FINAL DRAFT
International Standard

ISO/IEC FDIS 24970

Artificial intelligence — AI system logging

Intelligence artificielle — Journalisation d'événements des systèmes d'IA

ISO/IEC JTC **1**/SC **42**

Secretariat: **ANSI**

Voting begins on:
2026-08-28

Voting terminates on:
2026-10-23

ISO/CEN PARALLEL PROCESSING

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 24970:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **5**
5 Logging and use of logs **5**
5.1 AI system logs 5
5.2 Logging components 6
5.3 Logging in context 6
5.4 Log entries 8
5.5 AI system logging 8
5.6 Events 9
5.7 General requirements 9
5.7.1 General 9
5.7.2 Security and privacy 10
5.7.3 Recording of events 10
6 Design of the logging system **10**
6.1 General 10
6.2 Traceability 11
6.3 Additional functions 11
6.4 Anomaly monitoring of the logging component 11
6.5 Technical documentation 12
7 Implementation and testing **12**
8 Triggers for logging **13**
8.1 General 13
8.2 Triggers from operation 13
8.2.1 Errors 13
8.2.2 Outlier input 13
8.2.3 Potential attack 13
8.2.4 User requests 14
8.2.5 Request from an affected person 14
8.3 Triggers from automated monitoring 14
8.3.1 Operation outside of predefined limits 14
8.3.2 Safety events 15
8.3.3 Performance events 15
8.3.4 Use outside of the intended purpose 15
8.3.5 Adversarial attack 15
8.3.6 Unwanted bias detection 15
8.3.7 Out-of-domain inputs 15
8.3.8 Model drift 16
8.3.9 Logging for machine learning model development for auditability purposes 16
8.3.10 Data quality issues 17
8.3.11 Invalid data 17
8.4 Triggers indicating substantial modification 17
8.4.1 System version and configuration changes 17
8.4.2 Learning after deployment 18
8.4.3 Deployer initiated changes 19
8.5 Triggers from human oversight 19
9 Information to log **19**
9.1 Required information 19

© ISO/IEC 2026 – All rights reserved

9.2 Recommended information 20
10 AI system log storage and access **21**
10.1 General 21
10.2 Requirements for third party access 21
10.3 Access for AI users 21
10.4 Access for AI providers 22
10.5 Storage infrastructure implementation 22
10.6 Access control and access mechanisms 22
11 Continual improvement **22**
Annex A (informative) **Information model** **23**
Bibliography **26**

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of a patent which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 42, *Artificial intelligence*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 21, *Artificial Intelligence*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2026 – All rights reserved

Introduction

AI systems can log a wide range of events during various phases of the life cycle. While some aspects of logging can be defined in advance — based on the system's known purpose and operating context — real-world needs often emerge only after deployment. In practice, AI developers and AI stakeholders cannot fully know what is important to log until the system is running. Additionally, the relevance of logged events is not fixed. Relevance can shift over time due to changing AI user needs, operational conditions or even interactions with other AI systems. However, it is often unclear whether AI systems can adapt their logging practices themselves, or whether human intervention is required to reconfigure logging as contexts evolve. This raises important considerations for auditability, transparency and long-term AI system oversight.

AI system logs have the potential to support both operational tasks, such as system monitoring or troubleshooting, and management system-level functions, provided the logs are accessible, well-structured and aligned with the specific needs of AI stakeholders. When logs are properly collected, maintained and analyzed, they can inform activities such as alignment with the strategic direction of the organization, real-time monitoring, decision-making and continual improvement. However, the effectiveness of those activities depends on the quality of the logged data, appropriate access controls, the organization's analytical capabilities, and ability to understand how logged events relate to objectives, risks or opportunities. Leveraging logs can contribute to cost reduction, risk mitigation and compliance, if organizations have the appropriate tools and processes in place to interpret and act on the data and if logs are designed to consider compliance obligations, including statutory, regulatory and contractual obligations, as well as other organizational requirements.

When logs are systematically collected, structured and analyzed, they can provide valuable insights that help organizations and AI stakeholders better understand and respond to unexpected events or changing conditions. The effectiveness of such response can require real-time or near-real-time access to logs or warrant asynchronous access depending on the context. Logs can also support the iterative development and refinement of AI systems by highlighting effectiveness and efficiency issues or emerging patterns not noticeable during initial training or deployment. To contribute meaningfully to continuous improvement throughout the AI system life cycle, logs can be contextually rich, validated, securely stored and reviewed considering the needs and expectations of AI stakeholders and of the organization.

Logging activities present their own complexity and costs, and can reduce the performance and increase the footprint of the AI system, so there are considerations on the effectiveness and efficiency of logging to answer oversight and management needs.

