INTERNATIONAL STANDARD

ISO/IEC 27018

Second edition
2019-01

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

Reference number
ISO/IEC 27018:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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).

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).

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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27018:2014), of which it constitutes a minor revision. The main change compared to the previous edition is the correction of an editorial mistake in Annex A.

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.

Introduction

0.1 Background and context

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers need 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 can 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 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 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. 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 can be impractical technically and can increase risks to those physical and logical network security controls in place.

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.

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 document 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 document 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 document also apply to a PII controller. However, the PII controller is, in most cases, 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 can mandate the selection of particular controls and can 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 can 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 document (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 can be considered as an application of cloud computing rather than as a sector in itself. Nevertheless, the term "sector-specific" is used in this document, as this is the conventional term used within other standards in the ISO/IEC 27000 series.

The selection of controls is dependent on 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. It is also subject to relevant national and international legislation and regulations. Where controls from this document are not selected, this needs to be documented with justification for the omission.

Further, the selection and implementation of controls is dependent on 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 document 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" (see Bibliographic entry [9]).

0.5 Developing additional guidelines

This document 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 are applicable. Furthermore, additional controls and guidelines not included in this document can be required. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document 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 document 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, this document specifies guidelines based on ISO/IEC 27002, 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.

This document 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 document can also be relevant to organizations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, *Information technology — Cloud computing — Overview and vocabulary*

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

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

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.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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 27040:2015, 3.7]

3.2
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.4). 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 establish the link between the set of PII and the natural person.

Note 2 to entry: This definition is included to define the term PII as used in this document. A public cloud *PII processor* (3.5) 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.

[SOURCE: ISO/IEC 29100:2011/Amd 1:2018, 2.9, modified — Note 2 to entry has been added.]

3.3
PII controller
privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing *personally identifiable information (PII)* (3.2) other than natural persons who use data for personal purposes

Note 1 to entry: A PII controller sometimes instructs others [e.g. *PII processors* (3.5)] to process PII on its behalf while the responsibility for the processing remains with the PII controller.

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

3.4
PII principal
natural person to whom the *personally identifiable information (PII)* (3.2) 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)* (3.2) on behalf of and in accordance with the instructions of a *PII controller* (3.3)

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

3.6
processing of PII
operation or set of operations performed on *personally identifiable information (PII)* (3.2)

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]

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 document

This document 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.

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 Table 1.

This document shall be used in conjunction with ISO/IEC 27001 and the additional controls specified in Annex A shall be considered for adoption as part of the process of implementing an Information Security Management System based on ISO/IEC 27001.

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 Annex 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 Annex 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 Annex 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 Annex 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), can therefore be appropriate.

Other information for public cloud PII protection

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

5 Information security policies

5.1 Management direction for information security

The objective specified in ISO/IEC 27002:2013, 5.1 applies.

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 can differ depending on whether the public cloud PII processor is providing a SaaS service or rather is providing a PaaS or IaaS service on 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. In others, PII protection legislation can apply 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 can call for independently audited compliance, acceptable to the cloud service customer, e.g. via the implementation of the relevant controls in this document and in ISO/IEC 27002.

5.1.2 Review of the policies for information security

Control 5.1.2 and the associated implementation guidance specified in ISO/IEC 27002 apply.

6 Organization of information security

6.1 Internal organization

The objective specified in ISO/IEC 27002:2013, 6.1 applies.

6.1.1 Information security roles and responsibilities

Control 6.1.1 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 public cloud PII processor should designate a point of contact for use by the cloud service customer regarding the processing of PII under the contract.

6.1.2 Segregation of duties

Control 6.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.4 Contact with special interest groups

Control 6.1.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

6.1.5 Information security in project management

Control 6.1.5 and the associated implementation guidance specified in ISO/IEC 27002 apply.

6.2 Mobile devices and teleworking

The objective specified in, and the contents of, ISO/IEC 27002:2013, 6.2 apply.

