



ISO/IEC JTC 1/SC 27 **N14158**

ISO/IEC JTC 1/SC 27WG 5 **N514158**

REPLACES: N13502

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: text for publication

TITLE: Text for publication ISO/IEC DIS 27018 – Information technology – Security techniques
-- Code of practice for PII protection in public clouds acting as PII processors

SOURCE: Project editor

DATE: 2014-04-25

PROJECT: 1.27.97 (27018)

STATUS: In accordance with Resolution 11 (contained in SC 27 N14199) of the 17th SC 27/WG 5 meeting in Hong Kong, China, 7th – 11th April 2014 this document has been sent to the ISO Central Secretariat (ITTF) for publication. It is circulated for information.

ACTION ID: ITTF

DUE DATE:

DISTRIBUTION: P-, O, and L-Members

W. Fumy, SC 27 Chairman

M. De Soete, SC 27 Vice-Chair

E. J. Humphreys, T. Chikazawa, M. Bañón, J. Amsenga, K. Rannenberg, WG-Convenors

Ch. Mitchell, Project editor

MEDIUM: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

NO. OF PAGES: 1 + 35 + attachment

ISO/IEC JTC 1/SC 27 **N14158**

Date: 2014-04-22

ISO/IEC 27018

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Information technology — Security techniques — Code of practice for PII protection in public clouds acting as PII processors

Technologies de l'information — Techniques de sécurité — Code de pratique pour la protection PII dans les nuages publics agissant comme des processeurs PII

Document type: International Standard
Document subtype:
Document stage: (60) Publication
Document language: E

STD Version 2.1c2

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to 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
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	vi
0 Introduction.....	vii
0.1 Background and context	vii
0.2 PII protection controls for public cloud computing services	vii
0.3 PII protection requirements.....	viii
0.4 Selecting and implementing controls in a cloud computing environment	viii
0.5 Developing additional guidelines	ix
0.6 Lifecycle considerations.....	ix
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Overview.....	3
4.1 Structure of this standard.....	3
4.2 Control categories	4
5 Information security policies	5
5.1 Management direction for information security	5
5.1.1 Policies for information security	5
5.1.2 Review of the policies for information security	5
6 Organization of information security	6
6.1 Internal organization	6
6.1.1 Information security roles and responsibilities	6
6.1.2 Segregation of duties	6
6.1.3 Contact with authorities.....	6
6.1.4 Contact with special interest groups	6
6.1.5 Information security in project management	6
6.2 Mobile devices and teleworking	6
7 Human resource security	6
7.1 Prior to employment.....	6
7.2 During employment.....	6
7.2.1 Management responsibilities	6
7.2.2 Information security awareness, education and training.....	7
7.2.3 Disciplinary process	7
7.3 Termination and change of employment	7
8 Asset management.....	7
9 Access control	7
9.1 Business requirements of access control	7
9.2 User access management	7
9.2.1 User registration and de-registration	8
9.2.2 User access provisioning.....	8
9.2.3 Management of privileged access rights	8
9.2.4 Management of secret authentication information of users.....	8
9.2.5 Review of user access rights	8
9.2.6 Removal or adjustment of access rights	8
9.3 User responsibilities	8
9.3.1 Use of secret authentication information	8
9.4 System and application access control	8
9.4.1 Information access restriction	8