This document content is structured as follows:

— Clause 5 outlines logging and the use of logs, and provides general requirements for logging;

— Clause 6 provides requirements and guidance for design, including traceability;

— Clause 7 provides requirements for implementation and testing;

— Clause 8 details the triggers for logging in four categories: operation, automated monitoring, detecting substantial modification and human oversight.

— Clause 9 contains requirements and guidance for information to include in the logs;

— Clause 10 contains requirements for storing and access to logs;

— Clause 11 contains requirements for continual improvement;

— Annex A gives an example of an information model and data structure that can be used for AI system logging.

© ISO/IEC 2026 – All rights reserved

Artificial intelligence — AI system logging

1 Scope

This document describes common capabilities and provides requirements for logging of events in AI systems.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
log
management object that is organized by *log entries* (3.2)

Note 1 to entry: A log is a formally controlled record maintained to ensure traceability, accountability, and governance of AI system operations.

Note 2 to entry: In the context of Al system, logs can consist of structured, semi-structured, or unstructured data, and can originate from the Al system under consideration, its internal components, interacting Al systems, AI users or *interested parties* (3.15), whether human or automated, operating outside the AI system boundary.

Note 3 to entry: In the context of AI system, logs can be generated continuously, periodically or in response to specific conditions, and can serve a range of purposes including system *monitoring* (3.8), debugging, auditing, compliance, human oversight, iterative system improvement or accountability.

3.2
log entry
discrete unit of information that captures a specific event, condition, state, input, output, decision or contextual data related to functioning or environment

Note 1 to entry: A log entry can include, but is not limited to, information related to event, state, or other data associated with system operation.

Note 2 to entry: Log entries are composed of a combination of metadata, including timestamps, source identifiers, and severity levels and content-specific data relevant to the purpose of a log.

Note 3 to entry: Log entries are structured (e.g. a JSON object), semi-structured (e.g. textual annotations) or free-form (e.g. screenshots).

Note 4 to entry: Log entries vary in structure and content depending on the type of information being recorded and the intended use of the log.

Note 5 to entry: A log entry forms part of a formally controlled *log* (3.1) maintained to support traceability, accountability, and governance.

© ISO/IEC 2026 – All rights reserved

3.3
logging
process of generating, capturing, recording and storing a *log entry* (3.2) in a *log* (3.1) related to the operation, behaviour, decisions or context of an AI system

Note 1 to entry: Logging is performed automatically by AI system components, manually by *AI users* (3.14), or through hybrid methods.

Note 2 to entry: Logging occurs during all phases of the AI system life cycle.

3.4
model
physical, mathematical or otherwise logical representation of a system, *entity* (3.28), phenomenon, process or data

[SOURCE: ISO/IEC 22989:2022, 3.1.23]

3.5
audit
systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Note 1 to entry: Internal audits, sometimes called first party audits, are conducted by, or on behalf of, the *organization* (3.13) itself.

Note 2 to entry: External audits include those generally called second and third party audits. Second party audits are conducted by parties having an interest in the *organization*, such as customers, or by other individuals on their behalf. Third party audits are conducted by independent auditing *organizations*, such as those providing certification/ registration of conformity or governmental agencies.

[SOURCE: ISO 9000:2015, 3.13.1, modified to remove notes 3, 4 and 5]

3.6
auditability
capability of collecting and making available necessary evidential information related to the operation and use of an AI system, for the purpose of conducting an *audit* (3.5)

[SOURCE: ISO/IEC 22123-1:2023, 3.13.11, modified to replace cloud service with AI system]

3.7
error
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition

Note 1 to entry: An error within a system can be caused by failure of one or more of its components, or by the activation of a systematic fault.

[SOURCE: IEC 60050-192:2015, 192-03-02]

3.8
monitoring
ongoing observation and assessment of an AI system's behaviour, outputs and context by automated tools or human operators, to detect relevant events from expected operation

Note 1 to entry: Situations that warrant monitoring can include failure, malfunction, cyberattack, out of the intended domain of use, out of the operational design domain and abnormal usage.

© ISO/IEC 2026 – All rights reserved

3.9
logging component
functional part of an AI system, or another system interacting with it, that supports generation, capture, formatting, storage or management of *log entries* (3.2)

Note 1 to entry: A logging component can contain one or more subcomponents for generating *log entries* (3.2) based on different purposes.

Note 2 to entry: A logging component can forward information to other systems.

3.10
log user
organization (3.13) or *entity* (3.28) that accesses, reviews or analyzes *logs* (3.1) produced for an AI system

3.11
de-identification process
process of removing the association between a set of identifying attributes and the *data principal* (3.12)

Note 1 to entry: De-identification includes the process of altering the data, via modifying or removing data, so that individuals or entities cannot be as far as technically feasible identified directly or indirectly.

