

ICS Xx.xxx.xx
CCS X xx

T/ZGCIT

中关村智能科技发展促进会团体标准

T/ZGCIT 0xx—2026

博物馆 AR 导览系统技术规范

Technical Specification of Museum AR Guide System

2026 - 0x - xx 发布

2026 - 0x - xx 实施

中关村智能科技发展促进会 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 系统架构	2
5.1 总体架构	2
5.2 技术要求	2
6 核心功能要求	4
6.1 导览与定位	4
6.2 展馆内容呈现	5
6.3 系统管理	6
7 技术要求	7
7.1 定位与导航	7
7.2 交互技术	8
7.3 系统集成与接口	8
7.4 系统可靠性	8
7.5 国产化支持能力	9
8 内容制作与管理	9
9 运维管理	9
9.1 日常监控与维护	9
9.2 备份与更新	10
10 安全保障	10
10.1 物理环境安全	10
10.2 数据安全	10
10.3 网络安全	11

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中关村智能科技发展促进会提出并归口。

本文件起草单位：。

本文件主要起草人：。

本文件首次发布。

博物馆 AR 导览系统技术规范

1 范围

本文件规定了博物馆AR导览系统（以下简称“系统”）的总体架构、核心功能要求、技术要求、内容制作与管理、运维管理、安全保障等内容。

本文件适用于博物馆AR导览系统的研发、应用、管理等环节。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2887-2011 计算机场地通用规范

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 38247-2019 信息技术 增强现实 术语

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 45909-2025 网络安全技术、数字水印技术实现指南

GB 50174-2017 数据中心设计规范

T/ZGCIT-0XX 2026 AR文物数字化资源制作规范

T/ZGCIT-0XX 2026 AR文物展示交互技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

博物馆AR导览系统 museum AR guide system

基于增强现实技术，融合空间定位、虚实融合、多模态交互等技术手段，为博物馆游客提供展馆定位导航、展品数字化讲解、交互式探索，同时为馆方提供内容管理、数据运营、设备管控的一体化系统。

3.2

虚实融合 virtual-reality integration

将移动终端或计算机通过数字技术产生的虚拟场景与真实场景进行实时的数字化混合，使虚拟物体和真实物体共同存在同一个场景中。

[来源：GB/T 38247-2019,2.2.31]

3.3

空间配准 spatial registration

将增强现实系统中的虚拟坐标系与真实物理空间的坐标系进行匹配，使虚拟内容能够在真实空间中精准、稳定呈现的技术过程。

3.4

多模态交互 multi-modal interaction

用户通过手势、语音、触屏、眼动等一种或多种交互方式，与博物馆 AR 导览系统中的虚拟内容进行信息交互和操作控制的方式。

4 缩略语

下列缩略语适用于本文件。

SLAM: 即时定位与地图构建 (Simultaneous Localization and Mapping)

RTO: 恢复时间目标 (Recovery Time Objective)

RPO: 恢复点目标 (Recovery Point Objective)

UPS: 不间断电源 (Uninterruptible Power Supply)

5 系统架构

5.1 总体架构

博物馆AR导览系统应采用分层解耦、云端协同、弹性扩展的总体架构，整体分为应用层、终端层、网络层、服务层、数据层和基础层，各层之间通过标准化接口实现数据交互和业务协同，系统架构应满足可维护、可升级、可拓展的要求，适配不同规模博物馆的应用需求，如图1所示。



图1 博物馆AR导览系统架构

5.2 技术要求

5.2.1 基础层

基础层负责提供底层的计算、存储、网络及物理环境支撑，具体要求如下：

- 云基础设施宜采用具备弹性伸缩能力的公有云或私有云平台，支持计算资源的按需分配与动态扩展；云服务应满足 GB/T 22239-2019 中等级保护三级及以上要求，并具备同城或异地灾备能力；
- 机房环境应符合 GB 50174-2017 的要求；
- 硬件资源宜选用企业级服务器、存储设备，核心服务应采用集群化部署。

