



ISO/IEC JTC 1/SC 27 **N11742**

ISO/IEC JTC 1/SC 27/WG 5 **N511742**

REPLACES: N11253

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: working draft text

TITLE: Text for ISO/IEC 2nd WD 27018 – Information technology – Security techniques - Code of practice for data protection controls for public cloud computing services

SOURCE: Project editor (Ch. Mitchell)

DATE: 2012-12-18

PROJECT: 1.27.97 (27018)

STATUS: In accordance with resolution 14 (contained in SC 27 N11701) of the 14th SC 27/WG 5 held in Rome (Italy), 22nd – 16th October 2012 this document is circulated for study and comment within SC 27.

National Bodies, experts and liaison organizations of SC 27/WG 5 are requested to send their comments / contributions on the above-mentioned document by 2013-03-20.

PLEASE submit your comments / contributions on the hereby attached document via the SC 27 e-balloting website at: <http://isotc.iso.org/livelink/livelink/open/jtc1sc27>

PLEASE NOTE: For comments please use the SC 27 TEMPLATE separately attached to this document.

ACTION ID: COMM

DUE DATE: 2013-03-20

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. Rannenbergh, WG-Convenors

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

NO. OF PAGES: 1 + 32

ISO/IEC JTC 1/SC 27 N **11742**

Date: 2012-12-14

ISO/IEC WD 27018.2

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

Information technology — Security techniques — Code of practice for data protection controls for public cloud computing services

Technologies de l'information — Techniques de sécurité — Code de pratique pour la protection des données de contrôle des services publics de cloud computing

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard

Document subtype:

Document stage: (20) Preparatory

Document language: E

D:\Dokumente und Einstellungen\pas\Eigene
Dateien\PROJECT_admin\27018_NP_CodePractice_f_DP_contr_f_PUB_CC_serv\02_02_2ndWD_27018_20
1211214\N11742_2nd_WD_27018_20121214\N11742_2ndWD_27018_20121214.doc STD Version 2.1c2

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

Secretariat of ISO/IEC JTC 1/SC 27
DIN German Institute for Standardization
D-10772 Berlin

Tel. + 49 30 2601 2652
Fax + 49 30 2601 4 2652
E-mail krystyna.passia@din.de
Web <http://www.jtc1sc27.din.de/en> (public web site)
<http://isotc.iso.org/livelink/livelink/open/jtc1sc27> (SC 27 documents)

Reproduction for sales purposes 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 Cloud computing information security requirements	vii
0.4 Selecting controls	viii
0.5 Developing additional guidelines	viii
0.6 Lifecycle considerations.....	viii
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 Security policies	4
5.1 Management direction for information security	4
5.1.1 Policies for information security	4
5.1.2 Review of the policies for information security	5
6 Organisation of information security	5
7 Human resource security	5
7.1 Prior to employment.....	5
7.2 During employment.....	5
7.2.1 Management responsibilities	5
7.2.2 Information security awareness, education and training.....	5
7.2.3 Disciplinary process	5
7.3 Termination and change of employment	5
8 Asset management.....	6
8.1 Responsibility for assets	6
8.2 Information classification	6
8.3 Media handling	6
8.3.1 Management of removable media.....	6
8.3.2 Disposal of media	6
8.3.3 Physical media transfer	6
9 Access control	6
9.1 Business requirements of access control	6
9.2 User access management	6
9.2.1 User registration and de-registration	6
9.2.2 Privilege management	7
9.2.3 Management of secret authentication information of users	7
9.2.4 Review of user access rights	7
9.2.5 Removal or adjustment of access rights	7
9.3 User responsibilities	7
9.3.1 Use of secret authentication information	7
9.4 System and application access control	8
9.4.1 Information access restriction	8
9.4.2 Secure log-on procedures	8
9.4.3 Password management system	8

