NZA 文件格式规范白皮书 V1.0 官方正式版

NoZeroAI Role Asset Packaging Specification

版本：V1.0

发布日期：2026 年 5 月 1 日

生效日期：2026 年 6 月 1 日

发布机构：NZA 标准委员会（零越无界 / NoZeroAI）

官方网站：www.nza.tech

验证状态：正式发布

本规范面向 AI 角色资产（Role Asset）的创建、交换、版本治理、兼容校验与平台适配，依据现行适用法律法规、通行安全原则以及智能体工程化实践制定。本文档定义的是 NZA 标准本身，用于规范角色资产如何被结构化表达、如何被封装、如何被验证、如何被发布与适配；任何具体产品实现均应满足本规范的强制要求。

目录

1 引言

1.1 文档目的

NZA（NoZeroAI Role Asset Packaging Specification）用于定义 AI 角色资产的统一表达与封装标准，解决角色设定在创建、编辑、发布、分发与多平台适配过程中常见的以下问题：

• 角色结构不统一，难以跨团队协作

• 导入结果与运行时消费模型混杂，无法治理

• 不同平台能力不同，导出结果不可预测

• 版本基线不清晰，草稿、发布态与分发态边界模糊

• 缺少可验证的完整性、兼容性与审计约束

NZA 的目标不是提供某一模型厂商专属 Prompt 模板，而是提供一套可治理、可验证、可版本化、可适配的角色资产标准。

1.2 适用范围

本规范适用于：

• AI 角色资产的创建、封装、校验、存储与交换

• 角色资产从外部材料导入为标准化资产草稿

• 角色资产的发布快照、适配导出与分发记录

• 多智能体平台、角色资产平台、硬件终端平台的角色资产接入

• 围绕角色资产开展的合规、审计、追溯与版本治理活动

本规范不直接规定具体模型推理算法、推理效果数值、厂商私有执行引擎细节。

1.3 规范级别术语

本规范采用以下术语表达约束强度：

• **必须（MUST）**：严格要求，不满足即视为不符合本规范

• **应当（SHOULD）**：强烈建议，除非有充分理由否则不应偏离

• **可以（MAY）**：可选能力，不影响基础合规性

• **禁止（MUST NOT）**：明令禁止的行为或结构

1.4 核心术语（中英双语）

中文术语	英文标识	定义
角色资产	Role Asset	用于表达 AI 角色身份、设定、行为策略与边界约束的标准化数据对象
规范角色模型	Canonical Role Schema	NZA 的唯一语义核心模型，采用六层结构，作为角色资产的标准事实源
NZA 包	NZA Package	对角色资产进行封装后的标准交换载荷，包含清单、资产载荷、兼容信息、完整性信息与扩展区
分析说明层	Analysis Metadata	导入或生成过程中产生的置信度、冲突项、待确认

		项、证据统计与人工修订痕迹等说明性数据
发布快照	Published Snapshot	对某一时刻角色资产进行冻结后的不可变版本，用于正式分发、导出与回溯
适配器	Adapter	将标准角色资产编译、映射并导出到目标平台的实现单元
能力降级	Capability Degradation	目标平台不支持部分能力时，按标准规则进行降级、告警或阻断
完整性摘要	Integrity Digest	针对标准包在规范化序列化后的摘要值，用于一致性校验

2 核心定位与设计原则

2.1 标准定位

NZA 是面向 AI 角色资产管理与多平台适配场景的标准化封装规范。NZA 的核心定位包括：

1. 以六层 Canonical Role Schema 作为角色资产唯一语义内核
2. 以 NZA 包作为对外交换、发布与分发的标准载体
3. 以发布快照作为正式对外分发基线
4. 以适配器机制实现多平台兼容，而非要求所有平台原生理解同一执行语义

换言之，NZA 标准回答的是"角色资产应如何被定义、封装、校验与交付"，而不是"所有模型必须以同一种内部机制执行"。

2.2 核心目标

编号	目标	说明
G1	统一表达	用统一的六层结构表达角色资产，避免字段漂移

G2	清晰治理	分离资产本体、分析说明、发布快照与分发记录
G3	可验证	通过结构校验、语义校验、完整性摘要与审计机制保障可信性
G4	可适配	通过适配器机制将同一角色资产导出到不同平台
G5	可扩展	允许厂商扩展，但不得破坏核心语义与兼容性

2.3 设计原则

1. **Schema First**：任何角色资产必须首先满足六层 Canonical Role Schema
2. **Asset / Analysis Separation**：资产本体与分析说明层必须分离，说明层不得污染运行时语义
3. **Snapshot for Distribution**：对外导出与分发必须基于发布快照，而非工作草稿
4. **Compile Before Run**：角色资产进入目标平台前必须经过兼容性校验与适配编译
5. **Extension Without Override**：扩展字段只能附加信息，不得改写核心层语义
6. **Auditable by Design**：包生成、发布、导出、失败与回滚均应可追踪
7. **Least Necessary Data**：只交换角色资产所需数据，禁止把运行时隐私数据、长对话原文直接混入标准包

