

API接口开发规范约束文档

版本号：v2.0

生效日期：2025-10-10

适用对象：第三方合作开发团队

阳新县城发水务有限公司

一、核心规范要求

1. 接口合作方式

接口类型	请求方法	传参方式
必须使用	GET 或 POST	POST 必须使用 JSON 格式传参，且 JSON 结构需符合标准格式（键名使用小驼峰命名，如 "userId") ；GET 请求传参需在请求头中指定 Content-Type: application/x-www-form-urlencoded
禁止使用	PUT/DELETE	URL 参数拼接（如 /api?userId=123） ；POST 请求使用 form-data 或 x-www-form-urlencoded 格式传参

✔ 正确示例 (POST 请求)

```
{
  "userId": "U1001",
  "timestamp": 1696800000,
  "userName": "admin"
}
```

✘ 错误示例 (URL 参数)

```
/api?userId=U1001
```

× 错误示例 (POST 请求错误格式)

form-data 格式 : key=userId , value=U1001 ; key=timestamp , value=1696800000

2. 接口命名规范

- **命名格式** : 采用 RESTful 风格 , 使用名词复数形式表示资源集合 , 如 `/users` (用户列表) 、 `/orders` (订单列表) ; 单个资源操作在路径后加资源 ID , 如 `/users/U1001` (获取 ID 为 U1001 的用户信息)
- **操作标识** : 通过请求方法区分操作类型 , GET (查询) 、 POST (新增) , 禁止在接口路径中包含操作动词 , 如禁止使用 `/getUser` 、 `/addOrder`
- **版本控制** : 接口需包含版本标识 , 放在路径最前方 , 格式为 `/v1/users` 、 `/v2/orders` , 便于后续接口迭代与兼容性维护

二、响应数据结构规范

1. 基础响应结构

所有接口必须严格遵循以下 JSON 结构 , 键名统一使用小驼峰命名 :

```
{
  "code": 200,    // 状态码 (200=成功, 非200=失败)

  "message": "成功", // 通用状态描述, 成功时简洁说明, 失败时明确错误原因

  "data": {      // 业务数据对象 (必须包含) , 空数据时返回{}
    "userId": "U1001",
    "userName": "admin",
    "createTime": "2025-09-01 10:00:00"
  },

  "requestId": "req20251010123456789" // 请求唯一标识, 用于问题排查与日志追踪
}
```

2. 关键约束

字段名	类型	必填	说明
code	int	是	必须为标准 HTTP 状态码 (200/400/401/404/500/503) ，各状态码使用场景严格遵循本规范第三章要求
message	string	是	语言简洁、易懂，禁止暴露技术细节（如 "数据库连接失败""SQL 语法错误"）；成功时统一返回“操作成功”，失败时需明确错误点（如“参数 userId 缺失”“用户 ID 不存在”）
data	object	是	必须存在，空数据时返回{}；数据对象内部字段需明确类型（如时间字段使用“yyyy-MM-dd HH:mm:ss”格式，数值字段禁止返回字符串类型）
requestId	string	是	由合作方生成或服务端生成，格式为“req + 年月日时分秒 + 3 位随机数”（如 "req20251010123456789"） ，需在接口日志中记录该字段，便于问题定位

✘ 错误示例（违反规范）

- 1. 缺少关键字段 : { "userId": "U1001", "userName": "admin" } (缺少 code、message、requestId)
- 2. 数据类型错误 : { "code": 200, "message": "成功", "data": { "age": "25" }, "requestId": "req20251010123456789" } (age 为数值类型 , 却返回字符串)
- 3. 暴露技术细节 : { "code": 500, "message": "数据库连接超时 , 无法查询用户数据", "data": {}, "requestId": "req20251010123456789" }

