
**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*



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

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

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

Foreword

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

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

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

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

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

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

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

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