9.4.2	Secure log-on procedures	9
9.4.3	Password management system	9
9.4.4	Use of privileged utility programs.....	9
9.4.5	Access control to program source code.....	9
10	Cryptography	9
10.1	Cryptographic controls	9
10.1.1	Policy on the use of cryptographic controls	9
10.1.2	Key management	9
11	Physical and environmental security	10
11.1	Secure areas.....	10
11.2	Equipment	10
11.2.1	Equipment siting and protection.....	10
11.2.2	Supporting utilities	10
11.2.3	Cabling security	10
11.2.4	Equipment maintenance	10
11.2.5	Removal of assets	10
11.2.6	Security of equipment and assets off-premises.....	10
11.2.7	Secure disposal or re-use of equipment	10
11.2.8	Unattended user equipment	10
11.2.9	Clear desk and clear screen policy	11
12	Operations security	11
12.1	Operational procedures and responsibilities	11
12.1.1	Documented operating procedures	11
12.1.2	Change management	11
12.1.3	Capacity management.....	11
12.1.4	Separation of development, testing and operational environments	11
12.2	Protection from malware.....	11
12.3	Backup	11
12.3.1	Information backup.....	11
12.4	Logging and monitoring	12
12.4.1	Event logging	12
12.4.2	Protection of log information	12
12.4.3	Administrator and operator logs.....	13
12.4.4	Clock synchronization	13
12.5	Control of operational software	13
12.6	Technical vulnerability management.....	13
12.7	Information systems audit considerations	13
13	Communications security	13
13.1	Network security management.....	13
13.2	Information transfer.....	13
13.2.1	Information transfer policies and procedures	13
13.2.2	Agreements on information transfer	14
13.2.3	Electronic messaging.....	14
13.2.4	Confidentiality or non-disclosure agreements	14
14	System acquisition, development and maintenance	14
15	Supplier relationships	14
16	Information security incident management	14
16.1	Management of information security incidents and improvements.....	14
16.1.1	Responsibilities and procedures	14
16.1.2	Reporting information security events.....	15
16.1.3	Reporting information security weaknesses	15
16.1.4	Assessment of and decision on information security events	15
16.1.5	Response to information security incidents.....	15
16.1.6	Learning from information security incidents	15
16.1.7	Collection of evidence.....	15
17	Information security aspects of business continuity management	15

18	Compliance	15
18.1	Compliance with legal and contractual requirements	15
18.2	Information security reviews	15
18.2.1	Independent review of information security	16
18.2.2	Compliance with security policies and standards	16
18.2.3	Technical compliance review	16
Annex A	(normative) Public cloud PII processor extended control set for PII protection	17
A.1	Consent and choice	17
A.1.1	Obligation to co-operate regarding PII principals' rights	17
A.2	Purpose legitimacy and specification	17
A.2.1	Public cloud PII processor's purpose	17
A.2.2	Public cloud PII processor's commercial use	18
A.3	Collection limitation	18
A.4	Data minimization	18
A.4.1	Secure erasure of temporary files	18
A.5	Use, retention and disclosure limitation	18
A.5.1	PII disclosure notification	18
A.5.2	Recording of PII disclosures	19
A.6	Accuracy and quality	19
A.7	Openness, transparency and notice	19
A.7.1	Disclosure of sub-contracted PII processing	19
A.8	Individual participation and access	20
A.9	Accountability	20
A.9.1	Notification of a data breach involving PII	20
A.9.2	Retention period for administrative security policies and guidelines	20
A.9.3	PII return, transfer and disposal	21
A.10	Information security	21
A.10.1	Confidentiality or non-disclosure agreements	21
A.10.2	Restriction of the creation of hardcopy material	21
A.10.3	Control and logging of data restoration	22
A.10.4	Protecting data on storage media leaving the premises	22
A.10.5	Use of unencrypted portable storage media and devices	22
A.10.6	Encryption of PII transmitted over public data-transmission networks	22
A.10.7	Secure disposal of hardcopy materials	22
A.10.8	Unique use of user IDs	22
A.10.9	Records of authorized users	22
A.10.10	User ID management	23
A.10.11	Contract measures	23
A.10.12	Sub-contracted PII processing	23
A.10.13	Access to data on pre-used data storage space	24
A.11	Privacy compliance	24
A.11.1	Geographical location of PII	24
A.11.2	Intended destination of PII	24
Bibliography	25

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27018 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

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 may 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, may 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 may possibly 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 may 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 then it may 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 may 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 may be impractical technically and may 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 standard has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those PII protection requirements which may 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: firstly, implementation guidance applicable to public cloud PII protection is provided for certain of the existing ISO/IEC 27002 controls and, secondly, 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 may mandate the selection of particular controls and may also necessitate specific criteria for implementing those controls. These requirements may 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 may 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 should also be subject to all relevant national and international legislation and regulations. Where controls from this International Standard are not selected this should 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 may be involved in providing infrastructure and application services in a cloud computing environment. In some circumstances, selected controls may be unique to a particular service category of the cloud computing reference architecture. In other instances, there may be shared roles in implementing security controls. Contractual agreements should 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 standard can be considered as guiding principles and applicable for most organizations. They are explained in more detail below along with implementation guidance. Implementation may 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. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this 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 may 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 PII protection 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 may 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 may also be relevant to organizations acting as PII controllers; however, PII controllers may 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

The following referenced documents are indispensable for the application 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 17788:2014¹ | ITU-T Recommendation X.3500 (2014)¹, *Information technology — Cloud computing — Overview and Vocabulary*

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*

¹ To be published.