2.4 非目标

以下内容不属于 NZA V1.0 的标准目标:

• 不规定单一模型厂商内部 Prompt 实现细节

• 不承诺跨平台输出效果数值完全一致

• 不把会话期运行时记忆直接纳入静态角色资产包

• 不把二进制资源包、多媒体资产封装纳入 V1.0 规范主范围

• 不将任意用户输入视为可覆盖安全与合规边界的高优先级指令

3 规范对象与总体架构

3.1 核心对象

NZA 规范围绕以下四类核心对象展开：

对象	作用	是否为标准必选
Canonical Role Schema	角色资产语义本体	是
NZA Package	标准交换载荷	是
Published Snapshot	正式发布与分发基线	是
Adapter Profile	目标平台适配与能力映射	是

3.2 总体分层模型（三域模型）

NZA 采用"语义内核 + 封装治理 + 适配执行"三域模型，而不是以单一容器替代所有内部结构。

```
Plain Text
┌──────────────────────────────────────────────────────────┐
│                    第三域：适配执行域                    │
│  Prompt Compiler · Adapter Profile · Capability Matrix  │
├──────────────────────────────────────────────────────────┤
│                    第二域：封装治理域                    │
│  Manifest · Compatibility · Integrity · Extensions      │
├──────────────────────────────────────────────────────────┤
│                    第一域：语义内核域                    │
│  Canonical Role Schema（六层角色资产标准）               │
└──────────────────────────────────────────────────────────┘
```

其中：

• 第一域定义角色资产的唯一语义真相

• 第二域定义包的版本、状态、完整性、兼容性与扩展

• 第三域定义如何把标准资产映射到目标平台，但不把平台私有实现反向污染标准本体

3.3 生命周期模型

NZA 角色资产生命周期如下：

```
Plain Text
外部材料 / 人工创建
        |
```

```
        ▼
   draft（草稿）
        │
  审阅 / 修订 / 质量校验
        │
        ▼
 reviewing（可选）
        │
       发布
        │
        ▼
 published（已发布快照基线）
        │
  适配 / 导出 / 分发
        │
        ▼
distributed（形成分发记录）
        │
        ├─ 回滚：回到新 draft（复制历史快照，不改写历史）
        └─ 归档：archived
```

标准约束：

• 草稿用于编辑与修订

• 发布快照用于正式分发

• 历史快照一经发布即不可原地修改

• 回滚的本质是"复制历史快照生成新的草稿工作态"

3.4 标准数据流

```
Plain Text
外部内容 → 导入解析 → 证据抽取 / 结构映射 → 生成 schemaData + analysisMeta
→ 草稿审阅 → 发布快照 → 兼容性校验 → 适配编译 → 导出 / 分发记录
```

本规范明确：

• 导入阶段生成的是可编辑角色资产草稿

• 发布阶段生成的是不可变分发基线

• 分发阶段消费的是发布快照，不是草稿

• 运行时长期记忆与会话上下文不属于静态 NZA 包本体

3.5 NZA 角色资产生态全景与数据流

图 3-1 NZA 角色资产生态全景与数据流

阶段	参与方/工具	关键动作	标准输出物
创作域	角色设计师、AI 角色编辑器、IDE 插件	手动编写/外部材料导入/结构化编辑	.nza.yaml（草稿）
治理域	CI/CD 流水线、NZA 校验器、安全审计工具	结构校验、语义校验、完整性计算、安全扫描	Integrity Digest、draft→published
交换域	角色资产仓库、AI 角色市场、私有分发平台	版本管理、检索、授权、交易、溯源	Published Snapshot（不可变基线）
运行域	LLM 平台、智能体应用、终端设备、私有部署引擎	适配编译、能力降级、运行时装配、推理执行	Runtime Prompt/结构化角色配置

文字说明

NZA 不仅是文件格式，更是连接创作者与多平台运行环境的中间件协议。它以六层 Canonical Role Schema 为唯一语义内核，确保角色资产从创作工具→治理校验→分发交换→终端运行的全链路中，身份人设、行为逻辑、安全边界不被篡改、丢失或污染，实现"一次定义，多平台可信运行"。

生态全景的详细说明请参考《NZA 角色资产架构白皮书 V1.0》。

4 Canonical Role Schema（六层标准）

4.1 总体要求

schemaData 必须且只能包含以下六个顶层键:

- layer1_identity
- layer2_role
- layer3_personality
- layer4_memory
- layer5_behaviorStrategy

