ISO/IEC 27400:2022-06 (E)

Cybersecurity - IoT security and privacy - Guidelines

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **2**

5 IoT concepts ... **3**
5.1 General ... 3
5.2 Characteristics of IoT systems ... 3
5.3 Stakeholders of IoT systems ... 4
5.3.1 General ... 4
5.3.2 IoT service provider ... 4
5.3.3 IoT service developer ... 4
5.3.4 IoT user ... 5
5.4 IoT ecosystem ... 5
5.5 IoT service life cycles ... 5
5.6 Domain based reference model ... 7

6 Risk sources for IoT systems ... **8**
6.1 General ... 8
6.2 Risk sources ... 9
6.2.1 General ... 9
6.2.2 Sample risk sources related to IoT domains ... 9
6.2.3 Risk sources from outside the IoT domains ... 11
6.2.4 Privacy related risk sources ... 12

7 Security and privacy controls ... **13**
7.1 Security controls ... 13
7.1.1 General ... 13
7.1.2 Security controls for IoT service developer and IoT service provider ... 13
7.1.3 Security controls for IoT user ... 30
7.2 Privacy controls ... 32
7.2.1 General ... 32
7.2.2 Privacy controls for IoT service developer and IoT service provider ... 32
7.2.3 Privacy controls for IoT user ... 38

Annex A (informative) **IoT monitoring camera sample risk scenario** ... **40**

Bibliography ... **42**