National Standards Authority of Ireland

IRISH STANDARD

I.S. 17799-2:2002

ICS 35.020

National Standards
Authority of Ireland
Glasnevin, Dublin 9
Ireland

Tel: +353 1 807 3800
Fax: +353 1 807 3838
http://www.nsai.ie

Sales
http://www.standards.ie

INFORMATION SECURITY MANAGEMENT – PART 2: SPECIFICATION FOR INFORMATION SECURITY MANAGEMENT SYSTEMS

This Irish Standard was published under the authority of the National Standards Authority of Ireland and comes into effect on:

February 11, 2003

Price Code F

Údarás um Chaighdeáin Náisiúnta na hÉireann

AMENDMENT

No. 1 : 2001

OF

STANDARD SPECIFICATION

(INFORMATION SECURITY MANAGEMENT - PART 2: SPECIFICATION FOR INFORMATION SECURITY MANAGEMENT SYSTEMS)

DECLARATION, 2000

IRISH STANDARD 17799-2 : 2000

NSAI in exercise of the power conferred by section 16 (5) of the National Standards Authority of Ireland Act, 1996 (No. 28 of 1996) and with consent of the Minister for Enterprise, Trade and Employment, here by declares as follows:

1. This instrument may be cited as the Standard Specification (Information Security Management – Part 2: Specification for Information Security Management Systems) Declaration, 2000, (Amendment) No. 1 : 2001

2. Irish Standard 17799-2 : 2000 set out in the Schedule of the Standard Specification (Information Security Management – Part 2: Specification for Information Security Management Systems) Declaration, 2000 is hereby amended as indicated in the Schedule hereto.

SCHEDULE

Page ii, Foreword. Delete first three lines of third paragraph; replace succeeding four words with the words "I.S. 17799-2". Add at the end of the third paragraph the following:

> "It should be noted that what was formerly I.S. 17799-1, which was based on BS 7799-1:1999, has now been replaced by I.S. ISO/IEC 17799, the adoption of the international standard resulting from fast-track submission."

In fourth paragraph replace "Part 2" with "I.S. 17799-2, and replace "I.S. 17799-1" with "I.S. ISO/IEC 17799". In fifth paragraph replace "Part 2" with "I.S. 17799-2", and replace "Part 1" with "I.S. ISO/IEC 17799".

Page 1, Subclause 1. Replace in first line "This part of I.S. 17799" with "I.S. 17799-2". In NOTE replace "Part 1" with "I.S. ISO/IEC 17799", replace "this part of I.S. 17799" with "I.S. 17799-2", and replace "I.S. 17799-1:2000" with "I.S. ISO/IEC 17799".

Page 1, Subclause 2. Replace "this part of I.S. 17799" with "I.S. 17799-2", and replace "I.S. 17799-1" with "I.S. ISO/IEC 17799".

Page 1, Subclause 3.2. In NOTE replace "I.S. 17799-1" with "I.S. ISO/IEC 17799", and replace "this part of I.S. 17799" with "I.S. 17799-2".

Page 1, Subclause 3.3. In NOTE replace "I.S. 17799-1" with "I.S. ISO/IEC 17799".

Page 2, Figure 1. Replace "this part of I.S. 17799" with "I.S. 17799-2", and replace "I.S. 17799" with "I.S. 17799-2".

Page 2, Subclause 3.6. Replace "this part of I.S. 17799" with "I.S. 17799-2".

Contents

Foreword

The National Standards Authority of Ireland formulates standards at the request of the Minister for Enterprise, Trade and Employment. Proposed standards are circulated for comment to organizations and persons likely to be interested and are reviewed in the light of comments received. Standards when published by NSAI are declared to be Standard Specifications with the consent of the Minister.

False representation that a commodity, process or practice conforms to an Irish Standard Specification is an offence under the National Standards Authority of Ireland Act, 1996.

I.S. 17799-2 is based on BS 7799-2 and is reproduced with the permission of BSI. The BS was the result of an international consultation effected through an International User Group hosted by the UK Department of Trade and Industry. NSAI's Information and Communications Technology Standards Consultative Committee advised NSAI on the consultation and review of comments.

This new edition of I.S. 17799-2 has been produced to harmonize it with other management system standards such as I.S. EN ISO 9001:2000 and I.S. EN ISO 14001:1996 to provide consistent and integrated implementation and operation of management systems. It also introduces a Plan-Do-Check-Act (PDCA) model as part of a management system approach to developing, implementing and improving the effectiveness of an organization's information security management system.

The implementation of the PDCA model will also reflect the principles as set out in the OECD guidance (2002)[1)] governing the security of information systems and networks. In particular, this new edition gives a robust model for implementing the principles in those guidelines governing risk assessment, security design and implementation, security management and reassessment.

The control objectives and controls referred to in this edition are directly derived from and aligned with those listed in I.S. ISO/IEC 17799:2000. The list of control objectives and controls in this Irish standard is not exhaustive and an organisation might consider that additional control objectives and controls are necessary. Not all the controls described will be relevant to every situation, nor can they take into account the local environment or technological constraints, or be present in a form that suits every potential user in an organization.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

[1)] *OECD. OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security.* Paris: OECD, July 2002. www.oecd.org