5.2.2 数据层

数据层应实现空间数据、文物数字资产、用户数据及业务数据的存储和管理，具体要求如下：

- a) 空间数据应包含展厅三维地图、展品位置坐标、信标部署等信息。空间坐标系统应统一，宜支持多种定位技术的数据融合；
- b) 文物数字资产应符合 T/ZGCIT 0xx-2026 AR 文物数字化资源制作规范的要求；应建立文物数字资产的全生命周期数据档案，包含制作、审核、发布、更新、下架等全流程信息；
- c) 用户数据采集应符合 9.2 的要求，并经过用户授权；
- d) 业务数据应包含系统运行日志、展品访问统计、设备状态等，宜建立数据分级分类管理机制，并支持多维度统计分析。

5.2.3 服务层

服务层负责提供AR导览的核心业务能力，以微服务架构向上层应用提供API服务，具体要求如下：

- a) AI 能力应包含图像识别、自然语言理解、智能推荐等算法服务；
- b) 空间智能管理应提供空间地图的创建、存储、更新与分发服务；应支持高精度点云地图与语义地图的融合管理，地图更新宜采用增量方式下发；
- c) 导览服务应提供实时定位、路径规划与智能推荐等能力；
- d) 内容管理应提供对 AR 数字资产的全生命周期管理能力，包括但不限于上传、编目、审核、版本控制、发布与下线等。

5.2.4 网络层

网络层应提供融合网络传输能力，确保终端与云端之间音视频数据、定位信息及控制指令的实时、稳定交互。具体要求如下：

- a) 展厅内应实现无线网络全覆盖，重点展区宜部署 5G 微基站或 Wi-Fi 6 接入点；
- b) 宜支持本地局域网和公网双网络模式，当公网故障时，核心导览功能可通过本地局域网实现本地化运行；
- c) 应采用网络隔离技术，将数据层、服务层与外部网络进行逻辑隔离。

5.2.5 终端层

终端层应支持多形态硬件设备，具备实时空间定位跟踪、自然交互识别能力，具体要求如下：

- a) 宜支持多种终端设备类型，包括但不限于：
 - 1) 手持设备：智能手机、平板电脑；
 - 2) 头戴设备：AR 眼镜、MR 头显；
 - 3) 固定终端：展厅触摸屏、专用导览机。
- b) 终端应支持基于 SLAM 的实时定位与地图构建能力，在正常步行状态下实现连续稳定的定位输出；
- c) 宜支持多种交互方式的识别，包括但不限于手势识别、语音识别、触控交互等；
- d) 馆用专用导览终端应具备防摔、防水、长续航、操作便捷的特性；终端设备宜支持国产化操作系统和硬件平台。

5.2.6 应用层

应用层应面向游客、管理员等不同角色提供交互界面，通过调用服务层API实现导览、管理、运营等业务功能，具体要求如下：

- a) 游客端应提供面向游客的 AR 导览应用，宜支持以下功能：
 - 1) 展馆内定位与 AR 导航；
 - 2) 文物 AR 识别与虚实融合展示；
 - 3) 多模态讲解与交互式探索；
 - 4) 路线智能推荐；
 - 5) AR 合影、截图与社交分享。
- b) 管理端应提供面向博物馆管理员的 Web 后台或专用客户端，宜支持以下功能：
 - 1) AR 数字资产的上传、审核、发布、版本控制与下线；
 - 2) 馆内租赁终端的远程状态监控、固件升级与使用统计；

- 3) 支持多级管理员账号及权限分配;
- 4) 地图更新维护;
- c) 应用层宜支持多种访问方式,包括但不限于微信/支付宝小程序、独立 APP、Web 浏览器等。不同终端的用户数据与业务数据应实时同步;
- d) 应用界面设计应符合直观、简洁原则,关键功能应在 3 步操作内可达。应用启动时间不宜超过 3 秒,界面切换应平滑流畅;
- e) 应用应提供基本的无障碍功能,包括字体放大、语音辅助、高对比度模式等;
- f) 游客端与管理端之间的业务数据应支持实时或准实时同步。

6 核心功能要求

6.1 导览与定位

6.1.1 展馆内定位

系统宜在展厅内实现亚米级 (≤ 1 米) 的定位精度,应符合以下要求:

- a) 应采用多源融合定位技术,结合蓝牙、Wi-Fi RTT、惯性测量单元 (IMU)、视觉定位 (VPS) 等多种方式;
- b) 应覆盖所有开放展区及主要公共通道,无信号盲区;在电梯、楼梯等特殊区域应具备定位切换或保持能力;
- c) 应兼容不同品牌、型号的移动终端的传感器差异,提供一致的定位功能;
- d) 当用户位置出现明显偏离 (如穿越墙壁) 时,应具备自动纠偏机制;
- e) 应支持自动识别用户所在楼层、具体展厅或展区。

