ICS 35.240
CCS L67

团　　体　　标　　准

T/DGAG 027—2024

博物馆数据安全管理规范

Specification of museum data security management

2024－11－22 发布　　2024－12－01 实施

广东省数字政务协会　　发 布

目　　次

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。

本文件由广东省数字政务协会归口。

本文件起草单位：广东省博物馆协会、广东省文化和旅游发展与保障中心、南越王博物院（西汉南越国史研究中心）、广东颐点科技有限公司、广东省数字政务协会、广东省文物考古研究院、广东省博物馆(广州鲁迅纪念馆)、广东民间工艺博物馆、广州博物馆、广州市文物考古研究院（南汉二陵博物馆）、东莞市博物馆、清远市博物馆、江门市博物馆、广州艺术博物院（广州美术馆）、辛亥革命纪念馆、鸦片战争博物馆、雷州市博物馆、广州市迪士普音响博物馆、暨南大学、华南农业大学、广东工业大学、广东外语外贸大学、广东工程职业技术学院、广州番禺职业学院、培黎职业学院、广东金桥百信律师事务所、深圳华图测控系统有限公司、广东联通通信建设有限公司、广州赛宝联睿信息科技有限公司、广东省科技基础条件平台中心、广州市信息安全测评中心、大湾实验室（广东）标准认证有限公司、佛山新东方电子技术工程有限公司、武汉山海文博科技有限公司、广州赛悦网络安全技术有限公司、中国联合网络通信有限公司广东省分公司、中国图片社有限责任公司、睿冠（广东）信息科技有限公司、同方知网数字出版技术股份有限公司、广州治明科学技术研究院有限公司、北方实验室（沈阳）股份有限公司、郑州云智信安安全技术有限公司。

本文件主要起草人：陈邵峰、王芳、黄青松、李碧燕、蔡嘉璇、董耀艺、易偲、彭清云、罗立宏、李竞贤、刘炜胜、江鸿生、曾长缨、刘学超、陈洪海、樊媛媛、黄兆麟、付东生、郭舒琳、肖洋、刘国栋、梁华斌、沈伟强、潘敏青、肖建祯、苏振宗、李历松、林晓彩、刘平波、史艳群、李亮文、王恒、李永恒、刘倩、王婷、沈惠敏、郭华生、李茂沛、陈志华、孔源源、蔡小岚、程润秀、曾剑锋、张立志、王东伟、刘俊波、钟宇城、陈庆忠、姚祖发、张濛沁、谢锋彩、卢瑞敏、屠晨阳、刘爽、唐小露、吴平贞、曹瑜、曾立坚、李鹭君、尹榕慧、邓颖琪、郝瑞、冯金龙、吴杨松、李伟坚、代金梅、陶乃顺、刘鑫、李绮琪、黄劲、朱思霖、杨建强、王升泰、高翀。

博物馆数据安全管理规范

1 范围

本文件规定了博物馆数据安全管理的术语和定义、数据范围，以及规范要求，包括数据采集与录入、数据加工与维护、数据存储与备份、数据传输与交换、数据授权与开放、数据分析与挖掘、数据展示与内容审核、应急管理与容灾备份、数据删除与销毁等环节的工作与管理要求。

本文件适用于博物馆及其数据处理团队对数据安全管理的实施和执行，也适用于管理监督工作。

本文件不适用于涉及国家秘密数据的安全管理。

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 42250—2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 34960.5—2018 信息技术服务 治理 第5部分：数据治理规范

