

← 返回首页

提交规范 v1.2

想让你的技能 / 插件 / MCP 被天工开物收录？投稿前请先对照本规范自查。重点：**开源许可 · 合规结构 · 中文描述 · 连接真实 · 安全红线**。全部通过，3 个工作日内完成审核上架。

↓ 下载 PDF 版规范（离线可看）

- ① 核心要求
- ② 目录结构
- ③ SKILL.md 规范
- ④ 描述公式
- ⑤ 安全红线
- ⑥ 来源版权
- ⑦ 提交自查
- ⑧ 提交方式
- ⑨ 插件规范
- ② MCP 规范

1

核心要求

缺一不可

✓

合法可分发

开源许可（MIT / Apache-2.0 / BSD / CC-BY 等宽松许可）或自有版权

✓

含 SKILL.md

唯一核心文件，且格式符合本规范

✓

中文描述必填

面向国内用户，description_zh 必须有

✓

来源可追溯

注明原作者与原始出处（source / source_url）

✗

禁收

窃取 / 破解 / 违规抓取 / 恶意代码 / 绑定单一模型生态的技能

「绑定单一模型生态」举例：深度依赖 Claude、GPT、Gemini 专有 API 且无法替换的技能，会

按需评估是否收录；通用性强的优先。

2

目录结构

文件夹名 = 英文小写 + 连字符

skill-name/

- └─ SKILL.md

└─ scripts/

└─ references/

└─ assets/

└─ LICENSE

└─ README.md
- ← 【必填】唯一核心文件（技能定义 + 用法 + 示例）

← 可选：可执行代码

← 可选：参考文档（按需加载）

← 可选：模板 / 图标 / 数据等资源

← 强烈建议：许可文件

← 建议：中文使用说明

约束	限值	说明
目录层级	≤ 3 层	避免过深难维护
解压后体积	≤ 50 MB	含 references / assets
文件数量	≤ 200 个	控制拉取成本
压缩包格式	.zip	必须 zip； 包内文件名用英文/数字/连字符 （中文文件名会乱码/404）

⚠ 若用网盘压缩包提交，请先自测：解压后能正常访问所有文件，且包内不含乱码文件名。

3

SKILL.md frontmatter

```
---
name: pdf-summarizer           # 小写英文+连字符，全站唯一
description: |                  # 英文触发描述（做什么+何时用）
description_zh: |              # 【必填】中文触发描述（本站特色）
keywords:                      # 中文搜索关键词 3-8 个，第 1 个最重要（作卡片核心词）
  - 文档处理
  - PDF压缩
  - 摘要提取
category: 文档处理             # 与本站分类一致（见下表）
license: MIT                   # 许可证（MIT / Apache-2.0 / BSD / CC-BY 等）
version: 1.0.0                 # 推荐
author: 你的名字               # 推荐
source: 原作者/仓库名         # 搬运/改编必填：注明原出处
source_url: https://...       # 搬运/改编必填：原仓库链接
---
```

字段	必填	说明
<code>name</code>	必填	小写英文+连字符，全站唯一
<code>description</code>	必填	英文触发描述
<code>description_zh</code>	必填	中文触发描述
<code>keywords</code>	必填	中文搜索关键词 3-8 个； 第 1 个作卡片核心词
<code>category</code>	必填	与本站 6 大分类一致（见下表）
<code>license</code>	必填	MIT / Apache-2.0 / BSD / CC-BY 等
<code>version</code>	推荐	语义化版本
<code>author</code>	推荐	作者署名
<code>source</code> / <code>source_url</code>	搬运必填	搬运/改编须注明原出处

📁 **本站 6 大分类**（category 填中文，目录用英文）

中文分类（category）	英文目录（category_en）
办公自动化	<code>office-automation</code>
文档处理	<code>document-processing</code>
数据处理	<code>data-processing</code>
网页抓取	<code>web-scraping</code>
数据分析	<code>data-analysis</code>
编程辅助	<code>coding-assistant</code>

4

描述公式

描述 = 做什么 + 何时用 + 关键词（关键词最重要，决定触发率）

✗ 太泛，勿用

A skill for PDF processing.