6.1.2 AR 导航

宜在实景相机画面中,以虚拟箭头、路径线、浮动标识等方式,实时叠加导航指引至目标展品或设施,应符合以下要求:

- a) 导航指引应清晰、直观地叠加在实景画面中,虚拟箭头应沿真实地面延伸,关键拐角处宜悬浮动态方向标识。导航元素的色彩应与环境背景有明显区分;
- b) 虚拟导航指引应贴合真实环境,在用户移动过程中无明显漂移或抖动;
- c) 在路径拐弯处或分叉口,宜提前 3 米~5 米给出转弯提示,提示形式可包括箭头转向动画、语音播报、文字提示等,转弯后应自动更新路径指引;
- d) 当用户偏离规划路径超过 2 米时,应自动重新计算路线,并在 3 秒内更新导航指引;
- e) 当用户到达目标展品或设施附近 (距离 ≤ 3 米) 时,应给出到达提醒,并自动触发相关展品的 AR 内容介绍;
- f) 宜支持单点导航、多点连续导航两种模式,可同时设置多个目标点,实现多展品、多区域的连续参观导航。

6.1.3 智能路线

宜基于参观时间、用户兴趣标签、展品热度等因素,提供个性化的路线规划与推荐,应符合以下要求:

- a) 宜支持用户输入参观时长和兴趣偏好,自动生成符合时间约束和兴趣偏好的参观路线;
- b) 宜提供多种路线方案供用户选择,包括但不限于:
 - 1) 精选路线:以镇馆之宝、核心展品为核心的官方推荐路线;
 - 2) 快速路线:时间最短、效率最高的参观路径;
 - 3) 深度路线:覆盖展品最全、信息最丰富的参观路径;
 - 4) 主题路线:围绕特定主题设计的专题路线。
- c) 应集成展馆内全部可参观展品和服务设施的兴趣点,涵盖展品、卫生间、出口、文创店、餐饮等类别。兴趣点数量可根据展馆规模确定;
- d) 路线规划应支持动态调整,用户可在参观过程中随时增减目标展品,系统应实时重新计算最优路线;

- e) 当展厅临时闭馆、展品维护时，应自动规避并重新规划路线，同时向游客推送文字或语音提醒信息；
- f) 宜结合实时客流数据，在路线规划时避开人流密集区域，或在 3D 地图上以热力图形式展示各展区拥挤程度（如红、橙、黄、绿四色预警），辅助用户决策；
- g) 宜支持用户保存常用路线，并可分享给其他用户。

6.2 展馆内容呈现

6.2.1 虚实融合展示

宜将虚拟信息与真实展品及环境进行空间配准，实现文物复原、场景重现、内部结构透视等多种展示模式，应符合以下要求：

- a) 系统应支持多种虚实融合展示模式，包括但不限于：
 - 1) 文物复原展示：基于学术研究，对残损文物进行虚拟复原，复原部分应采用区别于现存部分的视觉风格（如半透明显示、不同色彩标注）；
 - 2) 历史场景重现：将文物置于其历史使用场景中，还原当时的空间环境、人物活动等；
 - 3) 内部结构透视：对于结构复杂的文物，支持分层透视或剖切展示；
 - 4) 纹饰动态解读：对文物表面的纹饰、铭文进行动态标注和解读，展示其工艺特点和文化内涵。
- b) 虚实融合展示应结合视觉、听觉等多感官通道，通过 AR 动画、3D 复原、历史影像、环境音效等多种媒体形式；
- c) 虚实融合展示内容应以权威学术研究为依据，虚拟复原或场景再现部分应有明确的学术来源，并在呈现时予以说明。