3 Terms and definitions

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

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 27040², 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 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, 2.9]

NOTE 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 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, 2.10]

3.4

PII principal

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

NOTE 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, 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, 2.12]

3.6

processing of PII

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

² To be published.

NOTE 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, 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 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 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), 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**5.1 Management direction for information security**

The objective specified in clause 5.1 of ISO/IEC 27002 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 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.

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 clause 6.1 of ISO/IEC 27002 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, clause 6.2 of ISO/IEC 27002 apply.

7 Human resource security

7.1 Prior to employment

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

7.2 During employment

The objective specified in clause 7.2 of ISO/IEC 27002 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 may 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 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, clause 7.3 of ISO/IEC 27002 apply.

8 Asset management

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

9 Access control

9.1 Business requirements of access control

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

9.2 User access management

The objective specified in clause 9.2 of ISO/IEC 27002 applies. The following sector-specific guidance also applies to the implementation of all of the controls under this subclause (9.2).

Public cloud PII protection implementation guidance

In the context of the service categories of the cloud computing reference architecture, the cloud service customer may 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 may impose specific requirements regarding the frequency of checks for unused authentication credentials. Organizations operating in these jurisdictions should 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 clause 9.3 of ISO/IEC 27002 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 clause 9.4 of ISO/IEC 27002 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 of Annex A (normative).

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 clause 10.1 of ISO/IEC 27002 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 may assist the cloud service customer in applying its own cryptographic protection.

NOTE In some jurisdictions it may 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, clause 11.1 of ISO/IEC 27002 apply.

11.2 Equipment

The objective specified in clause 11.2 of ISO/IEC 27002 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 may 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 clause 12.1 of ISO/IEC 27002 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, clause 12.2 of ISO/IEC 27002 apply.

12.3 Backup

The objective specified in clause 12.3 of ISO/IEC 27002 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 may 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 may 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 Individual jurisdictions may impose specific requirements regarding the frequency of backups. Organizations operating in these jurisdictions should 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 Individual jurisdictions may impose specific requirements regarding the frequency of reviews of backup and recovery procedures. Organizations operating in these jurisdictions should 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 International Standard applying to sub-contracted PII processing. Where physical media transfers take place this is also covered by controls in this International Standard.

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 clause 12.4 of ISO/IEC 27002 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 may 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 may 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, clause 12.5 of ISO/IEC 27002 apply.

12.6 Technical vulnerability management

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

12.7 Information systems audit considerations

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

13 Communications security

13.1 Network security management

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

13.2 Information transfer

The objective specified in clause 13.2 of ISO/IEC 27002 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, clause 14 of ISO/IEC 27002 apply.

15 Supplier relationships

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

NOTE Further information regarding supplier relationship management may be obtained from ISO/IEC 27036-4.

16 Information security incident management

16.1 Management of information security incidents and improvements

The objective specified in clause 16.1 of ISO/IEC 27002 applies. The following sector-specific guidance also applies to the implementation of all of the controls under this subclause (16.1).

Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, there may be shared roles in the management of information security incidents and making improvements. There may 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 may 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, clause 17 of ISO/IEC 27002 apply.

18 Compliance

18.1 Compliance with legal and contractual requirements

The objective specified in, and the contents of, clause 18.1 of ISO/IEC 27002 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 clause 18.2 of ISO/IEC 27002 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 may 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

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 eleven privacy principles of ISO/IEC 29100. In many cases the controls could be classified under more than one of the privacy principles. In such cases they are classified under the most relevant principle.

A.1 Consent and choice

A.1.1 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 may be defined by law, by regulations or by contract. These obligations may include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this could 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.2 Purpose legitimacy and specification

A.2.1 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 may 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 may 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 may 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.2.2 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.2.1 and does not replace or otherwise supersede it.