三、 错误处理强制要求

1. 错误码与响应示例

错误码	触发场景	响应示例
400	参数缺失 / 格式错误 (如 userId 为空、timestamp 格式非数字、userName 长度超过 50 字符)	{ "code": 400, "message": "参数userId缺失 , 请补充", "data": {}, "requestId": "req20251010123456789" }
401	Token 无效 / 过期 (Token 格式错误、已超过有效期、与用户身份不匹配)	{ "code": 401, "message": "无效的认证凭证 , 请重新获取Token", "data": {}, "requestId": "req20251010123456789" }
404	资源不存在 (用户 ID 不存在、订单号不存在、接口路径错误)	{ "code": 404, "message": "用户ID不存在 , 请检查参数有效性", "data": {}, "requestId": "req20251010123456789" }

500	服务器内部错误（服务端逻辑异常、第三方依赖调用失败等非客户端原因)	<pre>{"code":500,"message":"系统异常，请稍后重试","data":{},"requestId":"req20251010123456789"}</pre>
503	服务不可用（响应时间超过 500ms、服务过载、维护期间)	<pre>{"code":503,"message":"服务暂时不可用，请稍后重试","data":{},"requestId":"req20251010123456789"}</pre>

2. 禁止行为

- 返回纯字符串（如 "用户不存在""Token 过期"）
- 用 200 状态码返回错误数据（如`{"code":200,"message":"用户ID不存在","data":{}}`）
- 错误信息模糊不清（如仅返回“参数错误”，未明确具体错误参数）

四、安全与认证规范

1. 认证方式

- 必须通过 `Authorization` 请求头传递 Token，禁止在请求体或 URL 中携带 Token
- 格式：`Bearer YOUR_ACCESS_TOKEN`（Token 需为 32 位及以上随机字符串，包含大小写字母、数字、特殊字符）
- Token 获取：合作方需通过统一的认证接口（`/v1/auth/getToken`）获取 Token，获取时需传入 AppId 与 AppSecret（由我方提供，AppSecret 需加密存储，禁止明文传输）

2. Token 有效期与刷新

- 有效时间 ≤ 2 小时，超时后调用接口需返回 401 错误
- 合作方可在 Token 过期前 30 分钟内，通过刷新 Token 接口（`/v1/auth/refreshToken`）获取新 Token，刷新 Token 有效期为 12 小时，且仅可使用一次

3. 敏感数据保护

- 禁止在响应中返回密码、Token、身份证号、银行卡号、手机号等敏感字段；若需返回手机号、身份证号，需进行脱敏处理（如手机号显示为“138****5678”，身份证号显示为“110101*****1234”），特殊约定确实需要返回的除外。
- 请求与响应数据需通过 HTTPS 协议传输，尽量不使用 HTTP 协议
- 接口需对请求频率进行限制，单个 AppId 每分钟请求次数 ≤ 100 次，超过限制返回 429 错误（{"code":429,"message":"请求过于频繁，请稍后重试","data":{},"requestId":"req20251010123456789"}）

五、参数校验规范

1. 通用校验规则

参数类型	校验要求	示例
字符串类型	需指定长度范围（如 1-50 字符），禁止包含特殊字符（如 <、>、&、'、"），特殊场景需包含特殊字符时需进行转义处理	userName：长度 1-20 字符，仅允许大小写字母、数字、下划线
数值类型	需指定取值范围（如正整数、0-100），禁止传入非数值类型（如字符串、布尔值）	age：1-150 的正整数； amount：大于 0 的数字，保留 2 位小数
时间类型	统一使用“yyyy-MM-dd HH:mm:ss”格式，需校验	createTime：“2025-09-01 10:00:00”

	时间有效性（如禁止传入“2025-13-01 25:60:60”）	
数组类型	需指定数组长度范围（如 1-10 个元素），数组内元素类型需统一（如均为字符串、均为数值）	userIds：1-20 个元素，每个元素为用户 ID（字符串类型，格式为“U+5 位数字”）

2. 校验失败处理

参数校验失败时，需返回 400 错误，明确指出具体的错误参数及原因，示例：

```
{"code":400,"message":"参数userName不符合要求：长度需1-20字符，且仅允许大小写字母、数字、下划线","data":{"requestId":"req20251010123456789"}}
```