6.2.2 多模态讲解

宜结合 AR 动画、3D 复原、历史影像、专家解说音频、文字说明等多种媒体形式，对文物进行深度解读，应符合以下要求：

- a) 讲解内容应采用分层递进的信息结构，宜不超过三级：
 - 1) 第一层：文物名称、年代、出土信息、基本用途；
 - 2) 第二层：工艺特点、纹饰含义、历史背景；
 - 3) 第三层：学术研究、考古故事、相关文献。
- b) 针对不同讲解内容，应采用合适的媒体形式：
 - 1) AR 动画：用于展示文物制作工艺、使用方式、演变过程；
 - 2) 3D 复原：用于展示文物原始形态、色彩还原；
 - 3) 历史影像：用于展示考古发掘过程、历史场景资料；
 - 4) 专家解说音频：提供权威、生动的语音讲解；
 - 5) 图文标注：在文物模型上直接标注关键部位和术语。
- c) 应支持多种讲解触发方式，包括：
 - 1) 自动触发：用户靠近展品时自动播放概览讲解；
 - 2) 手动触发：用户点击信息热点时播放详细讲解；
 - 3) 扫码触发：用户扫描展品编号或二维码获取讲解；
 - 4) 语音触发：用户通过语音指令调取特定讲解内容。
- d) 系统应支持中英双语讲解，宜增加其他常用语种，同一讲解内容在不同语种间应保持一致性和准确性；
- e) 宜集成 AI 智能问答能力，用户可通过自然语言提问获取展品相关信息。智能讲解应基于文物知识库，对常见问题的回答准确率不宜低于 85%；
- f) 讲解内容应支持远程更新和动态发布，内容更新频率可根据博物馆需求确定。

6.2.3 交互式探索

用户应能通过自然手势、触屏或外部输入设备进行操作，与虚拟文物进行交互探索，应符合以下要求：

- a) 应支持用户对虚拟文物进行旋转、缩放、平移等基础操作；
- b) 宜根据文物特点和展示需求，提供深度交互模式，包括但不限于：
 - 1) 部件拆解：用户可逐层拆解文物部件，观察内部结构；
 - 2) 材质切换：用户可切换不同材质显示模式；
 - 3) 时间轴浏览：用户可通过滑动时间轴，观察文物在不同历史时期的形态变化；
 - 4) 尺寸对比：用户可将文物与常见物体进行尺寸对比，感知文物大小。
- c) 宜集成空间定位能力，实现空间音频反馈，虚拟音源的位置应与文物空间位置匹配，用户移动时音频方位实时变化；虚拟物体与真实环境应保持正确的遮挡关系；
- d) 宜提供多模态交互反馈，包括但不限于视觉反馈、听觉反馈、触觉反馈；
- e) 交互操作应符合人体工程学，操作方式应简单易懂，无复杂操作步骤，适配老人、儿童等不同年龄段用户的操作能力。

6.3 系统管理

6.3.1 内容管理

应提供Web端或专用后台，供管理员对AR数字内容进行管理，应符合以下要求：

- a) 应支持 AR 数字内容的在线发布、版本管理和更新回滚；对已发布的内容进行修改后，可保存新版本并实现灰度发布；支持内容的批量操作；内容更新频率可根据博物馆需求确定；
- b) 应实现对文物三维模型、AR 动画、多媒体讲解、历史影像等数字资产的统一管理，支持按展品、展区、主题等多维度分类检索；
- c) 应提供隐形数字水印的编码、植入、识读等功能，数字水印应符合 GB/T 45909-2025 的规定，水印信息宜包含制作单位、项目编号、版权声明、时间戳等，具备唯一性和可追溯性；
- d) 应支持主流三维模型格式和多媒体格式的导入导出，宜采用国产数据格式；
- e) 应提供内容预览功能，管理员可在发布前查看 AR 内容在真实环境中的叠加效果。审核流程应支持多级审批，审核记录应完整保存备查。

6.3.2 数据看板

宜提供可视化数据看板，显示并统计各展品/展区的访问热度、互动项目参与度等核心运营数据，应符合以下要求：

- a) 数据看板宜包含以下指标：
 - 1) 展品访问热度：各展品/展区的用户访问次数、平均停留时长、识别触发次数；
 - 2) 互动参与度：AR 互动项目的用户参与率、完成率、交互深度；
 - 3) 用户行为分析：用户参观路径、兴趣偏好、使用时段分布；
 - 4) 设备使用情况：AR 终端设备的使用频率、故障率、电池消耗。
- b) 宜采用图表形式直观呈现数据，展区热度宜以 3D 热力图形式叠加在展厅地图上，展示各区域拥挤程度；
- c) 应支持原始数据导出，并可按日、周、月、年自动生成运营报告。

