INTERNATIONAL STANDARD

ISO/IEC 27400

First edition
2022-06

Cybersecurity — IoT security and privacy — Guidelines

Cybersécurité — Sécurité et protection de la vie privée pour l'IoT — Lignes directrices

Reference number
ISO/IEC 27400:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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 2022 – 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 IoT concepts ... **3**
5.1 General ... 3
5.2 Characteristics of IoT systems ... 3
5.3 Stakeholders of IoT systems ... 4
5.3.1 General ... 4
5.3.2 IoT service provider ... 4
5.3.3 IoT service developer ... 4
5.3.4 IoT user ... 5
5.4 IoT ecosystem ... 5
5.5 IoT service life cycles ... 5
5.6 Domain based reference model ... 7
6 Risk sources for IoT systems ... **8**
6.1 General ... 8
6.2 Risk sources ... 9
6.2.1 General ... 9
6.2.2 Sample risk sources related to IoT domains ... 9
6.2.3 Risk sources from outside the IoT domains ... 11
6.2.4 Privacy related risk sources ... 12
7 Security and privacy controls ... **13**
7.1 Security controls ... 13
7.1.1 General ... 13
7.1.2 Security controls for IoT service developer and IoT service provider ... 13
7.1.3 Security controls for IoT user ... 30
7.2 Privacy controls ... 32
7.2.1 General ... 32
7.2.2 Privacy controls for IoT service developer and IoT service provider ... 32
7.2.3 Privacy controls for IoT user ... 38
Annex A (informative) **IoT monitoring camera sample risk scenario** ... **40**
Bibliography ... **42**

© ISO/IEC 2022 – 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 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.

© ISO/IEC 2022 – All rights reserved

Introduction

Information security is a major concern of any information and communication technology (ICT) system and Internet of Things (IoT) systems are no exception. IoT systems present particular challenges for information security in that they are highly distributed and involve a large number of diverse entities. This implies that there are a very large attack surface and a significant challenge for the information security management system (ISMS) to apply and maintain appropriate security controls across the whole system.

Privacy or personally identifiable information (PII) protection is a significant concern for some types of IoT systems. Where an IoT system acquires or uses PII, it is usually the case that there are laws and regulations that apply to the acquisition, storage and processing of PII. Even where regulations are not a concern, the handling of PII by an IoT system remains a reputational and trust concern for the organizations involved, for example, if the PII is stolen or is misused, potentially causing some form of harm to the people identified by the information.

Security and privacy controls in this document are developed for stakeholders in an IoT system environment, so as to be utilized by each IoT stakeholder, throughout the IoT system life cycle.

© ISO/IEC 2022 – All rights reserved

Cybersecurity — IoT security and privacy — Guidelines

1 Scope

This document provides guidelines on risks, principles and controls for security and privacy of Internet of Things (IoT) solutions.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 20924, ISO/IEC 27000, ISO/IEC 29100, ISO 31000 and the following 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
cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand

Note 1 to entry: Examples of resources include servers, operating systems, networks, software, applications and storage equipment.

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.5]

3.2
cloud service
one or more capabilities offered via *cloud computing* (3.1) invoked using a defined interface

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.8]

3.3
IoT device
entity of an IoT system that interacts and communicates with the physical world through sensing or actuating

3.4
IoT device developer
entity that creates an assembled final IoT device

Note 1 to entry: “final” in this definition means the stage of delivery to the IoT service developer in the assemble process.

3.5
IoT platform
infrastructure that enables the deployment, management and operation of IoT devices

© ISO/IEC 2022 – All rights reserved

3.6
IoT system
system providing functionalities of Internet of Things

Note 1 to entry: IoT system is inclusive of IoT devices, IoT gateways, sensors, and actuators.

Note 2 to entry: In the context of this document, this also includes applications and backend that support IoT solutions.

3.7
IoT solution
seamlessly integrated bundle of technologies, potentially including sensors, gateways and actuators

Note 1 to entry: These can solve a specific problem or need or they can be used to build additional functionality in other none IoT solutions

3.8
ecosystem
infrastructure and services based on a network of organizations and stakeholders

Note 1 to entry: Organizations can include public bodies.

[SOURCE: ISO/IEC TS 27570:2021, 3.8]

4 Abbreviated terms

ASD	Application and Service Domain
CRM	Customer Relationship Management
DoS	Denial of Service
IC	Integrated Circuit
ICT	Information and Communications Technology
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ITS	Intelligent Traffic System
OMD	Operations and Management Domain
OTA	Over The Air
PED	Physical Entity Domain
PII	Personally Identifiable Information
RAID	Resource Access and Interchange Domain
SCD	Sensing and Controlling Domain
UD	User Domain
Wi-Fi	Wireless Fidelity

© ISO/IEC 2022 – All rights reserved