GB/T 37092—2018 信息安全技术 密码模块安全要求

GB/T 43697—2024 数据安全技术 数据分类分级规则

WW/T0114—2023 可移动文物二维数字化采集与加工

WW/T0115—2023 可移动文物三维数字化采集与加工

3 术语和定义

下列术语和定义适用于本文件。

3.1

博物馆数据 museum data

博物馆在依法履行工作职责或开展业务活动采集、加工、存储、传输、使用、销毁等环节，以电子或者其他方式对信息的记录。

3.2

数据安全管理 data security management

为保障博物馆数据在生存周期中的真实性、完整性和可用性，所实施的管理措施和技术手段。

3.3

博物馆数据安全 museum data security

通过规范博物馆数据的安全服务与管理要求，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.4

数据生存周期 data life cycle

数据获取、存储、整合、分析、应用、呈现、归档和销毁等各种生存形态演变的过程。

［来源：GB/T 34960.5—2018，3.7］

3.5

数据分类分级 data classification and grading

根据数据的特性、业务需求和安全影响，对博物馆数据进行系统分类和分级管理的过程。

3.6

数据确权 data authentication

确定博物馆数据的权利属性、权利主体和权利内容，设置确定和行使数据权利的规则和程序架构。

3.7

数据产品 data products

基于博物馆数据加工形成的，可满足特定需求的数据加工品和数据服务。

3.8

数据处理团队 data processing team

按照博物馆的数据管理规范和安全要求，在数据生存周期各环节中，提供技术支持、数据处理和合规性审查等专业服务的博物馆内部机构或第三方机构。

4 数据范围

本文件的博物馆数据范围涵盖了数据生存周期中产生的各类主题数据，具体包括但不限于：陈列展示、公众服务、社会教育、藏品管理、保护修复、考古研究、文化创意、安防与消防管理、办公与运维等数据。各领域信息化业务主线职能和主题数据集见附录A.1。

5 规范要求

5.1 数据采集与录入

5.1.1 根据博物馆的业务需求和安全管理要求，使用安全的技术和工具，按照既定标准和流程采集各领域的主题数据，并完成数据录入工作。

5.1.2 数据采集与录入安全服务应包括不限于以下要求：

a) 数据采集范围与要求：应明确数据采集的范围和内容，严格遵循合法合规安全原则，采集的数据需符合业务需求；

b) 个人信息采集要求：涉及个人敏感信息收集应遵守《中华人民共和国个人信息保护法》规定，以最小影响方式、最小收集范围、最短保存期限为采集原则；

c) 数据采集技术与设备要求：应使用符合国产化要求的设备和工具，以及满足附录 A.2 数据采集安全能力的规定；采集完成后，需删除或销毁留存在非博物馆控制设备上的数据；

d) 数据采集精度要求：数据处理团队应参考 WW/T0114—2023、WW/T0115—2023 和博物馆的数据使用要求及不同数据类型的精度标准开展采集工作；

e) 数据录入标准与流程：应依据录入格式及 GB/T 43697—2024 分类分级管理的要求，有序完成数据录入工作。

5.1.3 数据采集与录入安全管理应满足以下要求：

a) 安全措施：应在数据采集与录入过程中实施数据加密、身份认证、访问控制等符合国家和行业标准的密码技术或相关措施，防止数据遭到篡改、破坏、泄露或者非法获取、非法利用。同时，应强化采集环境的防篡改、防病毒、防泄漏等安全功能，满足附录 A.3 的数据采集环境的要求；

b) 数据确权：参与各方签署的协议中，应包含数据确权的约定，明确数据的权利属性、主体和内容；

c) 管理职责：博物馆负责监督数据采集与录入过程的安全性、完整性和合规性，数据处理团队负责辅助按规则完成数据采集与录入工作。

5.2 数据加工与维护

5.2.1 根据博物馆的数据开放、应用、展示等业务需求，按照数据分类分级管理要求，对采集的领域主题数据进行加工与维护，保障数据安全性、完整性和可用性。

5.2.2 数据加工与维护安全服务应包括不限于以下要求：

a) 数据加工：应满足附录 A.2 加工安全能力要求，并在符合附录 A.3 的加工环境中，根据数据加工需求，对采集到的原始数据进行加工，包括格式转换、数据补全、细化、标注等操作；

b) 数据清洗与更新：应定期清洗数据，删除冗余或无效信息，并根据业务变化需求及时更新和维护数据；

c) 数据分类分级：应在数据加工过程中遵循既定的分类和分级标准（分类参考附录 B.1，分级参考附录 B.2），对数据进行分类和分级管理；
d) 数据加工过程备份：应根据数据安全级别要求进行数据备份，以便在数据加工过程中发生错误或意外时能够恢复到原始状态。