6.3.3 设备管理

应对馆方提供的AR设备进行状态监控与远程管理，应符合以下要求：

- a) 应实时监控 AR 设备的运行状态，包括但不限于在线/离线状态、电池电量、设备温度、软件版本和固件版本、故障代码和异常日志；
- b) 应支持对设备的远程操作，包括远程重启、关机、软件远程升级、应用推送、卸载、设备参数远程配置、设备锁定/解锁；
- c) 应支持设备固件的批量升级，升级过程应在后台静默进行，不影响设备的正常使用；
- d) 应在展厅地图上可视化展示各 AR 设备的实时位置和状态；
- e) 对于提供设备租借服务的博物馆，应支持租借流程管理，包括设备领用、归还、充电等环节的记录和提醒；
- f) 宜支持设备故障的在线报修和维修进度跟踪。

6.3.4 地图更新维护

当展厅布局发生变更时，可对系统底图进行局部更新与重新标注，应符合以下要求：

- a) 应提供可视化的地图编辑工具，当博物馆展厅布局变更、展品移位、新增展区 / 设施、拆除区域时，管理员可对系统底图进行局部更新、点位标注、区域划分、路径编辑等操作，无需整体重构地图；
- b) 地图数据应采用标准化的地理信息格式，支持与博物馆现有电子地图、安防地图的数据互通和同步更新；地图编辑完成后，应实现游客端和管理端的实时同步；
- c) 支持地图的版本管理，保存历史地图版本，当地图更新出现问题时，可快速回滚至历史版本；支持地图的备份和导出，防止地图数据丢失；同一时间只应有一个生效版本。

6.3.5 用户管理

应对系统用户进行统一管理和权限控制，应符合以下要求：

- a) 应根据使用角色对用户进行分类管理，至少包括：
 - 1) 游客用户：使用 AR 导览服务的普通参观者；
 - 2) 管理员用户：博物馆内部管理人员，负责内容更新、数据查看；
 - 3) 运维用户：系统维护人员，负责设备管理、故障处理；
 - 4) 超级管理员：拥有全部权限的系统管理员。
- b) 不同角色应被授予完成其职责所必需的最小数据访问和操作权限。权限设置应细化至功能模块级或数据项级；
- c) 管理员和运维用户访问后台系统应采用强身份认证措施，宜采用双因素认证；
- d) 所有用户的关键操作应记录操作日志，包括操作人、操作时间、操作内容、操作结果等信息。日志留存时间不宜少于 1 年；
- e) 游客用户数据的采集、存储和使用应符合 10.2 的要求，并经过用户授权。游客可查看和删除个人数据；
- f) 应实现游客和管理员的分级用户管理，包括用户注册、身份认证、账号信息管理、密码重置、账号冻结/解冻等功能；支持手机号、微信、支付宝等多种注册/登录方式；
- g) 对管理员用户应建立精细化的角色权限管理体系，划分超级管理员、内容管理员、设备管理员、运营管理员等不同角色，为每个角色授予完成其职责所必需的最小操作权限。

7 技术要求

7.1 定位与导航

7.1.1 定位精度性

定位精准性应满足以下要求：

- a) 在展厅内实现亚米级定位精度，水平定位误差不宜超过 1 米。重点展区或关键节点的定位精度宜优化至 0.5 米以内；
- b) 系统输出的设备朝向角度误差不宜超过 6 度。

7.1.2 定位连续性

定位连续性应满足以下要求：

- a) 用户首次进入展厅或应用启动时，系统完成定位初始化的时间宜控制在 3 秒以内。重定位时间不宜超过 1.5 秒；
- b) 在正常步行（0.5m/s~1.5m/s）速度下，无定位断点、位置跳跃、漂移等情况；应保持连续定位输出，定位数据更新频率不宜低于 10 Hz。在展厅遮挡、人员密集等复杂场景下，定位中断时间应≤3 秒，且恢复后无明显位置偏差；
- c) 系统应支持跨楼层自动识别，楼层切换延迟不宜超过 2 秒，跨楼层定位误差不宜超过 2 米。

7.1.3 跟踪稳定性

在识别成功后，虚拟内容相对于真实世界锚定点的位置和角度应保持稳定，宜满足以下要求：

- a) 在用户正常移动过程中，虚拟物体相对于真实世界锚定点的位置偏移量不宜超过 5 cm。静态观察时，位置抖动幅度宜小于 2 mm；
- b) 虚拟物体相对于真实世界锚定点的角度漂移不宜超过 2 度/秒。静态观察时，角度抖动幅度宜小于 0.5 度；
- c) 应具备周期性误差校正机制，可通过识别环境中的参考标记校正累积漂移。校正后位置误差不宜超过 3cm；
- d) 连续跟踪 5 分钟以上，虚拟物体的累积漂移不宜超过初始位置的 10%。

