INTERNATIONAL STANDARD

ISO/IEC 27032

Second edition
2023-06

Cybersecurity — Guidelines for Internet security

Cybersécurité — Lignes directrices relatives à la sécurité sur l'internet

Reference number
ISO/IEC 27032:2023(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 ... **4**
5 Relationship between Internet security, web security, network security and cybersecurity ... **5**
6 Overview of Internet security ... **7**
7 Interested parties ... **8**
7.1 General ... 8
7.2 Users ... 9
7.3 Coordinator and standardization organisations ... 10
7.4 Government authorities ... 10
7.5 Law enforcement agencies ... 10
7.6 Internet service providers ... 10
8 Internet security risk assessment and treatment ... **11**
8.1 General ... 11
8.2 Threats ... 11
8.3 Vulnerabilities ... 12
8.4 Attack vectors ... 12
9 Security guidelines for the Internet ... **13**
9.1 General ... 13
9.2 Controls for Internet security ... 14
9.2.1 General ... 14
9.2.2 Policies for Internet security ... 14
9.2.3 Access control ... 14
9.2.4 Education, awareness and training ... 15
9.2.5 Security incident management ... 15
9.2.6 Asset management ... 17
9.2.7 Supplier management ... 17
9.2.8 Business continuity over the Internet ... 18
9.2.9 Privacy protection over the Internet ... 18
9.2.10 Vulnerability management ... 19
9.2.11 Network management ... 20
9.2.12 Protection against malware ... 21
9.2.13 Change management ... 21
9.2.14 Identification of applicable legislation and compliance requirements ... 22
9.2.15 Use of cryptography ... 22
9.2.16 Application security for Internet-facing applications ... 22
9.2.17 Endpoint device management ... 24
9.2.18 Monitoring ... 24
Annex A (informative) **Cross-references between this document and ISO/IEC 27002** ... **25**
Bibliography ... **27**

© 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 security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27032:2012) which has been technically revised.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed;

— the risk assessment and treatment approach has been changed, with the addition of content on threats, vulnerabilities and attack vectors to identify and manage the Internet security risks;

— a mapping between the controls for Internet security cited in 9.2 and the controls contained in ISO/IEC 27002 has been added to Annex A.

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

The focus of this document is to address Internet security issues and provide guidance for addressing common Internet security threats, such as:

— social engineering attacks;

— zero-day attacks;

— privacy attacks;

— hacking; and

— the proliferation of malicious software (malware), spyware and other potentially unwanted software.

The guidance within this document provides technical and non-technical controls for addressing the Internet security risks, including controls for:

— preparing for attacks;

— preventing attacks;

— detecting and monitoring attacks; and

— responding to attacks.

The guidance focuses on providing industry best practices, broad consumer and employee education to assist interested parties in playing an active role to address the Internet security challenges. The document also focuses on preservation of confidentiality, integrity and availability of information over the Internet and other properties, such as authenticity, accountability, non-repudiation and reliability that can also be involved.

This includes Internet security guidance for:

— roles;

— policies;

— methods;

— processes; and

— applicable technical controls.

Given the scope of this document, the controls provided are necessarily at a high-level. Detailed technical specification standards and guidelines applicable to each area are referenced within the document for further guidance. See Annex A for the correspondence between the controls cited in this document and those in ISO/IEC 27002.

This document does not specifically address controls that organizations can require for systems supporting critical infrastructure or national security. However, most of the controls mentioned in this document can be applied to such systems.

This document uses existing concepts from ISO/IEC 27002, the ISO/IEC 27033 series, ISO/IEC TS 27100 and ISO/IEC 27701, to illustrate:

— the relationship between Internet security, web security, network security and cybersecurity;

— detailed guidance on Internet security controls cited in 9.2, addressing cyber-security readiness for Internet-facing systems.

© ISO/IEC 2023 – All rights reserved

As mentioned in ISO/IEC TS 27100, the Internet is a global network, used by organizations for all communications, both digital and voice. Given that some users target attacks towards these networks, it is critical to address the relevant security risks.

© ISO/IEC 2023 – All rights reserved

Cybersecurity — Guidelines for Internet security

1 Scope

This document provides:

— an explanation of the relationship between Internet security, web security, network security and cybersecurity;

— an overview of Internet security;

— identification of interested parties and a description of their roles in Internet security;

— high-level guidance for addressing common Internet security issues.

This document is intended for organizations that use the Internet.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, 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
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

EXAMPLE 1 IoT devices.

EXAMPLE 2 Smart phones.

3.2
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

[SOURCE: ISO/IEC 27033-1:2015, 3.3]

© ISO/IEC 2023 – All rights reserved