

INTERNATIONAL  
STANDARD

ISO/IEC  
17799

Second edition  
2005-06-15

---

---

**Information technology — Security  
techniques — Code of practice for  
information security management**

*Technologies de l'information — Techniques de sécurité — Code de  
pratique pour la gestion de sécurité d'information*

ISO/IEC 17799:2005 - Preview only Copy via ILNAS e-Shop

---

---

Reference number  
ISO/IEC 17799:2005(E)



© ISO/IEC 2005

**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.

© ISO/IEC 2005

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

<b>Contents</b>	<b>Page</b>
<b>FOREWORD</b> .....	<b>VII</b>
<b>0 INTRODUCTION</b> .....	<b>VIII</b>
0.1 WHAT IS INFORMATION SECURITY?.....	VIII
0.2 WHY INFORMATION SECURITY IS NEEDED? .....	VIII
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS .....	IX
0.4 ASSESSING SECURITY RISKS .....	IX
0.5 SELECTING CONTROLS.....	IX
0.6 INFORMATION SECURITY STARTING POINT.....	IX
0.7 CRITICAL SUCCESS FACTORS .....	X
0.8 DEVELOPING YOUR OWN GUIDELINES .....	XI
<b>1 SCOPE</b> .....	<b>1</b>
<b>2 TERMS AND DEFINITIONS</b> .....	<b>1</b>
<b>3 STRUCTURE OF THIS STANDARD</b> .....	<b>4</b>
3.1 CLAUSES .....	4
3.2 MAIN SECURITY CATEGORIES .....	4
<b>4 RISK ASSESSMENT AND TREATMENT</b> .....	<b>5</b>
4.1 ASSESSING SECURITY RISKS .....	5
4.2 TREATING SECURITY RISKS.....	5
<b>5 SECURITY POLICY</b> .....	<b>7</b>
5.1 INFORMATION SECURITY POLICY .....	7
5.1.1 <i>Information security policy document</i> .....	7
5.1.2 <i>Review of the information security policy</i> .....	8
<b>6 ORGANIZATION OF INFORMATION SECURITY</b> .....	<b>9</b>
6.1 INTERNAL ORGANIZATION .....	9
6.1.1 <i>Management commitment to information security</i> .....	9
6.1.2 <i>Information security co-ordination</i> .....	10
6.1.3 <i>Allocation of information security responsibilities</i> .....	10
6.1.4 <i>Authorization process for information processing facilities</i> .....	11
6.1.5 <i>Confidentiality agreements</i> .....	11
6.1.6 <i>Contact with authorities</i> .....	12
6.1.7 <i>Contact with special interest groups</i> .....	12
6.1.8 <i>Independent review of information security</i> .....	13
6.2 EXTERNAL PARTIES .....	14
6.2.1 <i>Identification of risks related to external parties</i> .....	14
6.2.2 <i>Addressing security when dealing with customers</i> .....	15
6.2.3 <i>Addressing security in third party agreements</i> .....	16
<b>7 ASSET MANAGEMENT</b> .....	<b>19</b>
7.1 RESPONSIBILITY FOR ASSETS.....	19
7.1.1 <i>Inventory of assets</i> .....	19
7.1.2 <i>Ownership of assets</i> .....	20
7.1.3 <i>Acceptable use of assets</i> .....	20
7.2 INFORMATION CLASSIFICATION .....	21
7.2.1 <i>Classification guidelines</i> .....	21
7.2.2 <i>Information labeling and handling</i> .....	21
<b>8 HUMAN RESOURCES SECURITY</b> .....	<b>23</b>
8.1 PRIOR TO EMPLOYMENT .....	23
8.1.1 <i>Roles and responsibilities</i> .....	23