7.2 交互技术

AR交互技术应符合T/ZGCIT-0XX 2026 AR文物展示交互技术要求的要求。

7.3 系统集成与接口

应提供开放的标准化API接口，实现与博物馆现有外部系统间的数据安全交换与业务协同，应符合以下要求：

- a) 应提供以下三类接口：
 - 1) 数据服务接口：支持文物数据、展品信息、用户数据等查询与交换；
 - 2) 业务协同接口：支持导览数据与票务系统、客流系统的联动；
 - 3) 管理接口：支持远程内容更新、设备状态监控等管理功能。
- b) API 接口应采用 RESTful 架构风格设计，接口定义应清晰规范，提供完整的接口文档；
- c) 应支持 JSON、XML 等主流数据格式和 HTTP/HTTPS、MQTT 等主流传输协议；
- d) 应实现与博物馆藏品管理系统的数据交换，支持文物基础信息、三维模型、多媒体资源的同步更新；
- e) 应支持与票务系统对接，获取分时预约数据、实时入馆人数等信息，为客流预警和动态路线规划提供数据支撑；
- f) 接口访问应采用身份认证机制，敏感数据传输应采用 TLS 1.2 及以上安全协议加密；
- g) 接口调用应有访问频率限制和流量控制，接口日志应记录调用信息，日志留存时间不宜少于 6 个月。

7.4 系统可靠性

7.4.1 服务可用性

核心导览服务（包括定位导航、AR内容呈现、用户交互）的月度可用性应不低于99.5%；系统全年计划外停机时间累计不宜超过44小时。

7.4.2 故障处理

7.4.2.1 故障分级

应根据故障影响范围和紧急程度，将故障分为以下级别：

- a) 一级故障（重大故障）：系统整体不可用，或核心功能完全丧失；
- b) 二级故障（严重故障）：部分功能不可用；
- c) 三级故障（一般故障）：非核心功能异常；
- d) 四级故障（轻微故障）：界面显示异常、个别用户操作不畅等轻微问题。

7.4.2.2 恢复时间目标

各级故障的恢复时间应满足以下要求：

- a) 一级故障：RTO 不宜超过 2 小时；
- b) 二级故障：RTO 不宜超过 4 小时；
- c) 三级故障：RTO 不宜超过 12 小时；
- d) 四级故障：可在后续版本迭代中修复。

7.4.3 并发支持能力

7.4.3.1 系统宜支持在展厅热点区域同时服务不少于 1000 名用户的并发访问。节假日高峰期，可根据用户并发量自动调整服务器资源，并发支持能力宜扩展至 5000 用户以上。

7.4.3.2 在额定并发用户数内，核心接口的平均响应时间宜小于 200 ms。用户操作界面响应时间不宜超过 1 秒。

7.4.3.3 当并发请求超过系统设计容量时，应启动过载保护机制，对部分非核心请求进行限流或排队。

7.4.4 数据备份与恢复

数据备份与恢复应满足以下要求：

- a) 核心服务应采用集群化部署，关键服务器和网络设备应配置硬件冗余，避免单点故障导致服务中断。系统应支持故障自动检测和切换，切换时间不宜超过 5 分钟；
- b) 对于关键业务数据，宜采用实时备份机制。应支持每日进行增量备份，每月进行一次全量备份；
- c) 备份数据应与生产数据分离存储，重要备份数据宜采用“两地三中心”的存储策略，即本地备份、同城灾备、异地容灾相结合。
- d) 应定期进行恢复演练，RTO 不宜超过 4 小时，RPO 不宜超过 24 小时；每次备份后应对备份数据的完整性和可读性进行验证；
- e) 全量备份宜保留至少 3 个月，年度备份宜长期保存。

7.5 国产化支持能力

7.5.1 硬件国产化要求

硬件国产化应满足以下要求：

- a) 服务器、存储设备、网络设备等核心硬件宜优先选用通过国家相关认证的国产产品。芯片宜选用飞腾、海光、龙芯、兆芯等国产 CPU；
- b) 面向公众的 AR 导览终端（如手持设备、AR 眼镜）宜优先选用国产终端产品；
- c) 供应链安全：硬件供应链应清晰可追溯，关键元器件应具备稳定的国产供应渠道。