• layer6_constraints

任何缺失、额外平铺旧结构或语义混层，均视为不符合本规范。

4.2 Layer 1：角色身份

职责：回答"角色是谁"。

字段	类型	约束	说明
name	string	MUST	角色名称
summary	string	MUST	一句话角色摘要
tags	string[]	SHOULD	角色标签
locale	string	MAY	默认语言与区域标识，如 zh-CN

边界要求：

• 不得在本层写入运行时状态

• 不得把行为策略、工具权限、敏感边界混入身份描述

4.3 Layer 2：角色定位

职责：回答"角色处在什么关系、场景与世界锚点中"。

字段	类型	约束	说明
identitySetting	string	MUST	身份定位与职业/职责描述
relationshipSetting	string	SHOULD	与用户或对象的关系设定
worldAnchor	string	SHOULD	世界观、背景、设定锚点

边界要求：

• 本层用于角色定位，不用于表达风格偏好

• 平台执行机制、接口信息不得写入本层

4.4 Layer 3：性格与偏好

职责：回答"角色稳定地如何表达、偏好什么、反感什么"。

字段	类型	约束	说明
toneAndStyle	string[]	MUST	语气与表达风格
values	string[]	SHOULD	价值偏好与原则
behaviorPreferences	string[]	SHOULD	稳定偏好
tabooBoundaries	string[]	SHOULD	个性层禁忌与不偏好

边界要求：

• 本层只表达稳定人格特征

• 情境化处置流程应进入 Layer 5

• 法律与平台安全边界应进入 Layer 6

4.5 Layer 4：静态记忆

职责：表达角色随版本发布而冻结的静态记忆。

字段	类型	约束	说明
staticMemories	string[]	SHOULD	固定记忆条目
backgroundMemories	string[]	SHOULD	背景经历、世界观事实

边界要求：

• 本层只允许写入随版本发布的静态记忆

• 长期用户事实、对话摘要、运行时偏好记忆不得写回本层

• 动态记忆属于运行时系统，不属于静态包本体

4.6 Layer 5：行为策略

职责：表达角色在特定场景下的处置方式。

字段	类型	约束	说明
scenarioStrategies	object[]	MUST	面向场景的行为策略列表
conflictStrategy	string	SHOULD	遇到冲突时的处理方式
refusalStrategy	string	SHOULD	需要拒绝时的表达策略
repairStrategy	string	SHOULD	偏离角色或误解后如何修复

scenarioStrategies[]推荐最小结构:

字段	类型	说明
scenario	string	场景名称
goal	string	该场景的目标
approach	string[]	推荐策略
avoid	string[]	需要避免的做法

边界要求:

• 本层描述"怎么做"，不描述法律边界

• 平台专属工具调用参数不应直接写死在本层

4.7 Layer 6：约束与边界

职责：定义角色资产的安全、品牌、敏感与工具边界。

字段	类型	约束	说明
safetyPolicy	string[]	MUST	安全边界与禁止事项
brandCompliance	string[]	SHOULD	品牌、口径、合规

			要求
sensitivePolicy	string[]	SHOULD	敏感场景处理策略
toolGuardrails	string[]	MAY	工具能力护栏与使用条件

边界要求：

• 本层为角色资产内最高业务约束层

• 但其优先级仍低于法律要求、平台系统安全策略与目标平台硬性限制

• 儿童保护特别提示：若 NZA 资产明确面向或可能面向未成年人提供服务，资产创建者应当在 layer6_constraints.safetyPolicy 中明确写入符合《未成年人保护法》的约束条款（如禁止诱导消费、禁止不当接触、内容分级过滤）

5 NZA 包结构规范

5.1 文件与编码要求

V1.0 采用 JSON 作为唯一规范化交换格式，同时推荐使用 YAML 作为人工编辑友好格式。

格式	用途	约束级别	说明
JSON	标准化交换、完整性校验、发布分发	MUST	所有正式分发包必须使用 JSON 格式
YAML	人工编辑、草稿阶段	SHOULD	仅用于内部编辑，发布前必须转换为规范化 JSON

JSON 格式强制要求：

• 文件扩展名：*.nza.json

• MIME Type：application/nza+json

• 字符编码：UTF-8（无 BOM）

• 换行：LF（\n）

• 规范化算法：JSON Canonicalization Scheme（RFC 8785）

YAML 格式推荐要求：

• 文件扩展名：*.nza.yaml

• MIME Type：application/nza+yaml

• 字符编码：UTF-8（无 BOM）

• 版本：YAML 1.2

• 禁止使用 YAML 锚点、别名等高级特性，确保与 JSON 语义完全等价

说明：

• 任意展示层转码可以存在，但对外交换与摘要计算必须回落到 RFC 8785 规范化 JSON

• 实现方应当提供 JSON 与 YAML 之间的双向无损转换工具

• 未来格式扩展规划：未来版本可能引入 TOML 等其他人类编辑友好格式，但所有格式在计算摘要、签名及跨系统交换前必须转换为符合本规范的规范化 JSON 表示

5.2 顶层对象结构

NZA 包顶层字段如下：

顶层键	类型	约束	说明
nza_manifest	object	MUST	包清单与版本信息
nza_payload	object	MUST	角色资产与说明层载荷
nza_compatibility	object	MUST	兼容与适配信息
nza_integrity	object	MUST	完整性摘要与可选签名
nza_extensions	object	MAY	厂商扩展区

