~~DRAFT INTERNATIONAL STANDARD~~

ISO/IEC ~~DIS~~ FDIS 27032:~~2022~~2023(E)

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Date: ~~2022-09-16~~2023-02-27

Cybersecurity — Guidelines for Internet security

Style Definition: Heading 1: Indent: Left: 0 pt, First line: 0 pt, Tab stops: Not at 21.6 pt

Style Definition: Heading 2: Font: Bold, Tab stops: Not at 18 pt

Style Definition: Heading 3: Font: Bold

Style Definition: Heading 4: Font: Bold

Style Definition: Heading 5: Font: Bold

Style Definition: Heading 6: Font: Bold

Style Definition: ANNEX

Style Definition: zzCopyright

Style Definition: AMEND Terms Heading: Font: Bold

Style Definition: AMEND Heading 1 Unnumbered: Font: Bold

Style Definition: List Bullet: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab

Style Definition: List Bullet 2: Indent: Left: 14.15 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 32.15 pt, List tab

Style Definition: List Bullet 3: Indent: Left: 28.3 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 46.3 pt, List tab

Style Definition: List Bullet 4: Indent: Left: 42.45 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 60.45 pt, List tab

Style Definition: List Bullet 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab

Style Definition: List Number: Indent: Left: 0 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 18 pt, List tab

Style Definition: List Number 5: Indent: Left: 56.6 pt, Hanging: 18 pt, No bullets or numbering, Tab stops: 74.6 pt, List tab

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font: 11 pt, Not Bold

Formatted: Header, Space After: 0 pt, Line spacing: single

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: std_publisher

Formatted: No page break before

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: English (United Kingdom)

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: Bold

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Header, Space After: 0 pt, Line spacing: single

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font: 11 pt, Not Bold

Contents

Formatted: Font: Bold

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Header, Space After: 0 pt, Line spacing: single

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font color: Custom Color(RGB(33;29;30))

Formatted: Font: 11 pt, Not Bold

Formatted: Font: Bold

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~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC 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~~www.iso.org/patents) or the IEC list of patent declarations received (see ~~https://patents.iec.ch~~https://patents.iec.ch).

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~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~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~~, presenting an overview of Internet security and detailed guidance on Internet security controls~~;

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

— ~~the correspondence~~a mapping between the controls for Internet security cited in 9.2 and the controls contained in ISO/IEC 27002 ~~can be found in~~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~~www.iso.org/members.html and ~~www.iec.ch/national-committees~~www.iec.ch/national-committees.

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Header, Space After: 0 pt, Line spacing: single
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font: 11 pt, Not Bold
Formatted: Font: Bold

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 ~~for~~to such systems.

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font: 11 pt, Not Bold
Formatted: Header, Space After: 0 pt, Line spacing: single
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font: Not Bold
Formatted: cite_app
Formatted: cite_app
Formatted: std_publisher
Formatted: std_docNumber
Formatted: Font: Bold

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

- 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.

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font: 11 pt, Not Bold
Formatted: Header, Space After: 0 pt, Line spacing: single
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_publisher
Formatted: std_documentType
Formatted: std_docNumber
Formatted: std_publisher
Formatted: std_docNumber
Formatted: List Continue 1, No bullets or numbering, Tab stops: 19.85 pt, Left + 39.7 pt, Left + 59.55 pt, Left + 79.4 pt, Left + 99.25 pt, Left + 119.05 pt, Left + 138.9 pt, Left + 158.75 pt, Left + 178.6 pt, Left + 198.45 pt, Left
Formatted: cite_sec
Formatted: std_publisher
Formatted: std_documentType
Formatted: std_docNumber
Formatted: Font: Bold

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/obphttps://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/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

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Section start: New page
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docTitle
Formatted: std_docTitle
Formatted: std_docTitle
Formatted: std_docTitle
Formatted: Don't keep with next
Formatted: std_publisher
Formatted: std_docNumber
Formatted: English (United Kingdom)
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Cambria, 11 pt, English (United Kingdom)
Formatted: No underline, Font color: Auto, English (United Kingdom)
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted: English (United Kingdom)
Formatted ...
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: English (United Kingdom)
Formatted: Font: Not Bold
Formatted: Font: Not Bold

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]

3.3
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple *attack vectors* (3.1)

3.4
bot
automated software program used to carry out specific tasks

Note 1 to entry: This word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

Note 2 to entry: A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

3.5
botnet
collection of remotely controlled malicious bots that run autonomously or automatically on compromised computers

EXAMPLE~~: DDoS; Distributed denial-of-service (DDoS)~~ nodes, where the botnet controller can direct the user's computer to generate traffic to a third-party site as part of a coordinated DDoS ~~(distributed denial of service)~~ attack.

3.6
cybersecurity
safeguarding of people, society, organizations and nations from cyber risks

Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level.

[SOURCE: ISO/IEC TS 27100:2020, 3.2]

3.7
dark net
network of secret websites within the Internet that can only be accessed with specific software

Note 1 to entry: The dark net is also known as dark web.

3.8
deceptive software
software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Header, Space After: 0 pt, Line spacing: single
Formatted: Font: 11 pt, Not Bold
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: cite_sec
Formatted: std_publisher, English (United Kingdom)
Formatted: std_documentType, English (United Kingdom)
Formatted: std_docNumber, English (United Kingdom)
Formatted: std_year, English (United Kingdom)
Formatted: std_section, English (United Kingdom)
Formatted: Font: Not Bold
Formatted: Font: Not Bold

EXAMPLE 3 Adware and spyware.

3.9
hacking
intentionally accessing a computer system without the authorization of the user or the owner

3.10
hacktivism
hacking (3.9) for a politically or socially motivated purpose

3.11
Internet
global system of inter-connected networks in the public domain

[SOURCE: ISO/IEC 27033-1:2015, 3.14, modified — "the" has been deleted from the term.]

3.12
Internet security
preservation of confidentiality, integrity and availability of information over the *Internet* (3.11)

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Note 2 to entry: Please refer to definitions on confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability in ISO/IEC 27000:2018, Clause 3.

3.13
Internet service provider
ISP
organization that provides Internet services to a user and enables its customers access to the *Internet* (3.11)

Note 1 to entry: Also, sometimes referred to as an Internet access provider (IAP).

3.14
malicious content
applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

3.15
malware
malicious software
software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system

EXAMPLE Viruses, worms and trojans.

3.16
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: In the context of this document, an individual is distinct from an organization.

Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Header, Space After: 0 pt, Line spacing: single
Formatted: Font color: Custom Color(RGB(33;29;30))
Formatted: Font: 11 pt, Not Bold
Formatted: cite_sec
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_year
Formatted: std_section
Formatted: Font: Not Italic
Formatted: cite_sec
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_year
Formatted: std_section
Formatted: std_section
Formatted: Font: Not Italic
Formatted: cite_sec
Formatted: Font: Not Bold
Formatted: Font: Not Bold