FINAL DRAFT INTERNATIONAL STANDARD

ISO/IEC FDIS~~-~~ 27018:~~202X(E~~2025(en)

~~ISO/IEC JTC 1/SC 27~~ ~~Secretariat: DIN~~

~~Voting begins on:~~ ~~Voting terminates on:~~
~~202X-MM-DD~~ ~~202X-MM-DD~~

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Date: 2025-05-12

Information security, cybersecurity and privacy protection ~~— Information security controls–~~ Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

~~*Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*~~

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158d s-27018

Style Definition: Heading 1: Indent: Left: 0 cm, First line: 0 cm, Tab stops: Not at 0.76 cm

Style Definition: Heading 2: Tab stops: Not at 0.63 cm

Style Definition: Heading 3

Style Definition: Heading 4

Style Definition: Heading 5

Style Definition: Heading 6

Style Definition: Default Paragraph Font

Style Definition: ANNEX

Style Definition: Comment Text

Style Definition: List Bullet: Indent: Left: 0 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 0.63 cm, List tab

Style Definition: List Bullet 2: Indent: Left: 0.5 cm, Hanging: 0.63 cm, No bullets or numbering, Tab stops: 1.13 cm, List tab

Style Definition ...

Style Definition ...

Style Definition ...

Style Definition ...

Style Definition ...

Style Definition: RefNorm

Style Definition: bib_comment: Font: Cambria

Style Definition: bib_deg: Font: Cambria

Style Definition: bib_suffix: Font: Cambria

Style Definition: bib_unpubl: Font: Cambria

Style Definition: cite_box: Font: Cambria

Style Definition: bib_medline: Font: Cambria

Style Definition ...

Style Definition: Body Text_Center

Style Definition ...

Style Definition: Dimension_100

Style Definition: Figure Graphic

Style Definition: Figure subtitle

Style Definition: List Continue 1

Style Definition: List Number 1: Tab stops: Not at 0.71 cm

Style Definition: Example indent 2: Tab stops: 2.39 cm,

Style Definition ...

Style Definition: Note indent 2

Style Definition: AMEND Terms Heading

Style Definition: AMEND Heading 1 Unnumbered

Formatted: zzCover, Left

Formatted: Font: 12 pt, English (United Kingdom)

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted ...

Formatted: English (United States)

Formatted ...

Formatted: Font: Arial, 12 pt, Font color: Black

Formatted: Right

Formatted: Font: Arial, 12 pt, Font color: Black

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158d561354e/iso-iec-fdis-27018

~~COPYRIGHT PROTECTED DOCUMENT~~

© ISO/IEC 2014 – All rights reserved

© ISO/IEC ~~2024~~2025

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.

~~or ISO's member body in the country of the requester.~~

ISO ~~copyright office~~Copyright Office

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

~~Email: copyright@iso.org~~

Email: copyright@iso.org

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Centered

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Font: Cambria, English (United Kingdom)

Formatted

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: zzCopyright, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: zzCopyright, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: zzCopyright, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: zzCopyright, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: zzCopyright, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font: 11 pt, English (United Kingdom)

Formatted: Font: 11 pt, English (United Kingdom)

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158d561354e/iso-iec-fdis-27018

Formatted: Normal, Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right

Contents

Page

Foreword viii

Introduction x

1 Scope 13

2 Normative references 13

3 Terms and definitions 13

4 Overview 15
4.1 Structure of this document 15
4.2 Control layout 23

5 Organizational controls 23
5.1 Policies for information security 23
5.2 Information security roles and responsibilities 24
5.3 Segregation of duties 24
5.4 Management responsibilities 24
5.5 Contact with authorities 24
5.6 Contact with special interest groups 24
5.7 Threat intelligence 24
5.8 Information security in project management 24
5.9 Inventory of information and other associated assets 24
5.10 Acceptable use of information and other associated assets 24
5.11 Return of assets 24
5.12 Classification of information 24
5.13 Labelling of information 24
5.14 Information transfer 25
5.15 Access control 25
5.16 Identity management 25
5.17 Authentication information 25
5.18 Access rights 25
5.19 Information security in supplier relationships 25
5.20 Addressing information security within supplier agreements 25
5.21 Managing information security in the ICT supply chain 26
5.22 Monitoring, review and change management of supplier services 26
5.23 Information security for use of cloud services 26
5.24 Information security incident management planning and preparation 26
5.25 Assessment and decision on information security events 26
5.26 Response to information security incidents 26
5.27 Learning from information security incidents 26
5.28 Collection of evidence 26
5.29 Information security during disruption 26
5.30 ICT readiness for business continuity 26
5.31 Legal and contractual requirements 26
5.32 Intellectual property rights 26
5.33 Protection of records 26
5.34 Privacy and protection of PII 27
5.35 Independent review of information security 27
5.36 Compliance with policies, rules and standards for information security 27
5.37 Documented operating procedures 27

6 People controls 27
6.1 Screening 27

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC FDIS 27018

Formatted ...
Formatted ...
Field Code Changed ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...