5.3 nza_manifest

nza_manifest 用于描述该包是什么、属于哪个版本、处于什么状态。

字段	类型	约束	说明
specVersion	string	MUST	NZA 标准版本，如 1.0
schemaVersion	string	MUST	六层 Schema 版

			本，如 1.0
packageId	string	MUST	包唯一标识
packageType	string	MUST	固定为 role_asset
status	string	MUST	draft / reviewing / published / archived
versionNo	string	MUST	业务版本号，如 v1.0.0
createdAt	string	MUST	ISO 8601 时间
updatedAt	string	MUST	ISO 8601 时间
publishedAt	string	MAY	发布时填写
locale	string	SHOULD	默认语言区域，如 zh-CN
issuer	object	SHOULD	发行主体信息

issuer 推荐最小结构：

字段	类型	说明
organization	string	组织名
product	string	产品名
ownerRef	string	发行主体引用标识

规则：

• status=published 时，publishedAt 必须存在

• 对外分发的 NZA 包必须为 published

• packageId + versionNo 共同标识一个可追溯分发基线

5.4 nza_payload

nza_payload 是包的核心载荷，包含资产本体与说明层。

字段	类型	约束	说明
assetMeta	object	MUST	资产元信息
schemaData	object	MUST	六层 Canonical Role Schema
analysisMeta	object	MAY	导入/生成说明层

assetMeta 推荐字段：

字段	类型	约束	说明
name	string	MUST	资产展示名
description	string	SHOULD	简介
tags	string[]	MAY	标签
sourceType	string	SHOULD	manual / chat_import / ai_import / role_import / template

analysisMeta 推荐字段：

字段	类型	约束	说明
overallConfidence	number	MAY	总体置信度（0-100）
layerConfidence	object	MAY	各层置信度
needsConfirmation	array	MAY	待确认项
conflicts	array	MAY	冲突项
evidenceStats	object	MAY	证据统计

sourceSummary	object	MAY	来源摘要与血缘信息
pipelineVersion	string	MAY	导入管道版本
parserVersion	string	MAY	解析器版本
manualOverrides	array	MAY	人工修订痕迹

强制规则：

• analysisMeta 必须与 schemaData 分离

• analysisMeta 不得直接参与运行时编译输入

• schemaData 只能包含六层标准字段

• 原始长对话、未脱敏原文、隐私敏感原始材料不得直接写入 nza_payload

5.5 nza_compatibility

nza_compatibility 用于表达该角色资产在适配与导出时需要的能力信息。

字段	类型	约束	说明
minReaderSpecVersion	string	MUST	最低读取标准版本
adapterProfiles	object[]	SHOULD	目标平台适配声明
capabilityRequirements	object	SHOULD	资产需要的能力要求
degradationPolicy	object	MUST	降级策略
validationHints	string[]	MAY	校验建议

adapterProfiles[]推荐最小结构：

字段	类型	说明
adapterId	string	适配器标识，如 openclaw
targetPlatform	string	目标平台名称

compileMode	string	prompt_only / prompt_with_tools / structured_export
capabilityMatrix	object	平台能力矩阵

capabilityRequirements 推荐字段：

• requiresStaticMemory: boolean

• requiresStructuredConstraints: boolean

• requiresToolGuardrails: boolean

• requiresLongContextSupport: boolean

degradationPolicy 推荐字段：

字段	类型	说明
onMissingMemorySupport	string	warn / block
onMissingToolGuardrails	string	warn / block
onConstraintLoss	string	block 为推荐默认
onStyleLoss	string	warn 为推荐默认

5.6 nza_integrity

nza_integrity 用于描述完整性摘要与可选签名。

字段	类型	约束	说明
algorithm	string	MUST	固定为 SHA-256
canonicalization	string	MUST	固定为 RFC 8785
scope	string	MUST	固定为 package_without_integrity_digest
digest	string	MUST	十六进制摘要值

signature	object	MAY	可选签名块

摘要计算规则：

1. 对整个 NZA 包执行 RFC 8785 规范化序列化
2. 计算前应暂时移除 nza_integrity.digest 与 nza_integrity.signature.value
3. 对规范化结果计算 SHA-256
4. 摘要结果写入 digest
5. 若启用签名，对同一规范化结果进行签名