7.5.2 软件国产化要求

- a) 服务器端宜优先选用国产操作系统；终端设备宜适配国产桌面操作系统；
- b) 宜优先选用国产数据库管理系统，数据库应支持主流的国产 CPU 和操作系统平台；
- c) 应用服务器中间件宜优先选用国产产品，中间件应支持 Java EE 标准，具备集群和扩展能力；
- d) 宜使用国产开发框架和开发工具，支持国产 IDE、国产 JDK 等开发环境。开发框架应具有良好的生态兼容性和技术文档支持。

7.5.3 系统在架构设计、数据格式、接口协议等方面应考虑国产化生态兼容。

8 内容制作与管理

应符合 T/ZGCIT-0XX 2026 AR 文物数字化资源制作规范的要求。

9 运维管理

9.1 日常监控与维护

应建立 7×24 小时系统监控机制，应符合以下要求：

- a) 监控宜覆盖以下关键要素：
 - 1) 服务器监控：CPU 使用率、内存占用率、磁盘空间使用率、系统负载、服务器在线/离线状态；
 - 2) 数据库监控：数据库连接数、慢查询数量、事务处理响应时间、数据文件增长趋势；
 - 3) 网络监控：网络流量、网络延迟、丢包率、核心网络设备状态；
 - 4) 应用服务监控：核心 API 接口可用性、接口响应时间、并发用户数、服务错误率；
 - 5) 终端设备监控：AR 终端设备在线状态、设备电量、设备温度、软件版本。

- b) 关键监控指标应设置合理的告警阈值，包括但不限于：
 - 1) CPU 使用率持续 5 分钟超过 85%时应告警；
 - 2) 内存使用率持续 5 分钟超过 90%时应告警；
 - 3) 磁盘空间剩余不足 20%时应告警；
 - 4) 服务可用性低于 99.5%时应告警。
- c) 应具备多渠道实时告警功能，通过短信、邮件、系统消息、微信公众号等方式向运维人员推送告警信息，告警响应时间 ≤ 30 分钟；建立告警分级处理机制，按紧急程度将告警分为一级、二级、三级，实施差异化的处理流程；
- d) 应建立设备维护机制，对馆用 AR 导览设备、网络设备、服务器等硬件设备每周至少进行 1 次现场巡检，及时发现并解决设备硬件故障、老化、损坏等问题；对软件系统每月至少进行 1 次漏洞扫描和性能优化；
- e) 应建立完善的运维日志管理体系，记录系统监控数据、告警信息、故障处理过程、设备巡检记录、系统优化操作等，运维日志保存周期 ≥ 1 年。

9.2 备份与更新

9.2.1 应制定标准化的系统内容更新、发布与回滚流程，内容更新需经过“编辑→审核→灰度发布→全量发布”四个环节，灰度发布应选择 $\leq 10\%$ 的小范围用户进行测试，测试通过并解决发现的问题后，再进行全量发布。

9.2.2 系统软件应进行定期更新和升级，包括功能优化、漏洞修复、性能提升、国产化兼容优化等，更新升级应选择博物馆非开放时间或低峰时段进行，并提前向游客发布公告。

9.2.3 客户端应支持自动更新和手动更新两种方式，更新包应进行轻量化处理，减小包体大小，减少用户下载时间和流量消耗；更新过程应支持断点续传。

9.2.4 应具备系统更新回滚机制，当系统更新、内容发布后出现故障或问题时，运维人员应能在 30 分钟内完成回滚操作，恢复至更新前的正常版本。

10 安全保障

10.1 物理环境安全

系统服务器及核心网络设备应托管在符合安全要求的机房环境中，应符合以下要求：

- a) 机房选址应避免易发生自然灾害的区域，机房内部布局应合理划分功能区域，包括主机区、网络区、电源区、监控区等，应符合 GB/T 2887-2011 的要求；
- b) 机房出入口应部署门禁系统，对进入人员进行身份验证和访问记录。重要区域宜采用双因素认证，未经授权人员不得进入机房核心区域；
- c) 机房宜配备温湿度监控系统，温度宜控制在 $20^{\circ}\text{C}\sim 25^{\circ}\text{C}$ ，相对湿度宜控制在 $40\%\sim 60\%$ ；
- d) 机房应配备 UPS，后备时间不宜少于 30 分钟。关键设备应采用双路供电；
- e) 机房内应部署 7×24 小时视频监控系统，监控录像保存时间不宜少于 90 天。

