 负责本部门服务数据的采集、整理、上报和使用，确保数据质量。

研发部

1. 负责本部门服务数据的采集、整理、上报和使用，确保数据质量。

服务数据管理

服务数据全生命周期管理

服务数据生命周期主要包括：

1. 数据采集
2. 数据存储
3. 数据处理与转换
4. 数据使用与分享
5. 数据销毁

数据采集

1. **采集范围**

包括服务需求信息（需求内容、紧急程度、客户信息等）、服务响应信息（响应时间、响应方式、响应人员等）、服务执行信息（执行步骤、资源消耗、进度情况等）、服务结果信息（交付成果、验收情况、服务成本等）、客户反馈信息（满意度评分、意见建议等）、应急交付信息（应急场景、处置措施、交付时效等）。

1. **采集标准**

明确各类服务数据的采集字段、数据格式、计量单位等，确保数据的一致性和可比性。例如，服务响应时间精确到分钟，满意度评分采用百分制。

1. **采集方式**

结合自动化采集和人工采集两种方式。对于可通过系统自动获取的数据（如服务系统中的响应时间、执行进度等），由 运维部配置自动采集规则；对于需人工录入的数据（如客户口头反馈、现场服务情况等），由业务人员通过指定系统或表单及时、准确录入。

1. **采集责任**

业务人员为数据采集的直接责任人，确保在数据产生后24小时内完成采集录入工作，运维部定期检查采集完成情况。

数据存储

1. **存储要求**：

采用安全可靠的存储介质和系统，满足数据存储容量、性能和可靠性需求。根据数据重要程度和访问频率，合理规划存储架构，对重要数据实行多副本存、储和异地备份。

1. **存储分类**

按照数据类型和敏感程度进行分类存储。敏感数据（如客户隐私信息、核心业务数据）需进行加密存储，普通数据可采用常规存储方式。

1. **存储期限**

根据数据的价值和相关规定，确定不同类型服务数据的存储期限。服务需求、结果等关键数据长期存储；应急交付数据存储至应急事件处理完毕后 5 年；其他一般性数据存储 3-5年，超过存储期限的数据按规定进行归档或销毁。

1. **数据备份**

运维部负责制定数据备份计划，定期对服务数据进行备份，备份频率至少为每日一次。备份数据需进行加密处理，并存储在安全的地点，定期进行备份恢复测试，确保备份数据的可用性。

数据处理与转换

1. **数据清洗**

运维部定期对服务数据进行清洗，去除重复数据、纠正错误数据、补充缺失数据，确保数据的准确性和完整性。对于清洗过程中发现的问题，及时反馈给相关业务部门进行整改。

1. **数据转换**

根据数据分析和应用需求，对服务数据进行格式转换、汇总计算等处理，形成符合要求的数据形式。例如，将分散的客户反馈数据汇总成月度满意度报告。

1. **数据整合**

整合不同来源、不同格式的服务数据，消除数据孤岛，形成统一的服务数据视图，为数据分析和应用提供支持。

数据使用与共享

1. **数据使用权限**

基于 “最小权限”原则，为不同部门和人员分配相应的数据使用权限。业务部门可使用本部门相关的服务数据；管理部门可使用全局服务数据进行分析和决策；外部机构如需使用服务数据，需经数据治理委员会审批，并签订数据使用协议。

1. **数据使用规范**

使用服务数据时，应遵守相关法律法规和组织规定，不得用于未经授权的用途。严禁泄露、篡改、出售服务数据，对敏感数据的使用需进行严格审批和记录。

1. **数据共享机制**

建立数据共享平台，实现各部门之间服务数据的有序共享。数据共享需通过数据共享平台进行，共享过程中需对数据进行脱敏处理，保护敏感信息。

数据提供部门负责确保共享数据的质量，数据使用部门对共享数据的合理使用负责。

数据销毁

1. **销毁条件**：

超过存储期限且无保留价值的数据、经批准需要销毁的过期备份数据、以及因业务调整等原因不再需要的数据，可进行销毁。

1. **销毁流程**：

由数据使用部门提出数据销毁申请，说明销毁数据的类型、数量、原因和销毁方式，经运维部经理审核，报总经理批准后，由运维部按照规定的销毁方式进行销毁。

1. **销毁方式**：

根据数据存储介质的不同，采用相应的销毁方式。电子数据可采用数据覆盖、物理销毁存储介质等方式；纸质数据采用粉碎等方式。

数据安全与合规

安全防护

1. **访问控制**

建立严格的访问控制机制，对服务数据的访问进行身份认证和权限管理。采用多因素认证方式（如密码 + 动态令牌），限制未授权人员访问数据。定期对访问权限进行审查和调整，确保权限与职责相符。