5.2.3 数据加工与维护安全管理应满足以下要求：
a) 流程管理：制定明确的数据加工与维护流程，监督数据处理团队的执行情况，并持续改进；
b) 权限管理：定期审核和更新数据加工操作权限，防止未经授权的操作，数据处理团队应按约定权限进行数据加工操作；
c) 可追溯性管理：应按可追溯性要求管理各环节流程的记录，包括数据的输入来源、加工方法、输出结果、操作人员等信息；
d) 管理职责：博物馆负责监督数据处理团队的日常数据加工与维护工作，确认各项操作符合安全性、合法性和规范性要求。

5.3 数据存储与备份

5.3.1 根据博物馆数据分类的安全要求，采用相应的加密技术和措施，将采集和加工后的主题数据存储在符合国产化要求的存储介质上，以防止未经授权的访问和数据泄露。

5.3.2 数据存储与备份安全服务应包括不限于以下要求：
a) 数据加密与存储：应确认数据的存储符合博物馆数据分类（见附录 B.1）的加密技术（商用密码、普通密码或核心密码）要求，并遵循国家标准进行存储；
b) 数据备份策略：应按数据分类分级管理要求定期备份各类型数据，核心数据和重要数据应同步进行异地备份存储；
c) 数据恢复机制：应建立数据恢复机制，明确恢复目标、流程和时间等，并定期演练以提高恢复的可靠性；
d) 存储系统的性能监控：定期监控数据存储系统的性能，包括存储容量、读写速度和故障率等，及时发现并解决潜在问题；
e) 数据安全评估：应建立数据安全评估机制，并定期开展数据安全评估服务，检查博物馆数据的合规性、完整性及潜在风险，以及根据评估结果优化数据安全策略。

5.3.3 数据存储与备份安全管理应满足以下要求：
a) 存储介质要求：核心数据和重要数据应存储在符合国产化要求的本地或私有云存储介质上，不应存储于公有云平台，以防止数据泄露；
b) 安全措施：应制定并实施数据存储与备份管理措施，包括数据加密、访问控制、身份认证、物理安全、定期核查等措施；
c) 备份管理：应从数据完整性和可用性角度实施备份策略，包括制定计划、执行任务、监控进度、验证完整性、管理存储介质等；
d) 恢复管理：应定期演练数据恢复，验证恢复机制的有效性；
e) 职责分工：博物馆负责数据的安全存储与备份管理，数据处理团队协助完成数据备份与恢复工作。

5.4 数据传输与交换

5.4.1 根据博物馆的数据共享和业务需求，采用符合行业标准的传输与交换方式及加密技术，保障数据传输与交换的完整性、保密性和可靠性。

5.4.2 数据传输与交换安全服务应包括不限于以下要求：
a) 脱敏处理：在数据传输与交换前，应根据数据的敏感级别对关键字段进行脱敏处理，以防止敏感信息的泄露；
b) 加密传输：根据数据级别，采用与之相匹配的核心密码、普通密码或商用密码应用要求的加密技术，防止数据在传输过程中被截获、篡改或泄露；
c) 身份验证：从数据发送方与接收方的身份真实性角度，实施多因素认证或其他安全验证措施；
d) 传输记录：按《中华人民共和国网络安全法》第二十一条要求，应留存相关的传输记录不少于六个月，包括传输时间、发送方与接收方、数据概要及结果等信息；

e） 交换安全：在数据交换过程中，应采用安全通道和加密技术，防止数据泄露和篡改；
f） 数据完整性校验：应使用哈希校验、数字签名、区块链等技术手段，验证数据传输的完整性，防止数据在传输与交换过程中被篡改或被损坏。

