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 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

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.

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).

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.