



**International
Standard**

ISO/IEC 27403

**Cybersecurity – IoT security
and privacy – Guidelines for IoT-
domotics**

*Cybersécurité — Sécurité et protection de la vie privée pour l'IDO
— Lignes directrices pour la domotique-IDO*

**First edition
2024-06**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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	2
5 Overview	2
5.1 General.....	2
5.2 Features.....	2
5.3 Stakeholders.....	4
5.4 Life cycles.....	4
5.5 Reference model.....	5
5.6 Security and privacy dimensions.....	8
6 Guidelines for risk assessment	8
6.1 General.....	8
6.2 Sources of security risks.....	9
6.2.1 Security risks for service sub-systems.....	9
6.2.2 Security risks for IoT-domotics gateway.....	10
6.2.3 Security risks for IoT-domotics devices and physical entities.....	12
6.2.4 Security risks for networks.....	13
6.3 Sources of privacy risks.....	13
6.3.1 Privacy risks for service sub-systems.....	13
6.3.2 Privacy risks for IoT-domotics gateway.....	14
6.3.3 Privacy risks for IoT-domotics devices and physical entities.....	16
6.3.4 Privacy risks for networks.....	16
7 Security and privacy controls	17
7.1 Principles.....	17
7.1.1 General.....	17
7.1.2 Different levels of security for different services.....	17
7.1.3 Easy security settings for users.....	17
7.1.4 Failsafe domotics devices.....	17
7.1.5 Restricted access to content services.....	17
7.1.6 Consideration for children.....	17
7.1.7 Scenario-specific privacy preferences.....	17
7.2 Security controls.....	18
7.2.1 Policy for IoT-domotics security.....	18
7.2.2 Organization of IoT-domotics security.....	18
7.2.3 Asset management.....	18
7.2.4 Equipment and assets located outside physical secured areas.....	18
7.2.5 Secure disposal or re-use of equipment.....	18
7.2.6 Learning from security incidents.....	19
7.2.7 Secure IoT-domotics system engineering principles.....	19
7.2.8 Secure development environment and procedures.....	19
7.2.9 Security of IoT-domotics systems in support of safety.....	20
7.2.10 Security in connecting varied IoT-domotics devices.....	20
7.2.11 Verification of IoT-domotics devices and systems design.....	20
7.2.12 Monitoring and logging.....	20
7.2.13 Protection of logs.....	20
7.2.14 Use of suitable networks for the IoT-domotics systems.....	20
7.2.15 Secure settings and configurations in delivery of IoT-domotics devices and services.....	20
7.2.16 User and device authentication.....	21

ISO/IEC 27403:2024(en)

7.2.17	Provision of software and firmware updates	21
7.2.18	Sharing vulnerability information	21
7.2.19	Security measures adapted to the life cycle of IoT-domotics system and services	21
7.2.20	Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services	21
7.2.21	Determination of security roles for stakeholders	22
7.2.22	Management of vulnerable devices	22
7.2.23	Management of supplier relationships in IoT-domotics security	22
7.2.24	Secure disclosure of Information regarding security of IoT-domotics devices	22
7.3	Privacy controls	22
7.3.1	Prevention of privacy invasive events	22
7.3.2	IoT-domotics privacy by default	22
7.3.3	Provision of privacy notice	23
7.3.4	Verification of IoT-domotics functionality	23
7.3.5	Consideration of IoT-domotics users	23
7.3.6	Management of IoT-domotics privacy controls	23
7.3.7	Unique device identity	24
7.3.8	Fail-safe authentication	24
7.3.9	Minimization of indirect data collection	24
7.3.10	Communication of privacy preferences	24
7.3.11	Verification of automated decision	24
7.3.12	Accountability for stakeholders	24
7.3.13	Unlinkability of PII	24
7.3.14	Sharing information on PII protection measures of IoT-domotics devices	25
Annex A	(informative) Use cases of IoT-domotics	26
Annex B	(informative) Security and privacy concerns from stakeholders	31
Annex C	(informative) Security and privacy responsibilities of stakeholders	35
Annex D	(informative) Security measures for different types of IoT-domotics devices	37
Bibliography		39

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

Although IoT-domotics have been widely applied worldwide, many IoT-domotics devices, communication protocols and platforms are developed without sufficient security and privacy considerations, which can pose security and privacy risks. Due to the long supply chain and the large number of stakeholders involved, it is important to establish the stakeholders, identify risks during the life cycle, and put forward proposals for resolving security and privacy issues in IoT-domotics. This document provides guidelines to analyse security and privacy risks and identifies controls that should be implemented in IoT-domotics systems.

IoT-domotics have some features that differ from other forms of IoT deployment, such as non-expert users, and ad hoc architecture. This document therefore adapts the general IoT security and privacy principles to IoT-domotics and provides stakeholders with thorough and tailored guidelines for scenarios specific to IoT-domotics.

The target audiences of this document include IoT-domotics service providers, IoT-domotics service developers, and those who supervise or verify security and privacy for IoT-domotics.

The goal of this document is to ensure that security and privacy for IoT-domotics are achieved without requiring end-users to have in-depth IT knowledge. Although this document can be used by interested end-users, they are not the target audience.

Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

1 Scope

This document provides guidelines to analyse security and privacy risks and identifies controls that can be implemented in Internet of Things (IoT)-domotics systems.

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 20924, *Internet of Things (IoT) and digital twin — Vocabulary*

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

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*