5.7 nza_extensions

扩展区用于承载厂商私有、平台私有或项目私有的附加字段。

规则：

• 扩展字段必须放在 nza_extensions.<namespace>下

• namespace 应使用稳定命名，如 vendor.openclaw、vendor.examplecorp

• 扩展字段不得覆盖、改名或删除 schemaData 六层核心语义

• 无法识别的扩展字段，Reader 应安全忽略，而不是报错崩溃

• 若扩展字段影响导出行为，必须同时更新 nza_compatibility 中的能力声明

6 导入、发布与分发规范

6.1 导入规范

NZA 支持将外部材料导入为标准角色资产草稿，但导入的标准终点不是"原文直接变成可运行包"，而是：

```
Plain Text
外部内容 → detect → preprocess → extract → merge → mapToSchema → assess
→ 产出 schemaData + analysisMeta → draft
```

强制规则：

• 导入过程应采用证据化抽取，不应绕过结构映射直接生成最终资产

• 导入结果默认落为 draft

• 低置信度、冲突字段应进入 needsConfirmation 或保持空值，而非强行填满

• 导入过程保留的是说明层与摘要，不是永久保存原始敏感内容

6.2 分析说明层规范

analysisMeta 的存在是为了支持审阅、修订、追溯与治理，而不是让说明数据混入运行时语义。

因此：

• schemaData 是运行时与发布的资产真相源

• analysisMeta 是解释层

• manualOverrides 只能表示人工覆盖痕迹，不能伪装成自动抽取得到的客观事实

• 任何编译器或适配器在运行时只消费 schemaData，不直接消费 analysisMeta

6.3 发布快照规范

对外分发必须基于发布快照，而不是工作草稿。

发布规则：

1. 草稿资产经审阅通过后进入发布
2. 发布时冻结完整 schemaData 与必要元数据，形成不可变快照
3. 发布快照必须具有唯一 versionNo 与 publishedAt
4. 历史快照禁止原地修改
5. 回滚时复制历史快照内容生成新草稿，不得改写历史记录

6.4 适配与分发规范

NZA 包不是直接执行引擎，角色资产进入目标平台前必须经过：

```
Plain Text
Published Snapshot → Compatibility Validation → Prompt Compiler / Mapper
→ Adapter → Distribution Record
```

强制规则：

• 适配导出必须以发布快照为输入

• 适配失败必须保留校验结果与失败上下文

• 有阻断级错误时，导出必须终止

• 仅存在告警级问题时，可在显式确认后继续导出

• 分发必须形成可追溯记录，包括时间、版本、适配器、结果、失败码与摘要

6.5 运行时装配边界

运行时装配通常由以下三部分组成：

• 发布快照中的 schemaData

• 运行时记忆系统中的长期记忆 / 会话摘要

• 当前会话上下文

本规范明确：

• 运行时记忆系统不属于静态 NZA 包本体

• 动态会话状态不应回写到静态 schemaData

• 只有版本化的静态资产才进入发布快照

• 编译器可按目标平台能力对静态资产与动态记忆进行装配，但不得篡改标准层定义

7 校验与兼容性规范

7.1 校验类型

NZA 包校验至少分为以下五类：

校验类型	目标	失败后果
结构校验	顶层结构、六层字段、数据类型是否符合规范	阻断
语义校验	字段是否混层、是否存在明显语义冲突	阻断或告警
安全校验	是否包含越权、危险注入、违禁表达	阻断
兼容校验	目标平台是否具备所需能力	阻断或告警
完整性校验	摘要、签名是否匹配	阻断

7.2 兼容性等级

NZA 定义四级兼容等级：

等级	名称	含义

L1	Parseable	可被标准 Reader 正确解析
L2	Schema-Compliant	满足六层 Schema 与顶层包结构要求
L3	Compilable	可被编译器转换为目标平台可消费表达
L4	Distribution-Ready	已通过目标适配器校验，可正式导出/分发

7.3 能力降级规范

目标平台能力不足时，适配器必须执行标准化降级决策：

缺失能力	推荐策略
不支持静态记忆注入	warn 或 block，取决于 degradationPolicy
不支持结构化约束	默认 block
不支持工具护栏	默认 block
不支持细粒度风格表达	可 warn 并退化为摘要表达
不支持长上下文	可 warn 并触发压缩编译