7 Human resource security

7.1 Prior to employment

The objective specified in, and the contents of, ISO/IEC 27002:2013, 7.1 apply.

7.2 During employment

The objective specified in ISO/IEC 27002:2013, 7.2 applies.

7.2.1 Management responsibilities

Control 7.2.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.2.2 Information security awareness, education and training

Control 7.2.2 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

Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor (e.g. legal consequences, loss of business and brand or reputational damage), on the staff member (e.g. disciplinary consequences) and on the PII principal (e.g. physical, material and emotional consequences) of breaching privacy or security rules and procedures, especially those addressing the handling of PII.

Other information for public cloud PII protection

In some jurisdictions, the public cloud PII processor can be subject to legal sanctions, including substantial fines directly from the local PII protection authority. In other jurisdictions, the use of International Standards such as this document in setting up the contract between the public cloud PII processor and the cloud service customer should help establish a basis for contractual sanctions for a breach of security rules and procedures.

7.2.3 Disciplinary process

Control 7.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

7.3 Termination and change of employment

The objective specified in, and the contents of, ISO/IEC 27002:2013, 7.3 apply.

8 Asset management

The objectives specified in, and the contents of, ISO/IEC 27002:2013, Clause 8 apply.

9 Access control

9.1 Business requirements of access control

The objective specified in, and the contents of, ISO/IEC 27002:2013, 9.1 apply.

9.2 User access management

The objective specified in ISO/IEC 27002:2013, 9.2 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause.

Public cloud PII protection implementation guidance

In the context of the service categories of the cloud computing reference architecture, the cloud service customer can be responsible for some or all aspects of access management for cloud service users under its control. Where appropriate, the public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control, such as by providing administrative rights to manage or terminate access.

9.2.1 User registration and de-registration

Control 9.2.1 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

Procedures for user registration and de-registration should address the situation where user access control is compromised, such as the corruption or compromise of passwords or other user registration data (e.g. as a result of inadvertent disclosure).

NOTE Individual jurisdictions can impose specific requirements regarding the frequency of checks for unused authentication credentials. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

9.2.2 User access provisioning

Control 9.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.3 Management of privileged access rights

Control 9.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.4 Management of secret authentication information of users

Control 9.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.5 Review of user access rights

Control 9.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.2.6 Removal or adjustment of access rights

Control 9.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.3 User responsibilities

The objective specified in ISO/IEC 27002:2013, 9.3 applies.

9.3.1 Use of secret authentication information

Control 9.3.1 and the associated implementation guidance specified in ISO/IEC 27002 apply.

9.4 System and application access control

The objective specified in ISO/IEC 27002:2013, 9.4 applies.

9.4.1 Information access restriction

Control 9.4.1 and the associated implementation guidance specified in ISO/IEC 27002 apply.

NOTE Additional controls and guidance relevant to information access restriction can be found in A.10.13.

9.4.2 Secure log-on procedures

Control 9.4.2 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

Where required, the public cloud PII processor should provide secure log-on procedures for any accounts requested by the cloud service customer for cloud service users under its control.

9.4.3 Password management system

Control 9.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4.4 Use of privileged utility programs

Control 9.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

9.4.5 Access control to program source code

Control 9.4.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

10 Cryptography

10.1 Cryptographic controls

The objective specified in ISO/IEC 27002:2013, 10.1 applies.

10.1.1 Policy on the use of cryptographic controls

Control 10.1.1 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 public cloud PII processor should provide information to the cloud service customer regarding the circumstances in which it uses cryptography to protect the PII it processes. The public cloud PII processor should also provide information to the cloud service customer about any capabilities it provides that can assist the cloud service customer in applying its own cryptographic protection.

NOTE In some jurisdictions, it can be required to apply cryptography to protect particular kinds of PII, such as health data concerning a PII principal, resident registration numbers, passport numbers and driver's licence numbers.

10.1.2 Key management

Control 10.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11 Physical and environmental security

11.1 Secure areas

The objective specified in, and the contents of, ISO/IEC 27002:2013, 11.1 apply.

