INTERNATIONAL STANDARD

ISO/IEC 27402

First edition
2023-11

Cybersecurity — IoT security and privacy — Device baseline requirements

Cybersécurité — Sécurité et protection de la vie privée pour l'IdO — Exigences de base relatives aux dispositifs

Reference number
ISO/IEC 27402:2023(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

Page

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 security, cybersecurity and privacy protection*.

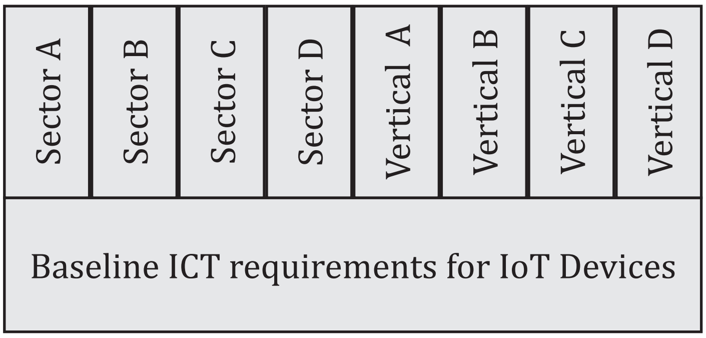
Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

With the increasing number of Internet of Things (IoT) devices and increasing reliance on such devices, the security and privacy risks relating to those "things" are expected to grow. Their widespread deployment in networks and systems make them easy and prime targets for cyber attacks.

This document provides a baseline set of information and communication technologies (ICT) requirements so that IoT devices are able to support security and privacy controls. A risk assessment is critical to develop a risk treatment plan that identifies the necessary IoT device features and countermeasures. The management of systems which use IoT devices depends upon the capabilities of those devices (among other factors).

Broadly speaking, this document addresses ICT requirements for IoT devices that are made available to the market. The requirements in this document are intended as a baseline, upon which vertical markets (such as health, financial services, industrial, consumer electronics and transportation) can build additional requirements for the expected use and risks of IoT devices in their applications, as depicted in Figure 1. In addition to this document, various sectors (e.g. private/industrial, public, defence, national security) and vertical markets have sector- or vertical-specific requirements, for example those found in ETSI EN 303 645[11] for consumer devices and the IEC 62443 series for industrial devices and systems. While this document can provide requirements for a conformity assessment scheme, it is expected that stakeholders for specific sectors and vertical markets will develop consensus around requirements specific to their contexts, building "on top" of this document. Subsequently, conformity assessment programmes can be developed around those specific sectors and vertical markets. This document would be effectively integrated into such programmes while providing a common set of baseline requirements.



NOTE Additional requirements can be developed or required by specific sectors and vertical markets.

Figure 1 — Relationship between baseline requirements in this document and potential additional requirements

As the complex technical landscape of IoT devices evolves, this document can support a scalable globally harmonized approach to the baseline security and privacy requirements and inform technical policy and regulatory initiatives.

Cybersecurity — IoT security and privacy — Device baseline requirements

1 Scope

This document provides baseline ICT requirements for IoT devices to support security and privacy controls.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27400:2022, *Cybersecurity — IoT security and privacy — Guidelines*

ISO 31000:2018, *Risk management — Guidelines*