



WRITTEN INFORMATION SECURITY PROGRAM (WISP)



INTERNAL USE

Access Limited to Internal Use Only

TABLE OF CONTENTS

WRITTEN INFORMATION SECURITY PROGRAM (WISP) OVERVIEW	7
INTRODUCTION	7
PURPOSE	7
SCOPE & APPLICABILITY	8
POLICY OVERVIEW	8
VIOLATIONS	8
EXCEPTIONS	8
UPDATES	9
KEY TERMINOLOGY	9
INFORMATION SECURITY PROGRAM STRUCTURE	12
MANAGEMENT DIRECTION FOR INFORMATION SECURITY	12
POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	12
CYBERSECURITY GOVERNANCE (GOV)	13
GOV-1: PUBLISHING CYBERSECURITY POLICIES & STANDARDS	13
GOV-2: PERIODIC REVIEW & UPDATE OF CYBERSECURITY DOCUMENTATION	13
GOV-3: ASSIGNED CYBERSECURITY RESPONSIBILITIES	13
GOV-4: MEASURES OF PERFORMANCE	14
ASSET MANAGEMENT (AST)	15
AST-1: ASSET GOVERNANCE	15
AST-2: ASSET INVENTORIES	15
AST-3: ASSIGNING OWNERSHIP OF ASSETS	15
AST-4: NETWORK DIAGRAMS	16
AST-5: SECURE DISPOSAL OR RE-USE OF EQUIPMENT	16
AST-6: REMOVAL OF ASSETS	16
AST-7: SECURITY OF ASSETS OFF-PREMISES	16
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD)	17
BCP-1: CONTINGENCY PLAN	17
BCP-2: CONTINGENCY TRAINING	17
BCP-3: CONTINGENCY PLAN TESTING & EXERCISES	18
BCP-4: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	18
BCP-5: CONTINGENCY PLAN UPDATE	18
BCP-6: INFORMATION SYSTEM RECOVERY & RECONSTITUTION	18
CAPACITY & PERFORMANCE PLANNING (CAP)	19
CAP-1: CAPACITY MANAGEMENT	19
CAP-2: RESOURCE PRIORITY	19
CHANGE MANAGEMENT (CHG)	20
CHG-1: CONFIGURATION CHANGE CONTROL	20
CHG-2: SECURITY IMPACT ANALYSIS FOR CHANGES	20
CHG-3: SECURITY FUNCTIONALITY VERIFICATION	21
COMPLIANCE (CPL)	22
CPL-1: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	22
CPL-2: SECURITY CONTROLS OVERSIGHT	22
CPL-3: SECURITY ASSESSMENTS	23
CONFIGURATION MANAGEMENT (CFG)	24
CFG-1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS	24
CFG-2: LEAST FUNCTIONALITY	24
CFG-3: SOFTWARE USAGE RESTRICTIONS	25
CONTINUOUS MONITORING (MON)	26
MON-1: CONTINUOUS MONITORING	26
MON-2: CENTRALIZED EVENT LOG COLLECTION	27