9.4.4	Use of privileged utility programs.....	8
9.4.5	Access control to program source code.....	8
10	Cryptography	8
11	Physical and environmental security	8
12	Operations security	9
12.1	Operational procedures and responsibilities	9
12.1.1	Documented operating procedures	9
12.1.2	Change management	9
12.1.3	Capacity management.....	9
12.1.4	Separation of development, testing and operational environments	9
12.2	Protection from malware.....	9
12.3	Backup	9
12.3.1	Information backup.....	9
12.4	Logging and monitoring	10
12.4.1	Event logging	10
12.4.2	Protection of log information	10
12.4.3	Administrator and operator logs.....	10
12.4.4	Clock synchronization	10
12.5	Control of operational software	11
12.6	Technical vulnerability management.....	11
12.7	Information systems audit considerations	11
13	Communications security	11
13.1	Network security management.....	11
13.2	Information transfer.....	11
13.2.1	Information transfer policies and procedures	11
13.2.2	Agreements on information transfer	11
13.2.3	Electronic messaging.....	11
13.2.4	Confidentiality or non-disclosure agreements	11
14	System acquisition, development and maintenance	12
15	Supplier relationships	12
16	Information security incident management	12
16.1	Management of information security incidents and improvements.....	12
16.1.1	Responsibilities and procedures	12
16.1.2	Reporting information security events.....	12
16.1.3	Reporting information security weaknesses	12
16.1.4	Assessment and decision of information security events	12
16.1.5	Response to information security incidents.....	12
16.1.6	Learning from information security weaknesses.....	13
16.1.7	Collection of evidence.....	13
17	Information security aspects of business continuity management	13
17.1	Information security aspects of business continuity management	13
17.1.1	Planning information security continuity.....	13
17.1.2	Implementing information security continuity	13
17.1.3	Verify, review and evaluate information security continuity.....	13
17.2	Redundancies	13
18	Compliance.....	13
18.1	Compliance with security policies and standards, and technical compliance	13
18.1.1	Independent review of information security	13
18.1.2	Compliance with security policies and standards	14
18.1.3	Technical compliance inspection	14
18.2	Compliance with legal and contractual requirements	14
Annex A	(normative) Public cloud PII processor extended control set for PII protection	15
A.1	Consent and choice.....	15
A.1.1	Obligation to co-operate regarding PII principals' rights.....	15
A.2	Purpose legitimacy and specification	15

A.2.1	PII controller's purpose	15
A.2.2	Cloud PII processor's commercial use	16
A.3	Collection limitation	16
A.4	Data minimization	16
A.4.1	Secure erasure of temporary files	16
A.5	Use, retention and disclosure limitation	16
A.6	Accuracy and quality	16
A.7	Openness, transparency and notice	17
A.7.1	Disclosure of sub-contracted PII processing	17
A.7.2	PII Disclosure notification	17
A.8	Individual participation and access	17
A.9	Accountability	17
A.9.1	Breach notification	17
A.9.2	Maintenance period for administrative security policies and guidelines	18
A.10	Information security	18
A.10.1	Confidentiality or non-disclosure agreements	18
A.10.2	Restriction of the use of printing	18
A.10.3	Control and logging of data restoration	19
A.10.4	Logging of PII disclosures	19
A.10.5	Protecting data on storage media leaving the premises	19
A.10.6	Use of unencrypted storage media	19
A.10.7	Encryption of PII transmitted over public networks	20
A.10.8	Secure disposal of hardcopy materials	20
A.10.9	Unique use of identifiers	20
A.10.10	Records of authorized users	21
A.10.11	Identifier management	21
A.10.12	Password storage	21
A.10.13	Data processing contract measures	21
A.10.14	Sub-contracted PII processing	22
A.11	Privacy compliance	22
A.11.1	Geographical location of PII	22
A.11.2	Intended destination of PII	23
	Bibliography	24

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) on behalf of others have to meet the requirements of applicable legislation and regulations covering the protection of PII. Such legislation, which governs how PII may be collected, used, processed and disposed of, is sometimes referred to as data protection legislation; personally identifiable information (PII) is sometimes referred to elsewhere as personal data. The objective of such legislation and regulations as relevant to the cloud computing service provider is to protect PII being processed from inappropriate disclosure and from inappropriate use.

