INTERNATIONAL STANDARD

ISO 28001

First edition
2007-10-15

Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance

Systèmes de management de la sûreté pour la chaîne d'approvisionnement — Meilleures pratiques pour la mise en application de la sûreté de la chaîne d'approvisionnement, évaluations et plans — Exigences et guidage

Reference number
ISO 28001:2007(E)

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

© ISO 2007

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Field of application 5
4.1 Statement of application 5
4.2 Business partners 5
4.3 Internationally accepted certificates or approvals 5
4.4 Business partners exempt from security declaration requirement 6
4.5 Security reviews of business partners 6

5 Supply chain security process 6
5.1 General 6
5.2 Identification of the scope of security assessment 6
5.3 Conduction of the security assessment 7
5.4 Development of the supply chain security plan 8
5.5 Execution of the supply chain security plan 8
5.6 Documentation and monitoring of the supply chain security process 8
5.7 Actions required after a security incident 8
5.8 Protection of the security information 9

Annex A (informative) Supply chain security process 10
A.1 General 10
A.2 Identification of the scope of the security assessment 10
A.3 Conduction of the security assessment 11
A.4 Development of the security plan 15
A.5 Execution of the security plan 17
A.6 Documentation and monitoring of the security process 17
A.7 Continual improvement 17

Annex B (informative) Methodology for security risk assessment and development of countermeasures 18
B.1 General 18
B.2 Step one – Consideration of the security threat scenarios 20
B.3 Step two – Classification of consequences 22
B.4 Step three – Classification of likelihood of security incidents 23
B.5 Step four – Security incident scoring 24
B.6 Step five – Development of countermeasures 24
B.7 Step six – Implementation of countermeasures 25
B.8 Step seven – Evaluation of countermeasures 25
B.9 Step eight – Repetition of the process 25
B.10 Continuation of the process 25

Annex C (informative) Guidance for obtaining advice and certification 26
C.1 General 26
C.2 Demonstrating conformance with ISO 28001 by audit 26
C.3 Certification of ISO 28001 by third party certification bodies 26

Bibliography 27

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale