System组测试文档 V0

# 一、测试计划（Test Plan）

#### 1.1 测试目标

确保 System 组构建的 RESTful API 接口正确、安全、稳定、可扩展，同时验证其与 UI、Data、Analysis 三组之间的数据流转与服务对接。

#### 1.2 涉及模块（详细分解）

| 模块名 | 职责说明 |
| --- | --- |
| API 服务模块 | 提供所有 REST API（含版本控制、文档） |
| 数据中转模块 | UI 提交数据接收 → 转发至 Data 与 Analysis |
| 安全模块 | 用户身份验证（JWT）与权限控制（Spring Security） |
| 日志/监控模块 | 系统日志采集（ELK）与运行指标（Prometheus） |
| 部署集成模块 | Jenkins/GitLab CI 脚本部署与 Docker 镜像 |

#### 1.3 测试资源

* 技术环境：Java 17 + Spring Boot 3.x + Redis + Kafka + MySQL
* 测试工具：Postman, pytest, JUnit, Spring Test, Prometheus
* 数据源：模拟 JSON 数据包、Token、Header 参数

# 二、测试方案（Test Strategy）

#### 2.1 测试类型一览

| 类型 | 目的 | 工具 |
| --- | --- | --- |
| 功能测试 | API 输入输出是否正确 | Postman |
| 安全测试 | 身份校验、权限控制是否合理 | Postman+JWT |
| 异常测试 | 数据错误、服务不可用、重试机制等 | pytest |
| 集成测试 | 与 Data/Analysis 调用链条是否流畅 | Spring Test |
| 性能测试 | 接口并发请求响应时间 | JMeter |
| 日志验证 | 系统操作是否正确记录，日志是否合规 | ELK |
| 部署验证 | Docker 镜像是否正确打包，CI/CD是否触发成功 | Jenkins |

#### 2.2 风险识别

| 风险类型 | 描述 | 缓解措施 |
| --- | --- | --- |
| API 异常 | 用户未登录仍可访问敏感接口 | 加强 JWT 校验 + 异常响应码统一 |
| 中间件异常 | Kafka 推送失败/超时 | 添加重试机制/断路器 |
| 数据不一致 | 转发数据与分析结果延迟 | 异步处理 + 消息追踪 ID |
| CI/CD 崩溃 | 镜像构建失败 / 无法部署 | 添加构建日志输出与验证脚本 |

# 三、测试用例（Test Case Design）

| TC ID | 测试点描述 | 请求方式 | 预期响应 |
| --- | --- | --- | --- |
| TC-API-001 | 用户登录成功，返回 JWT Token | POST /api/login | 200 OK，响应中含 "token" 字段 |
| TC-SEC-002 | 未登录用户访问需鉴权接口 | GET /api/user/info | 401 Unauthorized，错误提示 |
| TC-DATA-003 | UI 端提交数据是否被转发至 Data 组 | POST /api/data | 202 Accepted，Kafka 有入队记录 |
| TC-ANL-004 | Analysis 组结果是否成功转发给前端 | GET /api/result | 200 OK，返回 JSON 格式结果 |
| TC-EXCP-005 | 数据字段缺失时是否有错误提示 | POST /api/data | 400 Bad Request，提示缺失字段名 |
| TC-CACHE-006 | 用户 token 存储是否正确写入 Redis | 登录后查询 Redis | key 存在且值为有效 JSON 用户信息 |
| TC-DEPLOY-007 | 自动部署流程是否正确触发 | Git push 触发 Jenkins | 构建成功，打包镜像上传成功 |

# 四、测试报告框架（Test Report Outline）

| 项目 | 内容说明 |
| --- | --- |
| 测试版本 | System Test V0.1 |
| 测试人员 | System Group QA |
| 测试工具 | Postman, pytest, Jenkins, Redis-cli |
| 用例执行概况 | 总数 15 条，通过 12，失败 3，阻塞 0 |
| 问题记录 | JWT 权限校验不完善、部署流程未自动清除旧容器等 |
| 建议优化 | 增加日志级别区分、完善异常处理分支覆盖 |