[SOURCE: ISO/IEC 20889:2018, 3.6, modified to add the note]

3.12
data principal
entity (3.28) to which data relates

Note 1 to entry: The term "data principal" is broader than "PII principal" (or "data subject" as used elsewhere), and is able to denote any *entity* such as a person, an *organization* (3.13), a device, or a software application.

[SOURCE: ISO/IEC 20889:2018, 3.4]

3.13
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger *entity* (3.28), the term "organization" refers only to the part of the larger *entity* that is within the scope of the AI management system.

[SOURCE: ISO/IEC 42001:2023, 3.1]

3.14
AI user
organization (3.13) or *entity* (3.28) that deploys AI products or services

3.15
interested party
stakeholder
any individual, group, or *organization* (3.13) that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 42001:2023, 3.2, modified to add admitted term]

3.16
AI developer
organization (3.13) or *entity* (3.28) that is involved in the development of AI services and products

© ISO/IEC 2026 – All rights reserved

3.17
memory capacity
maximum number of items that can be held in a given *logging component* (3.9) memory; usually measured in words or bytes

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.2411, modified computer to logging component and removed note]

3.18
storage capacity
maximum number of items that can be held in a given storage device; usually measured in bytes

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.3994, modified to remove note and reference to words]

3.20
control (verb)
<controllability> in engineering, the *monitoring* (3.8) of system output to compare with expected output and taking corrective action when the actual output does not match the expected output

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.846]

3.21
control (noun)
action of *controlling* (3.20)

3.22
controller
authorized human or another external agent that performs a *control* (3.21)

Note 1 to entry: A controller interacts with the *control points* (3.23) of an AI system.

[SOURCE: ISO/IEC TS 8200:2024, 3.6]

3.23
control point
part of the interface of a system where *control* (3.21) can be applied

Note 1 to entry: A control point can be a function, physical facility (such as a switch) or a signal receiving subsystem.

[SOURCE: ISO/IEC TS 8200:2024, 3.16, modified to make control singular]

3.24
disengagement of control
control disengagement
process where a *controller* (3.22) releases a set of *control points* (3.23)

[SOURCE: ISO/IEC TS 8200:2024, 3.7]

3.25
engagement of control
control engagement
process where a *controller* (3.22) takes over a set of *control points* (3.23)

Note 1 to entry: Besides taking over a set of control points, an engagement of control can also include a confirmation about the transfer of control to a controller.

[SOURCE: ISO/IEC TS 8200:2024, 3.8]

© ISO/IEC 2026 – All rights reserved

3.26
transfer of control
control transfer
process of the change of the *controller* (3.22) that performs a *control* (3.21) over a system

Note 1 to entry: Transfer of control does not entail application of a control, but it is a handover of control points of the system interface between agents.

Note 2 to entry: Engagement of control and disengagement of control are two fundamental complementary parts of control transfer.

[SOURCE: ISO/IEC TS 8200:2024, 3.19]

3.27
AI provider
organization (3.13) or *entity* (3.28) that provides products or services that uses one or more AI systems

3.28
entity
object
item
anything perceivable or conceivable

EXAMPLE Product, service, process, person, *organization* (3.13), system , resource.

Note 1 to entry: Objects can be material (e.g. 'engine', 'sheet of paper', 'diamond'), immaterial (e.g. 'conversion ratio', 'project plan') or imagined (e.g. 'unicorn', 'scientific hypothesis').

[SOURCE: ISO 1087:2019, 3.1.1, modified — "entity" and "item" have been added as terms.]

4 Abbreviated terms

AI artificial intelligence

ML machine learning

5 Logging and use of logs

5.1 AI system logs

An AI system log can represent information related to the AI system life cycle, including its operation, behaviour, inputs, outputs or context of development and use, collected to support decisions related to the various stages of the AI system life cycle, including but not limited to retrieval of events, analysis, monitoring and control or decision review.

AI system logs can include:

— time-stamped events, including recorded occurrences linked to a specific moment in time, such as when a model generates a prediction, an error occurs or a user interaction takes place;

— status snapshots, including point-in-time captures of system conditions, such as memory usage, model state or active component;

— sensor or input data, including information received by the AI system from external sources, such as camera images, user inputs, location data or telemetry from connected devices;

— outputs, including results produced by the AI system, such as classifications, recommendations, predictions or generated content;

— decisions, including discrete choices or actions taken by the AI system, either autonomously or through human oversight mechanisms, such as approving a transaction or triggering an alert;

© ISO/IEC 2026 – All rights reserved