1. **数据加密**

对敏感服务数据在传输和存储过程中进行加密处理，采用国家认可的加密算法（如AES-256），防止数据泄露。

1. **安全审计**：

运维部经理负责对服务数据的访问、操作等行为进行安全审计，记录审计日志，定期分析审计结果，及时发现和处理安全隐患。

1. **应急响应**

制定数据安全应急响应预案，明确应急处理流程和责任分工。在发生数据泄露、篡改等安全事件时，及时启动应急预案，采取措施防止事态扩大，并按照规定向相关部门报告。

合规管理

1. **法律法规遵循**：

严格遵守《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规，确保服务数据管理活动合法合规。

1. **行业标准执行**：

遵循行业内相关数据管理标准和规范，结合组织实际情况，制定具体的实施细则。

1. **隐私保护**：

加强对客户隐私信息的保护，在数据采集、使用、共享等环节，明确隐私保护要求，获得客户授权，不得非法收集、使用客户隐私信息。

数据质量控制

质量指标

1. **准确性**

服务数据与实际情况的符合程度，错误数据占比不超过 1%。

1. **完整性**

数据采集的完整程度，关键数据字段缺失率不超过 2%。

1. **一致性**

同一数据在不同系统和场景中的一致性，数据不一致率不超过 1%。

1. **及时性**

数据采集和更新的及时程度，数据延迟采集率不超过 5%。

质量监控

1. **日常监控**

运维部通过数据管理系统对服务数据质量进行实时监控，设置数据质量预警阈值，当数据质量指标超出阈值时，及时发出预警信息。

1. **定期检查**

运维部每月组织一次服务数据质量检查，对数据准确性、完整性、一致性等进行全面检查，形成质量检查报告。

质量改进

1. **问题整改**

对监控和检查中发现的数据质量问题，运维部向相关业务部门下达整改通知，明确整改要求和期限，跟踪整改情况，确保问题及时解决。

1. **流程优化**

分析数据质量问题产生的原因，针对数据采集、处理等环节存在的漏洞，优化相关流程和制度，从源头上提高数据质量。

数据共享与应用

数据共享

1. **共享范围**

在组织内部，根据业务需求和权限设置，实现服务数据在各部门之间的合理共享，提高数据利用效率。

1. **共享流程**

部门之间需要共享服务数据时，由需求部门向运维部提出申请，运维部审核后，协调数据提供部门提供数据，并对共享数据进行脱敏处理。

数据应用

1. **服务优化**

利用服务数据进行分析，识别服务过程中的薄弱环节，为服务流程改进、服务质量提升提供依据。例如，通过分析服务响应时间数据，优化响应流程，缩短响应时间。

1. **决策支持**

基于服务数据统计分析结果，为服务规划、资源配置、应急交付等决策提供数据支持，提高决策的科学性和准确性。

1. **客户服务**

利用客户反馈数据，了解客户需求和期望，改进客户服务方式，提升客户满意度。

监督与审计

内部监督

1. **部门自查**

各业务部门每月对本部门服务数据管理情况进行自查，检查数据采集、存储、使用等环节是否符合制度要求，形成自查报告报送运维部。

1. **专项检查**：

运维部每季度组织一次服务数据管理专项检查，重点检查制度执行情况。

制度评审与改进

1. **评审周期**

本制度每年评审一次，由数据治理委员会组织开展，根据组织业务发展、法律法规变化、制度执行情况等，对制度进行评估和修订。

1. **持续改进**

根据评审结果和实际管理需求，不断完善服务数据管理制度和流程，适应组织发展和外部环境变化，提高服务数据管理水平。

外部审计

每年聘请第三方审计机构对服务数据管理制度的执行情况进行审计，出具审计报告，根据审计结果进行制度完善和管理改进。

培训与宣贯

1. **培训计划**

运维部制定年度服务数据管理培训计划，定期组织相关部门和人员参加培训，培训内容包括制度规定、数据采集方法、数据安全知识、数据分析工具使用等。

1. **宣贯活动**

通过内部网站、宣传栏、会议等多种形式，加强对服务数据管理制度的宣贯，提高全员数据管理意识和合规意识。

考核指标

|  |  |  |  |
| --- | --- | --- | --- |
| 指标度量性 | 计算方式 | 频次 | 指标要求 |
| 服务数据准确率 | 服务数据的准确数量/服务数据总数×100 % | 年度 | ≥95% |

附则

1. 本制度最终解释权和修订权归运维部。
2. 本制度自颁布之日起施行。

附件

无

记录

无