In general the regulations applicable to a public cloud service provider are those that apply to an entity which is often called a “PII processor” which processes data on behalf of and according to the instructions of another entity called the “PII controller”. Note that the PII controller has authority over the processing and use of the data, and may be subject to a wider set of legislation and regulations governing the protection of PII than the PII processor. Maintaining this distinction assumes that a PII processor has no data processing objective other than that set independently by the PII controller. These PII processor requirements vary from jurisdiction to jurisdiction, which makes it time-consuming for businesses providing cloud computing services to operate multi-nationally.

The objective of the standard is to create a common set of security categories and controls that apply to a public cloud computing service provider, and are aligned with legislation and regulations governing the protection of PII across a wide variety of geographies and jurisdictions. The standard does not aim to apply to the user of the cloud computing service (the customer). The aim is to help public cloud service providers comply with their obligations and to make this transparent to their customers so that customers can select cloud-based data processing services and enter into a contractual agreement that allow them to meet their own obligations. This 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 multi-national market.

Finally, collecting together requirements governing the protection of PII in the context of ISO/IEC 27001 and the guidance for implementing controls given in ISO/IEC 27002, may also help cloud service providers with their compliance audits.

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 organizations for implementing commonly accepted PII protection controls. 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.

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 of its customers. Implementation of the controls of ISO/IEC 27002 by the PII processor is both suitable for this purpose and necessary. However, 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 PII controller and the PII processor.

0.3 Cloud computing information security requirements

It is essential that an organization identifies its requirements for the protection of Personally Identifiable Information. There are two main sources of requirement.

- 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, regulation 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 Personally Identifiable Information, 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.

0.4 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

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 should also be subject to all relevant national and international legislation and regulations.

Further, the selection and implementation of controls is dependent upon the public cloud provider's role in context of the whole services stack. 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 layer of the service stack. In other instances, there may be shared roles in implementing security controls. Contractual agreements should clearly specify the responsibilities of each layer of the service stack.

Some of 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.

0.5 Developing additional guidelines

This International Standard can be regarded as a starting point for developing PII protection specific 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

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

Personally Identifying Information 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 data protection controls for public cloud computing services

EDITOR'S NOTE It was agreed in principle to change the title of this document to 'Code of practice for controls to protect personally identifiable information processed in public cloud computing services'. However, a final decision was deferred until the next meeting of WG 5 in April 2013, since such a change will require SC 27 approval.

1 Scope

This International Standard establishes commonly accepted control objectives, controls and guidelines for implementing controls to protect Personally Identifiable Information 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 Personally Identifiable Information 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 data processing services to other organizations via cloud computing, as part of their information processing.

This International Standard primarily applies to organizations providing cloud computing services that act as PII processors. Typically an organization implementing ISO/IEC 27001 is protecting its own information assets. However, in the context of the PII protection requirements for a public cloud service provider acting as a PII processor, the organization is protecting the information assets of its customers. Implementation of the controls of ISO/IEC 27002 by the PII processor is both suitable for this purpose and necessary. However, 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 PII controller and the PII processor.

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.

EDITOR'S NOTE At the October 2012 WG 2 meeting in Rome, two separate proposals to extend the scope of ISO/IEC 27018 were discussed. These involved (a) covering PII controllers in addition to PII processors, and (b) covering all PII processing, and not just PII processing by public cloud service providers. The relationship to the new work item on PII protection, a proposal for which was agreed in Rome, will also need to be considered. These issues will be revisited in the April 2013 meeting of WG 2. National Body contributions are sought on these questions.

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 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:20xx, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:20xx, *Information technology — Security techniques — Code of practice for information security controls*

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

3 Terms and definitions

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

3.1
cloud computing
paradigm for enabling [ubiquitous, convenient, on-demand] network access to a shared pool of configurable resources accessed through services that can be [rapidly] provisioned and released [with minimal management effort or service provider interaction]

NOTE Some of the terms in this definition are further defined in ISO/IEC CD 17788.

