

ISO/IEC 27032:2023-06 (E)

Cybersecurity - Guidelines for Internet security

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