MON-3: CONTENT OF AUDIT RECORDS	27
MON-4: MONITORING REPORTING	27
MON-5: TIME STAMPS	28
MON-6: ANOMALOUS BEHAVIOR	28
MON-7: THIRD-PARTY THREATS	28
MON-8: PRIVILEGED USERS	28
MON-9: UNAUTHORIZED ACTIVITIES	28
CRYPTOGRAPHIC PROTECTIONS (CRY)	30
CRY-1: USE OF CRYPTOGRAPHIC PROTECTIONS	30
CRY-2: TRANSMISSION CONFIDENTIALITY	30
CRY-3: TRANSMISSION INTEGRITY	31
CRY-4: ENCRYPTING DATA AT REST	31
DATA CLASSIFICATION & HANDLING (DCH)	32
DCH-1: DATA PROTECTION	32
DCH-2: DATA & ASSET CLASSIFICATION	32
DCH-3: MEDIA TRANSPORTATION	32
DCH-4: MEDIA SANITIZATION & DISPOSAL	33
DCH-5: SYSTEM OUTPUT HANDLING & DATA RETENTION	33
DCH-6: REMOVABLE MEDIA SECURITY	34
DCH-7: USE OF EXTERNAL INFORMATION SYSTEMS	34
DCH-8: INFORMATION SHARING	34
DCH-9: PUBLICLY ACCESSIBLE CONTENT	34
DCH-10: GEOGRAPHIC LOCATION OF DATA	35
ENDPOINT SECURITY (END)	36
END-1: WORKSTATION SECURITY	36
END-2: ENDPOINT PROTECTION MEASURES	36
END-3: MALICIOUS CODE PROTECTION (ANTIMALWARE)	36
END-4: AUTOMATIC ANTIMALWARE UPDATES	37
END-5: ANTIMALWARE ALWAYS-ON PROTECTION	37
END-6: FILE INTEGRITY MONITORING (FIM)	37
END-7: SOFTWARE FIREWALL	38
END-8: PHISHING & SPAM PROTECTION	38
END-9: MOBILE CODE	38
HUMAN RESOURCES SECURITY (HRS)	40
HRS-1: HUMAN RESOURCES SECURITY MANAGEMENT	40
HRS-2: POSITION CATEGORIZATION	40
HRS-3: USERS WITH ELEVATED PRIVILEGES	40
HRS-4: ROLES & RESPONSIBILITIES	40
HRS-5: PERSONNEL SCREENING	41
HRS-6: TERMS OF EMPLOYMENT	41
HRS-7: RULES OF BEHAVIOR	41
HRS-8: ACCESS AGREEMENTS	41
HRS-9: PERSONNEL SANCTIONS	42
HRS-10: PERSONNEL TRANSFER	42
HRS-11: PERSONNEL TERMINATION	42
HRS-12: THIRD-PARTY PERSONNEL SECURITY	42
IDENTIFICATION & AUTHENTICATION (IAC)	44
IAC-1: IDENTIFICATION & AUTHENTICATION	44
IAC-2: MULTIFACTOR AUTHENTICATION (MFA)	44
IAC-3: USER PROVISIONING & DE-PROVISIONING	44
IAC-4: ROLE-BASED ACCESS CONTROL (RBAC)	45
IAC-5: IDENTIFIER MANAGEMENT (USER NAMES)	45
IAC-6: AUTHENTICATOR MANAGEMENT (PASSWORDS)	45
IAC-7: PASSWORD AUTHENTICATION MANAGEMENT	45
IAC-8: ACCOUNT MANAGEMENT	47