5.4.3 数据传输与交换安全管理应满足以下要求：

a） 流程管理：应制定并执行标准化的传输流程，包括传输的准备、执行、监控、结束等环节；
b） 交换协议：与交换方共同制定数据交换协议，明确数据范围、权限、责任和安全要求；
c） 安全管理：定期验证和更新数据传输与交换的安全手段，并监控加密、身份验证和传输通道的安全状况；
d） 异常处置：根据应急处置机制，记录并分析异常情况，以及按照流程完成修复工作；
e） 跨境数据交换审查：涉及跨境数据交换时，应同时遵循交换地区的法律法规和标准，满足合规性和安全性要求；
f） 职责分工：博物馆负责流程管理和监控，数据处理团队协助完成传输加密、身份验证及异常处置等任务。

5.5 数据授权与开放

5.5.1 根据博物馆在数据授权使用、公共数据开放、学术数据共享、政府及机构数据对接和数据开放平台等方面的需求，向公众或特定用户群体提供经过授权的部分数据资源的访问和下载服务，促进博物馆数据的合理利用与共享。

5.5.2 数据授权与开放安全服务应包括不限于以下要求：

a） 数据授权范围与权限：应明确数据授权与开放的范围和权限，授权开放的数据不应包含敏感信息，同时应符合相关法律法规和标准要求；
b） 用户访问与下载服务：应提供便捷且安全的数据访问和下载方式，并在符合合规性的前提下，监控和记录用户的访问和下载行为；
c） 开放数据的更新与维护：应按更新机制定期维护授权开放的数据，并根据业务需求和用户反馈对机制进行调整和优化。

5.5.3 数据授权与开放安全管理应满足以下要求：

a） 审查与发布流程：建立并实施数据授权与开放的多级审核机制，核实发布流程及数据内容的合规性，并记录数据选择、审核、发布、更新等环节的信息；
b） 合规性审查：应根据法律法规和部门规章及地方性法规和规章，对数据授权与开放过程，以及个人隐私和知识产权保护等方面开展合规性审查；
c） 安全控制措施：实施必要的数据开放安全控制措施，包括管理用户数据访问权限、限制数据下载和记录数据开放情况，并定期进行安全评估；
d） 职责分工：博物馆负责数据开放的审查、发布及日常维护工作，数据处理团队协助合规性审查。

5.6 数据分析与挖掘

5.6.1 根据博物馆提升数据感知能力、管理效能等需求，按照既定的安全管理流程，利用数据分析与挖掘技术对多维数据进行深度分析，发掘潜在价值，形成可用于流通与交易的数据产品，支持博物馆的数据应用。

5.6.2 数据分析与挖掘安全服务应包括不限于以下要求：

a） 数据准备：根据博物馆数据产品的高可靠性和流通性要求，在分析前对数据进行清洗准备，包括数据质量检查、去重、补全等操作，以满足分析需求；
b） 分析方法与工具：根据数据挖掘的复杂性和多样性需求，采用经过验证的分析方法和符合国产化要求的分析工具；
c） 数据安全保护：为防止分析与挖掘过程中的数据泄露或篡改，应根据数据级别采取相应的加密、访问控制、数据脱敏、分级权限管理等安全管理措施；
d） 分析结果管理：对数据分析与挖掘形成的数据产品等成果，应进行标注并分类存储于符合国产化要求的介质中，在授权前提下对流通与交易进行管理。

5.6.3 数据分析与挖掘安全管理应满足以下要求：

a) 权限管理：通过数据访问、工具应用和结果访问权限等管理措施，控制仅授权人员可访问和加工数据；
b) 安全监控：采用数据加密、日志记录和异常检测等监控措施，对数据分析与挖掘过程进行监控，防止数据泄露和滥用；
c) 结果验证与审核：检查分析方法的合理性及结果数据的完整性和脱敏情况，并对分析结果进行验证和审核，以提升结果的准确性和可靠性；
d) 职责分工：博物馆负责数据分析过程和成果的安全管理，数据处理团队负责数据的整理、分析与挖掘，将结果转化为可用于流通和交易的合规数据产品。