A.3 Collection limitation

No additional controls are relevant to this privacy principle.

A.4 Data minimization

A.4.1 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.10.11.

Information systems may create temporary files in the normal course of their operation. Such files are specific to the system or application, but may 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.5 Use, retention and disclosure limitation

A.5.1 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.

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

A.5.2 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 may 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.6 Accuracy and quality

No additional controls are relevant to this privacy principle.

A.7 Openness, transparency and notice

A.7.1 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 may 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 may process data (see A.11.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.10.12).

Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.

A.8 Individual participation and access

No additional controls are relevant to this privacy principle.

A.9 Accountability

A.9.1 Notification of a data breach involving PII

Control

The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII.

Public cloud PII protection implementation guidance

Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the cloud service customer. The contract should specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfil his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal or within system components for which they are responsible. The contract should also define the maximum delay in notification of a data breach involving PII.

In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident (including the person in charge and the data recovered) and the fact that the incident resulted in loss, disclosure or alteration of PII.

In the event that a data breach involving PII has occurred, the record should also include a description of the data compromised, if known; and if notifications were performed, the steps taken to notify the cloud service customer and/or regulatory agencies.

In some jurisdictions, relevant legislation or regulations may require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g., a PII protection authority) of a data breach involving PII.

NOTE There may be other breaches requiring notification that are not covered here, e.g., collection without consent or other authorization, use for unauthorized purposes, etc.

A.9.2 Retention period for administrative security policies and guidelines

Control

Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating).

Public cloud PII protection implementation guidance

Review of current and historical policies and procedures may be required, e.g., in the cases of customer dispute resolution and investigation by a PII protection authority. A minimum retention period of five years is recommended in the absence of a specific legal or contractual requirement.

A.9.3 PII return, transfer and disposal

Control

The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer.

Public cloud PII protection implementation guidance

At some point in time, PII may need to be disposed of in some manner. This may involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g., as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it.

The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub-contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually.

The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to cloud service customer.

The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract.

NOTE This control and guidance is also relevant under the retention element of the “Use, retention and disclosure limitation” principle (see A.5).

A.10 Information security

A.10.1 Confidentiality or non-disclosure agreements

Control

Individuals under the public cloud PII processor’s control with access to PII should be subject to a confidentiality obligation.

Public cloud PII protection implementation guidance

A confidentiality agreement, in whatever form, between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer (see A.2.1). The obligations of the confidentiality agreement should survive termination of any relevant contract.

A.10.2 Restriction of the creation of hardcopy material

Control

The creation of hardcopy material displaying PII should be restricted.

Public cloud PII protection implementation guidance

Hardcopy material includes material created by printing.

A.10.3 Control and logging of data restoration

Control

There should be a procedure for, and a log of, data restoration efforts.

Public cloud PII protection implementation guidance

NOTE The above control makes generic the following requirement which applies in certain legal jurisdictions. The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.

A.10.4 Protecting data on storage media leaving the premises

Control

PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g., by encrypting the data concerned).

A.10.5 Use of unencrypted portable storage media and devices

Control

Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.

A.10.6 Encryption of PII transmitted over public data-transmission networks

Control

PII that is transmitted over public data-transmission networks should be encrypted prior to transmission.

Public cloud PII protection implementation guidance

In some cases, e.g., the exchange of e-mail, the inherent characteristics of public data-transmission network systems might require that some header or traffic data be exposed for effective transmission.

Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there may be varied or shared roles in implementing this guidance.

A.10.7 Secure disposal of hardcopy materials

Control

Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.

A.10.8 Unique use of user IDs

Control

If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.

A.10.9 Records of authorized users

Control

An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained.

Public cloud PII protection implementation guidance

A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, necessary to implement the technical controls providing authorized access to the information system.

A.10.10 User ID management

Control

De-activated or expired user IDs should not be granted to other individuals.

Public cloud PII protection implementation guidance

In the context of the whole cloud computing reference architecture, the cloud service customer may be responsible for some or all aspects of user ID management for cloud service users under its control.

A.10.11 Contract measures

Control

Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data is not processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor.

Public cloud PII protection implementation guidance

Information security and PII protection obligations relevant to the public cloud PII processor may arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor should be covered in the contract.