IAC-9: PERIODIC REVIEW	47
IAC-10: LEAST PRIVILEGE	48
INCIDENT RESPONSE (IRO)	49
IRO-1: INCIDENTS RESPONSE OPERATIONS	49
IRO-2: INCIDENT HANDLING	49
IRO-3: INCIDENT RESPONSE PLAN (IRP)	49
IRO-4: INCIDENT RESPONSE TRAINING	50
IRO-5: INCIDENT RESPONSE TESTING	50
IRO-6: INTEGRATED INCIDENT RESPONSE TEAM	50
IRO-7: CHAIN OF CUSTODY & FORENSICS	51
IRO-8: INCIDENT MONITORING	51
IRO-9: INCIDENT REPORTING	51
IRO-10: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	51
IRO-11: IRP UPDATE	52
MAINTENANCE (MNT)	53
MNT-1: MAINTENANCE OPERATIONS	53
MNT-2: CONTROLLED MAINTENANCE	53
MNT-3: TIMELY MAINTENANCE	53
MNT-4: REMOTE MAINTENANCE	54
NETWORK SECURITY (NET)	55
NET-1: LAYERED DEFENSES	55
NET-3: BOUNDARY PROTECTIONS	55
NET-3: DATA FLOW ENFORCEMENT (ACCESS CONTROL LISTS)	56
NET-4: INFORMATION SYSTEM CONNECTIONS	56
NET-5: SECURITY FUNCTION ISOLATION	56
NET-6: VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION	57
NET-7: GUEST NETWORKS	57
NET-8: NETWORK DISCONNECT	57
NET-9: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)	57
NET-10: SAFEGUARDING DATA OVER OPEN NETWORKS	58
NET-11: REMOTE ACCESS	58
PHYSICAL & ENVIRONMENTAL SECURITY (PES)	59
PES-1: PHYSICAL & ENVIRONMENTAL PROTECTIONS	59
PES-2: PHYSICAL ACCESS CONTROL	59
PES-3: MONITORING PHYSICAL ACCESS	59
PES-4: VISITOR CONTROL	60
PES-5: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS	60
PROJECT & RESOURCE MANAGEMENT (PRM)	61
PRM-1: ALLOCATION OF RESOURCES	61
PRM-2: SECURITY REQUIREMENTS DEFINITION	61
PRM-3: SECURITY IN PROJECT MANAGEMENT	61
PRM-4: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)	62
RISK MANAGEMENT (RSK)	63
RSK-1: RISK MANAGEMENT PROGRAM (RMP)	63
RSK-2: RISK IDENTIFICATION	63
RSK-3: RISK ASSESSMENT	63
RSK-4: RISK RANKING	64
RSK-5: RISK REMEDIATION	64
RSK-6: BUSINESS IMPACT ASSESSMENTS (BIAS)	64
SECURE ENGINEERING & ARCHITECTURE (SEA)	65
SEA-1: SECURITY ENGINEERING PRINCIPLES	65
SEA-2: SECURE CONFIGURATIONS	65
SEA-3: LEAST FUNCTIONALITY	66
SEA-4: FAIL SECURE IN KNOWN STATE	66

SEA-5: CLOCK SYNCHRONIZATION	67
SECURITY OPERATIONS (OPS)	68
OPS-1: OPERATIONS SECURITY	68
OPS-2: STANDARDIZED OPERATING PROCEDURES (SOPs)	68
SECURITY AWARENESS & TRAINING (SAT)	69
SAT-1: SECURITY-MINDED WORKFORCE	69
SAT-2: SECURITY AWARENESS	69
SAT-3: SECURITY TRAINING	70
SAT-4: SECURITY TRAINING RECORDS	70
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA)	71
TDA-1: TECHNOLOGY DEVELOPMENT & ACQUISITION	71
TDA-2: SECURITY REQUIREMENTS	71
TDA-3: DESIGN & IMPLEMENTATION OF SECURITY CONTROLS	71
TDA-4: FUNCTIONAL PROPERTIES OF SECURITY CONTROLS	71
TDA-5: SECURE DEVELOPMENT	71
TDA-6: SECURE DEVELOPMENT ENVIRONMENTS	72
TDA-7: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS	72
TDA-8: SECURITY TESTING THROUGHOUT DEVELOPMENT	72
THIRD-PARTY MANAGEMENT (TPM)	74
TPM-1: THIRD-PARTY MANAGEMENT	74
TPM-2: THIRD-PARTY CRITICALITY ASSESSMENTS	74
TPM-3: SUPPLY CHAIN PROTECTION	74
TPM-4: THIRD-PARTY SERVICES	75
TPM-5: WRITTEN CONTRACT REQUIREMENTS	75
TPM-6: REVIEW OF THIRD-PARTY SERVICES	76
TPM-7: THIRD-PARTY DEFICIENCY REMEDIATION	76
TPM-8: MANAGING CHANGES TO THIRD-PARTY SERVICES	76
TPM-9: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	76
THREAT MANAGEMENT (THR)	77
THR-1: THREAT AWARENESS PROGRAM	77
THR-2: THREAT INTELLIGENCE FEEDS	77
VULNERABILITY & PATCH MANAGEMENT (VPM)	78
VPM-1: VULNERABILITY & PATCH MANAGEMENT PROGRAM	78
VPM-2: VULNERABILITY RANKING	78
VPM-3: VULNERABILITY REMEDIATION	78
VPM-4: SOFTWARE PATCHING	79
VPM-5: VULNERABILITY SCANNING	79
VPM-6: PENETRATION TESTING	79
VPM-7: RED TEAM EXERCISES	80
WEB SECURITY (WEB)	81
WEB-1: USE OF DEMILITARIZED ZONES (DMZ)	81
WEB-2: CLOUD PROVIDERS	81
WEB-3: CLOUD SECURITY ARCHITECTURE	81
WEB-4: SECURITY MANAGEMENT SUBNET	82
WEB-5: MULTI-TENANT ENVIRONMENTS	82
WEB-6: GEOLOCATION REQUIREMENTS	82
WEB-7: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS	82
WRITTEN INFORMATION SECURITY PROGRAM (WISP) APPENDICES	83
APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES	83
A-1: DATA CLASSIFICATION	83
A-2: LABELING	84
A-3: GENERAL ASSUMPTIONS	84
A-4: PERSONALLY IDENTIFIABLE INFORMATION (PII)	84