5.7 数据展示与内容审核

5.7.1 根据博物馆的数字化展览、多平台数据展示、交互式展示体验等需求，按照内容审核安全管控流程，结合数字化技术手段，实现文物数字模型及相关信息的高效和可控展示，全面提升参观者的多维观展体验感。

5.7.2 数据展示与内容审核安全服务应包括不限于以下要求：

a) 展示内容的设计与开发：根据展示主题和互动体验需求，设计和开发数字展示内容，并审核展示数据的合规性和准确性；
b) 展示技术的应用：选用符合国产化要求的数字展示技术，包括虚拟现实（VR）、增强现实（AR）、混合现实（MR）、高精度数字化等展示技术，提供高质量和高可靠性的展示效果；
c) 数据安全保护：根据数据级别的安全要求，采用相应的数据加密和访问控制措施，包括角色权限管理（RBAC）、多因素认证（MFA）等，防止数据被篡改、复制或盗用；
d) 展示内容管理：基于数据的时效性和准确性，定期更新和维护展示内容，及时处理技术问题。

5.7.3 数据展示与内容审核安全管理应满足以下要求：

a) 展示系统的安全管理：负责展示系统的日常维护、软件更新和安全防护，防止外部及内部的攻击与滥用；
b) 内容管理与审查：制定并实施数据展示管理与审核安全机制，落实信息发布安全与保密，防止发布不准确或不合规的数据；
c) 内容知识产权管理：应遵循知识产权法律法规，对展示的文物、图像及其他文化资源等内容进行知识产权确权、管理和保护，避免侵权纠纷；
d) 访问权限管理：合理分配和控制展示系统的访问权限，严格控制管理主题策划人员、系统管理员、内容开发者和维护人员的权限；
e) 职责分工：博物馆负责建立数据展示与内容管理机制，数据处理团队协助完成内容设计和开发、系统维护、安全防护、知识产权管理等工作。

5.8 应急管理与容灾备份

5.8.1 根据博物馆对数据稳定供给的需求，建立数据应急管理和容灾备份机制，应对自然灾害、网络攻击、数据泄露等突发情况，保障数据的安全性和可恢复性。

5.8.2 应急管理与容灾安全服务应包括不限于以下要求：

a) 应急预案的制定与维护：制定并定期更新应急预案，涵盖自然灾害、网络攻击、数据泄露、勒索病毒等突发事件的处理方案；
b) 容灾备份：应根据数据的级别建立容灾备份机制，制定数据备份策略，包括备份方式、备份频率、存储介质、保存期限等内容；
c) 数据恢复：应制定数据恢复策略和恢复程序，并设置相关岗位职责，保障在突发事件后能迅速恢复数据；
d) 定期应急演练：定期组织应急演练，验证数据恢复、系统切换、数据泄露等事件应对机制的有效性，并记录演练过程、结果等信息。

5.8.3 应急管理与容灾安全管理应满足以下要求：

a) 应急预案监督管理：负责审核应急预案的可操作性，并定期评估预案的合理性和有效性；
b) 应急响应时间：应在发生突发事件后 24 小时内完成首次响应，并按照应急预案进行事件处置和数据恢复；

c) 备份与恢复管理协调：协调技术团队实施核心数据的异地备份和恢复操作，定期审查备份策略的有效性以及恢复时间目标的可行性；
d) 事件响应与跨部门协作：建立跨部门应急响应和沟通机制，突发事件发生时快速协调各部门行动，特别是在数据泄露事件中，及时响应并通报相关方；
e) 职责分工：博物馆负责整体预案的制定、演练和协调，数据处理团队协助备份实施、数据恢复、技术支持等工作。

