ICS 35.240.01
CCS L 70

DB37

山　东　省　地　方　标　准

DB37/T 4844—2025

人工智能系统的服务连续性　治理要求

Service continuity for artificial intelligence systems—Governance requirements

2025－05－24 发布　　2025－06－24 实施

山东省市场监督管理局　　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　训练数据 2
6　算法模型 2
7　算力中心 2
8　推理平台 3
9　系统运维 3
10　保障机制 5
参考文献 6

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。

本文件由山东省工业和信息化厅提出并组织实施。

本文件由山东省人工智能标准化技术委员会归口。

人工智能系统的服务连续性　治理要求

1　范围

本文件规定了人工智能系统在训练数据、算法模型、算力中心、推理平台、系统运维，以及保障机制等方面为实现服务连续性遵循的基本要求，描述了对应的治理方法。

本文件适用于规范人工智能系统的规划、设计、开发、运行和维护。

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 20984　信息安全技术　信息安全风险评估方法

GB/T 20988　信息安全技术　信息系统灾难恢复规范

GB/T 31722　信息技术　安全技术　信息安全风险管理

GB/T 36957　信息安全技术　灾难恢复服务要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

人工智能　artificial intelligence；AI

<学科>人工智能系统相关机制和应用的研究和开发。

[来源：GB/T 41867—2022，3.1.2]

3.2

人工智能系统　artificial intelligence system

针对人类定义的给定目标，产生诸如内容、预测、推荐或决策等输出的一类工程系统。

注1：该工程系统使用人工智能相关的多种技术和方法，开发表征数据、知识、过程等的模型，用于执行任务。

注2：人工智能系统具备不同的自动化级别。

[来源：GB/T 41867—2022，3.1.8]

3.3

服务连续性　service continuity

能够不间断地提供服务，或按计划和约定提供一致的可用性。

[来源：ISO/IEC/IEEE 24765:2017,3.3711]

4　缩略语

下列缩略语适用于本文件。

RPO：恢复点目标（Recovery Point Object）

RTO：恢复时间目标（Recovery Time Objective）

5 训练数据

人工智能系统训练数据的治理要求应包括但不限于以下内容。

a) 数据安全：
   1) 数据来源可靠性，包括但不限于传感器、数据采集卡等设备不受信息攻击等安全威胁，避免数据采集中断；
   2) 采取加密措施保证数据的可靠传输，降低敏感数据泄漏风险；
   3) 数据存储在具有强大数据保护功能的冗余环境中，以实现可用性、服务连续性和快速恢复；
   4) 设置数据备份系统，数据备份系统符合 GB/T 36957 和 GB/T 20988 的规定；
   5) 设置备用数据处理系统，包括备用的计算机、外围设备和软件等；
   6) 在中断事件发生后及时核对重要数据，追补丢失数据。
b) 数据质量：
   1) 数据在时间序列上的连贯性，避免数据中断或缺失，确保数据的连续性；
   2) 收集到的数据包含所有必要的特征和信息，避免遗漏重要数据，确保数据的完整性；
   3) 数据能够真实反映实际情况，对模型训练产生积极影响，对数据进行适当的预处理，以提高数据质量，确保数据的有效性；
   4) 采用高精度的数据收集方法和技术，使用抽样检测与全部检测相结合的方式，检验数据是否能准确表示其所描述的实际对象，无误差或偏差，确保数据的准确性。

6 算法模型

人工智能系统算法模型的治理要求应包括但不限于以下内容。

a) 算法模型设计：
   1) 通过人工智能算法和模型调优，智能识别代码冲突与恶意代码；
   2) 使用模型加密、代码混淆等防止模型被逆向的技术手段，提高模型的防逆向性，避免被逆向出模型参数文件以及代码文件；
   3) 基于特定开源框架或第三方库开发的模型在框架或第三方库更新时，及时做出相应调整；
   4) 保证人工智能系统的迭代速率满足用户需求。
b) 算法模型应用：
   1) 在应用前编制并备份算法逻辑、体系及结构等技术文档；
   2) 在应用前进行风险评估和测试，针对可能出现的风险制定应对措施；
   3) 对算法使用情况及算法结果进行监管，动态监测算法的实际运行情况，发现算法漏洞并及时处理，降低由于算法不可验证、算法问题解决方案复杂等特性可能导致的中断风险。