11.2 Equipment

The objective specified in ISO/IEC 27002:2013, 11.2 applies.

11.2.1 Equipment siting and protection

Control 11.2.1 and the associated implementation guidance specified in ISO/IEC 27002 apply.

11.2.2 Supporting utilities

Control 11.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.3 Cabling security

Control 11.2.3 and the associated implementation guidance specified in ISO/IEC 27002 apply.

11.2.4 Equipment maintenance

Control 11.2.4 and the associated implementation guidance specified in ISO/IEC 27002 apply.

11.2.5 Removal of assets

Control 11.2.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.6 Security of equipment and assets off-premises

Control 11.2.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

11.2.7 Secure disposal or re-use of equipment

Control 11.2.7 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

For the purposes of secure disposal or re-use, equipment containing storage media that can possibly contain PII should be treated as though it does.

NOTE Additional controls and guidance relevant to secure disposal or re-use of equipment can be found in A.10.13.

11.2.8 Unattended user equipment

Control 11.2.8 and the associated implementation guidance specified in ISO/IEC 27002 apply.

11.2.9 Clear desk and clear screen policy

Control 11.2.9 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12 Operations security

12.1 Operational procedures and responsibilities

The objective specified in ISO/IEC 27002:2013, 12.1 applies.

12.1.1 Documented operating procedures

Control 12.1.1 and the associated implementation guidance specified in ISO/IEC 27002 apply.

12.1.2 Change management

Control 12.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.3 Capacity management

Control 12.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.1.4 Separation of development, testing and operational environments

Control 12.1.4 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

Where the use of PII for testing purposes cannot be avoided a risk assessment should be undertaken. Technical and organizational measures should be implemented to minimize the risks identified.

12.2 Protection from malware

The objective specified in, and the contents of, ISO/IEC 27002:2013, 12.2 apply.

12.3 Backup

The objective specified in ISO/IEC 27002:2013, 12.3 applies.

12.3.1 Information backup

Control 12.3.1 and the associated implementation guidance specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection implementation guidance

Information processing systems based on the cloud computing model introduce additional or alternative mechanisms to off-site backups for protecting against loss of data, ensuring continuity of data processing operations, and providing the ability to restore data processing operations after a disruptive event. Multiple copies of data in physically and/or logically diverse locations (which can be within the information processing system itself) should be created or maintained for the purposes of backup and/or recovery.

PII-specific responsibilities in this respect can lie with the cloud service customer. Where the public cloud PII processor explicitly provides backup and restore services to the cloud service customer, the public cloud PII processor should provide clear information to the cloud service customer about the capabilities of the cloud service with respect to backup and restoration of the cloud service customer data.

NOTE 1 Some jurisdictions can impose specific requirements regarding the frequency of backups. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

Procedures should be put in place to allow for restoration of data processing operations within a specified, documented period after a disruptive event.

The back-up and recovery procedures should be reviewed at a specified, documented frequency.

NOTE 2 Some jurisdictions can impose specific requirements regarding the frequency of reviews of backup and recovery procedures. It is the responsibility of organizations operating in these jurisdictions to ensure that they comply with these requirements.

The use of sub-contractors to store replicated or backup copies of data being processed is covered by the controls in this document applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls in this document.

The public cloud PII processor should have a policy which addresses the requirements for backup of information and any further requirements (e.g. contractual and/or legal requirements) for the erasure of PII contained in information held for backup purposes.

12.4 Logging and monitoring

The objective specified in ISO/IEC 27002:2013, 12.4 applies.

12.4.1 Event logging

Control 12.4.1 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

A process should be put in place to review event logs with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, event logs should record whether or not PII has been changed (added, modified or deleted) as a result of an event and by whom. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there can be varied or shared roles in implementing this guidance.

The public cloud PII processor should define criteria regarding if, when and how log information can be made available to or usable by the cloud service customer. These procedures should be made available to the cloud service customer.

