

ISO/IEC 27018:2025-08 (E)

Information security, cybersecurity and privacy protection - Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Overview	3
4.1	Structure of this document	3
4.2	Control layout	10
5	Organizational controls	11
5.1	Policies for information security	11
5.2	Information security roles and responsibilities	11
5.3	Segregation of duties	11
5.4	Management responsibilities	11
5.5	Contact with authorities	11
5.6	Contact with special interest groups	12
5.7	Threat intelligence	12
5.8	Information security in project management	12
5.9	Inventory of information and other associated assets	12
5.10	Acceptable use of information and other associated assets	12
5.11	Return of assets	12
5.12	Classification of information	12
5.13	Labelling of information	12
5.14	Information transfer	12
5.15	Access control	12
5.16	Identity management	13
5.17	Authentication information	13
5.18	Access rights	13
5.19	Information security in supplier relationships	13
5.20	Addressing information security within supplier agreements	13
5.21	Managing information security in the ICT supply chain	13
5.22	Monitoring, review and change management of supplier services	13
5.23	Information security for use of cloud services	13
5.24	Information security incident management planning and preparation	13
5.25	Assessment and decision on information security events	13
5.26	Response to information security incidents	14
5.27	Learning from information security incidents	14
5.28	Collection of evidence	14
5.29	Information security during disruption	14
5.30	ICT readiness for business continuity	14
5.31	Legal, statutory, regulatory and contractual requirements	14
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	Compliance with policies, rules and standards for information security	15

5.37	Documented operating procedures	15
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	16
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	16
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	17
8.6	Capacity management	17
8.7	Protection against malware	17
8.8	Management of technical vulnerabilities	17
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	19
8.15	Logging	19
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	20
8.23	Web filtering	20
8.24	Use of cryptography	20
8.25	Secure development lifecycle	20
8.26	Application security requirements	20
8.27	Secure system architecture and engineering principles	20
8.28	Secure coding	20
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	21

8.33 Test information21
8.34 Protection of information systems during audit testing21
Annex A (informative) Public cloud PII processor extended control set for PII protection 22
Annex B (informative) Correspondence between this document and the first edition ISO/IEC
27018:201930
Bibliography33