7 算力中心

人工智能系统算力中心的治理要求应包括但不限于以下内容。

a) 物理基础设施要求：
   1) 具备稳定的电力供应和网络连接，包括配置应急电力设施，以及可靠的网络设备等；

2) 关键设备采用冗余配置，如双路供电、冗余冷却系统等，以确保在设备故障时能够迅速切换至备用设备，保障服务的连续性；
3) 机柜、线缆、光纤、消防安防等物理基础设施安全可靠，提供安全稳定的物理环境，防止因物理损坏导致服务中断。

b) 技术与系统要求：
1) 配置高可用性和容灾设备，如负载均衡器、缓存设备、容灾备份系统等，在发生故障时迅速恢复服务，减少业务中断时间；
2) 部署监控与管理系统对算力中心的运行状态进行实时监控和管理，及时发现并处理潜在故障。

8 推理平台

人工智能系统推理平台的治理要求应包括但不限于以下内容。

a) 平台性能要求：
1) 推理性能：采用经过深度优化的推理算法和引擎，利用先进的计算技术和加速库，提升推理速度和效率，确保在低延迟和高吞吐量下稳定运行；
2) 动态资源分配：具备基于需求动态调整资源的能力，根据推理任务的负载、优先级和实时性要求调度计算资源，确保资源高效利用和服务连续性；
3) 预推理：基于历史数据和用户行为模式，预测潜在的问题或需求，并进行相应的预处理和决策准备，增强系统的适应性和鲁棒性，确保平台持续稳定地提供服务；
4) 缓存机制：通过存储经常访问的数据或计算结果（如模型参数、中间计算结果等），以便在后续请求时快速响应，减少重复计算和访问原始数据源的时间，提升系统的推理速度，从而在面临高并发请求或复杂计算任务时，能够保持服务的连续性和高效性。

b) 故障快速恢复：
1) 建立自动故障检测和恢复机制，一旦发现故障，立即启动恢复程序，包括数据恢复、服务重启等步骤，确保服务的快速恢复和稳定性；
2) 对于无法自动恢复的故障，提供清晰的手动恢复指南和工具，指导运维人员快速完成恢复操作；
3) 采用冗余设计，如部署多个副本、使用负载均衡等，确保在部分节点故障时，其他节点能够接管任务，继续提供服务。

c) 用户机制：
1) 关注用户体验，提供友好、直观的用户界面和操作流程；
2) 实施用户身份验证、权限管理、数据加密等措施，防止未经授权的访问和数据泄露；
3) 定期对用户数据进行备份和恢复工作，确保数据的完整性和安全性；
4) 建立完善的用户服务机制，提供及时、专业的技术支持服务，持续改进推理服务的质量和用户体验。

9 系统运维

人工智能系统运维的治理要求应包括但不限于以下内容。

a) 风险评估：

1) 按照 GB/T 20984 和 GB/T 31722 规定的风险评估要求，定期开展面向人工智能系统服务连续性的风险评估，对人工智能系统服务及其依赖资源的中断风险进行识别、分析和评估；
2) 根据风险评估结果制定人工智能系统服务连续性计划，包括预防、处置、恢复等内容，并对计划定期进行更新维护和评估改进；
3) 收集来自监管机构、公共服务机构、供应商、业务关联机构等发布的预警信息，并及时采取措施预防可能发生的服务中断事件。

b) 系统使用：
1) 提供人工智能系统的服务应用说明并确保使用通俗易懂的语言，包括系统的功能、使用方法、配置信息、管理员信息、常见故障的解决方法等内容；
2) 考虑用户操作的可能性，避免用户操作多样化导致服务中断；
3) 在人工智能系统使用过程中实时监测异常流量，发现并阻止设备或网络攻击，提高人工智能系统网络安全水平；
4) 提供应急联系途径，接收来自用户或其他相关方的服务中断事件投诉或通知信息，对这些信息进行记录，通知相关部门进行核实和处置。

