

# ISO/IEC 29151:2017-08 (E)

## Information technology - Security techniques - Code of practice for personally identifiable information protection

---

<b>Contents</b>		<b>Page</b>
<b>1</b>	<b>Scope .....</b>	<b>1</b>
<b>2</b>	<b>Normative references .....</b>	<b>1</b>
<b>3</b>	<b>Definitions and abbreviated terms .....</b>	<b>1</b>
<b>3.1</b>	<b>Definitions .....</b>	<b>1</b>
<b>3.2</b>	<b>Abbreviated terms .....</b>	<b>1</b>
<b>4</b>	<b>Overview .....</b>	<b>2</b>
<b>4.1</b>	<b>Objective for the protection of PII .....</b>	<b>2</b>
<b>4.2</b>	<b>Requirement for the protection of PII .....</b>	<b>2</b>
<b>4.3</b>	<b>Controls .....</b>	<b>2</b>
<b>4.4</b>	<b>Selecting controls .....</b>	<b>2</b>
<b>4.5</b>	<b>Developing organization specific guidelines .....</b>	<b>3</b>
<b>4.6</b>	<b>Life cycle considerations .....</b>	<b>3</b>
<b>4.7</b>	<b>Structure of this Specification .....</b>	<b>3</b>
<b>5</b>	<b>Information security policies .....</b>	<b>4</b>
<b>5.1</b>	<b>Management directions for information security .....</b>	<b>4</b>
<b>6</b>	<b>Organization of information security .....</b>	<b>4</b>
<b>6.1</b>	<b>Internal organization .....</b>	<b>4</b>
<b>6.2</b>	<b>Mobile devices and teleworking .....</b>	<b>5</b>
<b>7</b>	<b>Human resource security .....</b>	<b>6</b>
<b>7.1</b>	<b>Prior to employment .....</b>	<b>6</b>
<b>7.2</b>	<b>During employment .....</b>	<b>6</b>
<b>7.3</b>	<b>Termination and change of employment .....</b>	<b>6</b>
<b>8</b>	<b>Asset management .....</b>	<b>7</b>
<b>8.1</b>	<b>Responsibility for assets .....</b>	<b>7</b>
<b>8.2</b>	<b>Information classification .....</b>	<b>7</b>
<b>8.3</b>	<b>Media handling .....</b>	<b>8</b>
<b>9</b>	<b>Access control .....</b>	<b>9</b>
<b>9.1</b>	<b>Business requirement of access control .....</b>	<b>9</b>
<b>9.2</b>	<b>User access management .....</b>	<b>9</b>
<b>9.3</b>	<b>User responsibilities .....</b>	<b>10</b>
<b>9.4</b>	<b>System and application access control .....</b>	<b>10</b>
<b>10</b>	<b>Cryptography .....</b>	<b>11</b>
<b>10.1</b>	<b>Cryptographic controls .....</b>	<b>11</b>
<b>11</b>	<b>Physical and environmental security .....</b>	<b>11</b>
<b>11.1</b>	<b>Secure areas .....</b>	<b>11</b>
<b>11.2</b>	<b>Equipment .....</b>	<b>12</b>
<b>12</b>	<b>Operations security .....</b>	<b>12</b>
<b>12.1</b>	<b>Operational procedures and responsibilities .....</b>	<b>12</b>
<b>12.2</b>	<b>Protection from malware .....</b>	<b>13</b>
<b>12.3</b>	<b>Backup .....</b>	<b>13</b>

12.4	Logging and monitoring .....	13
12.5	Control of operational software .....	14
12.6	Technical vulnerability management .....	14
12.7	Information systems audit considerations .....	14
13	Communications security .....	15
13.1	Network security management .....	15
13.2	Information transfer .....	15
14	System acquisition, development and maintenance .....	15
14.1	Security requirements of information systems .....	15
14.2	Security in development and support processes .....	16
iv Rec. ITU-T X.1058 (03/2017) 14.3 Test data .....		16
15	Supplier relationships .....	17
15.1	Information security in supplier relationships .....	17
15.2	Supplier service delivery management .....	18
16	Information security incident management .....	18
16.1	Management of information security incidents and improvements .....	18
17	Information security aspects of business continuity management .....	19
17.1	Information security continuity .....	19
17.2	Redundancies .....	19
18	Compliance .....	20
18.1	Compliance with legal and contractual requirements .....	20
18.2	Information security reviews .....	21
Annex A - Extended control set for PII protection (This annex forms an integral part of this Recommendation ..... International Standard.)		22
A.1	General .....	22
A.2	General policies for the use and protection of PII .....	22
A.3	Consent and choice .....	22
A.4	Purpose legitimacy and specification .....	24
A.5	Collection limitation .....	26
A.6	Data minimization .....	26
A.7	Use, retention and disclosure limitation .....	27
A.8	Accuracy and quality .....	30
A.9	Openness, transparency and notice .....	31
A.10	PII principal participation and access .....	32
A.11	Accountability .....	34
A.12	Information security .....	37
A.13	Privacy compliance .....	37
Bibliography .....		39