5.9 数据删除与销毁

5.9.1 根据博物馆的数据生存周期管理要求，对达到保存期限或不再使用的数据实施删除或销毁，以防止数据泄露、滥用或非法恢复。

5.9.2 数据删除与销毁安全服务应包括不限于以下要求：
a) 制定流程：建立数据删除与销毁流程，包括数据标记、分类、审核岗位设置、处置方式等；
b) 处置方式：核心数据应使用物理销毁、磁盘粉碎等不可恢复的方法，重要数据应通过多次覆盖或专业数据擦除工具进行销毁，一般数据可采用删除或覆盖技术；
c) 记录与证明：在删除或销毁完成后生成记录，包含时间、方法、操作人员、数据类型等信息，并由数据责任人签字确认。

5.9.3 数据删除与销毁安全管理应满足以下要求：
a) 权限管理：建立多级审核流程，严格限制数据删除与销毁的授权操作，记录审核和执行过程；
b) 定期审查与监督：应定期审查删除与销毁活动，检查活动记录、评估删除与销毁方法有效性，并监督流程实施，防止疏漏或失误；
c) 职责分工：博物馆负责制定删除与销毁的计划与审查标准，并监督过程的合规性与完整性；数据处理团队负责执行数据删除与销毁操作并生成记录。

附 录 A
（规范性）
安全管理要求

A.1 博物馆数据范围

博物馆主要业务域分为陈列展示、公众服务、社会教育、藏品管理、保护修复、考古研究、文化创意、安防与消防管理、办公与运维，各领域信息化业务主线职能和主题数据集见表A.1。

表 A.1 博物馆业务主题数据集分类表

序号	业务域	信息化业务主线职能	主题数据
1	陈列展示	展览策划、设计、布展、展示物质和非物质遗产	展品信息、展示建模、展览（策划、设计、布展）文档、虚拟展览、观众评估与反馈数据等
2	公众服务	为满足公众参观、学习、研究等需求所提供的各种服务和活动	票务与预约、设施服务、导览服务、讲解服务、数字服务、信息咨询、会员信息、志愿者信息、社交媒体信息等
3	社会教育	向社会公众提供、组织、实施各种教育项目和活动	教育项目（专题讲座、工作坊与课程、学术研讨会、研学）、学校合作（校外课堂、教学资源开发、志愿服务）、社区教育（社区讲座与活动、流动博物馆、联合推广）、家庭教育（亲子活动、家庭教育资源）、线上教育（在线课程与讲座、数字教育资源）等
4	藏品管理	在收藏、保护、记录、研究和展示藏品过程中的实施方法、技术及管理过程	征集与鉴定、入藏登记、藏品档案、库房管理、保存与利用等
5	保护修复	指运用技术与方法对藏品进行保护和修复	环境监测控制、预防性保护、修复与保养等
6	考古研究	运用多种现代技术与考古学方法对考古遗址、遗物及其相关资料进行系统研究	考古调查、勘探和发掘项目档案，修复与保护数据、实验室分析数据、研究报告等
7	文化创意	开发和推广文化产品和服务活动	文化产品设计与开发、文化IP数字资源授权、知识产权、市场推广、公众参与等
8	安防与消防管理	为确保博物馆的正常运营和藏品的安全制定和实施一系列安防和消防管理活动	安防与消防系统管理、安全制度、风险评估、应急预案、人员培训、人员管理、安全检查记录等
9	办公与运维	支持博物馆各项业务和管理活动的顺利开展，保障日常运营、业务开展和观众服务的需求，涵盖行政事务、设施设备的运行维护及综合办公的管理过程。	行政事务处理、沟通与协作、人事管理、财务管理、采购管理、项目合同管理、会议记录、工作计划、决策支持、能耗管理、空调与通风、楼宇智能控制、设备监控、故障与维修、通信系统、办公设备、资产管理，以及项目实施过程数据等