强制规则：

• 降级必须可见、可记录、可追溯

• 不得在用户无感知的情况下静默丢失关键约束

• 对安全、合规、敏感边界相关能力缺失，应优先阻断而非降级

7.4 评测与验收框架

NZA 不直接承诺某个固定数值的一致性结果，而要求平台以统一方法学进行评测。评测报告至少应覆盖：

• 完整性：六层是否完整、是否存在空洞关键字段

• 冲突度：不同层之间是否互相打架

• 稳定性：同类场景下策略与表达是否稳定

• 风险：是否触发安全、合规、敏感越界

• 适配保真度：导出前后语义损失是否可接受

评测报告必须说明：

• 测试集范围

• 模型/平台版本

• Adapter 版本

• 评分方法

• 告警与阻断阈值

• 结果摘要与改进建议

7.4.1 推荐量化评测指标（非强制）

以下量化指标供实现方参考，不构成标准强制要求：

维度	推荐量化指标	推荐计算方法	推荐合格阈值
完整性	字段完整率	已填充必填字段数 / 总必填字段数 × 100%	≥100%
冲突度	语义冲突率	存在语义冲突的字段对数 / 总字段对数 × 100%	≤5%
稳定性	输出一致性	相同输入下输出语义一致的次数 / 总测试次数 × 100%	≥90%
风险	违规触发率	触发安全/合规告警的测试用例数 / 总测试用例数 × 100%	0%
适配保真度	语义保留率	导出前后语义一致的测试点数量 / 总	≥85%

		测试点数量 × 100%	

冲突度计算示例：可采用 LLM-as-a-Judge 方法，构建包含矛盾指令的测试集（如"Layer 3 要求幽默，Layer 6 要求严肃"），计算模型输出偏离角色设定的语义距离。推荐报告包含：冲突场景数量、模型遵循约束层的比率、人工评估一致性系数。

7.5 版本迁移策略

7.5.1 向后兼容原则

NZA 标准遵循语义化版本控制，版本号格式为主版本号.次版本号.修订号：

• 修订号变更：仅修复 bug，完全向后兼容

• 次版本号变更：新增可选功能，完全向后兼容

• 主版本号变更：可能包含不兼容的核心变更

7.5.2 V1.x 到 V2.0 迁移规则

1. 兼容期：V2.0 发布后，V1.x 标准将继续支持至少 24 个月
2. 自动迁移：实现方应当提供从 V1.x 到 V2.0 的自动迁移工具
3. 字段映射：所有 V1.x 核心字段必须在 V2.0 中有明确的映射关系
4. 数据保留：迁移过程中不得丢失任何用户数据
5. 回滚支持：支持从 V2.0 回滚到 V1.x 格式（可能丢失 V2.0 新增字段）

7.5.3 迁移流程

1. 解析旧版本 NZA 包
2. 执行字段映射与结构转换
3. 生成新版本 NZA 包
4. 执行完整性校验与兼容性校验
5. 保留旧版本包作为备份

8 安全、合规与审计

8.1 安全优先级原则

NZA 在运行与适配时应遵循以下优先级：

```
Plain Text
法律法规与平台系统安全策略 > 目标平台硬性约束 > Layer 6 约束与边界
> Layer 5 行为策略 > Layer 2/3/4 角色语义 > 当前任务与表达风格细节
```

这意味着：

• 角色资产不能覆盖法律与系统安全要求

• 角色设定不能要求执行越权工具操作

• 平台私有安全策略应高于风格表达与个性偏好

8.2 完整性与签名

NZA V1.0 要求：

• 所有正式分发包必须包含 SHA-256 摘要

• 摘要计算必须基于 RFC 8785 规范化 JSON

• 支持可选数字签名块，用于校验发行主体

• 摘要证明的是完整性，签名证明的是来源可信度

• 仅有摘要而没有可信签名时，不应把包误判为"已认证来源"

8.3 数据保护

NZA 包必须遵循最小必要原则：

• 不得把可识别自然人的敏感原始资料直接封装进标准包

• 导入场景中的原始聊天长文本、音视频原始材料、明文身份信息应在标准包之外受控处理

• 对外分发包应尽量只包含角色资产语义本体、必要元信息与审计摘要

• 如涉及外部模型调用，应在实现侧履行数据出境、隐私提示与授权义务

跨境传输提示：NZA 包的设计目标是语义资产交换，应避免包含受《个人信息保护法》及《网络数据安全管理条例》管辖的个人信息或重要数据。若 NZA 包因特殊业务需要包含此类数据并进行跨境分发，分发主体必须独立履行数据出境安全评估、标准合同备案或保护认证等法定义务，NZA 标准本身不豁免上述义务。

8.4 合规与权属

标准约束如下：

• NZA 作为技术载体，不创设著作权本身

• 角色资产内容的权属以实际创作贡献、授权关系与适用法律为准

• 分发、商用、再授权等应以发行主体声明与实际合同关系为准

• 平台不得因采用 NZA 标准而默认取得用户资产的全部权利

8.5 审计要求

围绕 NZA 包的关键动作必须保留审计记录，至少包括：

• 包创建

• 发布快照生成

• 完整性校验

• 兼容性校验

• 导出与分发

• 导出失败与重试

• 版本回滚与归档

审计日志至少应包含：

• 操作类型

• 时间戳

• 操作者标识

• 目标包或版本号

• 结果状态

• 失败码与链路追踪标识

9 实施合规性要求 (Implementation Compliance)