10.2 数据安全

10.2.1 数据加密

10.2.1.1 不同用户的数据应在逻辑上进行隔离，防止越权访问。测试环境不得使用生产环境的真实用户数据。

10.2.1.2 对用户个人信息的处理应符合 GB/T 35273-2020 的要求，遵循最小必要原则，仅收集实现系统功能所必需的个人信息，不收集无关信息；用户个人信息的存储期限应与使用目的相匹配。

10.2.1.3 用户个人信息、行为轨迹、交互记录等敏感数据在数据库中应加密存储。宜采用国密算法进行数据加密，加密密钥与加密数据分开存储。密钥更换周期不宜超过 1 年，重要密钥应建立备份和恢复机制。密钥管理应符合 GB/T 39786-2021 的规定。

10.2.1.4 数据在非生产环境使用时，应进行脱敏处理，去除姓名、手机号、身份证号等敏感字段。

10.2.2 访问控制

10.2.2.1 应根据业务需求定义系统角色，宜至少包括：

- a) 游客角色：可访问与导览服务相关的公开内容；
- b) 内容管理员：可管理 AR 数字内容的发布、更新、下线；
- c) 数据管理员：可查看运营数据看板，但不可修改系统配置；
- d) 系统管理员：可管理系统配置、用户权限、设备状态；
- e) 审计管理员：可查看系统日志，但不可修改系统和数据。

10.2.2.2 权限分配应严格遵循最小权限原则，仅授予完成本职工作所必需的最小权限集。权限设置应细化至功能模块级或数据项级。

10.2.2.3 权限申请、审批、授予、变更、撤销应有规范的流程和记录。权限变更应在 24 小时内生效，人员离职时权限应立即撤销。

10.2.2.4 应定期对权限分配情况进行审计，检查是否存在权限冗余、越权等情况，并及时调整。审计记录应保存备查。

10.2.2.5 管理员和运维人员访问后台系统应采用双因素认证。

10.3 网络安全

10.3.1 网络防护

10.3.1.1 系统网络边界与互联网之间应部署防火墙，实施访问控制策略。防火墙规则应遵循最小开放原则，仅开放业务必需的端口和服务。

10.3.1.2 应在网络关键节点部署入侵检测系统或入侵防御系统，对网络攻击行为进行实时监测和阻断。检测规则应定期更新。

10.3.1.3 对于 Web 端应用，应部署 Web 应用防火墙，防范 SQL 注入、跨站脚本、CC 攻击等常见 Web 攻击。

10.3.1.4 应根据业务重要性进行网络分区，将核心业务区、办公区、测试区等不同安全域进行逻辑隔离。核心业务区与其他区域之间应部署防火墙。

10.3.1.5 关键网络设备应采用冗余部署，避免单点故障。冗余设备应支持故障自动切换，切换时间不宜超过 20 分钟。

10.3.1.6 应建立网络攻击应急处置机制，当发生网络攻击时，应能快速阻断攻击、排查问题、恢复网络正常运行，并及时记录攻击事件的详细信息，形成应急处置报告。

10.3.2 安全审计

10.3.2.1 审计日志应覆盖以下内容：

- a) 网络安全日志：防火墙、IDS/IPS 等安全设备的运行日志、告警日志；
- b) 访问日志：用户访问记录、API 调用记录、登录/登出记录；
- c) 操作日志：管理员操作记录、权限变更记录、配置修改记录；
- d) 数据库日志：数据查询、修改、删除操作记录。

10.3.2.2 每一条审计日志应包含时间戳、操作用户/源 IP、操作类型、操作对象、操作结果等信息。

10.3.2.3 审计日志应受到保护，防止被未授权访问、修改或删除。日志文件宜采用防篡改技术。

10.3.2.4 网络安全日志、访问日志、操作日志的留存时间不宜少于 6 个月。重要系统的关键日志宜延长留存至 1 年以上。

10.3.2.5 应定期对审计日志进行分析，发现异常行为和安全事件。可采用日志审计平台或 SIEM 系统进行集中分析和告警。