

YOUR LOGO GOES HERE

SECURITY, COMPLIANCE & RESILIENCE PROGRAM (SCRIP)

ACME Business Consulting, Inc.

SENSITIVE

Access Limited to Authorized Personnel

TABLE OF CONTENTS

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES	30
SECURITY, COMPLIANCE & RESILIENCE PROGRAM (SCRP) OVERVIEW	31
MANAGEMENT COMMITMENT	31
PURPOSE	31
SCOPE & APPLICABILITY	32
<i>PEOPLE, PROCESSES, TECHNOLOGY, DATA & FACILITIES (PPTDF) CONTROL APPLICABILITY</i>	32
ROLES	33
RESPONSIBILITIES	33
VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES	33
EXCEPTION TO STANDARDS	33
UPDATES TO POLICIES & STANDARDS	33
KEY TERMINOLOGY	34
CYBERSECURITY & DATA PROTECTION PROGRAM STRUCTURE	38
MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION	38
POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	38
CYBERSECURITY & DATA PROTECTION (GOV) POLICY & STANDARDS	39
GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM	39
<i>GOV-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM STEERING COMMITTEE & PROGRAM OVERSIGHT</i>	39
<i>GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM STATUS REPORTING TO GOVERNING BODY</i>	40
<i>GOV-01.3: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM COMMITMENT TO CONTINUAL IMPROVEMENTS</i>	40
GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION	40
<i>GOV-02.1: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION EXCEPTION MANAGEMENT</i>	41
GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY & DATA PROTECTION PROGRAM	41
GOV-04: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES	42
<i>GOV-04.1: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES ACCOUNTABILITY STRUCTURE</i>	42
<i>GOV-04.2: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES AUTHORITATIVE CHAIN OF COMMAND</i>	42
GOV-05: MEASURES OF PERFORMANCE	43
<i>GOV-05.1: MEASURES OF PERFORMANCE KEY PERFORMANCE INDICATORS (KPIs)</i>	43
<i>GOV-05.2: MEASURES OF PERFORMANCE KEY RISK INDICATORS (KRIs)</i>	43
GOV-06: CONTACTS WITH AUTHORITIES	43
GOV-07: CONTACTS WITH GROUPS & ASSOCIATIONS	44
GOV-08: DEFINED BUSINESS CONTEXT & MISSION	44
GOV-09: DEFINED CONTROL OBJECTIVES	44
GOV-10: DATA GOVERNANCE	44
GOV-11: PURPOSE VALIDATION	45
GOV-12: FORCED TECHNOLOGY TRANSFER (FTT)	45
GOV-13: STATE-SPONSORED ESPIONAGE	46
GOV-14: BUSINESS AS USUAL (BAU) SECURE PRACTICES	47
GOV-15: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES	47
<i>GOV-15.1: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES SELECT CONTROLS</i>	47
<i>GOV-15.2: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES IMPLEMENT CONTROLS</i>	48
<i>GOV-15.3: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES ASSESS CONTROLS</i>	48
<i>GOV-15.4: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES AUTHORIZE TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)</i>	48
<i>GOV-15.5: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES MONITOR CONTROLS</i>	48
GOV-16: MATERIALITY DETERMINATION	49
<i>GOV-16.1: MATERIALITY DETERMINATION MATERIAL RISKS</i>	49
<i>GOV-16.2: MATERIALITY DETERMINATION MATERIAL THREATS</i>	49
GOV-17: CYBERSECURITY & DATA PROTECTION STATUS REPORTING	50
GOV-18: QUALITY MANAGEMENT SYSTEM (QMS)	50
GOV-19: ASSURANCE	50
<i>GOV-19.1: ASSURANCE ASSURANCE LEVELS (AL)</i>	50
<i>GOV-19.2: ASSURANCE ASSESSMENT OBJECTIVES (AO)</i>	51
GOV-20: MERGERS, ACQUISITIONS & DIVESTITURES (MA&D)	52
<i>GOV-20.1: MERGERS, ACQUISITIONS & DIVESTITURES (MA&D) VIRTUAL DATA ROOM (VDR)</i>	52

ARTIFICIAL INTELLIGENCE AND AUTONOMOUS TECHNOLOGIES (AAT)	53
AAT-01: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE	53
AAT-01.1: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE AI & AUTONOMOUS TECHNOLOGIES-RELATED LEGAL REQUIREMENTS DEFINITION	54
AAT-01.2: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE TRUSTWORTHY AI & AUTONOMOUS TECHNOLOGIES	54
AAT-01.3: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE AI & AUTONOMOUS TECHNOLOGIES VALUE SUSTAINMENT	55
AAT-01.4: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE AI MODEL & AGENT INVENTORY & LIFECYCLE MANAGEMENT	55
AAT-02: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES	55
AAT-02.1: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES RISK MAPPING	56
AAT-02.2: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES INTERNAL CONTROLS	56
AAT-02.3: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES ADEQUATE PROTECTIONS FOR AI & AUTONOMOUS TECHNOLOGIES	56
AAT-02.4: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES AI THREAT MODELING & RISK ASSESSMENT	56
AAT-03: AI & AUTONOMOUS TECHNOLOGIES CONTEXT DEFINITION	57
AAT-03.1: AI & AUTONOMOUS TECHNOLOGIES CONTEXT DEFINITION AI & AUTONOMOUS TECHNOLOGIES MISSION AND GOALS DEFINITION	57
AAT-03.2: AI & AUTONOMOUS TECHNOLOGIES CONTEXT DEFINITION MODEL & AI AGENT DOCUMENTATION	57
AAT-04: AI & AUTONOMOUS TECHNOLOGIES BUSINESS CASE	58
AAT-04.1: AI & AUTONOMOUS TECHNOLOGIES BUSINESS CASE AI & AUTONOMOUS TECHNOLOGIES POTENTIAL BENEFITS ANALYSIS	58
AAT-04.2: AI & AUTONOMOUS TECHNOLOGIES BUSINESS CASE AI & AUTONOMOUS TECHNOLOGIES POTENTIAL COSTS ANALYSIS	58
AAT-04.3: AI & AUTONOMOUS TECHNOLOGIES BUSINESS CASE AI & AUTONOMOUS TECHNOLOGIES TARGETED APPLICATION SCOPE	58
AAT-04.4: AI & AUTONOMOUS TECHNOLOGIES BUSINESS CASE AI & AUTONOMOUS TECHNOLOGIES COST / BENEFIT MAPPING	59
AAT-05: AI & AUTONOMOUS-SPECIFIC TRAINING	59
AAT-06: AI & AUTONOMOUS TECHNOLOGIES FAIRNESS & BIAS	59
AAT-07: AI & AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS	59
AAT-07.1: AI & AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS AI & AUTONOMOUS TECHNOLOGIES IMPACT ASSESSMENT	60
AAT-07.2: AI & AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS AI & AUTONOMOUS TECHNOLOGIES LIKELIHOOD & IMPACT RISK ANALYSIS	60
AAT-07.3: AI & AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS AI & AUTONOMOUS TECHNOLOGIES CONTINUOUS IMPROVEMENTS	60
AAT-08: ASSIGNED RESPONSIBILITIES FOR AI & AUTONOMOUS TECHNOLOGIES	61
AAT-09: AI & AUTONOMOUS TECHNOLOGIES RISK PROFILING	61
AAT-09.1: AI & AUTONOMOUS TECHNOLOGIES RISK PROFILING AI & AUTONOMOUS TECHNOLOGIES HIGH RISK DESIGNATIONS	61
AAT-10: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV)	62
AAT-10.1: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV TRUSTWORTHINESS ASSESSMENT	62
AAT-10.2: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV TOOLS	62
AAT-10.3: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV TRUSTWORTHINESS DEMONSTRATION	62
AAT-10.4: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV SAFETY DEMONSTRATION	63
AAT-10.5: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV RESILIENCY ASSESSMENT	63
AAT-10.6: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV TRANSPARENCY & ACCOUNTABILITY ASSESSMENT	63
AAT-10.7: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV PRIVACY ASSESSMENT	63
AAT-10.8: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV FAIRNESS & BIAS ASSESSMENT	64
AAT-10.9: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI & AUTONOMOUS TECHNOLOGIES MODEL VALIDATION	64
AAT-10.10: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV RESULTS EVALUATION	64

AAT-10.11: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV EFFECTIVENESS	64
AAT-10.12: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV COMPARABLE DEPLOYMENT SETTINGS	64
AAT-10.13: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV POST-DEPLOYMENT MONITORING	65
AAT-10.14: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) UPDATING AI & AUTONOMOUS TECHNOLOGIES	65
AAT-10.15: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV REPORTING	65
AAT-10.16: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV EMPIRICALLY VALIDATED METHODS	65
AAT-10.17: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV BENCHMARKING CONTENT PROVENANCE	66
AAT-10.18: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV MODEL COLLAPSE MITIGATIONS	66
AAT-10.19: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION & VERIFICATION (AI TEVV) AI TEVV THIRD-PARTY RISK MANAGEMENT	66
AAT-11: ROBUST STAKEHOLDER ENGAGEMENT FOR AI & AUTONOMOUS TECHNOLOGIES	66
AAT-11.1: ROBUST STAKEHOLDER ENGAGEMENT FOR AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER FEEDBACK INTEGRATION	67
AAT-11.2: ROBUST STAKEHOLDER ENGAGEMENT FOR AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES ONGOING ASSESSMENTS	67
AAT-11.3: ROBUST STAKEHOLDER ENGAGEMENT FOR AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES END USER FEEDBACK	67
AAT-11.4: ROBUST STAKEHOLDER ENGAGEMENT FOR AI & AUTONOMOUS TECHNOLOGIES AI & AUTONOMOUS TECHNOLOGIES INCIDENT & ERROR REPORTING	68
AAT-12: AI & AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS	68
AAT-12.1: AI & AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS DATA SOURCE IDENTIFICATION	68
AAT-12.2: AI & AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS DATA SOURCE INTEGRITY	68
AAT-12.3: AI & AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS DATA SOURCE LINEAGE & ORIGIN DISCLOSURE	69
AAT-12.4: AI & AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS DIGITAL CONTENT MODIFICATION LOGGING	69
AAT-13: AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER DIVERSITY	69
AAT-13.1: AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER DIVERSITY AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER COMPETENCIES	69
AAT-14: AI & AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS	69
AAT-14.1: AI & AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS AI & AUTONOMOUS TECHNOLOGIES IMPLEMENTATION TASKS DEFINITION	70
AAT-14.2: AI & AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS AI & AUTONOMOUS TECHNOLOGIES KNOWLEDGE LIMITS	70
AAT-15: AI & AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS	70
AAT-15.1: AI & AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS AI & AUTONOMOUS TECHNOLOGIES NEGATIVE RESIDUAL RISKS	70
AAT-15.2: AI & AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS RESPONSIBILITY TO SUPERSEDE, DEACTIVATE AND/OR DISENGAGE AI & AUTONOMOUS TECHNOLOGIES	70
AAT-16: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING	71
AAT-16.1: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING AI & AUTONOMOUS TECHNOLOGIES MEASUREMENT APPROACHES	71
AAT-16.2: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING MEASURING AI & AUTONOMOUS TECHNOLOGIES EFFECTIVENESS	71
AAT-16.3: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING UNMEASURABLE AI & AUTONOMOUS TECHNOLOGIES RISKS	72
AAT-16.4: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING EFFICACY OF AI & AUTONOMOUS TECHNOLOGIES MEASUREMENT	72
AAT-16.5: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING AI & AUTONOMOUS TECHNOLOGIES DOMAIN EXPERT REVIEWS	72

AAT-16.6: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING AI & AUTONOMOUS TECHNOLOGIES PERFORMANCE CHANGES	72
AAT-16.7: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING PRE-TRAINED AI & AUTONOMOUS TECHNOLOGIES MODELS	73
AAT-16.8: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING AI & AUTONOMOUS TECHNOLOGIES EVENT LOGGING	73
AAT-16.9: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING SERIOUS INCIDENT REPORTING FOR AI & AUTONOMOUS TECHNOLOGIES	73
AAT-16.10: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING SERIOUS INCIDENT ROOT CAUSE ANALYSIS (RCA) FOR AI & AUTONOMOUS TECHNOLOGIES	73
AAT-16.11: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING ANOMALY DETECTION & HUMAN OVERSIGHT	74
AAT-16.12: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING HUMAN-IN-THE-LOOP & ESCALATION	74
AAT-16.13: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING EMERGENT BEHAVIOR & COLLUSION PROTECTIONS	74
AAT-16.14: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING MULTI-AGENT TRUST & COMMUNICATION VALIDATION	74
AAT-17: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION	75
AAT-17.1: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION AI & AUTONOMOUS TECHNOLOGIES HUMAN SUBJECT PROTECTIONS	75
AAT-17.2: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION AI & AUTONOMOUS TECHNOLOGIES ENVIRONMENTAL IMPACT & SUSTAINABILITY	76
AAT-17.3: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION PREVIOUSLY UNKNOWN AI & AUTONOMOUS TECHNOLOGIES THREATS & RISKS	76
AAT-17.4: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION NOVEL RISK ASSESSMENT METHODS & TECHNOLOGIES	77
AAT-17.5: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION FINE TUNING RISK MITIGATION	77
AAT-18: AI & AUTONOMOUS TECHNOLOGIES RISK TRACKING APPROACHES	77
AAT-18.1: AI & AUTONOMOUS TECHNOLOGIES RISK TRACKING APPROACHES AI & AUTONOMOUS TECHNOLOGIES RISK RESPONSE	78
AAT-19: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY	78
AAT-19.1: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY MANIPULATIVE OR DECEPTIVE TECHNIQUES	78
AAT-19.2: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY MATERIALLY DISTORTING BEHAVIORS	78
AAT-19.3: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY SOCIAL SCORING	79
AAT-19.4: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY DETRIMENTAL OR UNFAVORABLE TREATMENT	79
AAT-19.5: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY RISK AND CRIMINAL PROFILING	79
AAT-19.6: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY POPULATING FACIAL RECOGNITION DATABASES	79
AAT-19.7: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY EMOTION INFERENCE	80
AAT-19.8: AI & AUTONOMOUS TECHNOLOGIES CONFORMITY BIOMETRIC CATEGORIZATION	80
AAT-20: AI & AUTONOMOUS TECHNOLOGIES DEVELOPMENT PRACTICES	80
AAT-20.1: AI & AUTONOMOUS TECHNOLOGIES DEVELOPMENT PRACTICES AI & AUTONOMOUS TECHNOLOGIES TRANSPARENCY	80
AAT-20.2: AI & AUTONOMOUS TECHNOLOGIES DEVELOPMENT PRACTICES AI & AUTONOMOUS TECHNOLOGIES IMPLEMENTATION DOCUMENTATION	81
AAT-20.3: AI & AUTONOMOUS TECHNOLOGIES DEVELOPMENT PRACTICES AI & AUTONOMOUS TECHNOLOGIES HUMAN DOMAIN KNOWLEDGE RELIANCE	81
AAT-21: AI & AUTONOMOUS TECHNOLOGIES REGISTRATION	81
AAT-22: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT	82
AAT-22.1: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES HUMAN OVERSIGHT	82
AAT-22.2: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES OVERSIGHT MEASURES	82
AAT-22.3: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES SEPARATE VERIFICATION	82
AAT-22.4: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES OVERSIGHT FUNCTIONS COMPETENCY	83
AAT-22.5: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES DATA RELEVANCE	83
AAT-22.6: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES IRREGULARITY REPORTING	83
AAT-22.7: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES USE NOTIFICATION TO EMPLOYEES	83
AAT-22.8: AI & AUTONOMOUS TECHNOLOGIES DEPLOYMENT AI & AUTONOMOUS TECHNOLOGIES USE NOTIFICATION TO USERS	83
AAT-23: AI & AUTONOMOUS TECHNOLOGIES OUTPUT MARKING	84
AAT-24: REAL WORLD TESTING OF AI & AUTONOMOUS TECHNOLOGIES	84
AAT-25: AI & AUTONOMOUS TECHNOLOGIES SYSTEM VALUE CHAIN	84
AAT-25.1: AI & AUTONOMOUS TECHNOLOGIES SYSTEM VALUE CHAIN AI & AUTONOMOUS TECHNOLOGIES SYSTEM VALUE CHAIN FALLBACKS	84