[ISO/IEC CD 17788]

3.2
cloud service provider
party that makes cloud services available to cloud service customer

NOTE 1 The cloud service provider makes the cloud services (3.2.5) available according to the terms and conditions of a service level agreement

NOTE 2 Some of the terms in this definition are further defined in ISO/IEC CD 17788.

[ISO/IEC CD 17788]

3.3
cloud service user
party using one or more cloud services to accomplish some task

NOTE Some of the terms in this definition are further defined in ISO/IEC CD 17788.

[ISO/IEC CD 17788]

3.4
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.

[ISO/IEC 29100]

3.5
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.

[ISO/IEC 29100]

3.6

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”.

[ISO/IEC 29100]

3.7

PII processor

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

[ISO/IEC 29100]

3.8

public cloud

cloud computing made available to any cloud service customers

NOTE 1 Actual availability for specific cloud service customers may be subject to jurisdictional regulations.

NOTE 2 Some of the terms in this definition are further defined in ISO/IEC CD 17788.

[ISO/IEC 17788]

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. Control and implementation guidance specific to PII protection for cloud computing service providers is described in Annex A (normative).

In cases where controls need additional guidance specific to PII protection for cloud computing service providers, this is given under the heading *Public cloud PII protection specific implementation guidance*. Such sector-specific guidance and information is included in the following categories, as defined in ISO/IEC 27002. Clause numbers, which have been aligned with the corresponding clause numbers in ISO/IEC 27002, are indicated in parentheses.

- Security policy (clause 5)
- Organization of information security (clause 6)
- Asset management (clause 7)
- Human resources security (clause 8)
- Physical and environmental security (clause 9)
- Supplier relationship management (clause 10)

- Communications and operations (clause 11)
- Access control (clause 13)
- Systems acquisition, development and maintenance (clause 14)
- Information security incident management (clause 15)
- Business continuity management (clause 16)
- Compliance (clause 17)

EDITOR'S NOTE Clause 12 is omitted as this clause looks set to be removed from the next version of 27002.

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-specific 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.

EDITOR'S NOTE This draft of ISO/IEC 27018 is based on ISO/IEC DIS 27002 (SC 27 N 11907). Future drafts of this standard will be based on the latest version available at the time of drafting.

5 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 specific implementation guidance

The policies should contain a statement concerning support for and commitment to managing compliance with PII protection legislation and the contractual terms agreed between the organization (the cloud PII processor) and its clients (PII controllers).

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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 Organisation of information security

The objectives specified in, and the contents of, clause 6 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 specific implementation guidance

Measures should be put in place designed to ensure that relevant staff are aware of the possible consequences (for example, legal and disciplinary consequences) of breaching the security rules and procedures.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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

8.1 Responsibility for assets

The objective specified in, and the contents of, clause 8.1 of ISO/IEC 27002 apply.

8.2 Information classification

The objective specified in, and the contents of, clause 8.2 of ISO/IEC 27002 apply.

8.3 Media handling

The objective specified in clause 8.3 of ISO/IEC 27002 applies.

8.3.1 Management of removable media

Control 8.3.1 and the associated implementation guidance specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Public cloud PII protection specific implementation guidance

Measures should be put in place designed to ensure that the removal of physical media (e.g., USB sticks, CD-ROMs, and other data carriers) and documents, containing PII, from the premises where the database/application is located, is subject to authorization by an appointed responsible individual or relevant procedure.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

8.3.2 Disposal of media

Control 8.3.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

8.3.3 Physical media transfer

Control 8.3.3 and the associated implementation guidance and other information specified in 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.

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 specific implementation guidance

Procedures for user registration and de-registration should address the corruption or compromise of passwords, e.g. as a result of inadvertent disclosure.

Procedures for user registration and de-registration should include a periodic check for unused authentication credentials. Such a check should occur regularly and at least every six months in the absence of a specific legal or contractual requirement.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

9.2.2 Privilege management

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

9.2.3 Management of secret authentication information of users

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

9.2.4 Review of user access rights

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

9.2.5 Removal or adjustment of access rights

Control 9.2.5 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. The following sector-specific guidance also applies.

