

ISO/FDIS 18960:2025 (en)

ISO/TC 68/SC 2

Secretariat: BSI

ISO/TC 68/SC 2/WG 16

Date: 2025-02-18/05-05

Style Definition

Formatted: zzCover large

Formatted: Right: 42.55 pt, Bottom: 28.35 pt, Gutter: 0 pt, Section start: New page, Header distance from edge: 36 pt, Footer distance from edge: 36 pt

Formatted

Security controls and implementation for third-party payment service providers — Guidance and requirements

Formatted: Cover Title_A1

iTeh Standards
(<https://standards.itih.ai>)

FDIS stage Preview

ISO/FDIS 18960

<https://standards.itih.ai/catalog/standards/iso/4eb0502d-5a1b-42d2-af01-4454960ab690/iso-fdis-18960>

~~Edited DIS —~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

© ISO 20242025

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
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

- Formatted: Font: 11 pt, Bold
- Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single
- Formatted: Font: 11 pt, Bold
- Formatted: Font: 11 pt, Bold
- Formatted: Indent: Left: 0 pt, Right: 0 pt, Space Before: 0 pt, No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
- Formatted: Default Paragraph Font
- Formatted: French (Switzerland)
- Formatted: French (Switzerland)
- Formatted: French (Switzerland)
- Formatted: German (Germany)
- Formatted: German (Germany)

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

ISO/FDIS 18960
<https://standards.iteh.ai/catalog/standards/iso/4eb0502d-5a1b-42d2-af01-4454960ab690/iso-fdis-18960>

- Formatted: Font: 10 pt
- Formatted: Font: 10 pt
- Formatted: Font: 11 pt
- Formatted: FooterPageRomanNumber, Space After: 0 pt, Line spacing: single

Contents

Foreword.....vi

Introduction.....vii

1 Scope.....1

2 Normative references1

3 Terms and definitions.....1

4 Abbreviated terms2

5 Security governance controls.....3

5.1 Service security policies.....3

5.2 Roles and responsibilities.....5

5.3 Risk management.....6

5.4 Documentation.....6

5.5 Monitoring, review and improvement.....7

6 Cross-functional controls.....8

6.1 Asset management.....8

6.2 Access management.....8

6.3 Supplier security.....10

6.4 Data security11

6.5 TPP service continuity.....11

7 Function specific controls.....12

7.1 Vulnerability management.....12

7.2 Human security.....13

7.3 Physical security.....15

7.4 Server security16

7.5 Network security19

7.6 TPP application security21

Annex A (informative) Relation between ISO 18960 and ISO 23195.....24

Bibliography26

Foreword.....v

Introduction.....vi

1 Scope.....1

2 Normative references1

3 Terms and definitions.....1

4 Abbreviated terms2

5 Security governance controls.....2

5.1 Service security policies.....2

5.1.1 Establishment of information security policy.....2

5.1.2 PIH protection policy.....2

5.1.3 User permission.....3

5.1.4 User complaint handling policy.....3

5.2 Roles and responsibilities.....4

5.2.1 TPPSP security management organization.....4

5.2.2 Guide for users about security considerations.....4

Formatted: Font: 11 pt, Bold

Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single, Tab stops: Not at 487.55 pt

Formatted: Font: 11 pt, Bold

Formatted: Font: 11 pt, Bold

Formatted: Font: 10 pt

Formatted: FooterCentered, Left, Line spacing: single

Formatted: Font: 10 pt

Formatted: Font: 11 pt

Formatted: FooterPageRomanNumber, Left, Space After: 0 pt, Line spacing: single

5.3	Risk management	4
5.3.1	Establishing risk management process	4
5.3.2	Performing risk assessment and treatment	4
5.4	Documentation	5
5.4.1	Documented information	5
5.4.2	Management of documented information	5
5.5	Monitoring, review and improvement	5
5.5.1	Preservation of logs on incident responses and monitoring	5
5.5.2	Regular security review	6
5.5.3	Continual improvement	6
6	Cross-functional controls	6
6.1	Asset management	6
6.2	Access management	7
6.2.1	Access management of administrators	7
6.2.2	Access management of administrator programs	7
6.2.3	Designation and access management of terminals	7
6.3	Supplier security	8
6.3.1	Selection and management of suppliers	8
6.3.2	Identification and management of the use of cloud services	8
6.4	Data security	9
6.5	TPP service continuity	9
7	Function specific controls	9
7.1	Vulnerability management	9
7.1.1	Preparation of incident response procedures	9
7.1.2	Education and training for incident response	10
7.2	Human security	10
7.2.1	Establishment and implementation of information security education plans	10
7.2.2	Completion of information security education	10
7.2.3	Confidentiality and non-disclosure agreement	11
7.2.4	Segregation of duties	11
7.2.5	Removal or adjustment of access rights at termination and change of employment	11
7.3	Physical security	12
7.3.1	Designation of secure area and entry control	12
7.3.2	Management of secure area's check-in and check-out	12
7.3.3	Management of working environment security	13
7.4	Server security	13
7.4.1	Prevention of malware infection and information leakage	13
7.4.2	Removal of unnecessary functions	14
7.4.3	Important service operation on dedicated server	14
7.4.4	Public web server security	15
7.4.5	Security patch management	15
7.5	Network security	16
7.5.1	Control on remote management through Internet	16
7.5.2	DMZ configuration	16
7.5.3	Use of private IP and network segregation	16
7.5.4	Wireless network security	17
7.5.5	Application of secure communication when communicating with external organizations	17
7.6	TPP application security	18
7.6.1	Identification of security requirements during design stage	18
7.6.2	Web application security	18
7.6.3	Mobile application security	20
Annex A (informative)	Relation between ISO 18960 and ISO 23195	22

Formatted: Font: 11 pt, Bold

Formatted: Font: 11 pt, Bold

Formatted: HeaderCentered, Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt, Bold

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 11 pt

Formatted: FooterPageRomanNumber, Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt, Bold

Formatted: HeaderCentered, Left, Space After: 0 pt, Line spacing: single, Tab stops: Not at 487.55 pt

Formatted: Font: 11 pt, Bold

Formatted: Font: 11 pt, Bold

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

ISO/EDIS 18960
<https://standards.iteh.ai/catalog/standards/iso/4eb0502d-5a1b-42d2-af01-4454960ab690/iso-fdis-18960>

~~Edited DIS -~~
~~MUST BE USED~~
~~FOR FINAL~~
~~DRAFT~~

Formatted: Font: 10 pt

Formatted: FooterCentered, Left, Line spacing: single

Formatted: Font: 10 pt

Formatted: Font: 11 pt

Formatted: FooterPageRomanNumber, Left, Space After: 0 pt, Line spacing: single