✓ 正确示范

写清楚「什么时候用、处理什么」，即使没提到“PDF”字样也能被正确触发。中文描述同理。

5 安全红线

违反直接拒绝

✗ **禁止** eval / exec / 远程下载脚本执行 / base64 混淆代码

✗ **禁止** 连接未知境外 IP、未经同意外传数据

✗ **禁止** 窃取环境变量 / 密钥 / 删除用户文件

✗ **禁止** 声明功能与代码实际行为不符

✗ **禁止** 爬取需授权数据、破解、绕过付费

⚠ 审核时会用校验脚本自动扫描以上红线；含风险项直接驳回，不进入人工复查。

6 来源与版权声明

原创：声明「版权归我，采用 XX 许可」，并附 LICENSE 文件。

搬运 / 改编：必须注明

✓ 原作者、原仓库地址（source / source_url）

✓ 原始许可（license）

✓ 你改了什么（如「OpenAI API → 国内 DeepSeek API」「新增中文描述」）

✓ 如实标注来源是本站的底线，也是对原作者的基本尊重。

7 提交前自查清单

- ✓ 结构合规（含 SKILL.md）— 目录层级≤3、体积≤50MB、≤200文件
- ✓ frontmatter 字段齐全— name / description / description_zh / keywords / category / license
- ✓ description 是「做什么 + 何时用」
- ✓ 中文描述已填（description_zh）
- ✓ scripts 通过语法检查
- ✓ 无安全红线
- ✓ 已注明来源与许可
- ✓ ≤50MB
- ✓ 含「输入 → 输出」示例— 放 SKILL.md 正文的 Examples 小节，或独立的 examples/ 目录

💡 不确定哪条没达标？直接跑一下站点的 `validator.py`，它会告诉你每项过没过。

8 提交方式

方式	说明
① GitHub 仓库链接 (推荐)	直接把仓库地址发来，可自动拉取并校验
② 网盘压缩包链接	zip 包内用 ASCII 文件名
③ 投稿邮箱	打包发到投稿邮箱

🕒 3 个工作日内完成审核，合格即上架。

9

插件提交规范

更严格

插件（**plugin**）与技能核心区别在于：**代码更重、依赖运行时（Node/TS）**，通过 `tools / channels` 等 `contract` 提供更强的能力。收集、审核、上架流程与技能一致，**但审核更严格、安全红线更高**。

✳️ **插件必备字段**（在技能 `frontmatter` 基础上新增）

```
---
type: plugin                # 【必填】固定为 plugin
runtime: openclaw           # 【必填】依赖的运行时
install_cmd: openclaw plugins install clawhub:xxx # 【必填】真实可运行的安装命令
contracts:                  # 【必填】提供什么能力
  - tools
  - channels
compat: >=2026.3.24         # 【必填】兼容的 OpenClaw 版本
---
```

字段	必填	说明
<code>type</code>	必填	固定 <code>plugin</code> ，与技能区分的标志
<code>runtime</code>	必填	依赖的运行时（如 <code>openclaw / node</code> ）
<code>install_cmd</code>	必填	必须真实可跑 ——审核会在沙箱里执行验证
<code>contracts</code>	必填	提供的能力，如 <code>tools</code> <code>channels</code> <code>sessions</code>
<code>compat</code>	必填	注明兼容的 OpenClaw 版本，如 <code>>=2026.3.24</code>

🔒 **插件安全红线升级**（代码执行能力更强，下述为技能红线之上的额外项）

- ✗ **package.json 依赖审查** 逐条核查依赖项来源与风险，禁止不明来源 / 已废弃 / 含已知 CVE 的包
- ✗ **入口文件权限操作** 扫描入口是否越权读文件 / 写文件 / 执行系统命令 / 触碰环境变量