Public cloud PII protection specific implementation guidance

If authentication mechanisms used by the personnel of the cloud PII processor are based on passwords there should be an obligation for passwords to be of a specified, documented minimum length. The minimum length should not be less than eight characters in the absence of a specific legal or contractual requirement.

If authentication mechanisms used by the PII controllers are based on passwords, PII controllers should set password length requirements based on the needs of the PII controller.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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.

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 specific implementation guidance

Measures should be put in place designed to limit repeated unsuccessful attempts to gain access to the information system. Where multiple service providers are involved in providing service at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

9.4.3 Password management system

Control 9.4.3 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

Where the password management system enforces regular password changes it is recommended that changes should be enforced every three months in the absence of a specific legal or contractual requirement.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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

The objectives specified in, and the contents of, clause 10 of ISO/IEC 27002 apply.

11 Physical and environmental security

The objectives specified in, and the contents of, clause 11 of 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 specific implementation guidance

The use of PII in testing should be avoided; where the use of PII cannot be avoided, measures should be implemented to secure the testing environment.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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 specific implementation guidance

Multiple copies of data should be created or maintained for purposes of backup or recovery. A frequency of not less than once per week is recommended in the absence of a specific legal or contractual requirement. Where multiple service providers are involved in providing service at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

The back-up and recovery procedures should be reviewed at a specified, documented frequency. The review frequency should not be less than once every six months in the absence of a specific legal or contractual requirement.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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 specific implementation guidance

Measures should be put in place designed to ensure that a security officer has a process for verifying the event log with a specified, documented periodicity, to identify irregularities and propose remediation efforts.

Where possible, the event log 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 at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

The PII controller should be able to obtain relevant extracts from logs of processing operations performed by the cloud PII processor and its sub-contractors.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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, should be put in place designed to ensure that logged information is only used for its intended purposes.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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 specific implementation guidance

A system should be put in place designed to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, the number of physical media, and the types of PII they contain.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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.

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 27036-5.

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.

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 specific implementation guidance

A record of security breaches should be maintained with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data (including person in charge, data recovered, and an indication of any data that had to be inputted manually).

Other information

EDITOR'S NOTE To be drafted if required.

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 and decision of 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 weaknesses

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**17.1 Information security aspects of business continuity management**

The objective specified in clause 17.1 of ISO/IEC 27002 applies.

17.1.1 Planning information security continuity

Control 17.1.1 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17.1.2 Implementing information security continuity

Control 17.1.2 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

Procedures should be put in place designed to allow for continuity of data processing within a specified, documented period.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

17.1.3 Verify, review and evaluate information security continuity

Control 17.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

17.2 Redundancies

The objective specified in, and the contents of, clause 17.2 of ISO/IEC 27002 apply.

18 Compliance**18.1 Compliance with security policies and standards, and technical compliance**

The objective specified in clause 18.1 of ISO/IEC 27002 applies.

18.1.1 Independent review of information security

Control 18.1.1 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 specific implementation guidance

The PII controller should be able to request independent evidence that information security is implemented and operated in accordance with the cloud PII processor's policies and procedures. Relevant third-party certification as selected by the cloud PII processor should normally be an acceptable method for fulfilling the PII controller's interest in auditing the cloud PII processor's processing operations, provided sufficient transparency is provided.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

18.1.2 Compliance with security policies and standards

Control 18.1.2 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.1.3 Technical compliance inspection

Control 18.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply.

18.2 Compliance with legal and contractual requirements

The objective specified in, and the contents of, clause 18.2 of ISO/IEC 27002 apply.

Annex A (normative)

Public cloud PII processor extended control set for PII protection

This annex provides definitions for new controls and associated public cloud PII protection-specific implementation guidance, making up an extended control set to meet the specific requirements for PII protection applying to public cloud service providers acting as PII processors.