Where a cloud service customer is permitted to access log records controlled by the public cloud PII processor, the public cloud PII processor should ensure that the cloud service customer can only access records that relate to that cloud service customer's activities, and cannot access any log records which relate to the activities of other cloud service customers.

12.4.2 Protection of log information

Control 12.4.2 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 specific implementation guidance

Log information recorded for purposes such as security monitoring and operational diagnostics can contain PII. Measures, such as controlling access (see 9.2.3), should be put in place to ensure that logged information is only used for its intended purposes.

A procedure, preferably automatic, should be put in place to ensure that logged information is deleted within a specified and documented period.

12.4.3 Administrator and operator logs

Control 12.4.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.4.4 Clock synchronization

Control 12.4.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

12.5 Control of operational software

The objective specified in, and the contents of, ISO/IEC 27002:2013, 12.5 apply.

12.6 Technical vulnerability management

The objective specified in, and the contents of, ISO/IEC 27002:2013, 12.6 apply.

12.7 Information systems audit considerations

The objective specified in, and the contents of, ISO/IEC 27002:2013, 12.7 apply.

13 Communications security

13.1 Network security management

The objective specified in, and the contents of, ISO/IEC 27002:2013, 13.1 apply.

13.2 Information transfer

The objective specified in ISO/IEC 27002:2013, 13.2 applies.

13.2.1 Information transfer policies and procedures

Control 13.2.1 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

Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service customers should be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.

13.2.2 Agreements on information transfer

Control 13.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.3 Electronic messaging

Control 13.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

13.2.4 Confidentiality or non-disclosure agreements

Control 13.2.4 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

NOTE Additional controls and guidance relevant to confidentiality or non-disclosure agreements can be found in A.10.1.

14 System acquisition, development and maintenance

The objectives specified in, and the contents of, ISO/IEC 27002:2013, Clause 14 apply.

15 Supplier relationships

The objectives specified in, and the contents of, ISO/IEC 27002:2013, Clause 15 apply.

NOTE Further information regarding supplier relationship management is provided in ISO/IEC 27036-4.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in ISO/IEC 27002:2013, 16.1 applies. The following sector-specific guidance also applies to the implementation of all of the controls in this subclause.

Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, there can be shared roles in the management of information security incidents and making improvements. There can be a need for the public cloud PII processor to cooperate with the cloud service customer in implementing the controls in this subclause.

16.1.1 Responsibilities and procedures

Control 16.1.1 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

An information security incident should trigger a review by the public cloud PII processor, as part of its information security incident management process, to determine if a data breach involving PII has taken place (see A.9.1).

An information security event should not necessarily trigger such a review. An information security event is one that does not result in actual, or the significant probability of, unauthorized access to PII or to any of the public cloud PII processor's equipment or facilities storing PII, and can include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks and packet sniffing.

16.1.2 Reporting information security events

Control 16.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.3 Reporting information security weaknesses

Control 16.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.4 Assessment of and decision on information security events

Control 16.1.4 and the associated implementation guidance specified in ISO/IEC 27002 apply.

16.1.5 Response to information security incidents

Control 16.1.5 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.6 Learning from information security incidents

Control 16.1.6 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

16.1.7 Collection of evidence

Control 16.1.7 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17 Information security aspects of business continuity management

The objectives specified in, and the contents of, ISO/IEC 27002:2013, Clause 17 apply.

18 Compliance

18.1 Compliance with legal and contractual requirements

The objective specified in, and the contents of, ISO/IEC 27002:2013, 18.1 apply.

NOTE Additional controls and guidance relevant to compliance with legal and contractual requirements can be found in A.11.

18.2 Information security reviews

The objective specified in ISO/IEC 27002:2013, 18.2 applies.

