

---

---

**Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**

*Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

ISO/IEC 27018:2014

<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

ISO/IEC 27018:2014

<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014>



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2014

All rights reserved. Unless otherwise specified, 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  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>0 Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Overview</b> .....	<b>3</b>
4.1 Structure of this standard.....	3
4.2 Control categories.....	4
<b>5 Information security policies</b> .....	<b>4</b>
5.1 Management direction for information security.....	4
<b>6 Organization of information security</b> .....	<b>5</b>
6.1 Internal organization.....	5
6.2 Mobile devices and teleworking.....	5
<b>7 Human resource security</b> .....	<b>5</b>
7.1 Prior to employment.....	5
7.2 During employment.....	5
7.3 Termination and change of employment.....	6
<b>8 Asset management</b> .....	<b>6</b>
<b>9 Access control</b> .....	<b>6</b>
9.1 Business requirements of access control.....	6
9.2 User access management.....	6
9.3 User responsibilities.....	7
9.4 System and application access control.....	7
<b>10 Cryptography</b> .....	<b>8</b>
10.1 Cryptographic controls.....	8
<b>11 Physical and environmental security</b> .....	<b>8</b>
11.1 Secure areas.....	8
11.2 Equipment.....	9
<b>12 Operations security</b> .....	<b>9</b>
12.1 Operational procedures and responsibilities.....	9
12.2 Protection from malware.....	10
12.3 Backup.....	10
12.4 Logging and monitoring.....	11
12.5 Control of operational software.....	12
12.6 Technical vulnerability management.....	12
12.7 Information systems audit considerations.....	12
<b>13 Communications security</b> .....	<b>12</b>
13.1 Network security management.....	12
13.2 Information transfer.....	12
<b>14 System acquisition, development and maintenance</b> .....	<b>13</b>
<b>15 Supplier relationships</b> .....	<b>13</b>
<b>16 Information security incident management</b> .....	<b>13</b>
16.1 Management of information security incidents and improvements.....	13
<b>17 Information security aspects of business continuity management</b> .....	<b>14</b>
<b>18 Compliance</b> .....	<b>14</b>
18.1 Compliance with legal and contractual requirements.....	14

18.2 Information security reviews.....	14
<b>Annex A (normative) Public cloud PII processor extended control set for PII protection.....</b>	<b>15</b>
<b>Bibliography.....</b>	<b>23</b>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC 27018:2014](https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014)

<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014>

## 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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](http://www.iso.org/directives)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

[ISO/IEC 27018:2014  
https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014](https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014)

## 0 Introduction

### 0.1 Background and context

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers have 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 multinationally.

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, a 'PII principal', processing his or her own PII in the cloud, to an organization, a 'PII controller', processing PII relating to many PII principals. The cloud service customer might authorize one or more cloud service users associated with it to use the services made available to it under its contract with the public cloud PII processor. Note that the cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller might 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 Where the public cloud PII processor is processing cloud service customer account data, it might be acting as a PII controller for this purpose. This International Standard does not cover such activity.

The intention of this International Standard, 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. It has the following objectives.

- To help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract.
- 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 individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment might be impractical technically and might increase risks to those physical and logical network security controls in place.

This International Standard does not replace applicable legislation and regulations, but 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 International Standard 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 International Standard has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those PII protection requirements which might apply to public cloud computing service providers acting as PII processors.

Typically an organization implementing ISO/IEC 27001 is protecting its own information assets. However, in the context of PII protection requirements for a public cloud service provider acting as a PII processor, the organization is protecting the information assets entrusted to it by its customers. Implementation of the controls of ISO/IEC 27002 by the public cloud PII processor is both suitable for this purpose and necessary. This International Standard augments the ISO/IEC 27002 controls to accommodate the distributed nature of the risk and the existence of a contractual relationship between the cloud service customer and the public cloud PII processor. This International Standard augments ISO/IEC 27002 in two ways:

- implementation guidance applicable to public cloud PII protection is provided for certain of the existing ISO/IEC 27002 controls, and
- [Annex A](#) provides a set of additional controls and associated guidance intended to address public cloud PII protection requirements not addressed by the existing ISO/IEC 27002 control set.

Most of the controls and guidance in this International Standard will also apply to a PII controller. However, the PII controller will, in most cases, be subject to additional obligations not specified here.

### 0.3 PII protection requirements

It is essential that an organization identifies its requirements for the protection of PII. There are three main sources of requirement, as given below.

