ICS 35.240.01
L 70

DB37

山　　东　　省　　地　　方　　标　　准

DB 37/ XXXXX—XXXX

人工智能产品的服务连续性 治理要求

Service continuity for artificial intelligence products - Governance requirements

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

山东省市场监督管理局　　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。

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。

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。

人工智能产品的服务连续性 治理要求

1 范围

本文件规定了人工智能产品的服务连续性在数据、算法模型、服务应用、运维、组织等方面的治理要求。

本文件适用于人工智能产品的开发、应用和运维服务。

2 规范性引用文件

本文件没有规范性引用文件。

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（缩略语）
表现出与人类智能（如推理和学习）相关的各种功能的功能单元的能力。
[来源：GB/T 5271.28-2001，28.01.02]

3.2

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 概述

人工智能产品的服务连续性是智能化发展的基础，误操作、制度缺陷、技术缺陷和等因素都会影响人工智能产品的服务连续性。人工智能的核心在于数据的支撑，算法模型是人工智能技术在生产实践中真正落地、促进产业发展的重要保障，人工智能产品的服务应用会影响用户的直接体验，运维能够保证产品服务的持续运行，组织管理影响整个产品的发展。因此，应从数据、算法模型、服务应用、运维、组织五个方面对人工智能产品进行治理，以保证服务的连续性。

5 治理要求

5.1 对数据的治理要求

对数据的治理要求包括但不限于：

a） 应保证传感器不受信道攻击等安全威胁，以避免数据采集中断；
b） 应采取加密措施保证数据的可靠传输；
c） 应保证数据存储安全，对所用数据进行备份并确保数据可恢复。

5.2 对算法模型的治理要求

对算法模型的治理要求包括但不限于：
a） 算法模型在应用前应编制并备份算法逻辑、体系及结构等技术文档；
b） 算法模型在应用前应进行风险评估，针对可能出现的风险制定应对措施；
c） 在算法运行过程中应对其进行监管，动态监测算法的实际运行情况，发现算法漏洞等风险，及时处理。

5.3 对服务应用的治理要求

对服务应用的治理要求包括但不限于：
a） 应提供产品的服务应用说明，避免操作不当导致服务中断；
b） 应充分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；
c） 应设置产品反馈机制，及时发现、处理产品漏洞。

5.4 对运维的治理要求

对运维的治理要求包括但不限于：
a） 应定期对运维人员开展培训并建立完善的规章制度，避免运维操作不当造成服务中断；
b） 应保证人工智能产品的迭代速率满足用户需求；
c） 应建立应急管理工作机制，编制应急预案并定期演练，保证在服务中断后可以快速恢复。

5.5 对组织的治理要求

对组织的治理要求包括但不限于：
a） 应制定服务连续性计划，包括预防、响应、恢复等内容，并对计划定期进行更新维护及测试；
b） 应提升算法开发人员、运维人员等利益相关者的参与程度，开展多元主体共治；
c） 应制定问责制度，对恶意造成服务中断的相关人员或组织进行惩罚。

参考文献

[1] GB/T 5271.28-2001 信息技术 词汇 第28部分:人工智能 基本概念与专家系统
[2] ISO/IEC/IEEE 24765:2017 Systems and software engineering — Vocabulary