

ISO/IEC 27403:2024-06 (E)

Cybersecurity - IoT security and privacy - Guidelines for IoT-domotics

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	2
5	Overview	2
5.1	General	2
5.2	Features	2
5.3	Stakeholders	4
5.4	Life cycles	4
5.5	Reference model	5
5.6	Security and privacy dimensions	8
6	Guidelines for risk assessment	8
6.1	General	8
6.2	Sources of security risks	9
6.2.1	Security risks for service sub-systems	9
6.2.2	Security risks for IoT-domotics gateway	10
6.2.3	Security risks for IoT-domotics devices and physical entities	12
6.2.4	Security risks for networks	13
6.3	Sources of privacy risks	13
6.3.1	Privacy risks for service sub-systems	13
6.3.2	Privacy risks for IoT-domotics gateway	14
6.3.3	Privacy risks for IoT-domotics devices and physical entities	16
6.3.4	Privacy risks for networks	16
7	Security and privacy controls	17
7.1	Principles	17
7.1.1	General	17
7.1.2	Different levels of security for different services	17
7.1.3	Easy security settings for users	17
7.1.4	Failsafe domotics devices	17
7.1.5	Restricted access to content services	17
7.1.6	Consideration for children	17
7.1.7	Scenario-specific privacy preferences	17
7.2	Security controls	18
7.2.1	Policy for IoT-domotics security	18
7.2.2	Organization of IoT-domotics security	18
7.2.3	Asset management	18
7.2.4	Equipment and assets located outside physical secured areas	18
7.2.5	Secure disposal or re-use of equipment	18
7.2.6	Learning from security incidents	19
7.2.7	Secure IoT-domotics system engineering principles	19
7.2.8	Secure development environment and procedures	19
7.2.9	Security of IoT-domotics systems in support of safety	20
7.2.10	Security in connecting varied IoT-domotics devices	20
7.2.11	Verification of IoT-domotics devices and systems design	20
7.2.12	Monitoring and logging	20

7.2.13	Protection of logs	20
7.2.14	Use of suitable networks for the IoT-domotics systems	20
7.2.15	Secure settings and configurations in delivery of IoT-domotics devices and services	20
7.2.16	User and device authentication	21
7.2.17	Provision of software and firmware updates	21
7.2.18	Sharing vulnerability information	21
7.2.19	Security measures adapted to the life cycle of IoT-domotics system and services	21
7.2.20	Guidance for IoT-domotics users on the proper use of IoT-domotics devices and services	21
7.2.21	Determination of security roles for stakeholders	22
7.2.22	Management of vulnerable devices	22
7.2.23	Management of supplier relationships in IoT-domotics security	22
7.2.24	Secure disclosure of Information regarding security of IoT-domotics devices	22
7.3	Privacy controls	22
7.3.1	Prevention of privacy invasive events	22
7.3.2	IoT-domotics privacy by default	22
7.3.3	Provision of privacy notice	23
7.3.4	Verification of IoT-domotics functionality	23
7.3.5	Consideration of IoT-domotics users	23
7.3.6	Management of IoT-domotics privacy controls	23
7.3.7	Unique device identity	24
7.3.8	Fail-safe authentication	24
7.3.9	Minimization of indirect data collection	24
7.3.10	Communication of privacy preferences	24
7.3.11	Verification of automated decision	24
7.3.12	Accountability for stakeholders	24
7.3.13	Unlinkability of PII	24
7.3.14	Sharing information on PII protection measures of IoT-domotics devices	25
Annex A (informative) Use cases of IoT-domotics		26
Annex B (informative) Security and privacy concerns from stakeholders		31
Annex C (informative) Security and privacy responsibilities of stakeholders		35
Annex D (informative) Security measures for different types of IoT-domotics devices		37
Bibliography		39