- a) Legal, Statutory, Regulatory and Contractual Requirements: One source is the legal, statutory, regulatory and contractual requirements and obligations that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural responsibilities and operating environment. It should be noted that legislation, regulations and contractual commitments made by the PII processor might mandate the selection of particular controls and might also necessitate specific criteria for implementing those controls. These requirements can vary from one jurisdiction to another.
- b) Risks: Another source is derived from assessing risks to the organization associated with PII, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk acceptance, risk communication, risk monitoring and risk review. ISO/IEC 29134 provides guidance on privacy impact assessment.
- c) Corporate policies: While many aspects covered by a corporate policy are derived from legal and socio-cultural obligations, an organization might also choose voluntarily to go beyond the criteria that are derived from the requirements of a).

### 0.4 Selecting and implementing controls in a cloud computing environment

Controls can be selected from this International Standard (which includes by reference the controls from ISO/IEC 27002, creating a combined reference control set for the sector or application defined by the scope). If required, controls can also be selected from other control sets, or new controls can be designed to meet specific needs as appropriate.

**NOTE** A PII processing service provided by a public cloud PII processor could be considered as an application of cloud computing rather than as a sector in itself. Nevertheless, the term 'sector-specific' is used in this International Standard, as this is the conventional term used within other standards in the ISO/IEC 27000 series.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers, and will also be subject to all relevant

national and international legislation and regulations. Where controls from this International Standard are not selected, this needs to be documented with justification for the omission.

Further, the selection and implementation of controls is dependent upon the public cloud provider's actual role in the context of the whole cloud computing reference architecture (see ISO/IEC 17789). Many different organizations can be involved in providing infrastructure and application services in a cloud computing environment. In some circumstances, selected controls can be unique to a particular service category of the cloud computing reference architecture. In other instances, there can be shared roles in implementing security controls. Contractual agreements need to clearly specify the PII protection responsibilities of all organizations involved in providing or using the cloud services, including the public cloud PII processor, its sub-contractors and the cloud service customer.

The controls in this International Standard can be considered as guiding principles and applicable for most organizations. They are explained in more detail below along with implementation guidance. Implementation can be made simpler if requirements for the protection of PII have been considered in the design of the public cloud PII processor's information system, services and operations. Such consideration is an element of the concept that is often called "Privacy by Design". The bibliography lists relevant documents such as ISO/IEC 29101.

### 0.5 Developing additional guidelines

This International Standard can be regarded as a starting point for developing PII protection guidelines. It is possible that not all of the controls and guidance in this code of practice will be applicable. Furthermore, additional controls and guidelines not included in this International Standard might be required. When documents are developed containing additional guidelines or controls, it might be useful to include cross-references to clauses in this International Standard where applicable to facilitate compliance checking by auditors and business partners.

### 0.6 Lifecycle considerations

PII has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The risks to PII can vary during its lifetime but protection of PII remains important to some extent at all stages.

PII protection requirements need to be taken into account as existing and new information systems are managed through their lifecycle.



# Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

## 1 Scope

This International Standard establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

In particular, this International Standard specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which might be applicable within the context of the information security risk environment(s) of a provider of public cloud services.

This International Standard is applicable to all types and sizes of organizations, including public and private companies, government entities and not-for-profit organizations, which provide information processing services as PII processors via cloud computing under contract to other organizations.

The guidelines in this International Standard might also be relevant to organizations acting as PII controllers; however, PII controllers might be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This International Standard is not intended to cover such additional obligations.

## 2 Normative references

ISO/IEC 27018:2014

<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-190019191919/iso-iec-27018-2014>

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788 | Rec. ITU-T Y.3500, *Information technology — Cloud computing — Overview and vocabulary*<sup>1)</sup>

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17788, ISO/IEC 27000 and the following apply.

1) To be published.

**3.1  
data breach**

compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed

[SOURCE: ISO/IEC 27040:—<sup>2)</sup>, 3.7]

**3.2  
personally identifiable information  
PII**

any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

[SOURCE: ISO/IEC 29100:2011, 2.9]

Note 2 to entry: This definition is included to define the term PII as used in this International Standard. A public cloud PII processor is typically not in a position to know explicitly whether information it processes falls into any specified category unless this is made transparent by the cloud service customer.

**3.3  
PII controller**

privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others (e.g. PII processors) to process PII on its behalf while the responsibility for the processing remains with the PII controller.

[SOURCE: ISO/IEC 29100:2011, 2.10]

ISO/IEC 27018:2014  
<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014>

**3.4  
PII principal**

natural person to whom the personally identifiable information (PII) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.

