

ISO/IEC 27402:2023-11 (E)

Cybersecurity - IoT security and privacy - Device baseline requirements

| Contents | | Page |
|--------------------|--|-------------|
| Foreword | | iv |
| Introduction | | v |
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Terms, definitions and abbreviated terms | 1 |
| 3.1 | Terms and definitions | 1 |
| 3.2 | Abbreviated terms | 3 |
| 4 | Overview | 3 |
| 5 | Requirements | 4 |
| 5.1 | Requirements for IoT device policies and documentation | 4 |
| 5.1.1 | Risk management | 4 |
| 5.1.2 | Information disclosure | 5 |
| 5.1.3 | Vulnerability disclosure and handling processes | 6 |
| 5.2 | Requirements for IoT device capabilities and operations | 6 |
| 5.2.1 | General | 6 |
| 5.2.2 | Configuration | 7 |
| 5.2.3 | Software reset | 7 |
| 5.2.4 | User data removal | 8 |
| 5.2.5 | Protection of data | 8 |
| 5.2.6 | Interface access | 10 |
| 5.2.7 | Software and firmware updates | 11 |
| 5.2.8 | User notifications | 12 |
| | Annex A (informative) Risk management guidance | 13 |
| | Bibliography | 15 |