

ISO/IEC 13335-1:2004-11 (E)

Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management

Contents

Page

TABLE OF CONTENTS	iii
FOREWORD	iv
INTRODUCTION	v
1 SCOPE	1
2 DEFINITIONS	1
3 SECURITY CONCEPTS AND RELATIONSHIPS	5
3.1 SECURITY PRINCIPLES	5
3.2 ASSETS	5
3.3 THREATS	6
3.4 VULNERABILITIES	8
3.5 IMPACT	8
3.6 RISK	9
3.7 SAFEGUARDS	9
3.8 CONSTRAINTS	10
3.9 SECURITY ELEMENT RELATIONSHIPS	11
4 OBJECTIVES, STRATEGIES AND POLICIES	13
4.1 ICT SECURITY OBJECTIVES AND STRATEGY	14
4.2 POLICY HIERARCHY	16
4.3 CORPORATE ICT SECURITY POLICY ELEMENTS	18
5 ORGANIZATIONAL ASPECTS OF ICT SECURITY	20
5.1 ROLES AND RESPONSIBILITIES	20
5.1.1 Organizational roles, accountabilities and responsibilities	20
5.1.2 ICT security forum	23
5.1.3 Corporate ICT security officer	23
5.1.4 ICT users	24
5.2 ORGANIZATIONAL PRINCIPLES	25
5.2.1 Commitment	25
5.2.2 Consistent approach	25
5.2.3 Integrating ICT security	26
6 ICT SECURITY MANAGEMENT FUNCTIONS	27
6.1 OVERVIEW	27
6.2 CULTURAL AND ENVIRONMENTAL CONDITIONS	27
6.3 RISK MANAGEMENT	28