

附件一：Skill 技能封装技术标准（草案）

海南自贸港 OPC 全球智能体协会 Skill 技能封装技术标准（草案）

版本号： V1.0

发布日期： 2026 年 4 月

适用范围： 海南自贸港 OPC 全球智能体协会全体会员

第一章 总则

第一条 目的

为规范人工智能体（AI Agent）Skill 技能的封装、交易与应用，确保 Skill 的互操作性、安全性、可审计性，促进海南自贸港智能体生态健康发展，制定本标准。

第二条 定义

- **Skill（技能）**：封装在 AI Agent 中的可复用功能模块，具备明确输入输出接口、业务逻辑及数据处理能力
- **Skill 封装**：将特定领域知识、算法、数据接口打包为标准化组件的过程
- **Skill 市场**：协会运营的 Skill 交易平台，支持发布、检索、交易、评价全流程

第三条 原则

- **标准化**：统一接口规范，确保跨平台兼容
- **模块化**：高内聚、低耦合，支持灵活组合

- 安全性：通过伦理审查与安全测试，防范算法风险
- 可追溯：全流程上链存证，支持审计与维权

第二章 Skill 技术架构标准

第四条 Skill 基本结构

Skill 封装必须包含以下组件：

组件	说明	格式要求
Skill 描述文件	元数据（名称、版本、作者、领域、标签）	JSON-LD ， 符合 Schema.org 标准
接口定义	输入参数、输出结果、错误码定义	OpenAPI 3.0 规范
业务逻辑代码	核心算法、模型权重、执行脚本	Python 3.9+ 或 Node.js 18+
依赖清单	第三方库、数据集、API 接口	requirements.txt 或 package.json
测试用例	单元测试、集成测试、边界测试	pytest 或 Jest 框架
伦理声明	算法公平性说明、数据隐私承诺	协会模板文档
算力需求标签	预估 CPU/GPU 消耗、能耗等级	协会统一能效评级（A-G 级）

第五条 接口规范

输入接口标准:

JSON

```
{  
  "skill_id": "string",           // Skill 唯一标识 (协会分配)  
  "version": "semantic_version", // 语义化版本 (如 1.2.3)  
  "input": {  
    "required": ["param1", "param2"], // 必填参数  
    "optional": {"param3": "default"}, // 选填参数及默认值  
    "schema": {}                       // JSON Schema 校验规则  
  },  
  "context": {  
    "user_id": "string",           // 调用者身份 (匿名化处理)  
    "session_id": "string",        // 会话标识  
    "priority": "normal",          // 优先级 (low/normal/high)  
    "green_compute": true          // 是否启用算电协同优化  
  }  
}
```

输出接口标准:

JSON

```
{  
  "status": "success|error",      // 执行状态
```

```

"output": {},                                // 业务输出数据

"metadata": {

    "execution_time": "float", // 执行耗时（秒）

    "energy_consumed": "float", // 能耗（千瓦时，算电协同用）

    "carbon_offset": "float", // 碳减排量（克）

    "audit_hash": "string"      // 执行记录上链哈希

},

"logs": []                                // 审计日志（脱敏）

}

```

第六条 算电协同适配标准

海南特色要求：

- Skill 必须声明**算力需求等级**（A-G 级，A 级最节能）
- 支持**动态调度接口**：接收电网负荷信号，自动调整计算时序
- 优先使用**清洁能源标签**：在海南国际数据中心运行的 Skill 自动获得"

绿电认证"

算力-电力协同接口：

Python

示例: Skill 响应电网调度信号

```

def on_grid_signal(signal):

    """

    signal 包含：

    - price: 当前电价（元/千瓦时）

```

```
- carbon_intensity: 碳排放强度（克/千瓦时）
- renewable_ratio: 可再生能源占比（%）
"""

if signal.renewable_ratio > 80:
    return "full_speed"          # 绿电充足，全速运行
elif signal.price > 1.0:
    return "throttle"            // 电价高峰，降频运行
else:
    return "pause"               // 暂停非紧急任务
```

