



SLOVENSKI STANDARD

oSIST prEN 40000-1-2:2025

01-december-2025

Zahteve za kibernetško varnost za izdelke z digitalnimi elementi - 1-2 del: Načela kibernetške odpornosti

Cybersecurity requirements for products with digital elements - Part 1-2: Principles for cyber resilience

Cybersicherheitsanforderungen für Produkte mit digitalen Elementen - Grundsätze für die Cyberresilienz

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

Ta slovenski standard je istoveten z: prEN 40000-1-2

~~oSIST prEN 40000-1-2:2025~~

<https://standards.iteh.ai/catalog/standards/sist/f4ec5c27-ff55-42cd-b7e5-661e0090d24a/osist-pren-40000-1-2-2025>

ICS:

35.030

Informacijska varnost

IT Security

oSIST prEN 40000-1-2:2025

en,fr,de

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 40000-1-2

October 2025

ICS 35.030

English version

**Cybersecurity requirements for products with digital
elements - Part 1-2: Principles for cyber resilience**

Anforderungen an die Cybersicherheit von Produkten
mit digitalen Bestandteilen - Grundsätze für die
Cyberresilienz

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation. Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



Contents	Page
European foreword	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Introduction	6
5 Cybersecurity principles	7
5.1 General	7
5.2 Risk-based approach to cybersecurity	7
5.2.1 Principle	7
5.2.2 Guidance	7
5.3 Security by design	8
5.3.1 Principle	8
5.3.2 Guidance	8
5.4 Secure by default	9
5.4.1 Principle	9
5.4.2 Guidance	9
5.5 Transparency	9
5.5.1 Principle	9
5.5.2 Guidance	9
6 Risk management elements	10
6.1 General	10
6.2 Product context	12
6.2.1 General	12
6.2.2 Input	13
6.2.3 Requirement	14
6.2.4 Output	14
6.2.5 Assessment criteria	14
6.3 Risk acceptance criteria and risk management methodology	14
6.3.1 General	14
6.3.2 Input	16
6.3.3 Requirement	16
6.3.4 Output	16
6.3.5 Assessment criteria	16
6.4 Risk assessment	17
6.4.1 General	17
6.4.2 Asset and cybersecurity objective identification	17
6.4.3 Threat identification	18
6.4.4 Risk estimation	19
6.4.5 Risk evaluation	20
6.5 Risk treatment	21
6.5.1 General	21
6.5.2 Input	22
6.5.3 Requirement	22
6.5.4 Output	22
6.5.5 Assessment criteria	22
6.6 Risk communication	23
6.6.1 General	23
6.6.2 Input	23
6.6.3 Requirement	23
6.6.4 Output	24
6.6.5 Assessment criteria	24
6.7 Risk monitoring and review	24

6.7.1	General	24
6.7.2	Input	24
6.7.3	Requirement	24
6.7.4	Output	25
6.7.5	Assessment criteria	25
7	Cybersecurity activities	25
7.1	General	25
7.2	Product cybersecurity planning	26
7.2.1	General	26
7.2.2	Input	26
7.2.3	Requirement	26
7.2.4	Output	26
7.2.5	Assessment criteria	26
7.3	Product cybersecurity requirements	26
7.3.1	General	26
7.3.2	Input	27
7.3.3	Requirement	27
7.3.4	Output	28
7.3.5	Assessment criteria	28
7.4	Cybersecurity architecture and design	28
7.4.1	General	28
7.4.2	Input	28
7.4.3	Requirement	28
7.4.4	Output	29
7.4.5	Assessment criteria	29
7.5	Secure implementation	29
7.5.1	General	29
7.5.2	Input	30
7.5.3	Requirement	30
7.5.4	Output	30
7.5.5	Assessment criteria	30
7.6	Cybersecurity verification and validation	31
7.6.1	General	31
7.6.2	Input	32
7.6.3	Requirement	32
7.6.4	Output	33
7.6.5	Assessment criteria	33
7.7	Secure production and distribution	33
7.7.1	General	33
7.7.2	Digital production	34
7.7.3	Manufacturing	35
7.8	Cybersecurity issue management	36
7.8.1	General	36
7.8.2	Input	36
7.8.3	Requirement	36
7.8.4	Output	37
7.8.5	Assessment criteria	37
7.9	Product monitoring	37
7.9.1	General	37
7.9.2	Input	37
7.9.3	Requirement	37
7.9.4	Output	38
7.9.5	Assessment criteria	38
7.10	Planning for secure decommissioning	38
7.10.1	General	38
7.10.2	Input	38
7.10.3	Requirement	38

prEN 40000-1-2 (E)

7.10.4 Output	39
7.10.5 Assessment criteria	39
7.11 Third-party component cybersecurity management	39
7.11.1 General	39
7.11.2 Input	40
7.11.3 Requirement	40
7.11.4 Output	41
7.11.5 Assessment criteria	41
Annex A (informative) Coherence with vertical standards	42
A.1 Coherence elements	42
Annex B (informative) Example of a Cybersecurity Supplier Agreement (CSSA)	43
B.1 General	43
B.2 CSSA example	44
Annex C (informative) Relationship between this European Standard and the essential cybersecurity requirements of Regulation (EU) 2024/2847	48
C.1 General	48
C.2 Reference to essential requirements	48
C.3 Mapping to essential requirements	48
C.4 Normative or informative	51
C.5 Assessment criteria	52
Annex D (informative) Accessible and inclusive cybersecurity	53
D.1 Scope	53
D.2 Legal reasoning	53
D.3 The user	53
D.4 Nature of the required interaction	54
D.5 Consequences of the interaction method on the user's cybersecurity	54
D.6 Recommended solution to ensure maximum cybersecurity to the potential users	54
D.7 Communication with the user	55
Bibliography	56

oSIST prEN 40000-1-2:2025

<https://standards.iteh.ai/catalog/standards/sist/f4ec5c27-ff55-42cd-b7e5-661e0090d24a/osist-pren-40000-1-2-2025>

European foreword

This document (prEN 40000-1-2:2025) has been prepared by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection", the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a standardization request addressed to CEN by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 40000-1-2:2025](https://standards.iteh.ai/catalog/standards/sist/f4ec5c27-ff55-42cd-b7e5-661e0090d24a/osist-pren-40000-1-2-2025)

<https://standards.iteh.ai/catalog/standards/sist/f4ec5c27-ff55-42cd-b7e5-661e0090d24a/osist-pren-40000-1-2-2025>