ISO/IEC 29151:2026-07 (E)

Information security, cybersecurity and privacy protection - Controls, requirements, and guidance for personally identifiable information protection

Contents

			Page
1	Scope		1
2	Normative references		1
3	Terms, definitions and abbreviated terms		1
	3.1	Terms and definitions	1
	3.2	Abbreviated terms	2
4	Overview		2
	4.1	Protection of PII	2
	4.2	Requirement for the protection of PII	2
	4.3	Controls derived from privacy risk assessment	3
	4.4	Selecting controls	3
	4.5	Developing organization specific guidelines	3
	4.6	Life cycle considerations	3
	4.7	Structure of this Specification	4
5	Organizational controls		8
	5.1	Policies for information security	8
	5.2	Information security roles and responsibilities	8
	5.3	Segregation of duties	8
	5.4	Management responsibilities	9
	5.5	Contact with authorities	9
	5.6	Contact with special interest groups	9
	5.7	Threat intelligence	9
	5.8	Information security in project management	9
	5.9	Inventory of information and other associated assets	9
	5.10	Acceptable use of information and other associated assets	10
	5.11	Return of assets	10
	5.12	Classification of information	10
	5.13	Labelling of information	10
	5.14	Information transfer	10
	5.15	Access control	11
	5.16	Identity management	11
	5.17	Authentication information	11
	5.18	Access rights	11
	5.19	Information security in supplier relationships	11
	5.20	Addressing information security within supplier agreements	11
	5.21	Managing information security in the ICT supply chain	12
	5.22	Monitoring, review and change management of supplier services	12
	5.23	Information security for use of cloud services	12
	5.24	Information security incident management planning and preparation	12
	5.25	Assessment and decision on information security events	13

5.26 Response to information security incidents ... 13
5.27 Learning from information security incidents ... 13
5.28 Collection of evidence ... 13
5.29 Information security during disruption ... 13
5.30 ICT readiness for business continuity ... 13
5.31 Legal, statutory, regulatory and contractual requirements ... 13
5.32 Intellectual property rights ... 14
5.33 Protection of records ... 14
5.34 Privacy and protection of PII ... 14
5.35 Independent review of information security ... 14
5.36 Conformance with policies, rules and standards for information security ... 14
5.37 Documented operating procedures ... 14
6 People controls ... 15
6.1 Screening ... 15
6.2 Terms and conditions of employment ... 15
6.3 Information security awareness, education and training ... 15
6.4 Disciplinary process ... 15
6.5 Responsibilities after termination or change of employment ... 15
6.6 Confidentiality or non-disclosure agreements ... 15
6.7 Remote working ... 15
6.8 Information security event reporting ... 15
7 Physical controls ... 16
7.1 Physical security perimeters ... 16
7.2 Physical entry ... 16
7.3 Securing offices, rooms and facilities ... 16
7.4 Physical security monitoring ... 16
7.5 Protecting against physical and environmental threats ... 16
7.6 Working in secure areas ... 16
7.7 Clear desk and clear screen ... 16
7.8 Equipment siting and protection ... 16
7.9 Security of assets off-premises ... 16
7.10 Storage media ... 16
7.11 Supporting utilities ... 16
7.12 Cabling security ... 17
7.13 Equipment maintenance ... 17
7.14 Secure disposal or re-use of equipment ... 17
8 Technological controls ... 17
8.1 User endpoint devices ... 17
8.2 Privileged access rights ... 17
8.3 Information access restriction ... 17
8.4 Access to source code ... 17
8.5 Secure authentication ... 18
8.6 Capacity management ... 18
8.7 Protection against malware ... 18
8.8 Management of technical vulnerabilities ... 18

8.9 Configuration management 18
8.10 Information deletion 18
8.11 Data masking 18
8.12 Data leakage prevention 18
8.13 Information backup 18
8.14 Redundancy of information processing facilities 18
8.15 Logging 18
8.16 Monitoring activities 19
8.17 Clock synchronization 19
8.18 Use of privileged utility programs 19
8.19 Installation of software on operational systems 19
8.20 Networks security 19
8.21 Security of network services 19
8.22 Segregation of networks 19
8.23 Web filtering 19
8.24 Use of cryptography 19
8.25 Secure development life cycle 19
8.26 Application security requirements 19
8.27 Secure system architecture and engineering principles 19
8.28 Secure coding 19
8.29 Security testing in development and acceptance 20
8.30 Outsourced development 20
8.31 Separation of development, test and production environments 20
8.32 Change management 20
8.33 Test information 20
Annex A (normative) – Extended control set for PII protection 21
A.1 General 21
A.2 General policies for the use and protection of PII 21
A.3 Consent and choice 21
A.4 Purpose legitimacy and specification 23
A.5 Collection limitation 25
A.6 Data minimization 25
A.7 Use, retention and disclosure limitation 26
A.8 Accuracy and quality 29
A.9 Openness, transparency and notice 30
A.10 PII principal participation and access 31
A.11 Accountability 33
A.12 Information security 36
A.13 Privacy compliance 36
Annex B (informative) – Correspondence between this Specification and ISO/IEC 29151:2017 38
Bibliography 41