These additional controls are classified according to the eleven privacy principles of ISO/IEC 29100.

A.1 Consent and choice

A.1.1 Obligation to co-operate regarding PII principals' rights

Control

The cloud PII processor should co-operate with regard to the PII controller's obligation to facilitate the exercise of PII principals' rights to access, correct, and/or erase PII pertaining to them.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.2 Purpose legitimacy and specification

A.2.1 PII controller's purpose

Control

Measures should be put in place designed to ensure that PII to be processed as part of a contract may not be processed for any purpose independent of the instructions of the PII controller.

Public cloud PII protection-specific implementation guidance

Instructions may be contained in the contract between the cloud PII processor and the PII controller, including, for example, the objective and time frame to be achieved by the service.

In order to achieve the PII controller's purpose, there may be technical reasons why it is appropriate for a cloud PII processor to determine the processing method based on PII, consistent with the general instructions of the PII controller but without the PII controller'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 cloud PII processor's determination of the processing method involves the collection and use of PII, the cloud PII processor should adhere to the data minimization principle set forth in ISO/IEC 29100.

The cloud PII processor should provide the PII controller with all relevant information to allow the PII controller to ensure the cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed for further purposes by the cloud PII processor or any of its sub-contractors.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.2.2 Cloud PII processor's commercial use

Control

Measures should be put in place designed to ensure that PII processed as part of a data processing contract is not used for purposes of advertising without the consent of the PII principal. Such consent should not be a condition of receiving the service.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

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

Measures should be put in place designed to ensure that temporary files and documents are erased or destroyed within a specified, documented period after they are no longer needed.

Public cloud PII protection-specific implementation guidance

PII processing systems should implement a periodic check that unused temporary files above a specified age are deleted from the filing system.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.5 Use, retention and disclosure limitation

No additional controls are relevant to this privacy principle.

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 to process PII should be disclosed in a timely fashion to the relevant PII controllers.

Public cloud PII protection-specific implementation guidance

Provisions for the use of sub-contractors should be transparent in the contract between the cloud PII processor and the PII controller. The contract should specify that sub-contractors may only be commissioned on the basis of a consent that can generally be given by the PII controller at the beginning of the service. The cloud PII processor should inform the PII controller in a timely way of any intended changes in this regard so that the PII controller 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.1.2) and the means by which sub-contractors are obliged to meet or exceed the obligations of the cloud PII processor (see A.9.1).

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.7.2 PII Disclosure notification

Control

The contract should require the cloud PII processor to notify the PII controller 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-specific implementation guidance

The PII controller should obtain contractual guarantees that the cloud PII processor will reject any requests for PII disclosure that are not legally binding.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.8 Individual participation and access

No additional controls are relevant to this privacy principle.

A.9 Accountability

A.9.1 Breach notification

Control

The cloud PII processor should promptly notify the relevant PII controller 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-specific implementation guidance

Breach notification may form part of the contract between the cloud PII processor and the PII controller.

An unsuccessful security incident should not trigger a notification requirement. An unsuccessful security incident is one that does not result in unauthorized access to PII or to any of the 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, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers).

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.9.2 Maintenance period for administrative security policies and guidelines

Control

Measures should be put in place designed to ensure that security governance policies and principal implementing procedures are maintained for a specified, documented period upon replacement (including updating).

Public cloud PII protection-specific implementation guidance

A maintenance period of five years is recommended in the absence of a specific legal or contractual requirement.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10 Information security

A.10.1 Confidentiality or non-disclosure agreements

Control

Measures should be put in place designed to ensure that individuals under the cloud PII processor's control with access to PII are subject to a confidentiality obligation.

Public cloud PII protection-specific implementation guidance

A confidentiality clause should be included in the contract between the cloud PII processor and its employees.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.2 Restriction of the use of printing

Control

Measures should be put in place designed to restrict printing of PII.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.3 Control and logging of data restoration**Control**

Measures should be put in place designed to ensure that there is a procedure for, and a log of, data restoration efforts.