The controls in this International Standard, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the aspects of its services material to the protection of PII.

The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer's responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.

A.10.12 Sub-contracted PII processing

Control

Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor.

Public cloud PII protection implementation guidance

The use of sub-contractors to store backup copies is covered by this control (see A.7.1).

A.10.13 Access to data on pre-used data storage space

Control

The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer.

Public cloud PII protection implementation guidance

Upon deletion by a cloud service user of data held in an information system, performance issues may mean that explicit erasure of that data is impractical. This creates the risk that another user may be able to read the data. Such risk should be avoided by specific technical measures.

No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return zeroes if a cloud service user attempts to read storage space which has not been overwritten by that user's own data.

A.11 Privacy compliance

A.11.1 Geographical location of PII

Control

The public cloud PII processor should specify and document the countries in which PII might possibly be stored.

Public cloud PII protection implementation guidance

The identities of the countries where PII might possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. 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.

A.11.2 Intended destination of PII

Control

PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.

Bibliography

- [1] BS 10012:2009, *Data protection. Specification for a personal information management system*.
- [2] ENISA, *Report on Cloud Computing: Benefits, risks and recommendations for information security*, November 2009 (http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport).
- [3] European Union, Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, adopted July 2012 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf).
- [4] ISO/IEC 17789³, *Information technology — Cloud computing — Reference Architecture*.
- [5] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*.
- [6] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*.
- [7] ISO/IEC 27036-4³, *Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*.
- [8] ISO/IEC 27040³, *Information technology — Security techniques — Storage security*.
- [9] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*.
- [10] ISO/IEC 29134³, *Information technology — Security techniques — Privacy impact assessment — Methodology*.
- [11] ISO/IEC 29191, *Information technology — Security techniques — Requirements for partially anonymous, partially unlinkable authentication*.
- [12] ISO/IEC JTC 1/SC 27, WG 5 Standing Document 2 — Part 1: *Privacy References List*. Latest version available at: <http://www.jtc1sc27.din.de/sbe/wg5SD2-1>.
- [13] JIS Q 15001:2006, *Personal information protection management systems — Requirements*.
- [14] NIST SP 800-53 rev4, *DRAFT Security and Privacy Controls for Federal Information Systems and Organizations* (Initial Public Draft), February 2012 (<http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf>).
- [15] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010 (<http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>).
- [16] NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011 (<http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf>).

³ To be published.



REPORT OF VOTING ON ISO/IEC DIS 27018	
Closing date of voting 2014-04-09	ISO/IEC JTC 1/SC 27
Secretariat DIN	

A report shall be returned to ISO/CS no later than 3 months after the closing date of voting on the DIS, whether or not comments have been reviewed and/or a new text has been prepared.



Preliminary report

(submitted in those cases where comments are still to be considered and/or a decision has not yet been taken, or where it is decided that the nature of comments indicates a need for further consultation and/or reversion to a previous project development stage). To be followed by a 'Final report'. Any preliminary report is for ISO/CS for information, and is not circulated to member bodies)



Final report

(submitted either immediately, when all comments have been reviewed and a decision can be taken, or following a 'Preliminary report'. The final report is circulated by ISO/CS to member bodies, and is distributed with any associated DIS or FDIS text)

1 Result of the voting

The above-mentioned document was circulated to member bodies with a request that the ISO Central Secretariat be informed whether or not member bodies were in favour of registration of the DIS as a Final Draft International Standard or for publication in the case of unanimous approval.

The vote closed on the date indicated above. The replies listed in annex A have been received.

2 Comments received

See annex B (if appropriate)

3 Observations of the secretariat

4 Decision of the Chairman

Preliminary report (no annexes required)



The comments are under review and/or a decision on further procedure has not yet been taken

Final report

Where the approval criteria **are met**:



Having received 100% approval from the member bodies voting OR in light of the decision taken by the committee to skip the FDIS, the DIS is approved for direct publication
(Option not applicable to projects progressing under the Vienna Agreement)



A revised text is to be submitted to ISO/CS for the approval procedure (FDIS vote)

Where the approval criteria **are not met**:



A revised text is to be submitted to ISO/CS for a further enquiry (DIS) vote



The project is to revert to the Committee Stage (a new committee draft will be developed)

Remarks (e.g. observations on how comments were reviewed, date by which a decision is to be taken, date when a text is expected)

The voting results as presented in Annex A (= SC 27 N14157) are as follows:

- P-Members voting: 20 in favour out of 20 = 100 % (requirement $\geq 66.66\%$).
- Member bodies voting: 0 negative votes out of 31 = 0 % (requirement $\leq 25\%$).
- The dispositions of NB and liaison comments (see N13777, N13878) are provided in N14157.

