BS ISO/IEC 27032:2023

INTERNATIONAL STANDARD

**ISO 27032**

Second edition
2023-06-27

# Cybersecurity — Guidelines for Internet security

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

Reference number
ISO 27032:2023(E)

# 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*.

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.

# 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.

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.

INTERNATIONAL STANDARD ISO/IEC 27032:2023

# 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]

**国际标准**

国际标准化组织

27032

第二版 2023 年 6 月 27 日

# 网络安全——互联网安全指南

网络安全——互联网安全相关指导方针

Reference number ISO 27032:2023 (E)

# 目录

# 前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织为处理特定技术领域而设立的技术委员会参与国际标准的制定工作。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，通过与 ISO 和 IEC 的联络，也参与相关工作。

本文件的编制程序以及其后续维护所采用的程序在 ISO/IEC 指令第 1 部分中有详细说明。尤其应注意不同类型的文件所需的不同批准标准。本文件是依照 ISO/IEC 指令第 2 部分的编辑规则起草的（见 www.iso.org/directives 或 www.iec.ch/members-experts/refdocs）。

国际标准化组织（ISO）和国际电工委员会（IEC）提醒注意，实施本文件可能涉及使用（一项）专利（权）。ISO 和 IEC 对任何声称的专利权的有效性、适用性或相关证据不持立场。截至本文件出版之日，ISO 和 IEC 未收到有关实施本文件可能需要使用专利的通知。然而，实施者应注意，这可能不代表最新信息，可从 ISO 网站（www.iso.org/patents）和 IEC 网站（https://patents.iec.ch）的专利数据库获取最新信息。ISO 和 IEC 对于识别任何此类专利权不承担责任。

本文件中使用的任何商标名称均为方便用户而提供，不构成任何背书。

有关标准自愿性的说明、与合格评定相关的 ISO 特定术语和表达的含义，以及 ISO 遵守世界贸易组织（WTO）在技术性贸易壁垒（TBT）方面的原则的信息，请访问 www.iso.org/iso/foreword.html。在国际电工委员会（IEC），请访问 www.iec.ch/understanding-standards。

本文件由国际标准化组织/国际电工委员会联合技术委员会 ISO/IEC JTC 1（信息技术）下属的第 27 分技术委员会（信息安全、网络安全和个人隐私保护）编制。

本第二版废止并取代了第一版（ISO/IEC 27032:2012），并对其进行了技术修订。

主要变化如下：

— 标题已修改；

— 该文件的结构已更改；

— 风险评估和处理方法已作更改，增加了有关威胁、漏洞和攻击途径的内容，以识别和管理互联网安全风险；

— 在附录 A 中新增了 9.2 节中所提及的互联网安全控制措施与 ISO/IEC 27002 中所包含的控制措施之间的对应关系。

对于本文件的任何反馈或疑问，应向用户所在国家的标准机构提出。这些机构的完整列表可在 www.iso.org/members.html 和 www.iec.ch/national-committees 上找到。

# 引言

本文件的重点在于解决互联网安全问题，并为应对常见的互联网安全威胁提供指导，例如：

— 社会工程学攻击

— 零日攻击

— 隐私攻击

— 黑客攻击；黑客行为和

— 恶意软件（包括间谍软件）及其他潜在不需要的软件的泛滥。

本文件中的指导内容提供了应对互联网安全风险的技术和非技术控制措施，包括以下方面的控制措施：

— 准备应对攻击

— 防止攻击；

— 检测和监控攻击；和

— 应对攻击。

该指南侧重于提供行业最佳实践、广泛的消费者和员工教育，以协助相关方积极应对互联网安全挑战。该文件还侧重于保护互联网及其他网络中信息的保密性、完整性和可用性，以及可能涉及的其他属性，如真实性、可问责性、不可否认性和可靠性。

这包括以下方面的互联网安全指南：

— 角色；职责；职位；作用；功能

— 政策；政策方针；政策规定

— 方法；

— 过程；流程；工序和

— 适用的技术控制措施。

鉴于本文件的范围，所提供的控制措施必然是高层次的。针对每个领域的详细技术规范标准和指南在本文件中均有引用，以供进一步指导。有关本文件中所引用的控制措施与 ISO/IEC 27002 中的对应关系，请参见附录 A。

本文件并未专门针对组织可为支持关键基础设施或国家安全的系统所要求的控制措施进行阐述。不过，本文件中提及的大多数控制措施均可适用于此类系统。

本文件采用 ISO/IEC 27002、ISO/IEC 27033 系列、ISO/IEC TS 27100 和 ISO/IEC 27701 中现有的概念来说明：

— 互联网安全、网络安全、网络信息安全以及网络安全之间的关系；

— 关于 9.2 节中提到的互联网安全控制措施的详细指南，涉及面向互联网系统的网络安全准备情况。

正如 ISO/IEC TS 27100 中所提到的，互联网是一个全球性的网络，组织机构利用它进行所有形式的通信，包括数字通信和语音通信。鉴于一些用户会针对这些网络发起攻击，因此应对相关的安全风险予以重视。

INTERNATIONAL STANDARD

SO/IEC 27032:2023

# 网络安全——互联网安全指南

## 1 范围

本文件提供：

— 对互联网安全、网络安全、网络信息安全以及网络安全保障之间关系的解释；

— 互联网安全概览；

— 识别利益相关方并描述其在互联网安全中的角色；解决常见互联网安全问题的高级指导

本文件面向使用互联网的组织

## 2 规范性引用文件

文中提及的下列文件，其部分或全部内容构成本文件的要求。对于有日期的引用文件，仅所引用的版本适用。对于无日期的引用文件，适用所引用文件的最新版本（包括任何修订）。

ISO/IEC 27000《信息技术 安全技术 信息安全管理体系 概述和术语》

## 3 术语和定义

就本文件而言，ISO/IEC 27000 中给出的术语和定义以及以下内容适用。

国际标准化组织（ISO）和国际电工委员会（IEC）在以下网址维护用于标准化工作的术语数据库：

— 国际标准化组织在线浏览平台：访问网址为 https://www.iso.org/obp

— 国际电工委员会电工术语在线词典：访问网址 https://www.electropedia.org/

3.1

**攻击途径**

攻击者能够借此途径或手段访问计算机或网络服务器以造成恶意后果的路径或方法

示例 1 物联网设备

示例 2 智能手机

3.2

**攻击者**

故意利用技术及非技术安全控制措施中的漏洞，以窃取或破坏信息系统和网络，或破坏合法用户对信息系统和网络资源的可用性的人。

来源：ISO/IEC 27033-1:2015，3.3]

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。