[SOURCE: ISO/IEC 29100:2011, 2.11]

**3.5  
PII processor**

privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

**3.6  
processing of PII**

operation or set of operations performed upon personally identifiable information (PII)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2011, 2.23]

---

2) To be published.

## 3.7

**public cloud service provider**

party which makes cloud services available according to the public cloud model

## 4 Overview

### 4.1 Structure of this standard

This International Standard has a structure similar to that of ISO/IEC 27002. In cases where objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference is provided to ISO/IEC 27002. Additional controls and associated implementation guidance applicable to PII protection for cloud computing service providers are described in [Annex A](#) (normative).

In cases where controls need additional guidance applicable to PII protection for cloud computing service providers, this is given under the heading *Public cloud PII protection implementation guidance*. In some cases, further relevant information that enhances the additional guidance is provided under the heading *Other information for public cloud PII protection*.

As shown in [Table 1](#), such sector-specific guidance and information is included in the categories defined in ISO/IEC 27002. Clause numbers, which have been aligned with the corresponding clause numbers in ISO/IEC 27002, are as indicated in the table.

**Table 1 — Location of sector-specific guidance and other information for implementing controls in ISO/IEC 27002**

Clause number	Title	Remarks
5	Information security policies	Sector-specific implementation guidance and other information is provided.
6	Organization of information security	Sector-specific implementation guidance is provided.
7	Human resource security	Sector-specific implementation guidance and other information is provided.
8	Asset management	No additional sector-specific implementation guidance or other information is provided.
9	Access control	Sector-specific implementation guidance is provided, together with a cross-reference to control(s) in <a href="#">Annex A</a> .
10	Cryptography	Sector-specific implementation guidance is provided.
11	Physical and environmental security	Sector-specific implementation guidance is provided, together with a cross-reference to control(s) in <a href="#">Annex A</a> .
12	Operations security	Sector-specific implementation guidance is provided.
13	Communications security	Sector-specific implementation guidance is provided, together with a cross-reference to control(s) in <a href="#">Annex A</a> .
14	System acquisition, development and maintenance	No additional sector-specific implementation guidance or other information is provided.
15	Supplier relationships	No additional sector-specific implementation guidance or other information is provided.
16	Information security incident management	Sector-specific implementation guidance is provided.
17	Information security aspects of business continuity management	No additional sector-specific implementation guidance or other information is provided.
18	Compliance	Sector-specific implementation guidance is provided, together with a cross-reference to control(s) in <a href="#">Annex A</a> .

## 4.2 Control categories

In line with ISO/IEC 27002, each main control category contains:

- a) a control objective stating what is to be achieved; and
- b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

### **Control**

Defines the specific control statement to satisfy the control objective.

### **Public cloud PII protection implementation guidance**

Provides more detailed information to support the implementation of the control and meeting the control objectives. The guidance may not be entirely suitable or sufficient in all situations, and may not fulfil the organization's specific control requirements. Alternative or additional controls, or other forms of risk treatment (avoiding, transferring or accepting risks), may therefore be appropriate.

### **Other information for public cloud PII protection**

Provides further information that may need to be considered, such as legal considerations and references to other standards.

## 5 Information security policies

**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**

### 5.1 Management direction for information security

The objective specified in ISO/IEC 27002:2013, 5.1 applies.  
ISO/IEC 27018:2014  
<https://standards.iteh.ai/catalog/standards/sist/4ab5df7c-5414-414a-a426-85fd903b9127/iso-iec-27018-2014>

#### 5.1.1 Policies for information security

Control 5.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

### **Public cloud PII protection implementation guidance**

The information security policies should be augmented by a statement concerning support for and commitment to achieving compliance with applicable PII protection legislation and the contractual terms agreed between the public cloud PII processor and its clients (cloud service customers).

Contractual agreements should clearly allocate responsibilities between the public cloud PII processor, its sub-contractors and the cloud service customer, taking into account the type of cloud service in question (e.g. a service of an IaaS, PaaS or SaaS category of the cloud computing reference architecture). For example, the allocation of responsibility for application layer controls may differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service upon which the cloud service customer can build or layer its own applications.

### **Other information for public cloud PII protection**

In some jurisdictions the public cloud PII processor is directly subject to PII protection legislation. Elsewhere, PII protection legislation applies to the PII controller only.

A mechanism to ensure the public cloud PII processor is obliged to support and manage compliance is provided by the contract between the cloud service customer and the public cloud PII processor. The contract could call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this International Standard and in ISO/IEC 27002.