A.2 数据采集与加工安全能力要求

根据博物馆的数据级别要求，数据采集和加工的安全能力应满足表A.2的要求。

表 A.2 采集安全能力和加工安全能力要求表

序号	数据级别	采集安全能力要求	加工安全能力要求
1	核心数据	1. 加密设备：采集设备需符合国家加密标准，支持端到端加密。 2. 物理隔离设备：采集环境中使用的计算机或网络设备应与外部网络物理隔离。 3. 数据采集软件：应具备数据完整性检查和追溯功能，避免数据在采集过程中被篡改。	1. 隔离网络环境：数据加工需在与外部网络隔离的内网中进行。 2. 加密软件：全程使用符合密码相关国家、行业标准要求的硬件密码模块或密码产品，通过高强度加密算法进行数据加工。 3. 安全追溯工具：应配备日志记录和追溯工具，便于定期审查所有操作。

表A.2　采集安全能力和加工安全能力要求表（续）

序号	数据级别	采集安全能力要求	加工安全能力要求
2	重要数据	1. 加密设备：采集设备需支持数据加密，以减少采集过程中的泄露风险。 2. 身份认证设备：使用双因素身份认证工具，限制数据采集权限。 3. 监控工具：实时监控采集设备和网络流量，防止数据被非法获取。	1. 加密工具：加工数据时需使用达到GB/T 37092—2018二级及以上安全要求的密码安全产品来保护数据传输和存储过程的安全性。对于网络安全产品，产品标准和技术要求应符合GB 42250—2022，其中重要网络边界安全设备应具备硬件层面丢弃非法数据包的安全防御能力。 2. 身份认证系统：采用多层次身份认证系统限制访问权限。 3. 日志记录工具：需记录数据加工操作，便于追踪。
3	一般数据	1. 安全采集设备：采集设备应具备基础数据保护功能，如加密或密码保护。 2. 备份工具：采集完成后及时使用备份工具保护数据完整性。	1. 基础加密工具：加工过程中使用达到GB/T 37092—2018一级及以上安全要求的密码安全产品，防止数据被篡改或丢失。 2. 防病毒软件：加工环境需安装防病毒和防火墙软件以加强安全性。

A.3　数据采集与加工环境要求

根据博物馆数据级别要求，数据采集环境和加工环境应满足表A.3的要求。

表 A.3 采集环境和加工环境要求表

序号	数据级别	采集环境要求	加工环境要求
1	核心数据	1. 采集需在高度安全的物理隔离环境下进行。 2. 使用符合国家安全标准的加密设备进行采集，确保数据传输过程安全。 3. 采集区域应实施严格的人员控制，只有授权人员可进入。	1. 加工环境应为物理隔离网络或高度安全的内部网络，确保外部无法访问。 2. 数据加工应全程加密，并有严格的权限管理和监控。 3. 定期进行安全审计，防止未经授权的操作。
2	重要数据	1. 采集可在受控网络环境下进行，设备应具备数据加密功能。 2. 强化监控数据采集过程，避免数据泄露。 3. 采集人员应经过授权并接受安全培训。	1. 加工环境应具备安全的网络保护（如防火墙、入侵检测等）。 2. 数据应在加密的网络中传输和存储。 3. 数据加工操作应有详细的日志记录，以便追溯。
3	一般数据	1. 采集可在常规的网络环境下进行，但应使用博物馆标准的安全设备。 2. 数据采集完成后应及时备份。 3. 采集人员应遵守基本的安全规范。	1. 数据加工环境应有基础的安全防护措施（如防火墙、防病毒软件）。 2. 数据加工不需要严格隔离，但应定期检查系统的安全状况。 3. 加工过程中应避免数据丢失或篡改。