c) 资源保障：
1) 人工智能系统相关供应商的服务连续性；
2) 设置备用网络系统，包含备用网络通信设备和备用数据通信线路。备用网络系统的要求符合 GB/T 36957 的要求；
3) 识别并备份恢复系统服务所需的最低资源保障，包括系统、数据、基础设施、办公场所、通讯设施、保障设施、人员、供应商、文档等；
4) 根据需要，与相关机构签订协议，以便在服务中断事件发生后可获取所需的资源或服务。

d) 更新维护：
1) 对人工智能系统发起的计划内服务更新维护，提前告知用户可能影响的系统功能及维护时间；
2) 人工智能系统的计划内服务更新维护，选择服务使用率较低时计划维护；
3) 人工智能系统因计划外事件而影响服务交付时，告知用户可能影响的系统功能及预计恢复时间。

e) 事前规划：
1) 设计和部署备用系统，确保在主系统不可用时能够迅速切换，保持业务持续运行，定期进行备用系统的测试和演练，确保其可用性和可靠性；
2) 确定人工智能系统恢复的 RTO 和 RPO，服务恢复优先级别和资源需求等；
3) 制定并实施定期数据备份计划，将重要数据存储在安全的地方，在发生灾难时，利用备份数据快速恢复系统和业务操作；
4) 明确故障排查的步骤和方法，制定故障修复流程，包括临时解决方案的采用，以保证业务在修复期间的可用性；
5) 部署实时监控工具，对人工智能系统的运行状态进行持续监控，设置预警机制，当系统性能出现异常或即将达到阈值时，及时发出预警通知。

f) 事后审查：
1) 在影响人工智能系统服务连续性的计划外事件解决后进行审查并编制审查报告，包括用户体验和影响、事件开始和结束日期/时间、影响和解决措施的详细时间表，根本原因分析和为持续改进而采取的行动等；

2） 审查应急响应团队在中断事件中的表现，包括响应速度、协调能力、资源调配等，分析应急响应流程的有效性，识别流程中的瓶颈和不足之处；
3） 评估恢复策略的实施效果，包括备用系统的切换速度、数据恢复的准确性等，分析恢复过程中遇到的挑战和解决方案，为后续改进提供参考；
4） 将中断事件的事后审查结果纳入组织的知识管理体系，供组织内部分享；
5） 识别服务中断可能造成的经济损失、非经济影响等。

10 保障机制

人工智能系统服务连续性的保障机制要求应包括但不限于以下内容。

a） 组织管理：
1） 明确人工智能系统服务连续性管理的组织架构，确定各层级人员在服务连续性管理过程中的职责和分工；
2） 制定服务连续性管理制度和计划，或在相关制度中说明与人工智能服务连续性管理有关的要求；

注：服务连续性计划中一般规定保障服务连续性的措施，以及如何有效应对服务中断事件，通常包括对更详细的恢复计划的引用，以及将系统恢复到工作状态的具体说明。

3） 定期管理和维护服务连续性制度和计划，开展人工智能系统服务连续性计划演练。

b） 人员管理：
1） 为人员提供人工智能系统服务连续性管理培训和专业技能培训；
2） 为关键岗位安排备份人员；
3） 为关键操作程序安排交叉复核人员；
4） 制定人员继任计划；
5） 分散核心能力以减少中断事件的影响，如设立多个技术系统运营团队、多地办公等；
6） 建立保留知识和经验的文档；
7） 提升开发人员、运维人员等利益相关者的服务连续性意识，协同配合开展多元主体共治，将人工智能系统服务连续性治理融入到日常工作中。

参 考 文 献

[1] GB/T 30146—2023 安全与韧性 业务连续性管理体系 要求

[2] GB/T 41867—2022 信息技术 人工智能 术语

[3] GB/T 43782—2024 人工智能 机器学习系统技术要求

[4] ISO/IEC/IEEE 24765:2017 Systems and software engineering—Vocabulary

[5] ISO/IEC 42001:2023 Information technology—Artificial intelligence—Management system