

CONTENTS

INTRODUCTION.....	6
1 SECURITY POLICY	8
1.1 OBJECTIVE	8
1.2 POLICY	8
1.3 SECURITY POLICY FRAMEWORK (OR „SPF“)	9
1.4 CASE STUDY I	12
2 THE SCOPE OF INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	12
2.1 THE PURPOSE OF THE ISMS SCOPE.....	12
2.2 THE REQUIREMENTS OF ISO 27001 REGARDING THE SCOPE	12
2.3 INTERFACES AND DEPENDENCIES	13
2.4 THE BIGGEST MYTHS ABOUT THE ISMS SCOPE	15
2.4.1 <i>SMALLER SCOPE DOES NOT MEAN AN EASIER JOB.....</i>	<i>15</i>
2.4.2 <i>EXCLUSION OF CONTROLS HAS NOTHING TO DO WITH THE ISMS SCOPE.....</i>	<i>15</i>
2.5 BENEFITS OF DEFINING THE ISMS SCOPE	15
2.6 INFORMATION SECURITY	16
2.6.1 INTEGRITY.....	16
2.6.2 AVAILABILITY;	16
2.6.3 NON-REPUDIATION.....	17
2.7 SECURITY CONSIDERATIONS IN THE INFORMATION SYSTEM DEVELOPMENT LIFE CYCLE.....	17
2.8 THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)[6]	17
2.8.1 INITIATION PHASE.....	18
2.8.2 ACQUISITION / DEVELOPMENT PHASE.....	18
2.8.3 IMPLEMENTATION PHASE.....	20
2.8.4 OPERATIONS / MAINTENANCE PHASE.....	20
2.8.5 DISPOSITION PHASE	21
2.8.6 THE PDCA PROCESS MODEL.....	22
2.8.7 HISTORY OF ISO/IEC 27001	23
2.9 ISO 27001:2005 DOMAINS- ASSET MANAGEMENT DOMAIN	24
2.10 ASSEST CLASSIFICATION.....	25
2.11 ASSEST LABELING	25
2.12 BELL-LAPADULA MODEL I	25
2.12.1 STRONG PROPERTY	27
2.12.2 TRANQUILITY PRINCIPLE.....	27
2.12.3 LIMITATIONS.....	28
2.13 BELL-LAPADULA MODEL II.....	28
2.13.1 FEATURES	28
2.13.2 IMPLEMENTATIONS	29
2.14 SECURITY MODEL OF OPERATION.....	30
2.14.1 CONTENTS.....	30
2.14.2 DEDICATED SECURITY MODE.....	30
2.14.3 SYSTEM HIGH SECURITY MODE.....	31
2.14.4 COMPARTMENTED SECURITY MODE	31
2.14.5 MULTILEVEL SECURITY MODE.....	31
2.15 TAKE-GRANT PROTECTION MODEL.....	32
2.16 GRAHAM – DENNIG MODEL.....	33
2.16.1 FEATURES	33
2.16.2 LIMITATIONS.....	34

2.17	MULTILEVEL SECURITY MODEL.....	34
2.17.1	TRUSTED OPERATING SYSTEMS.....	34
2.17.2	MLS PROBLEM AREAS.....	37
2.17.3	THERE IS NO SUCH THING AS MLS.....	39
2.17.4	MILS ARCHITECTURE.....	40
2.17.5	MSL SYSTEMS.....	41
2.17.6	MLS APPLICATIONS.....	41
2.17.7	MLS FUTURE.....	42
2.18	ACCESS CONTROL DOMAIN.....	43
2.19	CASE STUDY II.....	43
2.20	CASE STUDY III.....	54
3	CONDUCT A RISK ASSESSMENT.....	56
3.1	INTERFACES AND DEPENDENCIES.....	57
3.2	RISK MANAGEMENT FRAMEWORK.....	58
3.3	RISK ASSESSMENT.....	60
3.4	CASE STUDY IV.....	62
4	CONTROL OBJECTIVES AND CONTROLS TO BE IMPLEMENTED.....	78
4.1	CASE STUDY V [35].....	83
5	APPLICABILITY STATEMENT.....	108
6	USER RESPONSIBILITY.....	113
6.1	CASE STUDY VI.....	121
	CONCLUSION.....	128
	REFERENCES.....	129