✗ 禁止安装期恶意脚本 postinstall / preinstall 等钩子不允许静默下载执行任意代码

✗ 禁止数据外传 运行时不得向未知域收集 / 上报用户数据与密钥

⚠ 插件审核比技能多一步「安装测试」：审核员会在隔离沙箱里实际执行 `openclaw plugins install ...`，验证能装得上、装得干净、跑得起来。仅描述可用但实际装不上的，直接驳回。

💡 投稿插件请一并附上：源码仓库 / `package.json` / 入口文件说明 / 已测环境（OpenClaw 版本 + Node 版本），以便快速通过安装测试。

10

MCP 提交规范

更严格

MCP（`mcp`）区别于 skill / plugin 的核心：它是让 AI 接入外部真实服务（数据库、企业微信、钉钉、云 API 等）的标准协议。本站 MCP 板块的差异化在「中文本地化适配 + 配置教程」：用户最卡的就是配置环节，做好教程就是最好的引流与留存。

🔑 **MCP 必备字段**（数据模型 type: mcp）

```
---
type: mcp                # 【必填】固定为 mcp
transport: stdio          # 【必填】stdio | sse | streamable-http
command: uvx              # stdio 型：启动命令（uvx/npx/python/java）
args: ["@xx/mcp@latest"]  # stdio 型：参数
url: https://mcp.example.com # http/sse 型：服务地址
env_required:             # 【必填】需要的环境变量/密钥（仅标名，不填值）
  - ALIBABA_CLOUD_ACCESS_KEY_ID
guide_url: /guide/mcp/xxx.html # 【必填】配置教程页（差异化核心）
tools: ["query", "n12sql"]     # 提供的工具列表（部分列出）
license: MIT                 # 【必填】开源许可
source_url: github.com/...    # 【必填】真实来源仓库
```

🔑 **配置教程页（guide_url）核心四段**

- ① **环境要求** 需要哪些软件 / 密钥 / 前置开通（如云厂商开通服务）

- ② 配置示例 给 OpenClaw (`openclaw mcp set / mcp add`) 与 Claude / Codex 的配置代码, 附「复制配置」按钮
- ③ 验证方法 如何确认连上了 (`openclaw mcp probe` / 一句测试话术)
- ④ 常见问题 连接失败排查表 / 权限错误 / 限流说明
-  MCP 审核红线 (比 skill 更严)
- 许可合规 同技能, 只收开源许可 (MIT / Apache / CC-BY 等), 保留署名与 LICENSE
- 连接信息真实 `url / command / args` 必须真实可测, 不能是占位或杜撰
- 密钥只标名不落值 仅说明需要哪些 `env_required`, 绝不收录硬编码密钥/令牌的条目
- 服务不稳定 远程 MCP 要标注是否免费、是否限流、是否需要代理
- 国内可用性 标注是否需要科学上网、是否有国内替代; 优先国产直连服务
- 配置教程完整 缺配置教程 (`guide_url` 空或 404) 的直接驳回——这是本站差异化承诺

?? MCP 审核比插件多一步「连接测试」: 审核员会在隔离沙箱里核对 `install_cmd / env_required` 真实、`url / command` 可用 (可用 `--no-probe` 先存配置再核对)。杜撰连接信息的直接驳回; 含数据库 / 有写权限的 MCP 需重点审查授权与审批机制。

?? 投稿 MCP 请一并附上: 官方 GitHub 仓库 / README / LICENSE / 各平台配置示例 (OpenClaw + Claude / Codex) / 已测环境。个人开发者做成「自带中文配置教程」的 MCP 最受欢迎。

天工开物 · 提交规范 v1.2 (技能 / 插件 / MCP)

本站承诺: 开源合规 · 来源可溯 · 中文触达 · 稳定分发