18.2.1 Independent review of information security

Control 18.2.1 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

In cases where individual cloud service customer audits are impractical or can increase risks to security (see 0.1), the public cloud PII processor should make available to prospective cloud service customers, prior to entering into, and for the duration of, a contract, independent evidence that information security is implemented and operated in accordance with the public cloud PII processor's policies and procedures. A relevant independent audit as selected by the public cloud PII processor should normally be an acceptable method for fulfilling the cloud service customer's interest in reviewing the public cloud PII processor's processing operations, provided sufficient transparency is provided.

18.2.2 Compliance with security policies and standards

Control 18.2.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2.3 Technical compliance review

Control 18.2.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

Annex A
(normative)

Public cloud PII processor extended control set for PII protection

A.1 General

This annex specifies new controls and associated implementation guidance which, in combination with the augmented controls and guidance in ISO/IEC 27002 (see Clauses 5 to 18), make up an extended control set to meet the requirements for PII protection which apply to public cloud service providers acting as PII processors.

These additional controls are classified according to the 11 privacy principles of ISO/IEC 29100. In many cases, the controls can be classified under more than one of the privacy principles. In such cases, they are classified under the most relevant principle.

A.2 Consent and choice

A.2.1 Obligation to co-operate regarding PII principals' rights

Control

The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them.

Public cloud PII protection implementation guidance

The PII controller's obligations in this respect can be defined by law, by regulations or by contract. These obligations can include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this can include the correction or deletion of PII in a timely fashion.

Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.

A.3 Purpose legitimacy and specification

A.3.1 Public cloud PII processor's purpose

Control

PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer.

Public cloud PII protection implementation guidance

Instructions can be contained in the contract between the public cloud PII processor and the cloud service customer including, e.g. the objective and time frame to be achieved by the service.

In order to achieve the cloud service customer's purpose, there can be technical reasons why it is appropriate for a public cloud PII processor to determine the method for processing PII, consistent with the general instructions of the cloud service customer but without the cloud service customer's

express instruction. For example, in order to efficiently utilize network or processing capacity it can be necessary to allocate specific processing resources depending on certain characteristics of the PII principal. In circumstances where the public cloud PII processor's determination of the processing method involves the collection and use of PII, the public cloud PII processor should adhere to the relevant privacy principles set forth in ISO/IEC 29100.

The public cloud PII processor should provide the cloud service customer with all relevant information, in a timely fashion, to allow the cloud service customer to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the cloud service customer.

A.3.2 Public cloud PII processor's commercial use

Control

PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

NOTE This control is an addition to the more general control in A.3.1 and does not replace or otherwise supersede it.

A.4 Collection limitation

No additional controls are relevant to this privacy principle.

A.5 Data minimization

A.5.1 Secure erasure of temporary files

Control

Temporary files and documents should be erased or destroyed within a specified, documented period.

Public cloud PII protection implementation guidance

Implementation guidance on PII erasure is provided in A.10.3.

Information systems can create temporary files in the normal course of their operation. Such files are specific to the system or application, but can include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they may not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used.

PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.

A.6 Use, retention and disclosure limitation

A.6.1 PII disclosure notification

Control

The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure

and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited.

Public cloud PII protection implementation guidance

The public cloud PII processor should provide contractual guarantees that it will:

— reject any requests for PII disclosure that are not legally binding;

— consult the corresponding cloud service customer where legally permissible before making any PII disclosure; and

— accept any contractually agreed requests for PII disclosures that are authorized by the corresponding cloud service customer.

EXAMPLE A possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

A.6.2 Recording of PII disclosures

Control

Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time.

Public cloud PII protection implementation guidance

PII can be disclosed during the course of normal operations. These disclosures should be recorded (see 12.4.1). Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.

A.7 Accuracy and quality

No additional controls are relevant to this privacy principle.

A.8 Openness, transparency and notice

A.8.1 Disclosure of sub-contracted PII processing

Control

The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use.

Public cloud PII protection implementation guidance

Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub-contractors can only be commissioned on the basis of a consent that can generally be given by the cloud service customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.

Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub-contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors can process data (see A.12.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.11.12).