

# ISO/IEC 30111:2019-10 (E)

## Information technology - Security techniques - Vulnerability handling processes

---

<b>Contents</b>		<b>Page</b>
Foreword .....		iv
Introduction .....		v
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>1</b>
<b>4</b>	<b>Abbreviated terms .....</b>	<b>1</b>
<b>5</b>	<b>Relationships to other International Standards .....</b>	<b>1</b>
<b>6</b>	<b>Policy and organizational framework .....</b>	<b>3</b>
6.1	General .....	3
6.2	Leadership .....	3
6.2.1	Leadership and commitment .....	3
6.2.2	Policy .....	3
6.2.3	Organizational roles, responsibilities, and authorities .....	4
6.3	Vulnerability handling policy development .....	4
6.4	Organizational framework development .....	4
6.5	Vendor CSIRT or PSIRT .....	5
6.5.1	General .....	5
6.5.2	PSIRT mission .....	5
6.5.3	PSIRT responsibilities .....	5
6.5.4	Staff capabilities .....	6
6.6	Responsibilities of the product business division .....	6
6.7	Responsibilities of customer support and public relations .....	7
6.8	Legal consultation .....	7
<b>7</b>	<b>Vulnerability handling process .....</b>	<b>7</b>
7.1	Vulnerability handling phases .....	7
7.1.1	General .....	7
7.1.2	Preparation .....	8
7.1.3	Receipt .....	8
7.1.4	Verification .....	9
7.1.5	Remediation development .....	10
7.1.6	Release .....	10
7.1.7	Post-release .....	10
7.2	Process monitoring .....	11
7.3	Confidentiality of vulnerability information .....	11
<b>8</b>	<b>Supply chain considerations .....</b>	<b>11</b>
Bibliography .....		13