AAT-26: AI & AUTONOMOUS TECHNOLOGIES TESTING TECHNIQUES	85
AAT-26.1: AI & AUTONOMOUS TECHNOLOGIES TESTING TECHNIQUES GENERATIVE ARTIFICIAL INTELLIGENCE (GAI) IDENTIFICATION	85
AAT-26.2: AI & AUTONOMOUS TECHNOLOGIES TESTING TECHNIQUES AI & AUTONOMOUS TECHNOLOGIES CAPABILITIES TESTING	85
AAT-26.3: AI & AUTONOMOUS TECHNOLOGIES TESTING TECHNIQUES REAL-WORLD TESTING	85
AAT-26.4: AI & AUTONOMOUS TECHNOLOGIES TESTING TECHNIQUES DOCUMENTING TESTING GUIDANCE	85
AAT-27: AI & AUTONOMOUS TECHNOLOGIES OUTPUT FILTERING	86
AAT-27.1: AI & AUTONOMOUS TECHNOLOGIES OUTPUT FILTERING HUMAN MODERATION	86
AAT-28: AI MODEL RESILIENCE	86
AAT-28.1: AI MODEL RESILIENCE MODEL POLLUTION	86
AAT-28.2: AI MODEL RESILIENCE CASCADING HALLUCINATION DEFENSE	86
AAT-28.3: AI MODEL RESILIENCE RESOURCE EXHAUSTION & DOS RESILIENCE	87
AAT-29: AI AGENT GOVERNANCE	87
AAT-29.1: AI AGENT GOVERNANCE INFRASTRUCTURE HARDENING & ISOLATION	87
AAT-29.2: AI AGENT GOVERNANCE AI AGENT LIMITATIONS	87
AAT-29.3: AI AGENT GOVERNANCE TOOL & API INVOCATION CONTROLS	88
AAT-29.4: AI AGENT GOVERNANCE ORCHESTRATION PROTOCOL SAFEGUARDS	88
AAT-29.5: AI AGENT GOVERNANCE DATA PIPELINE & INPUT INTEGRITY	88
AAT-29.6: AI AGENT GOVERNANCE PRIVILEGED ROLE & DELEGATION BOUNDARIES	89
AAT-29.7: AI AGENT GOVERNANCE AI AGENT DATA ACCESS RESTRICTIONS	89
AAT-29.8: AI AGENT GOVERNANCE DATA EXTRACTION	89
AAT-29.9: AI AGENT GOVERNANCE AI AGENT IDENTITY & IMPERSONATION DEFENSE	89
AAT-29.10: AI AGENT GOVERNANCE AI AGENT LOGIC INTEGRITY	90
AAT-29.11: AI AGENT GOVERNANCE SANDBOXING AI AGENTS	90
AAT-29.12: AI AGENT GOVERNANCE PROMPT INJECTION DEFENSE	90
AAT-29.13: AI AGENT GOVERNANCE AGENT KILL SWITCH / USER CONTROL	90
AAT-29.14: AI AGENT GOVERNANCE ADVERSARIAL & RED TEAM TESTING	90
AAT-29.15: AI AGENT GOVERNANCE SELF-MODIFICATION CONTROLS	91
AAT-29.16: AI AGENT GOVERNANCE PURGING AI AGENT DATA	91
AAT-29.17: AI AGENT GOVERNANCE DELEGATION AND CHAINING CONTROL	91
AAT-29.18: AI AGENT GOVERNANCE BEHAVIORAL DRIFT DETECTION	91
AAT-29.19: AI AGENT GOVERNANCE AI AGENT ACTION AUTHENTICATION & AUTHORIZATION	91
AAT-29.20: AI AGENT GOVERNANCE TRANSPARENCY & AUDIT	92
AAT-29.21: AI AGENT GOVERNANCE EXPLAINABILITY	92
AAT-29.22: AI AGENT GOVERNANCE ETHICS, FAIRNESS & BIAS DETECTION	92
AAT-29.23: AI AGENT GOVERNANCE AGENT OUTPUT INTEGRITY & VERIFICATION	92
AAT-30: AGENTIC OUTPUT TRACEABILITY & REPUDIATION	92
AAT-30.1: AGENTIC OUTPUT TRACEABILITY & REPUDIATION AI AGENT LOGGING	93
AAT-30.2: AGENTIC OUTPUT TRACEABILITY & REPUDIATION SESSION MANAGEMENT	93
AAT-31: HUMAN-IN-THE-LOOP WORKLOAD & MANIPULATION	93
AAT-32: ROBOTIC PROCESS AUTOMATION (RPA)	93
AAT-32.1: ROBOTIC PROCESS AUTOMATION (RPA) BUSINESS PROCESS TASK ENUMERATION	94
ASSET MANAGEMENT (AST) POLICY & STANDARDS	95
AST-01: ASSET GOVERNANCE	95
AST-01.1: ASSET GOVERNANCE ASSET-SERVICE DEPENDENCIES	95
AST-01.2: ASSET GOVERNANCE STAKEHOLDER IDENTIFICATION & INVOLVEMENT	96
AST-01.3: ASSET GOVERNANCE STANDARDIZED NAMING CONVENTION	96
AST-01.4: ASSET GOVERNANCE APPROVED TECHNOLOGIES	96
AST-02: ASSET INVENTORIES	96
AST-02.1: ASSET INVENTORIES UPDATES DURING INSTALLATIONS/REMOVALS	97
AST-02.2: ASSET INVENTORIES AUTOMATED UNAUTHORIZED COMPONENT DETECTION	97
AST-02.3: ASSET INVENTORIES COMPONENT DUPLICATION AVOIDANCE	98
AST-02.4: ASSET INVENTORIES APPROVED BASELINE DEVIATIONS	98
AST-02.5: ASSET INVENTORIES NETWORK ACCESS CONTROL (NAC)	98
AST-02.6: ASSET INVENTORIES DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING	98
AST-02.7: ASSET INVENTORIES SOFTWARE LICENSING RESTRICTIONS	99
AST-02.8: ASSET INVENTORIES DATA ACTION MAPPING	99

AST-02.9: ASSET INVENTORIES CONFIGURATION MANAGEMENT DATABASE (CMDB)	99
AST-02.10: ASSET INVENTORIES AUTOMATED LOCATION TRACKING	99
AST-02.11: ASSET INVENTORIES COMPONENT ASSIGNMENT	100
AST-03: ASSET OWNERSHIP ASSIGNMENT	100
AST-03.1: ASSET OWNERSHIP ASSIGNMENT ACCOUNTABILITY INFORMATION	100
AST-03.2: ASSET OWNERSHIP ASSIGNMENT PROVENANCE	100
AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	101
AST-04.1: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) ASSET SCOPE CLASSIFICATION	102
AST-04.2: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) CONTROL APPLICABILITY BOUNDARY GRAPHICAL REPRESENTATION	103
AST-04.3: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs) COMPLIANCE-SPECIFIC ASSET IDENTIFICATION	103
AST-05: SECURITY OF ASSETS & MEDIA	103
AST-05.1: SECURITY OF ASSETS & MEDIA MANAGEMENT APPROVAL FOR EXTERNAL MEDIA TRANSFER	104
AST-06: UNATTENDED END-USER EQUIPMENT	104
AST-06.1: UNATTENDED END-USER EQUIPMENT ASSET STORAGE IN AUTOMOBILES	104
AST-07: KIOSKS & POINT OF INTERACTION (POI) DEVICES	105
AST-08: PHYSICAL TAMPERING DETECTION	105
AST-09: SECURE DISPOSAL, DESTRUCTION OR RE-USE OF EQUIPMENT	106
AST-10: RETURN OF ASSETS	106
AST-11: REMOVAL OF ASSETS	107
AST-12: USE OF PERSONAL DEVICES	107
AST-13: USE OF THIRD-PARTY DEVICES	107
AST-14: USAGE PARAMETERS	108
AST-14.1: USAGE PARAMETERS BLUETOOTH & WIRELESS DEVICES	108
AST-14.2: USAGE PARAMETERS INFRARED COMMUNICATIONS	108
AST-15: LOGICAL TAMPERING PROTECTION	109
AST-15.1: LOGICAL TAMPERING PROTECTION TECHNOLOGY ASSET INSPECTIONS	109
AST-16: BRING YOUR OWN DEVICE (BYOD) USAGE	109
AST-17: PROHIBITED EQUIPMENT & SERVICES	110
AST-18: ROOTS OF TRUST PROTECTION	111
AST-19: TELECOMMUNICATIONS EQUIPMENT	111
AST-20: VIDEO TELECONFERENCE (VTC) SECURITY	112
AST-21: VOICE OVER INTERNET PROTOCOL (VOIP) SECURITY	112
AST-22: MICROPHONES & WEB CAMERAS	112
AST-23: MULTI-FUNCTION DEVICES (MFD)	113
AST-24: TRAVEL-ONLY DEVICES	113
AST-25: RE-IMAGING DEVICES AFTER TRAVEL	113
AST-26: SYSTEM ADMINISTRATIVE PROCESSES	114
AST-27: JUMP SERVER	114
AST-28: DATABASE ADMINISTRATIVE PROCESSES	115
AST-28.1: DATABASE ADMINISTRATIVE PROCESSES DATABASE MANAGEMENT SYSTEM (DBMS)	115
AST-29: RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY	115
AST-29.1: RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY CONTACTLESS ACCESS CONTROL SYSTEMS	116
AST-30: DECOMMISSIONING	116
AST-31: ASSET CATEGORIZATION	117
AST-31.1: ASSET CATEGORIZATION CATEGORIZE ARTIFICIAL INTELLIGENCE (AI)-RELATED TECHNOLOGIES	118
AST-31.2: ASSET CATEGORIZATION HIGH-RISK ASSET CATEGORIZATION	118
AST-31.3: ASSET CATEGORIZATION ASSET ATTRIBUTES	119
AST-32: AUTOMATED NETWORK ASSET DISCOVERY	119
BUSINESS CONTINUITY & DISASTER RECOVERY (BCD) POLICY & STANDARDS	120
BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	120
BCD-01.1: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH RELATED PLANS	120
BCD-01.2: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH EXTERNAL SERVICE PROVIDERS	121
BCD-01.3: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) TRANSFER TO ALTERNATE PROCESSING/STORAGE SITE	121
BCD-01.4: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY TIME/POINT OBJECTIVES (RTO/RPO)	122
BCD-01.5: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY OPERATIONS CRITERIA	122
BCD-01.6: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY OPERATIONS COMMUNICATIONS	122

BCD-02: IDENTIFY CRITICAL ASSETS	123
<i>BCD-02.1: IDENTIFY CRITICAL ASSETS RESUME ALL MISSIONS & BUSINESS FUNCTIONS</i>	123
<i>BCD-02.2: IDENTIFY CRITICAL ASSETS CONTINUE ESSENTIAL MISSION & BUSINESS FUNCTIONS</i>	123
<i>BCD-02.3: IDENTIFY CRITICAL ASSETS RESUME ESSENTIAL MISSION & BUSINESS FUNCTIONS</i>	124
<i>BCD-02.4: IDENTIFY CRITICAL ASSETS DATA STORAGE LOCATION REVIEWS</i>	124
BCD-03: CONTINGENCY TRAINING	124
<i>BCD-03.1: CONTINGENCY TRAINING SIMULATED EVENTS</i>	125
<i>BCD-03.2: CONTINGENCY TRAINING AUTOMATED TRAINING ENVIRONMENTS</i>	125
BCD-04: CONTINGENCY PLAN TESTING & EXERCISES	125
<i>BCD-04.1: CONTINGENCY PLAN TESTING & EXERCISES COORDINATED TESTING WITH RELATED PLANS</i>	125
<i>BCD-04.2: CONTINGENCY PLAN TESTING & EXERCISES ALTERNATE STORAGE & PROCESSING SITES</i>	126
BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	126
BCD-06: ONGOING CONTINGENCY PLANNING	126
BCD-06.1: ONGOING CONTINGENCY PLANNING CONTINGENCY PLANNING COMPONENTS	127
BCD-06.2: ONGOING CONTINGENCY PLANNING CONTINGENCY PLAN UPDATE NOTIFICATIONS	127
BCD-07: ALTERNATIVE SECURITY MEASURES	127
BCD-08: ALTERNATE STORAGE SITE	128
<i>BCD-08.1: ALTERNATE STORAGE SITE SEPARATION FROM PRIMARY SITE</i>	128
<i>BCD-08.2: ALTERNATE STORAGE SITE ACCESSIBILITY</i>	128
BCD-09: ALTERNATE PROCESSING SITE	128
<i>BCD-09.1: ALTERNATE PROCESSING SITE SEPARATION FROM PRIMARY SITE</i>	129
<i>BCD-09.2: ALTERNATE PROCESSING SITE ACCESSIBILITY</i>	129
<i>BCD-09.3: ALTERNATE PROCESSING SITE ALTERNATE SITE PRIORITY OF SERVICE</i>	129
<i>BCD-09.4: ALTERNATE PROCESSING SITE PREPARATION FOR USE</i>	129
<i>BCD-09.5: ALTERNATE PROCESSING SITE INABILITY TO RETURN TO PRIMARY SITE</i>	130
BCD-10: TELECOMMUNICATIONS SERVICES AVAILABILITY	130
<i>BCD-10.1: TELECOMMUNICATIONS SERVICES AVAILABILITY TELECOMMUNICATIONS PRIORITY OF SERVICE PROVISIONS</i>	130
<i>BCD-10.2: TELECOMMUNICATIONS SERVICES AVAILABILITY SEPARATION OF PRIMARY/ALTERNATE PROVIDERS</i>	130
<i>BCD-10.3: TELECOMMUNICATIONS SERVICES AVAILABILITY PROVIDER CONTINGENCY PLAN</i>	131
<i>BCD-10.4: TELECOMMUNICATIONS SERVICES AVAILABILITY ALTERNATE COMMUNICATIONS CHANNELS</i>	131
BCD-11: DATA BACKUPS	131
<i>BCD-11.1: DATA BACKUPS TESTING FOR RELIABILITY & INTEGRITY</i>	134
<i>BCD-11.2: DATA BACKUPS SEPARATE STORAGE FOR CRITICAL INFORMATION</i>	134
<i>BCD-11.3: DATA BACKUPS RECOVERY IMAGES</i>	134
<i>BCD-11.4: DATA BACKUPS CRYPTOGRAPHIC PROTECTION</i>	134
<i>BCD-11.5: DATA BACKUPS TEST RESTORATION USING SAMPLING</i>	135
<i>BCD-11.6: DATA BACKUPS TRANSFER TO ALTERNATE STORAGE SITE</i>	135
<i>BCD-11.7: DATA BACKUPS REDUNDANT SECONDARY SYSTEM</i>	135
<i>BCD-11.8: DATA BACKUPS DUAL AUTHORIZATION FOR BACKUP MEDIA DESTRUCTION</i>	135
<i>BCD-11.9: DATA BACKUPS BACKUP ACCESS</i>	136
<i>BCD-11.10: DATA BACKUPS BACKUP MODIFICATION AND/OR DESTRUCTION</i>	136
BCD-12: TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) RECOVERY & RECONSTITUTION	136
<i>BCD-12.1: TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) RECOVERY & RECONSTITUTION TRANSACTION RECOVERY</i>	136
<i>BCD-12.2: TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) RECOVERY & RECONSTITUTION FAILOVER CAPABILITY</i>	137
<i>BCD-12.3: INFORMATION SYSTEM RECOVERY & RECONSTITUTION ELECTRONIC DISCOVERY (EDISCOVERY)</i>	137
<i>BCD-12.4: TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) RECOVERY & RECONSTITUTION RESTORE WITHIN TIME PERIOD</i>	137
BCD-13: BACKUP & RESTORATION HARDWARE PROTECTION	137
<i>BCD-13.1: BACKUP & RESTORATION HARDWARE PROTECTION RESTORATION INTEGRITY VERIFICATION</i>	138
BCD-14: ISOLATED RECOVERY ENVIRONMENT	138
BCD-15: RESERVE HARDWARE	138
BCD-16: AI & AUTONOMOUS TECHNOLOGIES INCIDENTS	139
CAPACITY & PERFORMANCE PLANNING (CAP) POLICY & STANDARDS	140
CAP-01: CAPACITY & PERFORMANCE MANAGEMENT	140
CAP-02: RESOURCE PRIORITY	140

