

# 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>   |

