ISO/IEC 27018

Search

● Search this site

Home | ISO27k standards | FREE ISO27k Forum | FREE ISO27k Toolkit | FREE ISO27k FAQ | DONATE!

ISO/IEC 27000
ISO/IEC 27001
ISO/IEC 27002
ISO/IEC 27003
ISO/IEC 27004
ISO/IEC 27005
ISO/IEC 27006
ISO/IEC 27007
ISO/IEC TS 27008
ISO/IEC 27010
ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC 27019
ISO/IEC 27021
ISO/IEC TS 27022
ISO/IEC TR 27024
ISO/IEC TS 27028
ISO/IEC TR 27029
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035

< Previous standard ^ Up a level ^ Next standard >

New ISO/IEC 27018:2025 — Information security, cybersecurity and privacy protection — **Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors** *(third edition)*

Abstract

> *"[ISO/IEC 27018] establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, [ISO/IEC 27018] specifies guidelines based on ISO/IEC 27002:2022, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services ... The guidelines in [ISO/IEC 27018] can also be relevant to organizations acting as PII controllers."*

New *[Source: ISO/IEC 27018:2025]*

Introduction

This standard provides guidance aimed at ensuring that cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customers' clients by securing **P**ersonally **I**dentifiable **I**nformation entrusted to them.

See also ISO/IEC 27017 covering the wider information security angles of cloud computing, aside from privacy.

The standard development project had widespread support from national standards bodies plus the **C**loud **S**ecurity **A**lliance.

Scope and purpose

The standard intends to be "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 organisations for implementing commonly accepted PII protection controls".

The standard is primarily concerned with **public-cloud computing service providers acting as *PII processors*** . "A public cloud service provider is a 'PII processor' when it processes PII for and according to the instructions of a cloud service customer" [according to the DIS version]. It does not officially cover *PII principals* (*i.e.* individuals processing their own PII in the cloud, for example using Google Drive) or *PII controllers* (*i.e.* cloud service customers processing PII of their clients/customers/employees and others in the cloud), although they clearly share many concerns and have an interest in the cloud service provider's privacy controls.

The standard interprets rather than duplicates ISO/IEC 27002 in the context of securing personal data processed in the cloud. An annex extends 27002, for example advising cloud service providers to advise their customers if they use sub-contractors.

ISO/IEC 27000, ISO/IEC 27001 and ISO/IEC 27002 are cited as 'normative' (*i.e.* essential) standards, along with ISO/IEC 17788 "Cloud computing - overview and vocabulary" and ISO/IEC 29100 "Privacy framework" (a *free*

ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039
ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27046
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27090
ISO/IEC 27091
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27109
ISO/IEC TS 27110
ISO/IEC TS 27115
ISO/IEC 27116
ISO/IEC 27400
ISO/IEC 27402
ISO/IEC 27403
ISO/IEC 27404
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC 27557
ISO/IEC 27559
ISO/IEC TS 27560

download!).

Status of the standard

The *first* edition was published in **2014**.

The *second* edition (a minor revision) was published in **2019**.

New The current *third* edition was published in **2025**, having been updated to reflect ISO/IEC 27002:2022 and offering an ‘extended control set’ aligned with ISO/IEC 29100:2024

Personal comments

The standard builds on ISO/IEC 27002, expanding on its generic advice in a few areas, and referring to the OECD privacy principles that are enshrined in several privacy laws and regulations around the globe.

In most sections, it simply says:

> *“The objectives specified in, and the contents of,*
> *clause* [whatever] *of ISO/IEC 27002 apply.”*

The expansions or additions are straightforward - no surprises here.

< Previous standard ^ Up a level ^ Next standard >

ISO/IEC 27561

ISO/IEC 27562

ISO/IEC TR 27563

ISO/IEC 27564

ISO/IEC 27565

ISO/IEC 27566

ISO/IEC 27568

ISO/IEC 27569

ISO/IEC TS 27570

ISO/IEC 27573

ISO/IEC 27701

ISO/IEC 27706

ISO 27799

Copyright © 2025 IsecT Ltd. Contact us re Intellectual Property Rights