CAP-03: CAPACITY PLANNING	140
CAP-04: PERFORMANCE MONITORING	141
CAP-05: ELASTIC EXPANSION	141
CAP-06: REGIONAL DELIVERY	141
CHANGE MANAGEMENT (CHG) POLICY & STANDARDS	142
CHG-01: CHANGE MANAGEMENT PROGRAM	142
CHG-02: CONFIGURATION CHANGE CONTROL	143
<i>CHG-02.1: CONFIGURATION CHANGE CONTROL PROHIBITION OF CHANGES</i>	143
<i>CHG-02.2: CONFIGURATION CHANGE CONTROL TEST, VALIDATE & DOCUMENT CHANGES</i>	144
<i>CHG-02.3: CONFIGURATION CHANGE CONTROL CYBERSECURITY & DATA PROTECTION REPRESENTATIVE FOR ASSET LIFECYCLE CHANGES</i>	144
<i>CHG-02.4: CONFIGURATION CHANGE CONTROL AUTOMATED SECURITY RESPONSE</i>	144
<i>CHG-02.5: CONFIGURATION CHANGE CONTROL CRYPTOGRAPHIC MANAGEMENT</i>	145
CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES	145
CHG-04: ACCESS RESTRICTION FOR CHANGE	145
<i>CHG-04.1: ACCESS RESTRICTIONS FOR CHANGE AUTOMATED ACCESS ENFORCEMENT/AUDITING</i>	146
<i>CHG-04.2: ACCESS RESTRICTIONS FOR CHANGE SIGNED COMPONENTS</i>	146
<i>CHG-04.3: ACCESS RESTRICTIONS FOR CHANGE DUAL AUTHORIZATION FOR CHANGE</i>	146
<i>CHG-04.4: ACCESS RESTRICTIONS FOR CHANGE PERMISSIONS TO IMPLEMENT CHANGES</i>	146
<i>CHG-04.5: ACCESS RESTRICTIONS FOR CHANGE LIBRARY PRIVILEGES</i>	147
CHG-05: STAKEHOLDER NOTIFICATION OF CHANGES	147
CHG-06: CONTROL FUNCTIONALITY VERIFICATION	147
<i>CHG-06.1: CYBERSECURITY FUNCTIONALITY VERIFICATION REPORT VERIFICATION RESULTS</i>	148
CHG-07: EMERGENCY CHANGES	148
<i>CHG-07.1: EMERGENCY CHANGES DOCUMENTING EMERGENCY CHANGES</i>	148
CLOUD SECURITY (CLD) POLICY & STANDARDS	149
CLD-01: CLOUD SERVICES	149
<i>CLD-01.1: CLOUD SERVICES CLOUD INFRASTRUCTURE ONBOARDING</i>	149
<i>CLD-01.2: CLOUD SERVICES CLOUD INFRASTRUCTURE OFFBOARDING</i>	150
CLD-02: CLOUD SECURITY ARCHITECTURE	150
CLD-03: CLOUD INFRASTRUCTURE SECURITY SUBNET	151
CLD-04: APPLICATION PROGRAMMING INTERFACE (API) SECURITY	151
<i>CLD-04.1: APPLICATION & PROGRAM INTERFACE (API) SECURITY API GATEWAY</i>	151
CLD-05: VIRTUAL MACHINE IMAGES	151
CLD-06: MULTI-TENANT ENVIRONMENTS	151
<i>CLD-06.1: MULTI-TENANT ENVIRONMENTS CUSTOMER RESPONSIBILITY MATRIX (CRM)</i>	152
<i>CLD-06.2: MULTI-TENANT ENVIRONMENTS MULTI-TENANT EVENT LOGGING CAPABILITIES</i>	152
<i>CLD-06.3: MULTI-TENANT ENVIRONMENTS MULTI-TENANT FORENSICS CAPABILITIES</i>	152
<i>CLD-06.4: MULTI-TENANT ENVIRONMENTS MULTI-TENANT INCIDENT RESPONSE CAPABILITIES</i>	153
CLD-07: DATA HANDLING & PORTABILITY	153
CLD-08: STANDARDIZED VIRTUALIZATION FORMATS	153
CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS	153
CLD-10: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS	154
CLD-11: CLOUD ACCESS SECURITY BROKER (CASB)	154
CLD-12: SIDE CHANNEL ATTACK PREVENTION	154
CLD-13: HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	155
<i>CLD-13.1: HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) AUTHORIZED INDIVIDUALS FOR HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)</i>	155
<i>CLD-13.2: HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) SENSITIVE/REGULATED DATA ON HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)</i>	156
CLD-14: PROHIBITION ON UNVERIFIED HOSTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	156
CLD-15: SOFTWARE DEFINED STORAGE (SDS)	157
COMPLIANCE (CPL) POLICY & STANDARDS	158
CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	158
<i>CPL-01.1: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE NON-COMPLIANCE OVERSIGHT</i>	158
<i>CPL-01.2: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE COMPLIANCE SCOPE</i>	158
<i>CPL-01.3: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE ABILITY TO DEMONSTRATE CONFORMITY</i>	159

CPL-01.4: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE CONFORMITY ASSESSMENT	159
CPL-01.5: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE DECLARATION OF CONFORMITY	160
CPL-01.6: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE ASSESSMENT TEAM SUBJECT MATTER EXPERTISE	160
CPL-02: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT	161
CPL-02.1: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT INTERNAL AUDIT FUNCTION	162
CPL-02.2: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT PERIODIC AUDITS	162
CPL-02.3: CYBERSECURITY & DATA PROTECTION CONTROLS OVERSIGHT CORRECTIVE ACTION	162
CPL-03: CYBERSECURITY & DATA PROTECTION ASSESSMENTS	163
CPL-03.1: CYBERSECURITY & DATA PROTECTION ASSESSMENTS INDEPENDENT ASSESSORS	163
CPL-03.2: CYBERSECURITY & DATA PROTECTION ASSESSMENTS FUNCTIONAL REVIEW OF CYBERSECURITY & DATA PROTECTION CONTROLS	164
CPL-03.3: CYBERSECURITY & DATA PROTECTION ASSESSMENTS ASSESSOR ACCESS	164
CPL-03.4: CYBERSECURITY & DATA PROTECTION ASSESSMENTS ASSESSMENT METHODS	164
CPL-03.5: CYBERSECURITY & DATA PROTECTION ASSESSMENTS ASSESSMENT RIGOR	165
CPL-03.6: CYBERSECURITY & DATA PROTECTION ASSESSMENTS EVIDENCE REQUEST LIST (ERL)	166
CPL-03.7: CYBERSECURITY & DATA PROTECTION ASSESSMENTS EVIDENCE SAMPLING	166
CPL-04: AUDIT ACTIVITIES	167
CPL-05: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES	167
CPL-05.1: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES INVESTIGATION REQUEST NOTIFICATIONS	167
CPL-05.2: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES INVESTIGATION ACCESS RESTRICTIONS	167
CPL-06: GOVERNMENT SURVEILLANCE	168
CPL-07: GRIEVANCES	168
CPL-07.1: GRIEVANCES GRIEVANCE RESPONSE	168
CPL-08: LOCALIZED REPRESENTATION	168
CPL-08.1: LOCALIZED REPRESENTATION REPRESENTATIVE POWERS	169
CPL-09: CONTROL RECIPROCITY	169
CPL-10: CONTROL INHERITANCE	169
CPL-11: DUAL USE TECHNOLOGY	169
CPL-11.1: DUAL USE TECHNOLOGY USML OR CCL IDENTIFICATION	170
CPL-11.2: DUAL USE TECHNOLOGY EXPORT-CONTROLLED ACCESS RESTRICTIONS	170
CPL-11.3: DUAL USE TECHNOLOGY EXPORT ACTIVITIES DOCUMENTATION	170
CPL-12: STATEMENT OF APPLICABILITY (SOA)	170
CONFIGURATION MANAGEMENT (CFG) POLICY & STANDARDS	172
CFG-01: CONFIGURATION MANAGEMENT PROGRAM	172
CFG-01.1: CONFIGURATION MANAGEMENT PROGRAM ASSIGNMENT OF RESPONSIBILITY	172
CFG-02: SECURE BASELINE CONFIGURATIONS	173
CFG-02.1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS REVIEWS & UPDATES	174
CFG-02.2: SECURE BASELINE CONFIGURATIONS AUTOMATED CENTRAL MANAGEMENT & VERIFICATION	175
CFG-02.3: SECURE BASELINE CONFIGURATIONS RETENTION OF PREVIOUS CONFIGURATIONS	175
CFG-02.4: SECURE BASELINE CONFIGURATIONS DEVELOPMENT & TEST ENVIRONMENTS	175
CFG-02.5: SECURE BASELINE CONFIGURATIONS CONFIGURE TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) FOR HIGH-RISK AREAS	176
CFG-02.6: SECURE BASELINE CONFIGURATIONS NETWORK DEVICE CONFIGURATION FILE SYNCHRONIZATION	176
CFG-02.7: SECURE BASELINE CONFIGURATIONS APPROVED CONFIGURATION DEVIATIONS	177
CFG-02.8: SECURE BASELINE CONFIGURATIONS RESPOND TO UNAUTHORIZED CHANGES	177
CFG-02.9: SECURE BASELINE CONFIGURATIONS BASELINE TAILORING	177
CFG-03: LEAST FUNCTIONALITY	178
CFG-03.1: LEAST FUNCTIONALITY PERIODIC REVIEW	179
CFG-03.2: LEAST FUNCTIONALITY PREVENT UNAUTHORIZED SOFTWARE EXECUTION	179
CFG-03.3: LEAST FUNCTIONALITY EXPLICITLY ALLOW / DENY APPLICATIONS	180
CFG-03.4: LEAST FUNCTIONALITY SPLIT TUNNELING	180
CFG-04: SOFTWARE USAGE RESTRICTIONS	181
CFG-04.1: SOFTWARE USAGE RESTRICTIONS OPEN SOURCE SOFTWARE	181
CFG-04.2: SOFTWARE USAGE RESTRICTIONS UNSUPPORTED INTERNET BROWSERS & EMAIL CLIENTS	181
CFG-05: USER-INSTALLED SOFTWARE	182
CFG-05.1: USER-INSTALLED SOFTWARE UNAUTHORIZED INSTALLATION ALERTS	182
CFG-05.2: USER-INSTALLED SOFTWARE PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	182

CFG-06: CONFIGURATION ENFORCEMENT	182
<i>CFG-06.1: CONFIGURATION ENFORCEMENT INTEGRITY ASSURANCE & ENFORCEMENT (IAE)</i>	183
CFG-07: ZERO-TOUCH PROVISIONING (ZTP)	183
CFG-08: SENSITIVE / REGULATED DATA ACCESS ENFORCEMENT	183
<i>CFG-08.1: SENSITIVE / REGULATED DATA ACCESS ENFORCEMENT SENSITIVE / REGULATED DATA ACTIONS</i>	184
CONTINUOUS MONITORING (MON) POLICY & STANDARDS	185
MON-01: CONTINUOUS MONITORING	185
<i>MON-01.1: CONTINUOUS MONITORING INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)</i>	186
<i>MON-01.2: CONTINUOUS MONITORING AUTOMATED TOOLS FOR REAL-TIME ANALYSIS</i>	186
<i>MON-01.3: CONTINUOUS MONITORING INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC</i>	187
<i>MON-01.4: CONTINUOUS MONITORING SYSTEM GENERATED ALERTS</i>	187
<i>MON-01.5: CONTINUOUS MONITORING WIRELESS INTRUSION DETECTION SYSTEM (WIDS)</i>	188
<i>MON-01.6: CONTINUOUS MONITORING HOST-BASED DEVICES</i>	189
<i>MON-01.7: CONTINUOUS MONITORING FILE INTEGRITY MONITORING (FIM)</i>	189
<i>MON-01.8: CONTINUOUS MONITORING SECURITY EVENT MONITORING</i>	190
<i>MON-01.9: CONTINUOUS MONITORING PROXY LOGGING</i>	190
<i>MON-01.10: CONTINUOUS MONITORING DEACTIVATED ACCOUNT ACTIVITY</i>	190
<i>MON-01.11: CONTINUOUS MONITORING AUTOMATED RESPONSE TO SUSPICIOUS EVENTS</i>	191
<i>MON-01.12: CONTINUOUS MONITORING AUTOMATED ALERTS</i>	191
<i>MON-01.13: CONTINUOUS MONITORING ALERT THRESHOLD TUNING</i>	191
<i>MON-01.14: CONTINUOUS MONITORING INDIVIDUALS POSING GREATER RISK</i>	191
<i>MON-01.15: CONTINUOUS MONITORING PRIVILEGED USER OVERSIGHT</i>	192
<i>MON-01.16: CONTINUOUS MONITORING ANALYZE & PRIORITIZE MONITORING REQUIREMENTS</i>	192
<i>MON-01.17: CONTINUOUS MONITORING REAL-TIME SESSION MONITORING</i>	192
MON-02: CENTRALIZED EVENT LOG COLLECTION	193
<i>MON-02.1: CENTRALIZED EVENT LOG COLLECTION CORRELATE MONITORING INFORMATION</i>	194
<i>MON-02.2: CENTRALIZED EVENT LOG COLLECTION CENTRAL REVIEW & ANALYSIS</i>	194
<i>MON-02.3: CENTRALIZED EVENT LOG COLLECTION INTEGRATION OF SCANNING & OTHER MONITORING INFORMATION</i>	194
<i>MON-02.4: CENTRALIZED EVENT LOG COLLECTION CORRELATION WITH PHYSICAL MONITORING</i>	195
<i>MON-02.5: CENTRALIZED EVENT LOG COLLECTION PERMITTED ACTIONS</i>	195
<i>MON-02.6: CENTRALIZED EVENT LOG COLLECTION AUDIT LEVEL ADJUSTMENT</i>	195
<i>MON-02.7: CENTRALIZED EVENT LOG COLLECTION SYSTEM-WIDE/TIME-CORRELATED AUDIT TRAIL</i>	196
<i>MON-02.8: CENTRALIZED EVENT LOG COLLECTION CHANGES BY AUTHORIZED INDIVIDUALS</i>	196
<i>MON-02.9: CENTRALIZED EVENT LOG COLLECTION INVENTORY OF TECHNOLOGY ASSET EVENT LOGGING</i>	196
MON-03: CONTENT OF EVENT LOGS	197
<i>MON-03.1: CONTENT OF EVENT LOGS SENSITIVE AUDIT INFORMATION</i>	197
<i>MON-03.2: CONTENT OF EVENT LOGS AUDIT TRAILS</i>	198
<i>MON-03.3: CONTENT OF EVENT LOGS PRIVILEGED FUNCTIONS LOGGING</i>	198
<i>MON-03.4: CONTENT OF EVENT LOGS VERBOSITY LOGGING FOR BOUNDARY DEVICES</i>	199
<i>MON-03.5: CONTENT OF EVENT LOGS LIMIT PERSONAL DATA (PD) IN AUDIT RECORDS</i>	199
<i>MON-03.6: CONTENT OF EVENT LOGS CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT</i>	199
<i>MON-03.7: CONTENT OF EVENT LOGS DATABASE LOGGING</i>	199
MON-04: EVENT LOG STORAGE CAPACITY	200
MON-05: RESPONSE TO EVENT LOG PROCESSING FAILURES	200
<i>MON-05.1: RESPONSE TO AUDIT PROCESSING FAILURES REAL-TIME ALERTS OF EVENT LOGGING FAILURE</i>	201
<i>MON-05.2: RESPONSE TO AUDIT PROCESSING FAILURES EVENT LOG STORAGE CAPACITY ALERTING</i>	201
MON-06: MONITORING REPORTING	201
<i>MON-06.1: MONITORING REPORTING QUERY PARAMETER AUDITS OF PERSONAL DATA</i>	202
<i>MON-06.2: MONITORING REPORTING TREND ANALYSIS REPORTING</i>	202
MON-07: TIME STAMPS	202
<i>MON-07.1: TIME STAMPS SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE</i>	203
MON-08: PROTECTION OF EVENT LOGS	203
<i>MON-08.1: PROTECTION OF EVENT LOGS EVENT LOG BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS</i>	203
<i>MON-08.2: PROTECTION OF EVENT LOGS ACCESS BY SUBSET OF PRIVILEGED USERS</i>	204
<i>MON-08.3: PROTECTION OF EVENT LOGS CRYPTOGRAPHIC PROTECTION OF EVENT LOG INFORMATION</i>	204
<i>MON-08.4: PROTECTION OF EVENT LOGS DUAL AUTHORIZATION FOR EVENT LOG MOVEMENT</i>	204
MON-09: NON-REPUDIATION	204

<i>MON-09.1: NON-REPUDIATION IDENTITY BINDING</i>	205
MON-10: EVENT LOG RETENTION	206
MON-11: MONITORING FOR INFORMATION DISCLOSURE	206
<i>MON-11.1: MONITORING FOR INFORMATION DISCLOSURE ANALYZE TRAFFIC FOR COVERT EXFILTRATION</i>	206
<i>MON-11.2: MONITORING FOR INFORMATION DISCLOSURE UNAUTHORIZED NETWORK SERVICES</i>	207
<i>MON-11.3: MONITORING FOR INFORMATION DISCLOSURE MONITORING FOR INDICATORS OF COMPROMISE (IOC)</i>	207
MON-12: SESSION AUDIT	207
MON-13: ALTERNATE EVENT LOGGING CAPABILITY	207
MON-14: CROSS-ORGANIZATIONAL MONITORING	208
<i>MON-14.1: CROSS-ORGANIZATIONAL MONITORING SHARING OF EVENT LOGS</i>	208
MON-15: COVERT CHANNEL ANALYSIS	208
MON-16: ANOMALOUS BEHAVIOR	209
<i>MON-16.1: ANOMALOUS BEHAVIOR INSIDER THREATS</i>	209
<i>MON-16.2: ANOMALOUS BEHAVIOR THIRD-PARTY THREATS</i>	209
<i>MON-16.3: ANOMALOUS BEHAVIOR UNAUTHORIZED ACTIVITIES</i>	209
<i>MON-16.4: ANOMALOUS BEHAVIOR ACCOUNT CREATION AND MODIFICATION LOGGING</i>	210
MON-17: EVENT LOG ANALYSIS & TRIAGE	210
<i>MON-17.1: EVENT LOG ANALYSIS & TRIAGE EVENT LOG REVIEW ESCALATION MATRIX</i>	210
MON-18: FILE ACTIVITY MONITORING (FAM)	211
CRYPTOGRAPHIC PROTECTIONS (CRY) POLICY & STANDARDS	212
CRY-01: USE OF CRYPTOGRAPHIC CONTROLS	212
<i>CRY-01.1: USE OF CRYPTOGRAPHIC CONTROLS ALTERNATE PHYSICAL PROTECTION</i>	213
<i>CRY-01.2: USE OF CRYPTOGRAPHIC CONTROLS EXPORT-CONTROLLED CRYPTOGRAPHY</i>	213
<i>CRY-01.3: USE OF CRYPTOGRAPHIC CONTROLS PRE/POST TRANSMISSION HANDLING</i>	213
<i>CRY-01.4: USE OF CRYPTOGRAPHIC CONTROLS CONCEAL/RANDOMIZE COMMUNICATIONS</i>	213
<i>CRY-01.5: USE OF CRYPTOGRAPHIC CONTROLS CRYPTOGRAPHIC CIPHER SUITES AND PROTOCOLS INVENTORY</i>	214
CRY-02: CRYPTOGRAPHIC MODULE AUTHENTICATION	214
CRY-03: TRANSMISSION CONFIDENTIALITY	215
CRY-04: TRANSMISSION INTEGRITY	215
CRY-05: ENCRYPTING DATA AT REST	216
<i>CRY-05.1: ENCRYPTING DATA AT REST STORAGE MEDIA</i>	216
<i>CRY-05.2: ENCRYPTING DATA AT REST OFFLINE STORAGE</i>	217
<i>CRY-05.3: ENCRYPTING DATA AT REST DATABASE ENCRYPTION</i>	217
CRY-06: NON-CONSOLE ADMINISTRATIVE ACCESS	217
CRY-07: WIRELESS ACCESS AUTHENTICATION & ENCRYPTION	218
CRY-08: PUBLIC KEY INFRASTRUCTURE (PKI)	218
<i>CRY-08.1: PUBLIC KEY INFRASTRUCTURE (PKI) AVAILABILITY</i>	219
CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT	219
<i>CRY-09.1: CRYPTOGRAPHIC KEY MANAGEMENT SYMMETRIC KEYS</i>	221
<i>CRY-09.2: CRYPTOGRAPHIC KEY MANAGEMENT ASYMMETRIC KEYS</i>	221
<i>CRY-09.3: CRYPTOGRAPHIC KEY MANAGEMENT CRYPTOGRAPHIC KEY LOSS OR CHANGE</i>	221
<i>CRY-09.4: CRYPTOGRAPHIC KEY MANAGEMENT CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS</i>	222
<i>CRY-09.5: CRYPTOGRAPHIC KEY MANAGEMENT ASSIGNED OWNERS</i>	222
<i>CRY-09.6: CRYPTOGRAPHIC KEY MANAGEMENT THIRD-PARTY CRYPTOGRAPHIC KEYS</i>	222
<i>CRY-09.7: CRYPTOGRAPHIC KEY MANAGEMENT EXTERNAL SYSTEM CRYPTOGRAPHIC KEY CONTROL</i>	223
CRY-10: TRANSMISSION OF CYBERSECURITY & DATA PROTECTION ATTRIBUTES	223
CRY-11: CERTIFICATE AUTHORITIES	223
CRY-12: CERTIFICATE MONITORING	224
CRY-13: CRYPTOGRAPHIC HASH	224
DATA CLASSIFICATION & HANDLING (DCH) POLICY & STANDARDS	225
DCH-01: DATA PROTECTION	225
<i>DCH-01.1: DATA PROTECTION DATA STEWARDSHIP</i>	225
<i>DCH-01.2: DATA PROTECTION SENSITIVE/REGULATED DATA PROTECTION</i>	226
<i>DCH-01.3: DATA PROTECTION SENSITIVE / REGULATED MEDIA RECORDS</i>	226
<i>DCH-01.4: DATA PROTECTION DEFINING ACCESS AUTHORIZATIONS FOR SENSITIVE / REGULATED DATA</i>	227
DCH-02: DATA & ASSET CLASSIFICATION	227
<i>DCH-02.1: DATA & ASSET CLASSIFICATION HIGHEST CLASSIFICATION LEVEL</i>	227

DCH-03: MEDIA ACCESS	228
DCH-03.1: MEDIA ACCESS DISCLOSURE OF INFORMATION	228
DCH-03.2: MEDIA ACCESS MASKING DISPLAYED DATA	228
DCH-03.3: MEDIA ACCESS CONTROLLED RELEASE	229
DCH-04: MEDIA MARKING	229
DCH-04.1: MEDIA MARKING AUTOMATED MARKING	230
DCH-05: CYBERSECURITY & DATA PROTECTION ATTRIBUTES	230
DCH-05.1: CYBERSECURITY & DATA PROTECTION ATTRIBUTES DYNAMIC ATTRIBUTE ASSOCIATION	230
DCH-05.2: CYBERSECURITY & DATA PROTECTION ATTRIBUTES ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS	230
DCH-05.3: CYBERSECURITY & DATA PROTECTION ATTRIBUTES MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM	230
DCH-05.4: CYBERSECURITY & DATA PROTECTION ATTRIBUTES ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS	231
DCH-05.5: CYBERSECURITY & DATA PROTECTION ATTRIBUTES ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES	231
DCH-05.6: CYBERSECURITY & DATA PROTECTION ATTRIBUTES DATA SUBJECT ATTRIBUTE ASSOCIATIONS	231
DCH-05.7: CYBERSECURITY & DATA PROTECTION ATTRIBUTES CONSISTENT ATTRIBUTE INTERPRETATION	231
DCH-05.8: CYBERSECURITY & DATA PROTECTION ATTRIBUTES IDENTITY ASSOCIATION TECHNIQUES & TECHNOLOGIES	232
DCH-05.9: CYBERSECURITY & DATA PROTECTION ATTRIBUTES ATTRIBUTE REASSIGNMENT	232
DCH-05.10: CYBERSECURITY & DATA PROTECTION ATTRIBUTES ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS	232
DCH-05.11: CYBERSECURITY & DATA PROTECTION ATTRIBUTES AUDIT CHANGES	232
DCH-06: MEDIA STORAGE	233
DCH-06.1: MEDIA STORAGE PHYSICALLY SECURE ALL MEDIA	233
DCH-06.2: MEDIA STORAGE SENSITIVE DATA INVENTORIES	234
DCH-06.3: MEDIA STORAGE PERIODIC SCANS FOR SENSITIVE / REGULATED DATA	234
DCH-06.4: MEDIA STORAGE MAKING SENSITIVE DATA UNREADABLE IN STORAGE	234
DCH-06.5: MEDIA STORAGE STORING AUTHENTICATION DATA	234
DCH-07: MEDIA TRANSPORTATION	236
DCH-07.1: MEDIA TRANSPORTATION CUSTODIANS	236
DCH-07.2: MEDIA TRANSPORTATION ENCRYPTING DATA IN STORAGE MEDIA	236
DCH-08: PHYSICAL MEDIA DISPOSAL	237
DCH-09: SYSTEM MEDIA SANITIZATION	237
DCH-09.1: SYSTEM MEDIA SANITIZATION SYSTEM MEDIA SANITIZATION DOCUMENTATION	238
DCH-09.2: SYSTEM MEDIA SANITIZATION EQUIPMENT TESTING	238
DCH-09.3: SYSTEM MEDIA SANITIZATION SANITIZATION OF PERSONAL DATA (PD)	238
DCH-09.4: SYSTEM MEDIA SANITIZATION FIRST TIME USE SANITIZATION	239
DCH-09.5: SYSTEM MEDIA SANITIZATION DUAL AUTHORIZATION FOR SENSITIVE DATA DESTRUCTION	239
DCH-10: MEDIA USE	240
DCH-10.1: MEDIA USE LIMITATIONS ON USE	240
DCH-10.2: MEDIA USE PROHIBIT USE WITHOUT OWNER	240
DCH-11: DATA RECLASSIFICATION	240
DCH-12: REMOVABLE MEDIA SECURITY	241
DCH-13: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	241
DCH-13.1: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) LIMITS OF AUTHORIZED USE	242
DCH-13.2: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) PORTABLE STORAGE DEVICES	242
DCH-13.3: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) PROTECTING SENSITIVE / REGULATED DATA ON EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	243
DCH-13.4: USE OF EXTERNAL TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) NON-ORGANIZATIONALLY OWNED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	243
DCH-14: INFORMATION SHARING	244
DCH-14.1: INFORMATION SHARING INFORMATION SEARCH & RETRIEVAL	244
DCH-14.2: INFORMATION SHARING TRANSFER AUTHORIZATIONS	244
DCH-14.3: INFORMATION SHARING DATA ACCESS MAPPING	245
DCH-15: PUBLICLY ACCESSIBLE CONTENT	245
DCH-16: DATA MINING PROTECTION	246
DCH-17: AD-HOC TRANSFERS	246
DCH-18: MEDIA & DATA RETENTION	246
DCH-18.1: MEDIA & DATA RETENTION MINIMIZE SENSITIVE / REGULATED DATA	248
DCH-18.2: MEDIA & DATA RETENTION LIMIT SENSITIVE / REGULATED DATA IN TESTING, TRAINING & RESEARCH	248
DCH-18.3: MEDIA & DATA RETENTION TEMPORARY FILES CONTAINING PERSONAL DATA	248
DCH-19: GEOGRAPHIC LOCATION OF DATA	248

DCH-20: ARCHIVED DATA SETS	249
DCH-21: INFORMATION DISPOSAL	249
DCH-22: DATA QUALITY OPERATIONS	249
<i>DCH-22.1: DATA QUALITY OPERATIONS UPDATING & CORRECTING PERSONAL DATA (PD)</i>	250
<i>DCH-22.2: DATA QUALITY OPERATIONS DATA TAGS</i>	250
<i>DCH-22.3: DATA QUALITY OPERATIONS PRIMARY SOURCE PERSONAL DATA (PD) COLLECTION</i>	250
DCH-23: DE-IDENTIFICATION (ANONYMIZATION)	250
<i>DCH-23.1: DE-IDENTIFICATION (ANONYMIZATION) DE-IDENTIFY DATASET UPON COLLECTION</i>	251
<i>DCH-23.2: DE-IDENTIFICATION (ANONYMIZATION) ARCHIVING</i>	251
<i>DCH-23.3: DE-IDENTIFICATION (ANONYMIZATION) RELEASE</i>	251
<i>DCH-23.4: DE-IDENTIFICATION (ANONYMIZATION) REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS</i>	251
<i>DCH-23.5: DE-IDENTIFICATION (ANONYMIZATION) STATISTICAL DISCLOSURE CONTROL</i>	252
<i>DCH-23.6: DE-IDENTIFICATION (ANONYMIZATION) DIFFERENTIAL DATA PRIVACY</i>	252
<i>DCH-23.7: DE-IDENTIFICATION (ANONYMIZATION) AUTOMATED DE-IDENTIFICATION OF SENSITIVE DATA</i>	252
<i>DCH-23.8: DE-IDENTIFICATION (ANONYMIZATION) MOTIVATED INTRUDER</i>	252
<i>DCH-23.9: DE-IDENTIFICATION (ANONYMIZATION) CODE NAMES</i>	253
DCH-24: INFORMATION LOCATION	253
<i>DCH-24.1: INFORMATION LOCATION AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION</i>	253
DCH-25: TRANSFER OF SENSITIVE AND/OR REGULATED DATA	254
<i>DCH-25.1: TRANSFER OF SENSITIVE AND/OR REGULATED DATA TRANSFER ACTIVITY LIMITS</i>	254
DCH-26: DATA LOCALIZATION	254
DCH-27: DATA RIGHTS MANAGEMENT (DRM)	255
EMBEDDED TECHNOLOGY (EMB) POLICY & STANDARDS	256
EMB-01: EMBEDDED TECHNOLOGY SECURITY PROGRAM	256
EMB-02: INTERNET OF THINGS (IoT)	256
EMB-03: OPERATIONAL TECHNOLOGY (OT)	257
EMB-04: INTERFACE SECURITY	257
EMB-05: EMBEDDED TECHNOLOGY CONFIGURATION MONITORING	258
EMB-06: PREVENT ALTERATIONS	258
EMB-07: EMBEDDED TECHNOLOGY MAINTENANCE	258
EMB-08: RESILIENCE TO OUTAGES	258
EMB-09: POWER LEVEL MONITORING	259
EMB-10: EMBEDDED TECHNOLOGY REVIEWS	259
EMB-11: MESSAGE QUEUING TELEMETRY TRANSPORT (MQTT) SECURITY	259
EMB-12: RESTRICT COMMUNICATIONS	259
EMB-13: AUTHORIZED COMMUNICATIONS	259
EMB-14: OPERATING ENVIRONMENT CERTIFICATION	260
EMB-15: SAFETY ASSESSMENT	260
EMB-16: CERTIFICATE-BASED AUTHENTICATION	260
EMB-17: CHIP-TO-CLOUD SECURITY	260
EMB-18: REAL-TIME OPERATING SYSTEM (RTOS) SECURITY	260
EMB-19: SAFE OPERATIONS	261
ENDPOINT SECURITY (END) POLICY & STANDARDS	262
END-01: ENDPOINT DEVICE MANAGEMENT (EDM)	262
<i>END-01.1: ENTERPRISE DEVICE MANAGEMENT (EDM) UNIFIED ENDPOINT DEVICE MANAGEMENT (UEDM)</i>	262
END-02: ENDPOINT PROTECTION MEASURES	263
END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	263
<i>END-03.1: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS SOFTWARE INSTALLATION ALERTS</i>	263
<i>END-03.2: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS GOVERNING ACCESS RESTRICTION FOR CHANGE</i>	263
END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	264
<i>END-04.1: MALICIOUS CODE PROTECTION (ANTI-MALWARE) AUTOMATIC ANTIMALWARE SIGNATURE UPDATES</i>	265
<i>END-04.2: MALICIOUS CODE PROTECTION (ANTI-MALWARE) DOCUMENTED PROTECTION MEASURES</i>	265
<i>END-04.3: MALICIOUS CODE PROTECTION (ANTI-MALWARE) CENTRALIZED MANAGEMENT OF ANTIMALWARE TECHNOLOGIES</i>	265
<i>END-04.4: MALICIOUS CODE PROTECTION (ANTI-MALWARE) NONSIGNATURE-BASED DETECTION</i>	265
<i>END-04.5: MALICIOUS CODE PROTECTION (ANTI-MALWARE) MALWARE PROTECTION MECHANISM TESTING</i>	266
<i>END-04.6: MALICIOUS CODE PROTECTION (ANTI-MALWARE) EVOLVING MALWARE THREATS</i>	266

<i>END-04.7: MALICIOUS CODE PROTECTION (ANTI-MALWARE) ALWAYS ON PROTECTION</i>	266
END-05: SOFTWARE FIREWALL	267
END-06: ENDPOINT FILE INTEGRITY MONITORING (FIM)	267
<i>END-06.1: ENDPOINT FILE INTEGRITY MONITORING (FIM) INTEGRITY CHECKS</i>	268
<i>END-06.2: ENDPOINT FILE INTEGRITY MONITORING (FIM) ENDPOINT DETECTION & RESPONSE (EDR)</i>	268
<i>END-06.3: ENDPOINT FILE INTEGRITY MONITORING (FIM) AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS</i>	268
<i>END-06.4: ENDPOINT FILE INTEGRITY MONITORING (FIM) AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS</i>	269
<i>END-06.5: ENDPOINT FILE INTEGRITY MONITORING (FIM) VERIFY BOOT PROCESS</i>	269
<i>END-06.6: ENDPOINT FILE INTEGRITY MONITORING (FIM) PROTECTION OF BOOT FIRMWARE</i>	269
<i>END-06.7: ENDPOINT FILE INTEGRITY MONITORING (FIM) BINARY OR MACHINE-EXECUTABLE CODE</i>	269
<i>END-06.8: ENDPOINT FILE INTEGRITY MONITORING (FIM) EXTENDED DETECTION & RESPONSE (XDR)</i>	270
END-07: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS/HIPS)	270
END-08: PHISHING & SPAM PROTECTION	270
<i>END-08.1: PHISHING & SPAM PROTECTION CENTRAL MANAGEMENT</i>	271
<i>END-08.2: PHISHING & SPAM PROTECTION AUTOMATIC SPAM AND PHISHING PROTECTION UPDATES</i>	271
END-09: TRUSTED PATH	271
END-10: MOBILE CODE	272
END-11: THIN NODES	273
END-12: PORT & INPUT/OUTPUT (I/O) DEVICE ACCESS	273
END-13: SENSOR CAPABILITY	273
<i>END-13.1: SENSOR CAPABILITY AUTHORIZED USE</i>	274
<i>END-13.2: SENSOR CAPABILITY NOTICE OF COLLECTION</i>	274
<i>END-13.3: SENSOR CAPABILITY COLLECTION MINIMIZATION</i>	274
<i>END-13.4: SENSOR CAPABILITY SENSOR DELIVERY VERIFICATION</i>	274
END-14: COLLABORATIVE COMPUTING DEVICES	274
<i>END-14.1: COLLABORATIVE COMPUTING DEVICES DISABLING/REMOVAL IN SECURE WORK AREAS</i>	275
<i>END-14.2: COLLABORATIVE COMPUTING DEVICES EXPLICITLY INDICATE CURRENT PARTICIPANTS</i>	275
<i>END-14.3: COLLABORATIVE COMPUTING DEVICES PARTICIPANT IDENTITY VERIFICATION</i>	275
<i>END-14.4: COLLABORATIVE COMPUTING DEVICES PARTICIPANT CONNECTION MANAGEMENT</i>	276
<i>END-14.5: COLLABORATIVE COMPUTING DEVICES MALICIOUS LINK & FILE PROTECTIONS</i>	276
<i>END-14.6: COLLABORATIVE COMPUTING DEVICES EXPLICIT INDICATION OF USE</i>	276
END-15: HYPERVISOR ACCESS	276
END-16: RESTRICT ACCESS TO SECURITY FUNCTIONS	276
<i>END-16.1: RESTRICT ACCESS TO SECURITY FUNCTIONS HOST-BASED SECURITY FUNCTION ISOLATION</i>	277
HUMAN RESOURCES SECURITY (HRS) POLICY & STANDARDS	278
HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	278
<i>HRS-01.1: HUMAN RESOURCES SECURITY MANAGEMENT ONBOARDING, TRANSFERRING & OFFBOARDING PERSONNEL</i>	278
HRS-02: POSITION CATEGORIZATION	279
<i>HRS-02.1: POSITION CATEGORIZATION USERS WITH ELEVATED PRIVILEGES</i>	279
<i>HRS-02.2: POSITION CATEGORIZATION PROBATIONARY PERIODS</i>	280
HRS-03: DEFINED ROLES & RESPONSIBILITIES	280
<i>HRS-03.1: DEFINED ROLES & RESPONSIBILITIES USER AWARENESS</i>	280
<i>HRS-03.2: DEFINED ROLES & RESPONSIBILITIES COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS</i>	281
HRS-04: PERSONNEL SCREENING	281
<i>HRS-04.1: PERSONNEL SCREENING ROLES WITH SPECIAL PROTECTION MEASURES</i>	282
<i>HRS-04.2: PERSONNEL SCREENING FORMAL INDOCTRINATION</i>	282
<i>HRS-04.3: PERSONNEL SCREENING CITIZENSHIP REQUIREMENTS</i>	282
<i>HRS-04.4: PERSONNEL SCREENING CITIZENSHIP IDENTIFICATION</i>	282
HRS-05: TERMS OF EMPLOYMENT	283
<i>HRS-05.1: TERMS OF EMPLOYMENT RULES OF BEHAVIOR</i>	283
<i>HRS-05.2: TERMS OF EMPLOYMENT SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS</i>	284
<i>HRS-05.3: TERMS OF EMPLOYMENT TECHNOLOGY USE RESTRICTIONS</i>	284
<i>HRS-05.4: TERMS OF EMPLOYMENT USE OF CRITICAL TECHNOLOGIES</i>	284
<i>HRS-05.5: TERMS OF EMPLOYMENT USE OF MOBILE DEVICES</i>	285
<i>HRS-05.6: TERMS OF EMPLOYMENT SECURITY-MINDED DRESS CODE</i>	285
<i>HRS-05.7: TERMS OF EMPLOYMENT POLICY FAMILIARIZATION & ACKNOWLEDGEMENT</i>	285
HRS-06: ACCESS AGREEMENTS	286

HRS-06.1: ACCESS AGREEMENTS CONFIDENTIALITY AGREEMENTS	286
HRS-06.2: ACCESS AGREEMENTS POST-EMPLOYMENT REQUIREMENTS AWARENESS	286
HRS-07: PERSONNEL SANCTIONS	287
HRS-07.1: PERSONNEL SANCTIONS WORKPLACE INVESTIGATIONS	288
HRS-07.2: PERSONNEL SANCTIONS UPDATING DISCIPLINARY PROCESSES	288
HRS-07.3: PERSONNEL SANCTIONS PREVENTATIVE ACCESS RESTRICTION	288
HRS-08: PERSONNEL TRANSFER	289
HRS-09: PERSONNEL TERMINATION	289
HRS-09.1: PERSONNEL TERMINATION ASSET COLLECTION	290
HRS-09.2: PERSONNEL TERMINATION HIGH-RISK TERMINATIONS	290
HRS-09.3: PERSONNEL TERMINATION POST-EMPLOYMENT REQUIREMENTS NOTIFICATION	291
HRS-09.4: PERSONNEL TERMINATION AUTOMATED EMPLOYMENT STATUS NOTIFICATION	291
HRS-10: THIRD-PARTY PERSONNEL SECURITY	291
HRS-11: SEPARATION OF DUTIES (SOD)	292
HRS-12: INCOMPATIBLE ROLES	292
HRS-12.1: INCOMPATIBLE ROLES TWO-PERSON RULE	293
HRS-13: IDENTIFY CRITICAL SKILLS & GAPS	293
HRS-13.1: IDENTIFY CRITICAL SKILLS & GAPS REMEDIATE IDENTIFIED SKILLS DEFICIENCIES	293
HRS-13.2: IDENTIFY CRITICAL SKILLS & GAPS IDENTIFY VITAL CYBERSECURITY & DATA PRIVACY STAFF	293
HRS-13.3: IDENTIFY CRITICAL SKILLS & GAPS ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & DATA PRIVACY STAFF	294
HRS-13.4: IDENTIFY CRITICAL SKILLS & GAPS PERFORM SUCCESSION PLANNING	294
HRS-14: IDENTIFYING AUTHORIZED WORK LOCATIONS	294
HRS-14.1: IDENTIFYING AUTHORIZED WORK LOCATIONS COMMUNICATING AUTHORIZED WORK LOCATIONS	294
HRS-15: REPORTING SUSPICIOUS ACTIVITIES	295
IDENTIFICATION & AUTHENTICATION (IAC) POLICY & STANDARDS	296
IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	296
IAC-01.1: IDENTITY & ACCESS MANAGEMENT (IAM) RETAIN ACCESS RECORDS	297
IAC-01.2: IDENTITY & ACCESS MANAGEMENT (IAM) AUTHENTICATE, AUTHORIZE AND AUDIT (AAA)	297
IAC-01.3: IDENTITY & ACCESS MANAGEMENT (IAM) USER & SERVICE ACCOUNT INVENTORIES	297
IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	298
IAC-02.1: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS GROUP AUTHENTICATION	298
IAC-02.2: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS REPLAY-RESISTANT AUTHENTICATION	299
IAC-02.3: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS ACCEPTANCE OF PIV CREDENTIALS	299
IAC-02.4: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS OUT-OF-BAND AUTHENTICATION (OOBA)	299
IAC-03: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS	299
IAC-03.1: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF PIV CREDENTIALS FROM OTHER ORGANIZATIONS	300
IAC-03.2: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF THIRD-PARTY CREDENTIALS	300
IAC-03.3: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS USE OF FICAM-ISSUED PROFILES	300
IAC-03.4: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS DISASSOCIABILITY	300
IAC-03.5: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF EXTERNAL AUTHENTICATORS	301
IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	301
IAC-04.1: IDENTIFICATION & AUTHENTICATION FOR DEVICES DEVICE ATTESTATION	301
IAC-04.2: IDENTIFICATION & AUTHENTICATION FOR DEVICES DEVICE AUTHORIZATION ENFORCEMENT	302
IAC-05: IDENTIFICATION & AUTHENTICATION FOR THIRD-PARTY TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	302
IAC-05.1: IDENTIFICATION & AUTHENTICATION FOR THIRD-PARTY TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) INFORMATION EXCHANGE	302
IAC-05.2: IDENTIFICATION & AUTHENTICATION FOR THIRD-PARTY TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS) PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	303
IAC-06: MULTI-FACTOR AUTHENTICATION (MFA)	303
IAC-06.1: MULTI-FACTOR AUTHENTICATION (MFA) NETWORK ACCESS TO PRIVILEGED ACCOUNTS	303
IAC-06.2: MULTI-FACTOR AUTHENTICATION (MFA) NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	304
IAC-06.3: MULTI-FACTOR AUTHENTICATION (MFA) LOCAL ACCESS TO PRIVILEGED ACCOUNTS	304
IAC-06.4: MULTI-FACTOR AUTHENTICATION (MFA) OUT OF BAND (OOB) FACTOR	304
IAC-07: USER PROVISIONING & DE-PROVISIONING	304