APPENDIX B: DATA CLASSIFICATION EXAMPLES	87
APPENDIX C: DATA RETENTION PERIODS	89
APPENDIX D: BASELINE SECURITY CATEGORIZATION GUIDELINES	91
<i>D-1: DATA SENSITIVITY</i>	91
<i>D-2: SAFETY & CRITICALITY</i>	91
<i>D-3: BASIC ASSURANCE REQUIREMENTS</i>	92
<i>D-4: ENHANCED ASSURANCE REQUIREMENTS</i>	92
APPENDIX E: INFORMATION SECURITY ROLES & RESPONSIBILITIES	93
<i>E-1: INFORMATION SECURITY ROLE CATEGORIES</i>	93
<i>E-2: INFORMATION SECURITY SPECIALTY AREAS (ROLES)</i>	94
<i>E-3: INFORMATION SECURITY WORK ROLES & RESPONSIBILITIES</i>	97
APPENDIX F: RULES OF BEHAVIOR / USER ACCEPTABLE USE	102
<i>F-1: ACCEPTABLE USE</i>	102
<i>F-2: PROHIBITED USE</i>	102
<i>F-3: GUIDANCE ON THE PERSONAL USE OF COMPANY-OWNED TECHNOLOGY</i>	103
<i>F-4: ADDITIONAL RULES FOR SECURITY & PRIVILEGED USERS</i>	103
GLOSSARY: ACRONYMS & DEFINITIONS	105
ACRONYMS	105
DEFINITIONS	105
KEY WORD INDEX	106
RECORD OF CHANGES	107
ANNEX 1 – CYBERSECURITY POLICIES	108
CYBERSECURITY GOVERNANCE (GOV)	108
ASSET MANAGEMENT (AST)	108
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD)	108
CAPACITY & PERFORMANCE PLANNING (CAP)	108
CHANGE MANAGEMENT (CHG)	108
COMPLIANCE (CPL)	108
CONFIGURATION MANAGEMENT (CFG)	109
CONTINUOUS MONITORING (MON)	109
CRYPTOGRAPHIC PROTECTIONS (CRY)	109
DATA CLASSIFICATION & HANDLING (DCH)	109
ENDPOINT SECURITY (END)	109
HUMAN RESOURCES SECURITY (HRS)	110
IDENTIFICATION & AUTHENTICATION (IAC)	110
INCIDENT RESPONSE (IRO)	110
MAINTENANCE (MNT)	110
NETWORK SECURITY (NET)	110
PHYSICAL & ENVIRONMENTAL SECURITY (PES)	110
PROJECT & RESOURCE MANAGEMENT (PRM)	111
RISK MANAGEMENT (RSK)	111
SECURE ENGINEERING & ARCHITECTURE (SEA)	111
SECURITY OPERATIONS (OPS)	111
SECURITY AWARENESS & TRAINING (SAT)	111
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA)	111
THIRD-PARTY MANAGEMENT (TPM)	112
THREAT MANAGEMENT (THR)	112
VULNERABILITY & PATCH MANAGEMENT (VPM)	112