As per Resolution 11 (see N14199) of the 17th SC 27/WG 5 Plenary the final text as contained in N14158 has been submitted to ITTF for publication on 2014-04-25.

Enclosures



Annex A Report of voting



Annex B Note: Comments and observations will be circulated later on.

Signature of the Secretary	Signature of the Chairman
Passia, Krystyna Mrs	Fumy Walter Mr
Date 2014-04-25	Date 2014-04-25

Ballot Information			
Reference	ISO/IEC DIS 27018	Committee	ISO/IEC JTC 1/SC 27
Edition number	1		
English title	Information technology -- Security techniques -- Code of practice for PII protection in public cloud acting as PII processors		
French title	Technologies de l'information -- Techniques de sécurité -- Code de pratique pour la protection PII dans les nuages publics agissant comme des processeurs PII		
Start date	2014-01-07	End date	2014-04-07
Opened by ISO/CS on	2014-01-07 00:23:57	Closed by ISO/CS on	2014-04-09 00:06:24
Status	Closed		
Voting stage	Enquiry	Version number	1
Note			

Result of voting
<p>P-Members voting: 20 in favour out of 20 = 100 % (requirement \geq 66.66%)</p> <p><i>(P-Members having abstained are not counted in this vote.)</i></p> <p>Member bodies voting: 0 negative votes out of 31 = 0 % (requirement \leq 25%)</p> <p><i>Approved</i></p>

Votes by members					
Country	Member	Status	Approval	Disapproval	Abstention
Argentina	IRAM	O-Member			X
Armenia	SARM	P-Member			X
Australia	SA	P-Member			X
Austria	ASI	P-Member			X
Belarus	BELST	O-Member	X		
Belgium	NBN	P-Member	X		
Brazil	ABNT	O-Member	X		
Canada	SCC	P-Member	X *		
China	SAC	P-Member	X		
Côte d'Ivoire	CODINORM	P-Member			X
Czech Republic	UNMZ	P-Member	X		
Denmark	DS	P-Member	X		
Estonia	EVS	O-Member	X		
Finland	SFS	P-Member			X
France	AFNOR	P-Member	X *		
Germany	DIN	P-Member	X		
India	BIS	P-Member	X		
Ireland	NSAI	P-Member	X		
Italy	UNI	P-Member	X		
Japan	JISC	P-Member	X *		
Kazakhstan	KAZMEMST	P-Member	X		
Korea, Republic of	KATS	P-Member	X *		
Lebanon	LIBNOR	P-Member			X
Luxembourg	ILNAS	O-Member			X
Malaysia	DSM	P-Member	X		
Malta	MCCAA	P-Member			X
Mexico	DGN	O-Member	X		
Netherlands	NEN	P-Member			X
New Zealand	SNZ	O-Member	X		
Norway	SN	P-Member	X		
Peru	INDECOPI	O-Member	X		
Poland	PKN	O-Member	X		
Russian Federation	GOST R	P-Member			X
Singapore	SPRING SG	P-Member	X		
Slovenia	SIST	O-Member	X		
South Africa	SABS	P-Member			X
Spain	AENOR	P-Member			X
Sweden	SIS	P-Member	X		
Switzerland	SNV	P-Member			X
Thailand	TISI	O-Member	X		
The Former Yugoslav Republic of Macedonia	ISRM	O-Member	X		

Total of P-Members voting: 20			
TOTALS	31	0	15
(*) A comment file was submitted with this vote			

Comments from Voters		
Canada	SCC	P-Member
France	AFNOR	P-Member
Japan	JISC	P-Member
Korea, Republic of	KATS	P-Member
United Kingdom	BSI	P-Member
United States	ANSI	Secretariat