第三章 Skill 分类与分级

第七条 领域分类

一级分类	二级分类（示例）	监管要求
商业服务	跨境电商、客服、营销、财税	一般备案
专业服务	法律、医疗、金融、教育	强伦理审查
工业智能	质检、预测维护、供应链	安全评估
公共服务	政务、环保、应急、公益	政府背书
创意内容	设计、写作、音乐、视频	版权审查

一级分类	二级分类（示例）	监管要求
基础能力	翻译、OCR、语音识别、数据分析	通用标准

第八条 安全分级

等级	定义	适用场景	审查要求
L1 公开级	通用工具，无敏感数据	翻译、计算器	自动化检测
L2 备案级	处理商业数据	客服、营销	形式审查+抽测
L3 审核级	影响用户权益	金融推荐、医疗咨询	实质审查+专家评估
L4 许可级	涉及公共安全	自动驾驶、诊断治疗	政府许可+持续监管

第四章 封装流程与认证

第九条 封装流程

步骤 1：开发测试（开发者完成）

↓ 提交申请

步骤 2：形式审查（协会秘书处，3 个工作日）

- 检查材料完整性
- 自动化代码扫描

↓ 通过

步骤 3：伦理审查（AI 伦理委员会，7 个工作日）

- 算法公平性评估
- 数据隐私合规检查
- 社会风险研判

↓ 通过

步骤 4：技术测试（技术委员会，10 个工作日）

- 功能测试
- 性能测试（含算电协同）
- 安全渗透测试

↓ 通过

步骤 5：上链存证（自动完成）

- 生成 Skill NFT（仅含元数据，不含代码）
- 部署至海南国际数据中心

↓

步骤 6：发布上市（Skill 市场）

第十条 认证标识

通过认证的 Skill 获得以下标识：

标识	含义	展示位置
----	----	------

标识	含义	展示位置
OPC 认证	通过协会全项审查	Skill 详情页首屏
绿电 Skill	算电协同 A/B 级	名称旁绿色闪电图标
可信 AI	通过伦理审查	底部信任栏
跨境就绪	符合 DEPA 数据跨境标准	国际版特别标注
海南智造	开发者在海南实地工作	政府背书标签

第五章 交易与结算

第十一条 定价机制

三种定价模式：

1. 按次计费：每次调用支付固定费用（适合低频场景）
2. 订阅制：月费/年费，无限次调用（适合高频场景）
3. 收益分成：按 Skill 产生的实际业务收益比例分成（适合高价值场景）

第十二条 5%公益金计提

自动执行：

- 每笔交易完成后，系统自动从成交金额计提 **5%**至公益金账户
- 实时分账：95%至开发者账户，5%至协会公益金监管账户

-
- 区块链记录：每笔计提均可追溯、可审计

结算周期：

- 开发者提现：T+7 工作日（人民币）/ T+14 工作日（外币，通过 FT 账户）
- 公益金使用：按季度预算执行，年度审计公示

第六章 安全与合规

第十三条 数据安全

- 数据不出境：核心训练数据存储于海南国际数据中心
- 最小必要原则：Skill 仅获取完成服务所必需的数据
- 脱敏处理：用户敏感信息（身份证号、生物特征）必须脱敏
- 审计日志：所有数据访问记录上链，保存不少于 5 年

第十四条 算法伦理

禁止封装以下 Skill：

- 涉及种族、性别、宗教歧视的算法
- 用于监控、追踪特定人群的识别系统
- 自动武器、网络攻击等危害公共安全的功能
- 深度伪造（Deepfake）用于欺诈或诽谤

高风险 Skill 额外要求：

- 提供算法可解释性说明（XAI）

-
- 建立人工复核机制 (Human-in-the-loop)
 - 购买职业责任保险

第七章 附则

第十五条 标准更新

本标准每年修订一次，由技术委员会提出，会员代表大会表决通过。

第十六条 解释权

本标准解释权归海南自贸港 OPC 全球智能体协会理事会。

第十七条 生效日期

本标准自发布之日起试行，试行期 6 个月。

附录：

附录 A：Skill 描述文件 JSON Schema

附录 B：伦理审查 checklist (100 项)

附录 C：算电协同接口 SDK (Python/JavaScript)

附录 D：常见 Skill 封装模板 (法律/医疗/电商)