



FINAL DRAFT International Standard

ISO/IEC FDIS 27018

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

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2025-05-26

Voting terminates on:
2025-07-21

IT Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27018

<https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158d561354e/iso-iec-fdis-27018>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 27018

<https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158d561354e/iso-iec-fdis-27018>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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 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 information	21
8.34	Protection of information systems during audit testing	21
	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 27018:2019	30
	Bibliography	33

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27018:2019), which has been technically revised.

The main changes are as follows:

- the text has been aligned with ISO/IEC 27002:2022;
- [Annex B](#) has been added.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

0.1 Background and context

Cloud service providers who process personally identifiable information (PII) under contract to their customers are expected to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate in a multinational environment.

A public cloud service provider is a “PII processor” when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person (i.e. a “PII principal”, processing his or her own PII in the cloud) to an organization (i.e. a “PII controller”, processing PII relating to many PII principals). The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to the customer under its contract with the public cloud PII processor. The cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives.

NOTE 1 Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity.

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. This document has the following objectives:

- to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;
- to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;
- to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where the individual cloud service customer data, which are hosted in a multi-party, virtualized server (cloud) environment, can be technically impractical to audit and can potentially increase risks to those physical and logical network security controls in place.

NOTE 2 It is expected that public cloud service providers comply with applicable obligations when acting as a PII processor.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

0.2 PII protection controls for public cloud computing services

This document is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for implementing commonly accepted PII protection controls for organizations acting as public cloud PII processors. In particular, this document has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those PII protection requirements which can apply to public cloud computing service providers acting as PII processors.