IAC-07.1: USER PROVISIONING & DE-PROVISIONING CHANGE OF ROLES & DUTIES	305
IAC-07.2: USER PROVISIONING & DE-PROVISIONING TERMINATION OF EMPLOYMENT	305
IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	306
IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)	307
IAC-09.1: IDENTIFIER MANAGEMENT USER IDENTITY (ID) MANAGEMENT	307
IAC-09.2: IDENTIFIER MANAGEMENT IDENTITY USER STATUS	308
IAC-09.3: IDENTIFIER MANAGEMENT DYNAMIC MANAGEMENT	308
IAC-09.4: IDENTIFIER MANAGEMENT CROSS-ORGANIZATION MANAGEMENT	308
IAC-09.5: IDENTIFIER MANAGEMENT PRIVILEGED ACCOUNT IDENTIFIERS	309
IAC-09.6: IDENTIFIER MANAGEMENT PAIRWISE PSEUDONYMOUS IDENTIFIERS (PPID)	309
IAC-10: AUTHENTICATOR MANAGEMENT	309
IAC-10.1: AUTHENTICATOR MANAGEMENT PASSWORD-BASED AUTHENTICATION	310
IAC-10.2: AUTHENTICATOR MANAGEMENT PKI-BASED AUTHENTICATION	312
IAC-10.3: AUTHENTICATOR MANAGEMENT IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION	312
IAC-10.4: AUTHENTICATOR MANAGEMENT AUTOMATED SUPPORT FOR PASSWORD STRENGTH	312
IAC-10.5: AUTHENTICATOR MANAGEMENT PROTECTION OF AUTHENTICATORS	313
IAC-10.6: AUTHENTICATOR MANAGEMENT NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS	313
IAC-10.7: AUTHENTICATOR MANAGEMENT HARDWARE TOKEN-BASED AUTHENTICATION	313
IAC-10.8: AUTHENTICATOR MANAGEMENT DEFAULT AUTHENTICATORS	313
IAC-10.9: AUTHENTICATOR MANAGEMENT MULTIPLE SYSTEM ACCOUNTS	314
IAC-10.10: AUTHENTICATOR MANAGEMENT EXPIRATION OF CACHED AUTHENTICATORS	314
IAC-10.11: AUTHENTICATOR MANAGEMENT PASSWORD MANAGERS	314
IAC-10.12: AUTHENTICATOR MANAGEMENT BIOMETRIC AUTHENTICATION	315
IAC-10.13: AUTHENTICATOR MANAGEMENT EVENTS REQUIRING AUTHENTICATOR CHANGE	315
IAC-10.14: AUTHENTICATOR MANAGEMENT PASSKEYS	315
IAC-11: AUTHENTICATOR FEEDBACK	316
IAC-12: CRYPTOGRAPHIC MODULE AUTHENTICATION	316
IAC-12.1: CRYPTOGRAPHIC MODULE AUTHENTICATION HARDWARE SECURITY MODULES (HSM)	316
IAC-13: ADAPTIVE IDENTIFICATION & AUTHENTICATION	316
IAC-13.1: ADAPTIVE IDENTIFICATION & AUTHENTICATION SINGLE SIGN-ON (SSO) TRANSPARENT AUTHENTICATION	317
IAC-13.2: ADAPTIVE IDENTIFICATION & AUTHENTICATION FEDERATED CREDENTIAL MANAGEMENT	317
IAC-13.3: ADAPTIVE IDENTIFICATION & AUTHENTICATION CONTINUOUS AUTHENTICATION	317
IAC-14: RE-AUTHENTICATION	317
IAC-15: ACCOUNT MANAGEMENT	318
IAC-15.1: ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT (DIRECTORY SERVICES)	320
IAC-15.2: ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS	320
IAC-15.3: ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS	321
IAC-15.4: ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS	321
IAC-15.5: ACCOUNT MANAGEMENT RESTRICTIONS ON SHARED GROUPS/ACCOUNTS	321
IAC-15.6: ACCOUNT MANAGEMENT ACCOUNT DISABLING FOR HIGH RISK INDIVIDUALS	322
IAC-15.7: ACCOUNT MANAGEMENT SYSTEM ACCOUNT REVIEWS	322
IAC-15.8: ACCOUNT MANAGEMENT USAGE CONDITIONS	322
IAC-15.9: ACCOUNT MANAGEMENT EMERGENCY ACCOUNTS	322
IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)	323
IAC-16.1: PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED ACCOUNT INVENTORIES	324
IAC-16.2: PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED ACCOUNT SEPARATION	324
IAC-16.3: PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED COMMAND EXECUTION	324
IAC-16.4: PRIVILEGED ACCOUNT MANAGEMENT (PAM) DEDICATED PRIVILEGED ACCOUNT	324
IAC-17: PERIODIC REVIEW OF ACCOUNT PRIVILEGES	324
IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT	325
IAC-19: CREDENTIAL SHARING	326
IAC-20: ACCESS ENFORCEMENT	326
IAC-20.1: ACCESS ENFORCEMENT ACCESS TO SENSITIVE DATA	327
IAC-20.2: ACCESS ENFORCEMENT DATABASE ACCESS	327
IAC-20.3: ACCESS ENFORCEMENT USE OF PRIVILEGED UTILITY PROGRAMS	327
IAC-20.4: ACCESS ENFORCEMENT DEDICATED ADMINISTRATIVE MACHINES	328
IAC-20.5: ACCESS ENFORCEMENT DUAL AUTHORIZATION FOR PRIVILEGED COMMANDS	328
IAC-20.6: ACCESS ENFORCEMENT REVOCATION OF ACCESS AUTHORIZATIONS	328

IAC-20.7: ACCESS ENFORCEMENT AUTHORIZED SYSTEM ACCOUNTS	328
IAC-21: LEAST PRIVILEGE	329
IAC-21.1: LEAST PRIVILEGE AUTHORIZE ACCESS TO SECURITY FUNCTIONS	329
IAC-21.2: LEAST PRIVILEGE NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS	329
IAC-21.3: LEAST PRIVILEGE MANAGEMENT APPROVAL FOR PRIVILEGED ACCOUNTS	330
IAC-21.4: LEAST PRIVILEGE AUDITING USE OF PRIVILEGED FUNCTIONS	330
IAC-21.5: LEAST PRIVILEGE PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	330
IAC-21.6: LEAST PRIVILEGE NETWORK ACCESS TO PRIVILEGED COMMANDS	330
IAC-21.7: LEAST PRIVILEGE PRIVILEGE LEVELS FOR CODE EXECUTION	331
IAC-22: ACCOUNT LOCKOUT	331
IAC-23: CONCURRENT SESSION CONTROL	331
IAC-24: SESSION LOCK	332
IAC-24.1: SESSION LOCK PATTERN-HIDING DISPLAYS	332
IAC-25: SESSION TERMINATION	332
IAC-25.1: SESSION TERMINATION USER-INITIATED LOGOUTS/MESSAGE DISPLAYS	333
IAC-26: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHORIZATION	333
IAC-27: REFERENCE MONITOR	333
IAC-28: IDENTITY PROOFING (IDENTITY VERIFICATION)	334
IAC-28.1: IDENTITY PROOFING (IDENTITY VERIFICATION) MANAGEMENT APPROVAL FOR NEW OR CHANGED ACCOUNTS	334
IAC-28.2: IDENTITY PROOFING (IDENTITY VERIFICATION) IDENTITY EVIDENCE	334
IAC-28.3: IDENTITY PROOFING (IDENTITY VERIFICATION) IDENTITY EVIDENCE VALIDATION & VERIFICATION	334
IAC-28.4: IDENTITY PROOFING (IDENTITY VERIFICATION) IN-PERSON VALIDATION & VERIFICATION	335
IAC-28.5: IDENTITY PROOFING (IDENTITY VERIFICATION) ADDRESS CONFIRMATION	335
IAC-29: ATTRIBUTE-BASED ACCESS CONTROL (ABAC)	335
IAC-29.1: ATTRIBUTE-BASED ACCESS CONTROL (ABAC) REAL-TIME ACCESS DECISIONS	335
IAC-29.2: ATTRIBUTE-BASED ACCESS CONTROL (ABAC) ACCESS PROFILE RULES	336
INCIDENT RESPONSE (IRO) POLICY & STANDARDS	337
IRO-01: INCIDENTS RESPONSE OPERATIONS	337
IRO-02: INCIDENT HANDLING	337
IRO-02.1: INCIDENT HANDLING AUTOMATED INCIDENT HANDLING PROCESSES	338
IRO-02.2: INCIDENT HANDLING INSIDER THREAT RESPONSE CAPABILITY	338
IRO-02.3: INCIDENT HANDLING DYNAMIC RECONFIGURATION	339
IRO-02.4: INCIDENT HANDLING INCIDENT CLASSIFICATION & PRIORITIZATION	339
IRO-02.5: INCIDENT HANDLING CORRELATION WITH EXTERNAL ORGANIZATIONS	341
IRO-02.6: INCIDENT HANDLING AUTOMATIC DISABLING OF TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	341
IRO-03: INDICATORS OF COMPROMISE (IOC)	341
IRO-04: INCIDENT RESPONSE PLAN (IRP)	342
IRO-04.1: INCIDENT RESPONSE PLAN (IRP) DATA BREACH	342
IRO-04.2: INCIDENT RESPONSE PLAN (IRP) IRP UPDATE	343
IRO-04.3: INCIDENT RESPONSE PLAN (IRP) CONTINUOUS INCIDENT RESPONSE IMPROVEMENTS	343
IRO-05: INCIDENT RESPONSE TRAINING	343
IRO-05.1: INCIDENT RESPONSE TRAINING SIMULATED INCIDENTS	344
IRO-05.2: INCIDENT RESPONSE TRAINING AUTOMATED INCIDENT RESPONSE TRAINING ENVIRONMENTS	344
IRO-06: INCIDENT RESPONSE TESTING	344
IRO-06.1: INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS	345
IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)	345
IRO-08: CHAIN OF CUSTODY & FORENSICS	345
IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS	346
IRO-09.1: SITUATIONAL AWARENESS FOR INCIDENTS AUTOMATED TRACKING, DATA COLLECTION & ANALYSIS	346
IRO-09.2: SITUATIONAL AWARENESS FOR INCIDENTS RECURRING INCIDENT ANALYSIS	346
IRO-10: INCIDENT STAKEHOLDER REPORTING	346
IRO-10.1: INCIDENT STAKEHOLDER REPORTING AUTOMATED REPORTING	347
IRO-10.2: INCIDENT STAKEHOLDER REPORTING CYBER INCIDENT REPORTING FOR SENSITIVE / REGULATED DATA	347
IRO-10.3: INCIDENT STAKEHOLDER REPORTING VULNERABILITIES RELATED TO INCIDENTS	348
IRO-10.4: INCIDENT STAKEHOLDER REPORTING SUPPLY CHAIN COORDINATION	348
IRO-10.5: INCIDENT STAKEHOLDER REPORTING SERIOUS INCIDENT REPORTING	348
IRO-11: INCIDENT REPORTING ASSISTANCE	349

IRO-11.1: INCIDENT REPORTING ASSISTANCE AUTOMATION SUPPORT OF AVAILABILITY OF INFORMATION/SUPPORT	349
IRO-11.2: INCIDENT REPORTING ASSISTANCE COORDINATION WITH EXTERNAL PROVIDERS	349
IRO-12: SENSITIVE / REGULATED DATA SPILL RESPONSE	349
IRO-12.1: SENSITIVE / REGULATED DATA SPILL RESPONSE SENSITIVE / REGULATED DATA SPILL RESPONSIBLE PERSONNEL	350
IRO-12.2: SENSITIVE / REGULATED DATA SPILL RESPONSE SENSITIVE / REGULATED DATA SPILL TRAINING	350
IRO-12.3: SENSITIVE / REGULATED DATA SPILL RESPONSE POST-SENSITIVE / REGULATED DATA SPILL OPERATIONS	350
IRO-12.4: SENSITIVE / REGULATED DATA SPILL RESPONSE SENSITIVE / REGULATED DATA EXPOSURE TO UNAUTHORIZED PERSONNEL	350
IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	351
IRO-14: REGULATORY & LAW ENFORCEMENT CONTACTS	351
IRO-15: DETONATION CHAMBERS (SANDBOXES)	351
IRO-16: PUBLIC RELATIONS & REPUTATION REPAIR	351
INFORMATION ASSURANCE (IAO) POLICY & STANDARDS	353
IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS	353
IAO-01.1: INFORMATION ASSURANCE (IA) OPERATIONS ASSESSMENT BOUNDARIES	353
IAO-02: ASSESSMENTS	353
IAO-02.1: ASSESSMENTS INDEPENDENT ASSESSORS	354
IAO-02.2: ASSESSMENTS SPECIALIZED ASSESSMENTS	354
IAO-02.3: ASSESSMENTS THIRD-PARTY ASSESSMENTS	355
IAO-02.4: ASSESSMENTS SECURITY ASSESSMENT REPORT (SAR)	355
IAO-03: SYSTEM SECURITY & PRIVACY PLAN (SSPP)	355
IAO-03.1: SYSTEM SECURITY & PRIVACY PLAN (SSPP) PLAN/COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	357
IAO-03.2: SYSTEM SECURITY & PRIVACY PLAN (SSPP) ADEQUATE SECURITY FOR SENSITIVE / REGULATED DATA IN SUPPORT OF CONTRACTS	358
IAO-04: THREAT ANALYSIS & FLAW REMEDIATION DURING DEVELOPMENT	358
IAO-05: PLAN OF ACTION & MILESTONES (POA&M)	360
IAO-05.1: PLAN OF ACTION & MILESTONES (POA&M) POA&M AUTOMATION	361
IAO-06: TECHNICAL VERIFICATION	361
IAO-07: SECURITY AUTHORIZATION	361
MAINTENANCE (MNT) POLICY & STANDARDS	362
MNT-01: MAINTENANCE OPERATIONS	362
MNT-02: CONTROLLED MAINTENANCE	362
MNT-02.1: CONTROLLED MAINTENANCE AUTOMATED MAINTENANCE ACTIVITIES	363
MNT-03: TIMELY MAINTENANCE	363
MNT-03.1: TIMELY MAINTENANCE PREVENTATIVE MAINTENANCE	363
MNT-03.2: TIMELY MAINTENANCE PREDICTIVE MAINTENANCE	364
MNT-03.3: TIMELY MAINTENANCE AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE	364
MNT-04: MAINTENANCE TOOLS	364
MNT-04.1: MAINTENANCE TOOLS INSPECT TOOLS	365
MNT-04.2: MAINTENANCE TOOLS INSPECT MEDIA	365
MNT-04.3: MAINTENANCE TOOLS PREVENT UNAUTHORIZED REMOVAL	365
MNT-04.4: MAINTENANCE TOOLS RESTRICT TOOL USE	365
MNT-05: REMOTE MAINTENANCE	366
MNT-05.1: REMOTE MAINTENANCE AUDITING REMOTE MAINTENANCE	366
MNT-05.2: REMOTE MAINTENANCE REMOTE MAINTENANCE NOTIFICATIONS	366
MNT-05.3: REMOTE MAINTENANCE REMOTE MAINTENANCE CRYPTOGRAPHIC PROTECTION	367
MNT-05.4: REMOTE MAINTENANCE REMOTE MAINTENANCE DISCONNECT VERIFICATION	367
MNT-05.5: REMOTE MAINTENANCE REMOTE MAINTENANCE PRE-APPROVAL	367
MNT-05.6: REMOTE MAINTENANCE REMOTE MAINTENANCE COMPARABLE SECURITY & SANITIZATION	367
MNT-05.7: REMOTE MAINTENANCE SEPARATION OF MAINTENANCE SESSIONS	368
MNT-06: MAINTENANCE PERSONNEL	368
MNT-06.1: MAINTENANCE PERSONNEL MAINTENANCE PERSONNEL WITHOUT APPROPRIATE ACCESS	368
MNT-06.2: MAINTENANCE PERSONNEL NON-SYSTEM RELATED MAINTENANCE	369
MNT-07: MAINTAIN CONFIGURATION CONTROL DURING MAINTENANCE	369
MNT-08: FIELD MAINTENANCE	369
MNT-09: OFF-SITE MAINTENANCE	369
MNT-10: MAINTENANCE VALIDATION	370

