INTERNATIONAL STANDARD

ISO/IEC 27018

Second edition
2019-01

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

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

iTeh Standards
Document Preview

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

Reference number
ISO/IEC 27018:2019(E)

© ISO/IEC 2019

iTeh Standards
Document Preview

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Overview 3
- 4.1 Structure of this document 3
- 4.2 Control categories 4

5 Information 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 Organization of information security 5
- 6.1 Internal organization 5
  - 6.1.1 Information security roles and responsibilities 5
  - 6.1.2 Segregation of duties 5
  - 6.1.3 Contact with authorities 5
  - 6.1.4 Contact with special interest groups 5
  - 6.1.5 Information security in project management 5
- 6.2 Mobile devices and teleworking 5

7 Human resource security 5
- 7.1 Prior to employment 5
- 7.2 During employment 5
  - 7.2.1 Management responsibilities 6
  - 7.2.2 Information security awareness, education and training 6
  - 7.2.3 Disciplinary process 6
- 7.3 Termination and change of employment 6

8 Asset management 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 7
  - 9.2.2 User access provisioning 7
  - 9.2.3 Management of privileged access rights 7
  - 9.2.4 Management of secret authentication information of users 7
  - 9.2.5 Review of user access rights 7
  - 9.2.6 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 7
  - 9.4.1 Information access restriction 7
  - 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
- 10.1 Cryptographic controls 8
  - 10.1.1 Policy on the use of cryptographic controls 8
  - 10.1.2 Key management 8

iTeh Standards
Document Preview
ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/3b6b30b2-2f-d0fd-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

11 Physical and environmental security ... 8
- 11.1 Secure areas ... 8
- 11.2 Equipment ... 9
  - 11.2.1 Equipment siting and protection ... 9
  - 11.2.2 Supporting utilities ... 9
  - 11.2.3 Cabling security ... 9
  - 11.2.4 Equipment maintenance ... 9
  - 11.2.5 Removal of assets ... 9
  - 11.2.6 Security of equipment and assets off-premises ... 9
  - 11.2.7 Secure disposal or re-use of equipment ... 9
  - 11.2.8 Unattended user equipment ... 9
  - 11.2.9 Clear desk and clear screen policy ... 9

12 Operations security ... 9
- 12.1 Operational procedures and responsibilities ... 9
  - 12.1.1 Documented operating procedures ... 10
  - 12.1.2 Change management ... 10
  - 12.1.3 Capacity management ... 10
  - 12.1.4 Separation of development, testing and operational environments ... 10
- 12.2 Protection from malware ... 10
- 12.3 Backup ... 10
  - 12.3.1 Information backup ... 10
- 12.4 Logging and monitoring ... 11
  - 12.4.1 Event logging ... 11
  - 12.4.2 Protection of log information ... 11
  - 12.4.3 Administrator and operator logs ... 11
  - 12.4.4 Clock synchronization ... 12
- 12.5 Control of operational software ... 12
- 12.6 Technical vulnerability management ... 12
- 12.7 Information systems audit considerations ... 12

13 Communications security ... 12
- 13.1 Network security management ... 12
- 13.2 Information transfer ... 12
  - 13.2.1 Information transfer policies and procedures ... 12
  - 13.2.2 Agreements on information transfer ... 12
  - 13.2.3 Electronic messaging ... 12
  - 13.2.4 Confidentiality or non-disclosure agreements ... 12

14 System acquisition, development and maintenance ... 13

15 Supplier relationships ... 13

16 Information security incident management ... 13
- 16.1 Management of information security incidents and improvements ... 13
  - 16.1.1 Responsibilities and procedures ... 13
  - 16.1.2 Reporting information security events ... 13
  - 16.1.3 Reporting information security weaknesses ... 13
  - 16.1.4 Assessment of and decision on information security events ... 13
  - 16.1.5 Response to information security incidents ... 14
  - 16.1.6 Learning from information security incidents ... 14
  - 16.1.7 Collection of evidence ... 14

17 Information security aspects of business continuity management ... 14

18 Compliance ... 14
- 18.1 Compliance with legal and contractual requirements ... 14
- 18.2 Information security reviews ... 14
  - 18.2.1 Independent review of information security ... 14
  - 18.2.2 Compliance with security policies and standards ... 14
  - 18.2.3 Technical compliance review ... 14

iTeh Standards
Document Preview
ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

Annex A (normative) **Public cloud PII processor extended control set for PII protection** 15
Bibliography 23

iTeh Standards
Document Preview

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

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

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

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b21a1f5/iso-iec-27018-2019

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 Background and context

Cloud service providers who process Personally Identifiable Information (PII) under contract to their customers need to operate their services in ways that allow both parties to meet the requirements of applicable legislation and regulations covering the protection of PII. The requirements and the way in which the requirements are divided between the cloud service provider and its customers vary according to legal jurisdiction, and according to the terms of the contract between the cloud service provider and the customer. Legislation which governs how PII is allowed to be processed (i.e. collected, used, transferred and disposed of) is sometimes referred to as data protection legislation; PII is sometimes referred to as personal data or personal information. The obligations falling on a PII processor vary from jurisdiction to jurisdiction, which makes it challenging for businesses providing cloud computing services to operate multinationally.

