DIN ISO 28000:2023-11 (E)

Security and resilience - Security management systems - Requirements (ISO 28000:2022)

Contents

Page

National foreword ... **4**

National Annex NA (informative) **Bibliography** ... **6**

Foreword ... **7**

Introduction ... **8**

1 Scope ... **10**

2 Normative references ... **10**

3 Terms and definitions ... **10**

4 Context of the organization ... **13**
4.1 Understanding the organization and its context ... 13
4.2 Understanding the needs and expectations of interested parties ... 13
4.2.1 General ... 13
4.2.2 Legal, regulatory and other requirements ... 13
4.2.3 Principles ... 14
4.3 Determining the scope of the security management system ... 15
4.4 Security management system ... 15

5 Leadership ... **16**
5.1 Leadership and commitment ... 16
5.2 Security policy ... 16
5.2.1 Establishing the security policy ... 16
5.2.2 Security policy requirements ... 17
5.3 Roles, responsibilities and authorities ... 17

6 Planning ... **17**
6.1 Actions to address risks and opportunities ... 17
6.1.1 General ... 17
6.1.2 Determining security-related risks and identifying opportunities ... 18
6.1.3 Addressing security-related risks and exploiting opportunities ... 18
6.2 Security objectives and planning to achieve them ... 18
6.2.1 Establishing security objectives ... 18
6.2.2 Determining security objectives ... 19
6.3 Planning of changes ... 19

7 Support ... **19**
7.1 Resources ... 19
7.2 Competence ... 19
7.3 Awareness ... 20
7.4 Communication ... 20
7.5 Documented information ... 20
7.5.1 General ... 20
7.5.2 Creating and updating documented information ... 20
7.5.3 Control of documented information ... 21

8 Operation ... **21**
8.1 Operational planning and control ... 21
8.2 Identification of processes and activities ... 21
8.3 Risk assessment and treatment ... 22

8.4 Controls 22
8.5 Security strategies, procedures, processes and treatments 23
8.5.1 Identification and selection of strategies and treatments 23
8.5.2 Resource requirements 23
8.5.3 Implementation of treatments 23
8.6 Security plans 23
8.6.1 General 23
8.6.2 Response structure 23
8.6.3 Warning and communication 24
8.6.4 Content of the security plans 24
8.6.5 Recovery 25
9 Performance evaluation 25
9.1 Monitoring, measurement, analysis and evaluation 25
9.2 Internal audit 26
9.2.1 General 26
9.2.2 Internal audit programme 26
9.3 Management review 26
9.3.1 General 26
9.3.2 Management review inputs 27
9.3.3 Management review results 27
10 Improvement 27
10.1 Continual improvement 27
10.2 Nonconformity and corrective action 28
Bibliography 29