DIN EN ISO/IEC 30111:2020-07 (E)

Information technology - Security techniques - Vulnerability handling processes (ISO/ IEC 30111:2019)

Contents

Page

European foreword ... **3**

Foreword ... **4**

Introduction ... **5**

1 Scope ... **6**

2 Normative references ... **6**

3 Terms and definitions ... **6**

4 Abbreviated terms ... **6**

5 Relationships to other International Standards ... **6**
5.1 ISO/IEC 29147 ... 6
5.2 ISO/IEC 27034 (all parts) ... 7
5.3 ISO/IEC 27036-3 ... 7
5.4 ISO/IEC 15408-3 ... 8

6 Policy and organizational framework ... **8**
6.1 General ... 8
6.2 Leadership ... 8
6.2.1 Leadership and commitment ... 8
6.2.2 Policy ... 8
6.2.3 Organizational roles, responsibilities, and authorities ... 9
6.3 Vulnerability handling policy development ... 9
6.4 Organizational framework development ... 9
6.5 Vendor CSIRT or PSIRT ... 10
6.5.1 General ... 10
6.5.2 PSIRT mission ... 10
6.5.3 PSIRT responsibilities ... 10
6.5.4 Staff capabilities ... 11
6.6 Responsibilities of the product business division ... 11
6.7 Responsibilities of customer support and public relations ... 12
6.8 Legal consultation ... 12

7 Vulnerability handling process ... **12**
7.1 Vulnerability handling phases ... 12
7.1.1 General ... 12
7.1.2 Preparation ... 13
7.1.3 Receipt ... 13
7.1.4 Verification ... 14
7.1.5 Remediation development ... 15
7.1.6 Release ... 15
7.1.7 Post-release ... 15
7.2 Process monitoring ... 16
7.3 Confidentiality of vulnerability information ... 16

8 Supply chain considerations ... **16**

Bibliography ... **18**