Public cloud PII protection-specific implementation guidance

This log should contain the person responsible, a description of the restored data, and the data that were restored manually.

EDITOR'S NOTE To be completed.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.4 Logging of PII disclosures**Control**

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

Public cloud PII protection-specific implementation guidance

The disclosure of PII does occur as part of normal operation, so regular operational access to PII will be logged (see 12.4.1). Additional disclosures, if any, should also be logged including the person making the disclosure and the source of the authority to make the disclosure.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.5 Protecting data on storage media leaving the premises**Control**

A procedure should be put in place designed to ensure that PII on media leaving the organization's premises is not accessible to anyone other than authorized personnel (e.g., by encrypting the data concerned).

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.6 Use of unencrypted storage media**Control**

Measures should be put in place designed to ensure that physical media and portable devices that do not permit encryption are not used except where it is unavoidable, and designed to ensure that any use of such media and portable devices is documented.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.7 Encryption of PII transmitted over public networks

Control

A procedure should be put in place designed to encrypt PII that is transmitted over public networks.

Public cloud PII protection-specific implementation guidance

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

Where multiple service providers are involved in providing service at different layers of the cloud stack, there may be varied or shared roles in implementing this guidance.

Cryptographic keys should be properly and securely managed.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.8 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.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.9 Unique use of identifiers

Control

If more than one individual has access to stored PII, then measures should be put in place designed to ensure that they each have a distinct identifier for identification, authentication and authorization purposes.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.10 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-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.11 Identifier management**Control**

Measures should be put in place to ensure that de-activated or expired identifiers are not granted to other individuals.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.12 Password storage**Control**

While they are in force, passwords should be stored in a way which makes them unintelligible.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.13 Data processing contract measures**Control**

Data processing contracts between the PII controller and the cloud PII processor should specify concrete, minimum technical and organizational measures designed to ensure information security 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 cloud PII processor.

Public cloud PII protection-specific implementation guidance

The cloud PII processor should inform a prospective PII controller, before entering into a contract, about the aspects of its services material to the protection of PII.

The cloud PII processor should provide the information necessary to allow the PII controller to ensure that PII is erased (by the cloud PII processor and any of its sub-contractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes of the PII controller. The nature of the erasure mechanisms (de-linking, overwriting, demagnetization, destruction, or other forms of erasure) should be provided for contractually.

The cloud PII processor should be transparent about its capabilities during contract negotiations. However, it is ultimately the PII controller's responsibility to ensure that the measures implemented by the cloud PII processor meet its obligations.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.10.14 Sub-contracted PII processing

Control

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

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.11 Privacy compliance

A.11.1 Geographical location of PII

Control

A policy should be put in place designed to specify and document the countries where it is possible that PII might be stored.

Public cloud PII protection-specific implementation guidance

The information about the countries where PII might be stored should be made available to cloud PII processors. The use of sub-contracted PII processing should be taken into account.

Where possible, the cloud PII processor should limit PII transfers to countries chosen by the PII controller.

The cloud PII processor should fulfil its legal obligations regarding cross-border data transfers.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted if required.

A.11.2 Intended destination of PII

Control

Measures should be put in place designed to ensure that it may be ascertained where exactly (to which organization and/or to which individual) PII is intended to be transmitted using data-transmission equipment.

Public cloud PII protection-specific implementation guidance

EDITOR'S NOTE To be drafted if required.

Other information for public cloud PII protection

EDITOR'S NOTE To be drafted.

Bibliography

- [1] 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).
- [2] 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)
- [3] ISO/IEC 17788:xxxx¹, *Information technology — Cloud computing — Vocabulary*.
- [4] ISO/IEC 17789:xxxx¹, *Information technology — Cloud computing — Reference Architecture*.
- [5] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*.
- [6] ISO/IEC 27036-5:xxxx¹, *Information technology — Security techniques — Information security for supplier relationships — Part 5: Guidelines for security of cloud services*
- [7] 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>
- [8] 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>).
- [9] 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>).
- [10] 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>).

¹ To be published.