9.1 生成流程

1. 创建或导入角色资产
2. 生成标准 schemaData
3. 如来源于导入链路，附加 analysisMeta
4. 写入 nza_manifest 与 nza_compatibility
5. 计算 nza_integrity.digest
6. 在需要时附加签名与扩展区
7. 输出.nza.json 标准包

9.2 校验流程

1. 解析 JSON 并校验顶层结构
2. 校验 schemaData 是否为六层结构
3. 校验 analysisMeta 是否与资产层分离
4. 校验 nza_compatibility 是否完整
5. 校验 nza_integrity 摘要与签名
6. 根据目标平台执行适配兼容性验证

9.3 发布流程

1. 草稿经人工审阅与质量检查
2. 生成发布快照
3. 写入版本号与发布时间
4. 重新计算摘要
5. 输出正式分发包
6. 将历史版本作为不可变快照保留

9.4 分发流程

1. 选择目标适配器与平台
2. 读取发布快照
3. 执行兼容性校验
4. 若存在阻断项则终止
5. 若仅有告警项，经确认后继续
6. 执行适配编译与导出
7. 记录分发结果与失败上下文

10 附录

10.1 标准 JSON 示例

```JSON
{
  "nza_manifest": {
    "specVersion": "1.0",
    "schemaVersion": "1.0",
```

```
    "packageId": "role_pkg_9f31b5b2",
    "packageType": "role_asset",
    "status": "published",
    "versionNo": "v1.0.0",
    "createdAt": "2026-05-01T08:00:00Z",
    "updatedAt": "2026-05-01T08:00:00Z",
    "publishedAt": "2026-05-01T08:30:00Z",
    "locale": "zh-CN",
    "issuer": {
      "organization": "NoZeroAI",
      "product": "Role Asset Platform",
      "ownerRef": "owner_001"
    }
  },
  "nza_payload": {
    "assetMeta": {
      "name": "星海陪伴型科幻作家助手",
      "description": "用于辅助用户进行中长篇科幻创作与叙事规划。",
      "tags": ["科幻", "创作", "陪伴"],
      "sourceType": "manual"
    },
    "schemaData": {
      "layer1_identity": {
        "name": "星海",
        "summary": "理性、耐心、具有人文关怀的科幻创作助手",
        "tags": ["理性", "耐心", "科幻"]
      },
      "layer2_role": {
        "identitySetting": "长期陪伴式科幻创作顾问",
        "relationshipSetting": "与用户共同讨论设定、角色与叙事结构",
        "worldAnchor": "偏硬科幻与人文融合的未来叙事框架"
      },
      "layer3_personality": {
        "toneAndStyle": ["冷静", "鼓励式", "结构化表达"],
        "values": ["尊重原创", "重视逻辑闭环", "鼓励长期创作"],
        "behaviorPreferences": ["先澄清目标再给建议", "避免空泛夸赞
"],
        "tabooBoundaries": ["不代替用户完成声称原创的最终作品"]
      },
      "layer4_memory": {
        "staticMemories": ["用户偏好硬科幻与人物成长线并重"],
        "backgroundMemories": ["熟悉太空歌剧、赛博朋克与第一接触题材
"]
      },
```

```
      "layer5_behaviorStrategy": {
        "scenarioStrategies": [
          {
            "scenario": "创意发散",
            "goal": "帮助用户扩展题材可能性",
            "approach": ["给出三个方向", "分别说明冲突与亮点"],
            "avoid": ["直接替用户定稿"]
          },
          {
            "scenario": "结构诊断",
            "goal": "发现设定与情节的不一致",
            "approach": ["先列问题", "再给修复路径"],
            "avoid": ["跳过逻辑链直接给结论"]
          }
        ],
        "conflictStrategy": "当设定冲突时，先指出冲突源，再给出候选修正方案。",
        "refusalStrategy": "遇到越界创作要求时，应明确解释边界并给出可替代帮助。",
        "repairStrategy": "当输出偏离角色定位时，先承认偏离，再按当前目标重构回答。"
      },
      "layer6_constraints": {
        "safetyPolicy": ["不得生成违法违规内容", "不得泄露个人敏感信息", "面向未成年用户时不得诱导消费或不当接触"],
        "brandCompliance": ["保持专业、克制、可信的产品语气"],
        "sensitivePolicy": ["涉及高风险主题时先收缩建议范围并提示边界"],
        "toolGuardrails": ["未经显式授权不得调用外部写操作工具"]
      }
    },
    "analysisMeta": {
      "overallConfidence": 96,
      "layerConfidence": {
        "layer1_identity": 98,
        "layer2_role": 96,
        "layer3_personality": 95,
        "layer4_memory": 92,
        "layer5_behaviorStrategy": 94,
        "layer6_constraints": 97
      },
      "needsConfirmation": [],
      "conflicts": [],
```

```
    "evidenceStats": {
      "total": 0,
      "byLayer": {}
    },
    "sourceSummary": {
      "sourceType": "manual"
    },
    "manualOverrides": []
  }
},
"nza_compatibility": {
  "minReaderSpecVersion": "1.0",
  "adapterProfiles": [
    {
      "adapterId": "openclaw",
      "targetPlatform": "OpenClaw",
      "compileMode": "structured_export",
      "capabilityMatrix": {
        "supportsMemory": true,
        "supportsTools": false,
        "supportsRag": false,
        "supportsStructuredExport": true
      }
    }
  ],
  "capabilityRequirements": {
    "requiresStaticMemory": true,
    "requiresStructuredConstraints": true,
    "requiresToolGuardrails": false,
    "requiresLongContextSupport": false
  },
  "degradationPolicy": {
    "onMissingMemorySupport": "warn",
    "onMissingToolGuardrails": "warn",
    "onConstraintLoss": "block",
    "onStyleLoss": "warn"
  },
  "validationHints": [
    "导出前应先执行结构校验与适配器兼容校验"
  ]
},
"nza_integrity": {
  "algorithm": "SHA-256",
  "canonicalization": "RFC 8785",
  "scope": "package_without_integrity_digest",
```

```
    "digest":
"8e49b59b1a5f9f69d8d7b621d31d71f5265d5b6d0f1a0c54f2b2d57b8c0b11af"
  },
  "nza_extensions": {
    "vendor.openclaw": {
      "preferredTemplate": "openclaw_prompt_bundle_v1"
    }
  }
}
```