MNT-11: MAINTENANCE MONITORING	370
MOBILE DEVICE MANAGEMENT (MDM) POLICY & STANDARDS	371
MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES	371
MDM-02: ACCESS CONTROL FOR MOBILE DEVICES	371
MDM-03: FULL DEVICE & CONTAINER-BASED ENCRYPTION	372
MDM-04: TAMPER PROTECTION & DETECTION	372
MDM-05: REMOTE PURGING	373
MDM-06: PERSONALLY-OWNED MOBILE DEVICES	373
MDM-07: ORGANIZATION-OWNED MOBILE DEVICES	374
MDM-08: MOBILE DEVICE DATA RETENTION LIMITATIONS	374
MDM-09: MOBILE DEVICE GEOFENCING	374
MDM-10: SEPARATE MOBILE DEVICE PROFILES	374
MDM-11: RESTRICTING ACCESS TO AUTHORIZED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	375
NETWORK SECURITY (NET) POLICY & STANDARDS	376
NET-01: NETWORK SECURITY CONTROLS (NSC)	376
<i>NET-01.1: NETWORK SECURITY CONTROLS (NSC) ZERO TRUST ARCHITECTURE (ZTA)</i>	376
NET-02: LAYERED DEFENSES	376
<i>NET-02.1: LAYERED DEFENSES DENIAL OF SERVICE (DoS) PROTECTION</i>	377
<i>NET-02.2: LAYERED DEFENSES GUEST NETWORKS</i>	377
<i>NET-02.3: LAYERED DEFENSES CROSS DOMAIN SOLUTIONS (CDS)</i>	377
NET-03: BOUNDARY PROTECTION	378
<i>NET-03.1: BOUNDARY PROTECTION LIMIT NETWORK CONNECTIONS</i>	379
<i>NET-03.2: BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES</i>	379
<i>NET-03.3: BOUNDARY PROTECTION PREVENT DISCOVERY OF INTERNAL INFORMATION</i>	380
<i>NET-03.4: BOUNDARY PROTECTION PERSONAL DATA (PD)</i>	380
<i>NET-03.5: BOUNDARY PROTECTION PREVENT UNAUTHORIZED EXFILTRATION</i>	380
<i>NET-03.6: BOUNDARY PROTECTION DYNAMIC ISOLATION & SEGREGATION (SANDBOXING)</i>	381
<i>NET-03.7: BOUNDARY PROTECTION ISOLATION OF INFORMATION SYSTEM COMPONENTS</i>	381
<i>NET-03.8: BOUNDARY PROTECTION SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS</i>	381
NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)	382
<i>NET-04.1: DATA FLOW ENFORCEMENT DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION</i>	382
<i>NET-04.2: DATA FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES</i>	383
<i>NET-04.3: DATA FLOW ENFORCEMENT CONTENT CHECK FOR ENCRYPTED DATA</i>	383
<i>NET-04.4: DATA FLOW ENFORCEMENT EMBEDDED DATA TYPES</i>	383
<i>NET-04.5: DATA FLOW ENFORCEMENT METADATA</i>	383
<i>NET-04.6: DATA FLOW ENFORCEMENT HUMAN REVIEWS</i>	384
<i>NET-04.7: DATA FLOW ENFORCEMENT POLICY DECISION POINT (PDP)</i>	384
<i>NET-04.8: DATA FLOW ENFORCEMENT DATA TYPE IDENTIFIERS</i>	385
<i>NET-04.9: DATA FLOW ENFORCEMENT DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS</i>	385
<i>NET-04.10: DATA FLOW ENFORCEMENT DETECTION OF UNSANCTIONED INFORMATION</i>	385
<i>NET-04.11: DATA FLOW ENFORCEMENT APPROVED SOLUTIONS</i>	386
<i>NET-04.12: DATA FLOW ENFORCEMENT CROSS DOMAIN AUTHENTICATION</i>	386
<i>NET-04.13: DATA FLOW ENFORCEMENT METADATA VALIDATION</i>	386
<i>NET-04.14: DATA FLOW ENFORCEMENT APPLICATION PROXY</i>	387
NET-05: INTERCONNECTION SECURITY AGREEMENTS (ISAs)	387
<i>NET-05.1: INTERCONNECTION SECURITY AGREEMENTS (ISAs) EXTERNAL SYSTEM CONNECTIONS</i>	388
<i>NET-05.2: INTERCONNECTION SECURITY AGREEMENTS (ISAs) INTERNAL SYSTEM CONNECTIONS</i>	388
NET-06: NETWORK SEGMENTATION (MACROSEGMENTATION)	389
<i>NET-06.1: NETWORK SEGMENTATION SECURITY MANAGEMENT SUBNETS</i>	389
<i>NET-06.2: NETWORK SEGMENTATION VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION</i>	390
<i>NET-06.3: NETWORK SEGMENTATION SENSITIVE / REGULATED DATA ENCLAVE (SECURE ZONE)</i>	390
<i>NET-06.4: NETWORK SEGMENTATION SEGREGATION FROM ENTERPRISE SERVICES</i>	390
<i>NET-06.5: NETWORK SEGMENTATION DIRECT INTERNET ACCESS RESTRICTIONS</i>	390
<i>NET-06.6: NETWORK SEGMENTATION MICROSEGMENTATION</i>	391
<i>NET-06.7: NETWORK SEGMENTATION SOFTWARE DEFINED NETWORKING (SDN)</i>	391
NET-07: NETWORK CONNECTION TERMINATION	391
NET-08: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)	391

NET-08.1: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS) DMZ NETWORKS	392
NET-08.2: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS) WIRELESS INTRUSION DETECTION/PREVENTION SYSTEMS (WIDS/WIPS)	392
NET-08.3: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS) HOST CONTAINMENT	392
NET-08.4: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS) RESOURCE CONTAINMENT	393
NET-09: SESSION INTEGRITY	393
NET-09.1: SESSION INTEGRITY INVALIDATE SESSION IDENTIFIERS AT LOGOUT	393
NET-09.2: SESSION INTEGRITY UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	393
NET-10 DOMAIN NAME SERVICE (DNS) RESOLUTION	393
NET-10.1: DOMAIN NAME SERVICE (DNS) RESOLUTION ARCHITECTURE & PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	394
NET-10.2: DOMAIN NAME SERVICE (DNS) RESOLUTION SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	394
NET-10.3: DOMAIN NAME SERVICE (DNS) RESOLUTION SENDER POLICY FRAMEWORK (SPF)	395
NET-10.4: DOMAIN NAME SERVICE (DNS) RESOLUTION DOMAIN REGISTRAR SECURITY	395
NET-11: OUT-OF-BAND CHANNELS	395
NET-12: SAFEGUARDING DATA OVER OPEN NETWORKS	395
NET-12.1: SAFEGUARDING DATA OVER OPEN NETWORKS WIRELESS LINK PROTECTION	396
NET-12.2: SAFEGUARDING DATA OVER OPEN NETWORKS END-USER MESSAGING TECHNOLOGIES	396
NET-13: ELECTRONIC MESSAGING	397
NET-14: REMOTE ACCESS	397
NET-14.1: REMOTE ACCESS AUTOMATED MONITORING & CONTROL	398
NET-14.2: REMOTE ACCESS PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION	398
NET-14.3: REMOTE ACCESS MANAGED ACCESS CONTROL POINTS	398
NET-14.4: REMOTE ACCESS PRIVILEGED COMMANDS & ACCESS	398
NET-14.5: REMOTE ACCESS WORK FROM ANYWHERE (WFA) – TELECOMMUTING SECURITY	399
NET-14.6: REMOTE ACCESS THIRD-PARTY REMOTE ACCESS GOVERNANCE	399
NET-14.7: REMOTE ACCESS ENDPOINT SECURITY VALIDATION	399
NET-14.8: REMOTE ACCESS EXPEDITIOUS DISCONNECT/DISABLE CAPABILITY	400
NET-15: WIRELESS NETWORKING	400
NET-15.1: WIRELESS ACCESS AUTHENTICATION & ENCRYPTION	401
NET-15.2: WIRELESS ACCESS DISABLE WIRELESS NETWORKING	401
NET-15.3: WIRELESS ACCESS RESTRICT CONFIGURATION BY USERS	401
NET-15.4: WIRELESS ACCESS WIRELESS BOUNDARIES	401
NET-15.5: WIRELESS ACCESS ROGUE WIRELESS DETECTION	402
NET-16: INTRANETS	402
NET-17: DATA LOSS PREVENTION (DLP)	402
NET-18: DNS & CONTENT FILTERING	403
NET-18.1: DNS & CONTENT FILTERING ROUTE INTERNAL TRAFFIC TO PROXY SERVERS	403
NET-18.2: DNS & CONTENT FILTERING VISIBILITY OF ENCRYPTED COMMUNICATIONS	403
NET-18.3: DNS & CONTENT FILTERING ROUTE PRIVILEGED NETWORK ACCESS	404
NET-18.4: DNS & CONTENT FILTERING PROTOCOL COMPLIANCE ENFORCEMENT	404
NET-18.5: DNS & CONTENT FILTERING DOMAIN NAME VERIFICATION	404
NET-18.6: DNS & CONTENT FILTERING INTERNET ADDRESS DENYLING	404
NET-18.7: DNS & CONTENT FILTERING BANDWIDTH CONTROL	405
NET-18.8: DNS & CONTENT FILTERING AUTHENTICATED PROXY	405
NET-18.9: DNS & CONTENT FILTERING CERTIFICATE DENYLING	405
NET-19: CONTENT DISARM AND RECONSTRUCTION (CDR)	405
NET-20: EMAIL CONTENT PROTECTIONS	405
NET-20.1: EMAIL CONTENT PROTECTIONS EMAIL DOMAIN REPUTATION PROTECTIONS	406
NET-20.2: EMAIL CONTENT PROTECTIONS SENDER DENYLING	406
NET-20.3: EMAIL CONTENT PROTECTIONS AUTHENTICATED RECEIVED CHAIN (ARC)	406
NET-20.4: EMAIL CONTENT PROTECTIONS DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)	406
NET-20.5: EMAIL CONTENT PROTECTIONS USER DIGITAL SIGNATURES FOR OUTGOING EMAIL	406
NET-20.6: EMAIL CONTENT PROTECTIONS ENCRYPTION FOR OUTGOING EMAIL	407
NET-20.7: EMAIL CONTENT PROTECTIONS ADAPTIVE EMAIL PROTECTIONS	407
NET-20.8: EMAIL CONTENT PROTECTIONS EMAIL LABELING	407

PHYSICAL & ENVIRONMENTAL SECURITY (PES) POLICY & STANDARDS**407****PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS****408***PES-01.1: PHYSICAL & ENVIRONMENTAL PROTECTIONS | PHYSICAL SECURITY PLAN (PSP)*

408

PES-01.2: PHYSICAL & ENVIRONMENTAL PROTECTIONS | ZONE-BASED PHYSICAL SECURITY

408

PES-02: PHYSICAL ACCESS AUTHORIZATIONS**409***PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS | ROLE-BASED PHYSICAL ACCESS*

410

PES-02.2: PHYSICAL ACCESS AUTHORIZATIONS | DUAL AUTHORIZATION FOR PHYSICAL ACCESS

410

PES-03: PHYSICAL ACCESS CONTROL**410***PES-03.1: PHYSICAL ACCESS CONTROL | CONTROLLED INGRESS & EGRESS POINTS*

411

PES-03.2: PHYSICAL ACCESS CONTROL | LOCKABLE PHYSICAL CASINGS

412

PES-03.3: PHYSICAL ACCESS CONTROL | PHYSICAL ACCESS LOGS

412

PES-03.4: PHYSICAL ACCESS CONTROL | ACCESS TO INFORMATION SYSTEMS

413

PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES**413***PES-04.1: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES | WORKING IN SECURE AREAS*

414

PES-04.2: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES | SEARCHES

414

PES-04.3: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES | TEMPORARY STORAGE

414

PES-05: MONITORING PHYSICAL ACCESS**415***PES-05.1: MONITORING PHYSICAL ACCESS | INTRUSION ALARMS/SURVEILLANCE EQUIPMENT*

415

PES-05.2: MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS

416

PES-06: VISITOR CONTROL**416***PES-06.1: VISITOR CONTROL | DISTINGUISH VISITORS FROM ON-SITE PERSONNEL*

416

PES-06.2: VISITOR CONTROL | IDENTIFICATION REQUIREMENT

417

PES-06.3: VISITOR CONTROL | RESTRICT UNESCORTED ACCESS

417

PES-06.4: VISITOR CONTROL | AUTOMATED RECORDS MANAGEMENT & REVIEW

417

PES-06.5: VISITOR CONTROL | MINIMIZE VISITOR PERSONAL DATA (PD)

417

PES-06.6: VISITOR CONTROL | VISITOR ACCESS REVOCATION

418

PES-07: SUPPORTING UTILITIES**418***PES-07.1: SUPPORTING UTILITIES | AUTOMATIC VOLTAGE CONTROLS*

418

PES-07.2: SUPPORTING UTILITIES | EMERGENCY SHUTOFF

418

PES-07.3: SUPPORTING UTILITIES | EMERGENCY POWER

419

PES-07.4: SUPPORTING UTILITIES | EMERGENCY LIGHTING

419

PES-07.5: SUPPORTING UTILITIES | WATER DAMAGE PROTECTION

419

PES-07.6: SUPPORTING UTILITIES | AUTOMATION SUPPORT FOR WATER DAMAGE PROTECTION

419

PES-07.7: SUPPORTING UTILITIES | REDUNDANT CABLING

420

PES-08: FIRE PROTECTION**420***PES-08.1: FIRE PROTECTION | FIRE DETECTION DEVICES*

420

PES-08.2: FIRE PROTECTION | FIRE SUPPRESSION DEVICES

420

PES-08.3: FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION

421

PES-09: TEMPERATURE & HUMIDITY CONTROLS**421***PES-09.1: TEMPERATURE & HUMIDITY CONTROLS | MONITORING WITH ALARMS/NOTIFICATIONS*

421

PES-10: DELIVERY & REMOVAL**421****PES-11: ALTERNATE WORK SITE****422****PES-12: EQUIPMENT SITING & PROTECTION****422***PES-12.1: EQUIPMENT SITING & PROTECTION | TRANSMISSION MEDIUM SECURITY*

423

PES-12.2: EQUIPMENT SITING & PROTECTION | ACCESS CONTROL FOR OUTPUT DEVICES

423

PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS**423****PES-14: ASSET MONITORING AND TRACKING****424****PES-15: ELECTROMAGNETIC PULSE (EMP) PROTECTION****424****PES-16: COMPONENT MARKING****424****PES-17: PROXIMITY SENSOR****425****PES-18: ON-SITE CLIENT SEGREGATION****425****PES-19: PHYSICAL ACCESS DEVICE INVENTORIES****425****DATA PRIVACY (PRI) POLICY & STANDARDS****426****PRI-01: DATA PRIVACY PROGRAM****426***PRI-01.1: DATA PRIVACY PROGRAM | CHIEF PRIVACY OFFICER (CPO)*