A public cloud service provider is a “PII processor” when it processes PII for and according to the instructions of a cloud service customer. The cloud service customer, who has the contractual relationship with the public cloud PII processor, can range from a natural person, a “PII principal”, processing his or her own PII in the cloud, to an organization, a “PII controller”, processing PII relating to many PII principals. The cloud service customer can authorize one or more cloud service users associated with it to use the services made available to it under its contract with the public cloud PII processor. Note that the cloud service customer has authority over the processing and use of the data. A cloud service customer who is also a PII controller can be subject to a wider set of obligations governing the protection of PII than the public cloud PII processor. Maintaining the distinction between PII controller and PII processor relies on the public cloud PII processor having no data processing objectives other than those set by the cloud service customer with respect to the PII it processes and the operations necessary to achieve the cloud service customer's objectives.

NOTE Where the public cloud PII processor is processing cloud service customer account data, it can be acting as a PII controller for this purpose. This document does not cover such activity.

The intention of this document, when used in conjunction with the information security objectives and controls in ISO/IEC 27002, is to create a common set of security categories and controls that can be implemented by a public cloud computing service provider acting as a PII processor. It has the following objectives:

- to help the public cloud service provider to comply with applicable obligations when acting as a PII processor, whether such obligations fall on the PII processor directly or through contract;
- to enable the public cloud PII processor to be transparent in relevant matters so that cloud service customers can select well-governed cloud-based PII processing services;
- to assist the cloud service customer and the public cloud PII processor in entering into a contractual agreement;
- to provide cloud service customers with a mechanism for exercising audit and compliance rights and responsibilities in cases where individual cloud service customer audits of data hosted in a multi-party, virtualized server (cloud) environment can be impractical technically and can increase risks to those physical and logical network security controls in place.

This document can assist by providing a common compliance framework for public cloud service providers, in particular those that operate in a multinational market.

0.2 PII protection controls for public cloud computing services

This document is designed for organizations to use as a reference for selecting PII protection controls within the process of implementing a cloud computing information security management system based on ISO/IEC 27001, or as a guidance document for implementing commonly accepted PII protection controls for organizations acting as public cloud PII processors. In particular, this document has been based on ISO/IEC 27002, taking into consideration the specific risk environment(s) arising from those

PII protection requirements which can apply to public cloud computing service providers acting as PII processors.

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

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

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

0.3 PII protection requirements

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

a) Legal, Statutory, Regulatory and Contractual Requirements: One source is the legal, statutory, regulatory and contractual requirements and obligations that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural responsibilities and operating environment. It should be noted that legislation, regulations and contractual commitments made by the PII processor can mandate the selection of particular controls and can also necessitate specific criteria for implementing those controls. These requirements can vary from one jurisdiction to another.

b) Risks: Another source is derived from assessing risks to the organization associated with PII, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated. ISO/IEC 27005 provides information security risk management guidance, including advice on risk assessment, risk acceptance, risk communication, risk monitoring and risk review. ISO/IEC 29134 provides guidance on privacy impact assessment.

iTeh Standards
Document Preview
ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b3a1f15/iso-iec-27018-2019

c) Corporate policies: While many aspects covered by a corporate policy are derived from legal and socio-cultural obligations, an organization can also choose voluntarily to go beyond the criteria that are derived from the requirements of a).

0.4 Selecting and implementing controls in a cloud computing environment

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

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

The selection of controls is dependent on organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization and, through contractual agreements, its customers and suppliers. It is also subject to relevant national and international legislation and regulations. Where controls from this document are not selected, this needs to be documented with justification for the omission.

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

The controls in this document can be considered as guiding principles and applicable for most organizations. They are explained in more detail below along with implementation guidance. Implementation can be made simpler if requirements for the protection of PII have been considered in the design of the public cloud PII processor's information system, services and operations. Such consideration is an element of the concept that is often called "Privacy by Design" (see Bibliographic entry [9]).

0.5 Developing additional guidelines

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

0.6 Lifecycle considerations

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

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

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

iTeh Standards
Document Preview

ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-a8096b2fa1f5/iso-iec-27018-2019

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

1 Scope

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

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

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

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

iTeh Standards
Document Preview
ISO/IEC 27018:2019
https://standards.iteh.ai/catalog/standards/iso/86300122-d81d-40e5-bde8-c8096b2fa1f5/iso-iec-27018-2019

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*

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

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

3 Terms and definitions

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

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

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
data breach
compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed

[SOURCE: ISO/IEC 27040:2015, 3.7]