六、文档与测试要求

项	要求	补充说明
接口文档	需提供 Swagger 2.0/3.0 格式文档（地址需公开），文档需包含接口功能描述、请求参数（名称、类型、必填性、说明、示例）、响应参数（名称、类型、说明、示例）、错误码说明、调用示例	文档需实时更新，接口迭代后 24 小时内完成文档修订；文档需提供在线调试功能，支持合作方直接在文档中测试接口
测试环境	尽可能提供独立测试环境（URL 以 - test 后缀标	测试环境需稳定可用，维护时间需提前 48 小时通

	识) ，测试环境数据需与生产环境数据结构一致，但数据内容为模拟数据(禁止使用真实用户数据)	知合作方；
响应时间	95% 请求响应时间 ≤ 500ms (超时返回 503) ，单次请求最大响应时间 ≤ 1000ms	若因业务需求需延长响应时间，需提前提交申请，经我方审核通过后方可调整
兼容性要求	接口迭代需保证向后兼容，新增参数需设为非必填，删除参数需提前 6 个月通知合作方	接口版本升级后，旧版本接口需继续维护至少 12 个月；若因重大业务调整无法兼容旧版本，需与合作方协商确定过渡期，确保合作方有足够时间适配

七、违规处罚机制

1. 违规等级与处罚措施

违规等级	违规行为	处罚措施
一级	响应结构不符合规范 (缺少 code、message、data、requestId 中任一字段，字段类型错误，数据格式不规范) ；参数校验未按要求执行；接口命名不符合 RESTful 风	1. 拒绝接入生产环境，需 48 小时内修复；2. 修复后需提交测试报告，经我方验证通过后方可重新申请接入；3. 同一接口 30 天内累计出现 3 次一级违

	格	规，升级为二级违规
二级	未使用 Token 认证（未携带 Authorization 请求头、Token 格式错误）；请求频率超过限制且未整改；测试环境使用真实用户数据；接口迭代未通知合作方导致兼容性问题	1. 临时冻结 API 调用权限（冻结时长：首次违规 24 小时，二次违规 72 小时，三次及以上违规 7 天）；2. 需提交整改报告，说明违规原因及整改措施，经我方审核通过后方可解冻；3. 同一合作周期内累计出现 2 次二级违规，升级为三级违规
三级	敏感数据泄露（响应中包含未脱敏的身份证号、手机号、银行卡号、密码、Token 等）；故意伪造 Token 或使用非法 Token 调用接口；因违规操作导致我方系统故障或数据安全事故	1. 立即终止合作，永久冻结 API 调用权限；2. 追究法律责任，要求赔偿我方因此遭受的损失；3. 将违规情况纳入合作方黑名单，禁止未来合作

2. 违规处理流程

- 1. 违规发现：**通过系统监控、接口测试、合作方反馈等方式发现违规行为，我方在 2 小时内将违规信息（违规接口、违规类型、违规证据）通知合作方
- 2. 整改通知：**明确整改要求与截止时间，合作方需在截止时间前完成整改，并提交整改报告
- 3. 验证与处罚：**我方在收到整改报告后 24 小时内进行验证，验证通过则解除相应处罚；未按时整改或整改未通过，按对应违规等级执行处罚措施
- 4. 申诉机制：**合作方对违规判定或处罚措施有异议，可在收到违规通知后 12 小时内提交申诉材料，我方在 24 小时内复核，复核结果为最终结论

八、附则

1. 本规范自 2025-10-10 起生效，替代 v1.0 版本规范
2. 我方有权根据业务发展与技术升级需求修订本规范，修订后将提前 7 天通知合作方，合作方需在 30 天内完成适配
3. 合作方在使用 API 接口过程中，需遵守国家相关法律法规及我方其他相关规定，若因合作方违规使用导致的一切后果，由合作方自行承担
4. 本规范未尽事宜，由双方协商解决，协商结果可作为本规范的补充条款