



FINAL DRAFT International Standard

ISO/FDIS 18960

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

ISO/TC 68/SC 2

Secretariat: **BSI**

Voting begins on:
2025-05-19

Voting terminates on:
2025-07-14

Itch Standards
(<https://standards.itch.ai>)
Document Preview

ISO/FDIS 18960

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

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.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

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

ISO/FDIS 18960

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



COPYRIGHT PROTECTED DOCUMENT

© ISO 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.

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

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	2
5 Security governance controls	3
5.1 Service security policies	3
5.1.1 Establishment of information security policy	3
5.1.2 PII protection policy	3
5.1.3 User permission	4
5.1.4 User complaint handling policy	4
5.2 Roles and responsibilities	4
5.2.1 TPPSP security management organization	4
5.2.2 Guide for users about security considerations	4
5.3 Risk management	5
5.3.1 Establishing risk management process	5
5.3.2 Performing risk assessment and treatment	5
5.4 Documentation	6
5.4.1 Documented information	6
5.4.2 Management of documented information	6
5.5 Monitoring, review and improvement	6
5.5.1 Preservation of logs on incident responses and monitoring	6
5.5.2 Regular security review	7
5.5.3 Continual improvement	7
6 Cross-functional controls	7
6.1 Asset management	7
6.2 Access management	8
6.2.1 Access management of administrators	8
6.2.2 Access management of administrator programs	8
6.2.3 Designation and access management of terminals	8
6.3 Supplier security	9
6.3.1 Selection and management of suppliers	9
6.3.2 Identification and management of the use of cloud services	9
6.4 Data security	10
6.5 TPP service continuity	10
7 Function specific controls	11
7.1 Vulnerability management	11
7.1.1 Preparation of incident response procedures	11
7.1.2 Education and training for incident response	11
7.1.3 Documentation of vulnerability management policy	12
7.2 Human security	12
7.2.1 Establishment and implementation of information security education plans	12
7.2.2 Completion of information security education	12
7.2.3 Confidentiality and non-disclosure agreement	12
7.2.4 Segregation of duties	13
7.2.5 Removal or adjustment of access rights at termination and change of employment	13
7.3 Physical security	13
7.3.1 Designation of secure area and entry control	13
7.3.2 Management of check-in and check-out of secure area	14
7.3.3 Management of working environment security	14

ISO/FDIS 18960:2025(en)

7.4	Server security	15
7.4.1	Prevention of malware infection and information leakage	15
7.4.2	Removal of unnecessary functions	15
7.4.3	Important service operation on dedicated server	16
7.4.4	Public web server security	16
7.4.5	Security patch management	16
7.4.6	Data sanitization	17
7.5	Network security	17
7.5.1	Control on remote management through Internet	17
7.5.2	Demilitarized zone configuration	17
7.5.3	Use of private IP and network segregation	17
7.5.4	Wireless network security	18
7.5.5	Application of secure communication when communicating with external organizations	18
7.6	TPP application security	19
7.6.1	Identification of security requirements during design stage	19
7.6.2	Web application security	19
7.6.3	Mobile application security	21
Annex A (informative) Relation between ISO 18960 and ISO 23195		22
Bibliography		24

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

ISO/FDIS 18960

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

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

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.

ISO/FDIS 18960

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