PD ISO/IEC TR 27563:2023



BSI Standards Publication

Security and privacy in artificial intelligence use cases — Best practices

National foreword

This Published Document is the UK implementation of ISO/IEC TR 27563:2023.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 27130 0

ICS 35.020

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 June 2023.

Amendments/corrigenda issued since publication

Date	Text affected

PD ISO/IEC TR 27563:2023

TECHNICAL REPORT

ISO/IEC TR 27563

First edition
2023-05

Security and privacy in artificial intelligence use cases — Best practices

Sécurité et respect de la vie privée dans les cas d'usage de l'intelligence artificielle — Bonnes pratiques

Reference number
ISO/IEC TR 27563:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Analysis of security and privacy **3**
5.1 General 3
5.2 Application domains in ISO/IEC TR 24030:2021 use cases 3
5.3 Security in ISO/IEC TR 24030:2021 use cases 3
5.4 Privacy in ISO/IEC TR 24030:2021 use cases 4
6 Templates for analysis **5**
7 Supporting information **6**
7.1 Describe ecosystem 6
7.2 Provide assessment of systems of interest 7
7.3 Identify security and privacy concerns 7
7.4 Identify security and privacy risks 9
7.5 Identify security and privacy controls 11
7.6 Identify security and privacy assurance concerns 15
7.7 Identify security and privacy plan requirements 16
Annex A (informative) **Additional use cases** **18**
Bibliography **28**

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC had not received notice of (a) patent(s) 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 and https://patents.iec.ch. ISO and IEC 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. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information technology, cyber security and privacy protection*.

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 and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Introduction

Artificial intelligence (AI) and machine learning (ML) are increasingly being adopted by the digital industry, using algorithms to make decisions that have the potential to negatively impact the privacy of individuals and in some cases can even cause harm to some of them, unless adequate safeguards are deployed. Such safeguards to protect privacy often depend on a variety of factors including the specific type of process, sensitivity of data used, and potential harm likely to be caused.

This concern has been expressed by:

— Practitioners, who identified 23 principles for AI at the 2017 Asilomar conference[1] covering research, ethics and values, as well as longer term issues.

— Standard developers, as evidenced by the report on ethically aligned design published by the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems[2].

— Policy makers, as exemplified by the appointment by the European Commission of a high-level expert group on artificial intelligence and the subsequent publication of an assessment list[3].

This document provides an analysis of security and privacy of use cases provided in ISO/IEC TR 24030, which should be used in parallel. A number of additional use cases are provided in Annex A.

This document also uses concepts from ISO/IEC TR 24028, which addresses trustworthiness in AI systems, including approaches to establish trust (e.g. transparency, explainability, controllability), and to achieve trustworthiness properties (e.g. resiliency, reliability, accuracy, safety, security, or privacy).

© ISO/IEC 2023 – All rights reserved

Security and privacy in artificial intelligence use cases — Best practices

1 Scope

This document outlines best practices on assessing security and privacy in artificial intelligence use cases, covering in particular those published in ISO/IEC TR 24030.

The following aspects are addressed:

— an overall assessment of security and privacy on the AI system of interest;

— security and privacy concerns;

— security and privacy risks;

— security and privacy controls;

— security and privacy assurance; and

— security and privacy plans.

Security and privacy are treated separately as the analysis of security and the analysis of privacy can differ.

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
personally identifiable information
PII
information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.3). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

© ISO/IEC 2023 – All rights reserved