© ISO/IEC 2014 – All rights reserved

6.2 Terms and conditions of employment 27
6.3 Information security awareness, education and training 27
6.4 Disciplinary process 27
6.5 Responsibilities after termination or change of employment 28
6.6 Confidentiality or non-disclosure agreements 28
6.7 Remote working 28
6.8 Information security event reporting 28

7 Physical controls 28
7.1 Physical security perimeters 28
7.2 Physical entry 28
7.3 Securing offices, rooms and facilities 28
7.4 Physical security monitoring 28
7.5 Protecting against physical and environmental threats 28
7.6 Working in secure areas 28
7.7 Clear desk and clear screen 28
7.8 Equipment siting and protection 28
7.9 Security of assets off-premises 28
7.10 Storage media 28
7.11 Supporting utilities 28
7.12 Cabling security 29
7.13 Equipment maintenance 29
7.14 Secure disposal or re-use of equipment 29

8 Technological controls 29
8.1 User endpoint devices 29
8.2 Privileged access rights 29
8.3 Information access restriction 29
8.4 Access to source code 29
8.5 Secure authentication 29
8.6 Capacity management 29
8.7 Protection against malware 29
8.8 Management of technical vulnerabilities 30
8.9 Configuration management 30
8.10 Information deletion 30
8.11 Data masking 30
8.12 Data leakage prevention 30
8.13 Information backup 30
8.14 Redundancy of information processing facilities 31
8.15 Logging 31
8.16 Monitoring activities 31
8.17 Clock synchronization 31
8.18 Use of privileged utility programs 31
8.19 Installation of software on operational systems 31
8.20 Networks security 31
8.21 Security of network services 31
8.22 Segregation of networks 32
8.23 Web filtering 32
8.24 Use of cryptography 32
8.25 Secure development ~~life cycle~~lifecycle 32

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a3[illegible]0-d1[illegible]c/iso-iec-fdis-27018

~~© ISO/IEC 2014 – All rights reserved~~

© ISO/IEC 2025 – All rights reserved

Formatted ...
Formatted ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...
Field Code Changed ...
Formatted ...
Formatted ...

8.26 Application security requirements 32

8.27 Secure system architecture and engineering principles 32

8.28 Secure coding 32

8.29 Security testing in development and acceptance 32

8.30 Outsourced development 32

8.31 Separation of development, test and production environments 32

8.32 Change management 33

8.33 Test information 33

8.34 Protection of information systems during audit testing 33

Annex A (~~normative~~informative) Public cloud PII processor extended control set for PII protection 34

A.1 General 34

A.2 Consent and choice 34

A.2.1 Obligation to co-operate regarding PII principals' rights 34

A.3 Purpose legitimacy and specification 34

A.3.1 Public cloud PII processor's purpose 34

A.3.2 Public cloud PII processor's commercial use 35

A.4 Collection limitation 35

A.5 Data minimization 35

A.5.1 Secure erasure of temporary files 35

A.6 Use, retention and disclosure limitation 35

A.6.1 PII disclosure notification 35

A.6.2 Recording of PII disclosures 36

A.7 Accuracy and quality 36

A.8 Openness, transparency and notice 36

A.8.1 Disclosure of sub-contracted PII processing 36

A.9 Individual participation and access 37

A.10 Accountability 37

A.10.1 Notification of a data breach involving PII 37

A.10.2 Retention period for administrative security policies and guidelines 37

A.10.3 PII return, transfer and disposal 38

A.11 Information security 3838

A.11.1 Confidentiality or non-disclosure agreements 38

A.11.2 Restriction of the creation of hardcopy material 38

A.11.3 Control and logging of data restoration 38

A.11.4 Protecting data on storage media leaving the premises 39

A.11.5 Use of unencrypted portable storage media and devices 39

A.11.6 Encryption of PII transmitted over public data-transmission networks 39

A.11.7 Secure disposal of hardcopy materials 39

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a5?0-d1...-iec-fdis-27018

Formatted
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted
Field Code Changed
Formatted

© ISO/IEC 2014 – All rights reserved

A.11.8 Unique use of user IDs 39

A.11.9 User ID management 39

A.11.10- Records of authorized users 40

A.11.11- Contract measures 40

A.11.12- Sub-contracted PII processing 40

A.11.13- Access to data on pre-used data storage space 40

A.12 Privacy compliance 41

A.12.1 Geographical location of PII 41

A.12.2 Intended destination of PII 41

~~Appendix~~ Annex B (informative) 42

Correspondence ~~of ISO/IEC 27018:202X (~~between this document~~) with~~ and the first edition ISO/IEC 27018:2019 42

Bibliography ....4~~8~~4

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 27018
https://standards.iteh.ai/catalog/standards/iso/23b8f18f-d16c-4fae-a500-d158

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Font: Cambria, English (United Kingdom)

Formatted: Centered

Formatted: Font: Cambria, English (United Kingdom)

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Formatted: Font: Not Bold

Formatted: Right: 0.88 cm, Tab stops: 17.2 cm, Right,Leader: … + Not at 17 cm

Formatted: Not Expanded by / Condensed by

Formatted: Not Expanded by / Condensed by

Field Code Changed

Formatted: Font: 11 pt, English (United States), Ligatures: None

Formatted: Font: 11 pt, English (United States), Ligatures: None

Formatted: TOC 1, Right: 0 cm, Tab stops: Not at 1.27 cm + 17 cm

Formatted: Normal, Centered, Space After: 24 pt, Tab stops: 17.2 cm, Right