

ISO/IEC 27404:2025-10 (E)

Cybersecurity - IoT security and privacy - Cybersecurity labelling framework for consumer IoT

| Contents | | Page |
|--------------------|--|-------------|
| Foreword | | v |
| Introduction | | vi |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms and definitions | 2 |
| 4 | Abbreviated terms | 4 |
| 5 | Overview of cybersecurity labelling for consumer IoT | 5 |
| 5.1 | Cybersecurity labelling for consumer IoT | 5 |
| 5.2 | Guiding principles | 5 |
| 5.3 | Programme objectives | 6 |
| 5.4 | Threats and risks to consumer IoT products | 6 |
| 5.4.1 | General | 6 |
| 5.4.2 | Assumptions | 6 |
| 5.4.3 | Risk considerations and high-level categories | 7 |
| 5.4.4 | Security threats and risks | 7 |
| 5.4.5 | Privacy threats and risks | 8 |
| 5.5 | Relevant standards and guidance documents | 9 |
| 6 | International alignment through a cybersecurity labelling framework | 9 |
| 6.1 | Objectives for international alignment | 9 |
| 6.2 | Determination of cybersecurity requirements through relevant standards and guidance documents | 9 |
| 7 | Requirements and guidance for the components of the cybersecurity labelling framework for consumer IoT | 10 |
| 7.1 | General | 10 |
| 7.2 | Requirements for the cybersecurity labelling framework components | 10 |
| 7.3 | Guidance on the core components of cybersecurity labelling framework | 11 |
| 7.4 | Guidance on key stakeholders' roles and responsibilities | 12 |
| 7.5 | Guidance on binary and multi-level labelling schemes | 13 |
| 7.5.1 | General | 13 |
| 7.5.2 | Binary versus multi-level labelling schemes | 13 |
| 7.5.3 | Basis for levels | 14 |
| 7.6 | Guidance on mutual- and cross-recognition | 14 |
| 7.6.1 | General | 14 |
| 7.6.2 | Benefits | 14 |
| 7.6.3 | Equivalency determination | 15 |
| 7.7 | Guidance on conformity assessment | 15 |
| 7.7.1 | General | 15 |
| 7.7.2 | Assessment activities considerations | 15 |
| 7.8 | Guidance on implementation considerations | 16 |
| 8 | Requirements and guidance for labelling issuance and maintenance for consumer IoT | 16 |
| 8.1 | General | 16 |
| 8.2 | Requirements for labelling issuance and maintenance for consumer IoT | 17 |

| | | |
|--|---|----|
| 8.3 | Guidance on acceptance criteria and validation of application | 17 |
| 8.4 | Guidance on label validity | 18 |
| 8.4.1 | Scope of validity | 18 |
| 8.4.2 | Recommendations for labelled consumer IoT products during validity period | 18 |
| 8.5 | Guidance on surveillance and monitoring | 18 |
| 8.6 | Guidance on label maintenance and lifecycle of consumer IoT | 19 |
| 8.7 | Guidance on renewal of labels | 19 |
| 8.8 | Guidance on revocation of labels | 19 |
| 8.9 | Guidance on change of underlying standard | 20 |
| 8.10 | Guidance on label design and characteristics | 20 |
| 8.10.1 | General | 20 |
| 8.10.2 | Label design | 20 |
| 8.10.3 | Label characteristics | 21 |
| Annex A (informative) Types and features of cybersecurity labels | | 22 |
| Annex B (informative) Illustrative examples of multi-level labelling schemes | | 25 |
| Annex C (informative) Illustrative examples of binary labelling schemes | | 34 |
| Annex D (informative) Determination of equivalency among labelling schemes | | 39 |
| Annex E (informative) Examples of cybersecurity baseline provisions | | 47 |
| Annex F (informative) Examples of security-by-design provisions | | 58 |
| Annex G (informative) Examples of privacy assessment requirements | | 60 |
| Bibliography | | 62 |