10.2 字段约束摘要

区块	必填性	备注
nza_manifest	必填	描述包身份、版本与状态
nza_payload.assetMeta	必填	描述资产元信息
nza_payload.schemaData	必填	六层标准本体
nza_payload.analysisMeta	可选	说明层，不参与运行时编译
nza_compatibility	必填	兼容、适配与降级
nza_integrity	必填	完整性摘要与可选签名
nza_extensions	可选	厂商扩展区

10.3 法律与标准参考

1. 《中华人民共和国个人信息保护法》
2. 《中华人民共和国数据安全法》
3. 《网络数据安全管理条例》（2025 年 1 月 1 日施行）
4. 《生成式人工智能服务管理暂行办法》
5. 《中华人民共和国著作权法》
6. GB/T 35273—2020《信息安全技术 个人信息安全规范》
7. RFC 8785《JSON Canonicalization Scheme》

8. OWASP Prompt Injection 防护最佳实践

10.3.1 学术参考文献与背景

核心参考文献：

• Wang, Z., Zhou, Y., Luo, Z., et al. "DeepPersona: A Generative Engine for Scaling Deep Synthetic Personas." arXiv preprint, arXiv:2511.07338, 2025.

• Zhou, J., et al. "Character-LLM: A Trainable Agent for Role-Playing." EMNLP, 2023.

学术背景对比：

上述工作侧重评估角色人格一致性或训练角色扮演模型（DeepPersona 侧重于生成海量合成角色档案，Character-LLM 侧重于训练可扮演特定角色的模型），NZA 侧重定义角色资产的可交换结构。二者是生成/训练/评估标准与交换标准的互补关系。NZA 的 Layer 3（性格与偏好层）可与 DeepPersona 等模型的输出相结合，实现更精准的角色建模与资产复用。

10.4 指标术语解释

术语	含义
完整性	包在规范化序列化后摘要与签名可被验证
兼容性	包可被 Reader、Compiler 与 Adapter 正确消费
保真度	资产语义在适配前后被保留的程度
降级	因目标平台能力不足而执行的显式退化处理
发布快照	对某一时刻角色资产冻结后的不可变基线

10.5 未来工作与实证研究计划

1. 保真度基准测试：计划建立标准测试集，评估同一角色在使用 NZA 六层 Schema 描述与使用纯文本 Prompt 描述时，在行为一致性、人设稳定性等指标上的差异

2. 冲突度量化研究：研究 Layer 3 至 Layer 6 之间的语义冲突检测算法及其对生成质量的影响，并细化冲突度的量化计算方法

3. 多格式支持评估：评估 YAML、TOML 等格式作为人工编辑友好格式的可行性，并制定向规范化 JSON 转换的标准流程

4. 跨平台适配实证：收集不同平台适配器实现下的保真度数据，持续优化 degradationPolicy 规则

5. 工具链生态建设：开发参考实现的开源工具链，包括校验器、编译器、迁移工具及可视化编辑器，降低生态准入门槛

版权声明与免责声明