附 录 B
（资料性）
数据分类分级规范

B.1 博物馆数据分类参考

从数据描述对象角度，将博物馆数据分为用户数据、业务数据、经营管理数据、系统运维数据四个类别，数据分类参考见表B.1。

表 B.1 博物馆数据分类示例

序号	数据类型	定义	示例	安全要求
1	用户数据	博物馆在开展业务服务过程中从个人用户或组织用户收集的数据，以及在业务服务过程中产生的归属于用户的数据	票务与预约记录、会员信息、志愿者信息、信息咨询记录、导览服务数据、社交媒体数据	强制进行机密性与完整性保护存储，严格访问控制，保障用户隐私不泄露，符合《中华人民共和国个人信息保护法》要求
2	业务数据	在博物馆业务的研发、生产、运营过程中收集和产生的非用户类数据	展品信息、展览（策划、设计、布展）文档、观众评估与反馈数据、藏品档案、教育项目数据、考古调查与发掘记录	权限分级管理，保障数据的机密性和完整性，定期备份以防数据丢失或损坏
3	经营管理数据	博物馆在经营和内部管理过程中收集和产生的数据	财务管理记录、人事管理数据、采购管理数据、项目合同管理记录、会议记录、工作计划与决策支持数据	分级访问控制，并进行机密性、完整性保护，保障敏感财务及人力资源数据的安全，符合相关法律法规
4	系统运维数据	可能对博物馆的正常运营或涉及隐私的敏感信息	安防与技防系统数据、环境监测与控制数据、设备监控与维护记录、能耗管理数据、楼宇智能控制数据、故障与维修数据	监控和日志分析，定期安全审计，及时处理安全漏洞，防止网络安全事件
注1：依据GB/T 43697—2024《数据安全技术 数据分类分级规则》附录A的“A.1 基于描述对象的数据分类参考”。 **注2：**真实性——身份鉴别；机密性——加密解密；完整性——防篡改保护；不可否认性——抗抵赖保护。				

B.2 博物馆数据分级参考

根据数据在博物馆发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为核心数据、重要数据、一般数据三个级别。博物馆数据分级参考见表B.2。

表 B.2 博物馆数据分级示例

序号	数据级别	定义	示例	影响范围
1	核心数据	涉及国家文化安全、重要文物或历史遗产的关键数据，任何损失或使用不当都会对国家或文化遗产造成无法弥补的损害	藏品档案、考古发掘记录、重要文化遗产的保护修复数据	数据一旦泄露、篡改或非法获取，将对国家安全、社会秩序或公共利益造成严重影响
2	重要数据	涉及博物馆核心业务和运营的敏感数据，损害可能导致博物馆运营受阻、经济损失或公众信任度下降	财务数据、博物馆人员信息、展览策划与设计文档、会员信息、教育项目数据	数据泄露或篡改可能影响博物馆的正常运营、经济利益或公众的信任度
3	一般数据	日常运营中产生的普通数据，虽然影响较小，但仍需适当保护，以维持博物馆的日常运作和公众信任	票务与预约记录、访客反馈数据、设施维护记录	数据泄露或篡改对国家安全或博物馆运营影响较小，但可能影响公众感知或博物馆内部流程
注：依据GB/T 43697—2024《数据安全技术 数据分类分级规则》“6 数据分级规则”。				

参 考 文 献

[1]GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2]GB/T 25069—2022 信息安全技术 术语
[3]GB/T 31219.3—2014 图书馆馆藏资源数字化加工规范 第3部分：图像资源
[4]GB/T 31219.5—2016 图书馆馆藏资源数字化加工规范 第5部分：视频资源
[5]GB/T 35273—2020 信息安全技术 个人信息安全规范
[6]GB/T 37092—2018 信息安全技术 密码模块安全要求
[7]DB33/T 2487—2022 公共数据安全体系建设指南
[8]WW/T 0024—2008 文物保护工程文件归档整理规范
[9]T/ISC 0048—2024 数据确权风险控制通则
[10]ISO/IEC 27001:2022 信息安全—网络安全—隐私保护—信息安全管理体系要求
[11]中华人民共和国网络安全法
[12]中华人民共和国数据安全法
[13]中华人民共和国密码法
[14]中华人民共和国个人信息保护法
[15]网络数据安全管理条例
[16]《博物馆运行评估办法》《博物馆运行评估标准》（文物博发〔2022〕28号）
[17]TP309.2;D63;G259.2 数字生态视角下公共数据安全保障体系研究