426

PRI-01.2: DATA PRIVACY PROGRAM | PRIVACY ACT STATEMENTS

426

<i>PRI-01.3: DATA PRIVACY PROGRAM DISSEMINATION OF PRIVACY PROGRAM INFORMATION</i>	427
<i>PRI-01.4: DATA PRIVACY PROGRAM DATA PROTECTION OFFICER (DPO)</i>	427
<i>PRI-01.5: DATA PRIVACY PROGRAM BINDING CORPORATE RULES (BCR)</i>	427
<i>PRI-01.6: DATA PRIVACY PROGRAM SECURITY OF PERSONAL DATA</i>	428
<i>PRI-01.7: DATA PRIVACY PROGRAM LIMITING PERSONAL DATA (PD) DISCLOSURES</i>	428
<i>PRI-01.8: DATA PRIVACY PROGRAM DATA FIDUCIARY</i>	428
<i>PRI-01.9: DATA PRIVACY PROGRAM PERSONAL DATA (PD) PROCESS MANAGER</i>	428
<i>PRI-01.10: DATA PRIVACY PROGRAM FINANCIAL INCENTIVES FOR PERSONAL DATA (PD)</i>	428
<i>PRI-01.11: DATA PRIVACY PROGRAM REASONABLE DATA PRIVACY PRACTICES</i>	429
PRI-02: DATA PRIVACY NOTICE	429
<i>PRI-02.1: DATA PRIVACY NOTICE PURPOSE SPECIFICATION</i>	430
<i>PRI-02.2: DATA PRIVACY NOTICE AUTOMATED DATA MANAGEMENT PROCESSES</i>	430
<i>PRI-02.3: DATA PRIVACY NOTICE COMPUTER MATCHING AGREEMENTS (CMA)</i>	430
<i>PRI-02.4: DATA PRIVACY NOTICE SYSTEM OF RECORDS NOTICE (SORN)</i>	430
<i>PRI-02.5: DATA PRIVACY NOTICE SYSTEM OF RECORDS NOTICE (SORN) REVIEW PROCESS</i>	431
<i>PRI-02.6: DATA PRIVACY NOTICE PRIVACY ACT EXEMPTIONS</i>	431
<i>PRI-02.7: DATA PRIVACY NOTICE REAL-TIME OR LAYERED NOTICE</i>	432
<i>PRI-02.8: DATA PRIVACY NOTICE PURPOSE COMPATIBILITY</i>	432
<i>PRI-02.9: DATA PRIVACY NOTICE PRIVACY NOTICE FORMATTING</i>	432
<i>PRI-02.10: DATA PRIVACY NOTICE SYMMETRY IN CHOICE</i>	432
<i>PRI-02.11: DATA PRIVACY NOTICE CHOICE ARCHITECTURE</i>	433
<i>PRI-02.12: DATA PRIVACY NOTICE CHOICE ARCHITECTURE TESTING</i>	433
<i>PRI-02.13: DATA PRIVACY NOTICE NOTICE OF RIGHT TO LIMIT</i>	433
<i>PRI-02.14: DATA PRIVACY NOTICE ALTERNATIVE MEANS TO DELIVER PRIVACY NOTICE</i>	433
PRI-03: CHOICE & CONSENT	433
<i>PRI-03.1: CHOICE & CONSENT TAILORED CONSENT</i>	434
<i>PRI-03.2: CHOICE & CONSENT JUST-IN-TIME NOTICE & UPDATED CONSENT</i>	434
<i>PRI-03.3: CHOICE & CONSENT PROHIBITION OF SELLING, PROCESSING AND/OR SHARING PERSONAL DATA (PD)</i>	434
<i>PRI-03.4: CHOICE & CONSENT REVOKE CONSENT</i>	435
<i>PRI-03.5: CHOICE & CONSENT PRODUCT OR SERVICE DELIVERY RESTRICTIONS</i>	435
<i>PRI-03.6: CHOICE & CONSENT AUTHORIZED AGENT</i>	435
<i>PRI-03.7: CHOICE & CONSENT ACTIVE PARTICIPATION BY DATA SUBJECTS</i>	435
<i>PRI-03.8: CHOICE & CONSENT GLOBAL PRIVACY CONTROL (GPC)</i>	435
<i>PRI-03.9: CHOICE & CONSENT CONTINUED USE OF PERSONAL DATA (PD)</i>	436
<i>PRI-03.10: CHOICE & CONSENT CEASE PROCESSING, STORING AND/OR SHARING PERSONAL DATA (PD)</i>	436
<i>PRI-03.11: CHOICE & CONSENT COMMUNICATING PROCESSING CHANGES</i>	436
<i>PRI-03.12: CHOICE & CONSENT DATA SUBJECT OPT-IN CONSENT</i>	436
<i>PRI-03.13: CHOICE & CONSENT PARENT OR GUARDIAN OPT-IN CONSENT FOR MINORS</i>	437
PRI-04: RESTRICT COLLECTION TO IDENTIFIED PURPOSE	437
<i>PRI-04.1: RESTRICT COLLECTION TO IDENTIFIED PURPOSE AUTHORITY TO COLLECT, USE, MAINTAIN & SHARE PERSONAL DATA (PD)</i>	437
<i>PRI-04.2: RESTRICT COLLECTION TO IDENTIFIED PURPOSE PRIMARY SOURCES</i>	437
<i>PRI-04.3: RESTRICT COLLECTION TO IDENTIFIED PURPOSE IDENTIFIABLE IMAGE COLLECTION</i>	438
<i>PRI-04.4: RESTRICT COLLECTION TO IDENTIFIED PURPOSE ACQUIRED PERSONAL DATA (PD)</i>	438
<i>PRI-04.5: RESTRICT COLLECTION TO IDENTIFIED PURPOSE VALIDATE COLLECTED PERSONAL DATA (PD)</i>	438
<i>PRI-04.6: RESTRICT COLLECTION TO IDENTIFIED PURPOSE RE-VALIDATE COLLECTED PERSONAL DATA (PD)</i>	438
<i>PRI-04.7: RESTRICT COLLECTION TO IDENTIFIED PURPOSE PERSONAL DATA (PD) COLLECTION METHODS</i>	438
PRI-05: PERSONAL DATA (PD) RETENTION & DISPOSAL	439
<i>PRI-05.1: PERSONAL DATA (PD) RETENTION & DISPOSAL INTERNAL USE OF PERSONAL DATA (PD) FOR TESTING, TRAINING AND RESEARCH</i>	439
<i>PRI-05.2: PERSONAL DATA (PD) RETENTION & DISPOSAL PERSONAL DATA ACCURACY & INTEGRITY</i>	439
<i>PRI-05.3: PERSONAL DATA (PD) RETENTION & DISPOSAL DATA MASKING</i>	439
<i>PRI-05.4: PERSONAL DATA (PD) RETENTION & DISPOSAL USAGE RESTRICTIONS OF PERSONAL DATA (PD)</i>	440
<i>PRI-05.5: PERSONAL DATA (PD) RETENTION & DISPOSAL INVENTORY OF PERSONAL DATA (PD)</i>	440
<i>PRI-05.6: PERSONAL DATA (PD) RETENTION & DISPOSAL PERSONAL DATA (PD) INVENTORY AUTOMATION SUPPORT</i>	440
<i>PRI-05.7: PERSONAL DATA (PD) RETENTION & DISPOSAL PERSONAL DATA (PD) CATEGORIES</i>	441
<i>PRI-05.8: PERSONAL DATA RETENTION & DISPOSAL PERSONAL DATA (PD) FORMATS</i>	441
PRI-06: DATA SUBJECT EMPOWERMENT	441

<i>PRI-06.1: DATA SUBJECT ACCESS CORRECTING INACCURATE PERSONAL DATA</i>	442
<i>PRI-06.2: DATA SUBJECT ACCESS NOTICE OF CORRECTION OR PROCESSING CHANGE</i>	442
<i>PRI-06.3: DATA SUBJECT ACCESS APPEAL ADVERSE DECISION</i>	442
<i>PRI-06.4: DATA SUBJECT ACCESS USER FEEDBACK MANAGEMENT</i>	442
<i>PRI-06.5: DATA SUBJECT ACCESS RIGHT TO ERASURE</i>	443
<i>PRI-06.6: DATA SUBJECT ACCESS DATA PORTABILITY</i>	443
<i>PRI-06.7: DATA SUBJECT ACCESS PERSONAL DATA (PD) EXPORTS</i>	443
<i>PRI-06.8: DATA SUBJECT ACCESS DATA SUBJECT AUTHENTICATION</i>	443
PRI-07: INFORMATION SHARING WITH THIRD PARTIES	444
<i>PRI-07.1: INFORMATION SHARING WITH THIRD PARTIES PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS</i>	444
<i>PRI-07.2: INFORMATION SHARING WITH THIRD PARTIES JOINT PROCESSING OF PERSONAL DATA (PD)</i>	444
<i>PRI-07.3: INFORMATION SHARING WITH THIRD PARTIES OBLIGATION TO INFORM THIRD PARTIES</i>	444
<i>PRI-07.4: INFORMATION SHARING WITH THIRD PARTIES REJECT UNAUTHENTICATED OR UNTRUSTWORTHY DISCLOSURE REQUESTS</i>	445
<i>PRI-07.5: INFORMATION SHARING WITH THIRD PARTIES JUSTIFICATION TO REJECT DISCLOSURE REQUESTS</i>	445
PRI-08: TESTING, TRAINING & MONITORING	445
PRI-09: PERSONAL DATA LINEAGE	445
PRI-10: DATA QUALITY MANAGEMENT	446
<i>PRI-10.1: DATA QUALITY MANAGEMENT DATA QUALITY AUTOMATION</i>	446
<i>PRI-10.2: DATA QUALITY MANAGEMENT DATA ANALYTICS BIAS</i>	447
PRI-11: DATA TAGGING	447
PRI-12: UPDATING PERSONAL DATA (PD) PROCESS	447
<i>PRI-12.1: UPDATING PERSONAL DATA (PD) PROCESS ENABLING DATA SUBJECTS TO UPDATE PERSONAL DATA (PD)</i>	447
PRI-13: DATA MANAGEMENT BOARD	447
PRI-14: DOCUMENTING DATA PROCESSING ACTIVITIES	448
<i>PRI-14.1: DOCUMENTING DATA PROCESSING ACTIVITIES ACCOUNTING OF DISCLOSURES</i>	448
<i>PRI-14.2: DOCUMENTING DATA PROCESSING ACTIVITIES NOTIFICATION OF DISCLOSURE REQUEST TO DATA SUBJECT</i>	449
PRI-15: REGISTER AS A DATA CONTROLLER AND/OR DATA PROCESSOR	449
PRI-16: POTENTIAL HUMAN RIGHTS ABUSES	449
PRI-17: DATA SUBJECT COMMUNICATIONS	450
<i>PRI-17.1: DATA SUBJECT COMMUNICATIONS CONSPICUOUS LINK TO PRIVACY NOTICE</i>	450
<i>PRI-17.2: DATA SUBJECT COMMUNICATIONS NOTICE OF FINANCIAL INCENTIVE</i>	450
<i>PRI-17.3: DATA SUBJECT COMMUNICATIONS DATA SUBJECT COMMUNICATIONS DOCUMENTATION</i>	450
<i>PRI-17.4: DATA SUBJECT COMMUNICATIONS DATA SUBJECT COMMUNICATIONS METRICS</i>	450
<i>PRI-17.5: DATA SUBJECT COMMUNICATIONS DATA SUBJECT COMMUNICATIONS DISCLOSURE</i>	451
PRI-18: DATA CONTROLLER COMMUNICATIONS	451
PRI-19: AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) FOR DATA SUBJECT ACTIONS	451
<i>PRI-19.1: AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) FOR DATA SUBJECT ACTIONS AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) USE NOTIFICATION</i>	451
<i>PRI-19.2: AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) FOR DATA SUBJECT ACTIONS AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) OPT-OUT CONSENT</i>	452
<i>PRI-19.3: AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) FOR DATA SUBJECT ACTIONS AUTOMATED DECISION-MAKING TECHNOLOGY (ADMT) TRANSPARENCY</i>	452
PRI-20: DATA BROKERS	452
PRI-21: NOTICE OF RIGHT TO OPT-OUT	452
<i>PRI-21.1: NOTICE OF RIGHT TO OPT-OUT OPT-OUT LINKS</i>	452
<i>PRI-21.2: NOTICE OF RIGHT TO OPT-OUT ALTERNATIVE OUT-OUT LINK</i>	453
PROJECT & RESOURCE MANAGEMENT (PRM) POLICY & STANDARDS	454
PRM-01: CYBERSECURITY & DATA PROTECTION PORTFOLIO MANAGEMENT	454
<i>PRM-01.1: CYBERSECURITY & DATA PROTECTION PORTFOLIO MANAGEMENT STRATEGIC PLAN & OBJECTIVES</i>	454
<i>PRM-01.2: CYBERSECURITY & DATA PROTECTION PORTFOLIO MANAGEMENT TARGETED CAPABILITY MATURITY LEVELS</i>	454
PRM-02: CYBERSECURITY & DATA PROTECTION RESOURCE MANAGEMENT	455
<i>PRM-02.1: CYBERSECURITY & DATA PROTECTION RESOURCE MANAGEMENT PRIORITIZATION TO ADDRESS EVOLVING RISKS & THREATS</i>	455
PRM-03: ALLOCATION OF RESOURCES	455
PRM-04: CYBERSECURITY & DATA PROTECTION IN PROJECT MANAGEMENT	455
PRM-05 CYBERSECURITY & DATA PROTECTION REQUIREMENTS DEFINITION	456

PRM-06: BUSINESS PROCESS DEFINITION	456
PRM-07: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT	456
PRM-08: MANAGE ORGANIZATIONAL KNOWLEDGE	457
RISK MANAGEMENT (RSK) POLICY & STANDARDS	458
RSK-01: RISK MANAGEMENT PROGRAM (RMP)	458
<i>RSK-01.1: RISK MANAGEMENT PROGRAM (RMP) RISK FRAMING</i>	458
<i>RSK-01.2: RISK MANAGEMENT PROGRAM (RMP) RISK MANAGEMENT RESOURCING</i>	459
<i>RSK-01.3: RISK MANAGEMENT PROGRAM (RMP) RISK TOLERANCE</i>	459
<i>RSK-01.4: RISK MANAGEMENT PROGRAM (RMP) RISK THRESHOLD</i>	460
<i>RSK-01.5: RISK MANAGEMENT PROGRAM (RMP) RISK APPETITE</i>	461
RSK-02: RISK-BASED SECURITY CATEGORIZATION	461
<i>RSK-02.1: RISK-BASED SECURITY CATEGORIZATION IMPACT-LEVEL PRIORITIZATION</i>	462
RSK-03: RISK IDENTIFICATION	462
<i>RSK-03.1: RISK IDENTIFICATION RISK CATALOG</i>	462
RSK-04: RISK ASSESSMENT	463
<i>RSK-04.1: RISK ASSESSMENT RISK REGISTER</i>	464
<i>RSK-04.2: RISK ASSESSMENT RISK ASSESSMENT METHODOLOGY</i>	464
<i>RSK-04.3: RISK ASSESSMENT INSTANCES REQUIRING A RISK ASSESSMENT</i>	464
<i>RSK-04.4: RISK ASSESSMENT RISK ASSESSMENT STAKEHOLDER INVOLVEMENT</i>	464
RSK-05: RISK RANKING	465
RSK-06: RISK REMEDIATION	465
<i>RSK-06.1: RISK REMEDIATION RISK RESPONSE</i>	465
<i>RSK-06.2: RISK REMEDIATION COMPENSATING COUNTERMEASURES</i>	466
<i>RSK-06.3: RISK REMEDIATION RISK TREATMENT OPTIONS</i>	466
<i>RSK-06.4: RISK REMEDIATION RISK TREATMENT PLAN</i>	467
RSK-07: RISK ASSESSMENT UPDATE	467
RSK-08: BUSINESS IMPACT ANALYSIS (BIA)	467
RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM	468
<i>RSK-09.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM SUPPLY CHAIN RISK ASSESSMENT</i>	469
<i>RSK-09.2: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM AI & AUTONOMOUS TECHNOLOGIES SUPPLY CHAIN IMPACTS</i>	469
RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)	470
RSK-11: RISK MONITORING	471
RSK-12: RISK CULTURE	471
RSK-13: EXECUTIVE LEADERSHIP APPROVAL FOR MANAGING MATERIAL RISK	471
<i>RSK-13.1: EXECUTIVE LEADERSHIP APPROVAL FOR MANAGING MATERIAL RISK DOCUMENTED ALTERNATIVES</i>	471
<i>RSK-13.2: EXECUTIVE LEADERSHIP APPROVAL FOR MANAGING MATERIAL RISK DOCUMENTED JUSTIFICATION FOR MATERIAL RISK MANAGEMENT DECISIONS</i>	472
SECURE ENGINEERING & ARCHITECTURE (SEA) POLICY & STANDARDS	473
SEA-01: SECURE ENGINEERING PRINCIPLES	473
<i>SEA-01.1: SECURE ENGINEERING PRINCIPLES CENTRALIZED MANAGEMENT OF CYBERSECURITY & DATA PROTECTION CONTROLS</i>	474
<i>SEA-01.2: SECURE ENGINEERING PRINCIPLES ACHIEVING RESILIENCE REQUIREMENTS</i>	474
<i>SEA-01.3: SECURE ENGINEERING PRINCIPLES RESILIENCE CAPABILITIES</i>	475
SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE	475
<i>SEA-02.1: ALIGNMENT WITH ENTERPRISE ARCHITECTURE STANDARDIZED TERMINOLOGY</i>	476
<i>SEA-02.2: ALIGNMENT WITH ENTERPRISE ARCHITECTURE OUTSOURCING NON-ESSENTIAL FUNCTIONS OR SERVICES</i>	477
<i>SEA-02.3: ALIGNMENT WITH ENTERPRISE ARCHITECTURE TECHNICAL DEBT REVIEWS</i>	477
SEA-03: DEFENSE-IN-DEPTH (DID) ARCHITECTURE	477
<i>SEA-03.1: DEFENSE-IN-DEPTH (DID) ARCHITECTURE SYSTEM PARTITIONING</i>	478
<i>SEA-03.2: DEFENSE-IN-DEPTH (DID) ARCHITECTURE APPLICATION PARTITIONING</i>	478
SEA-04: PROCESS ISOLATION	478
<i>SEA-04.1: PROCESS ISOLATION SECURITY FUNCTION ISOLATION</i>	479
<i>SEA-04.2: PROCESS ISOLATION HARDWARE SEPARATION</i>	480
<i>SEA-04.3: PROCESS ISOLATION THREAD SEPARATION</i>	480
<i>SEA-04.4: PROCESS ISOLATION SYSTEM PRIVILEGES ISOLATION</i>	480
SEA-05: INFORMATION IN SHARED RESOURCES	480
SEA-06: PREVENT PROGRAM EXECUTION	480

SEA-07: PREDICTABLE FAILURE ANALYSIS	481
SEA-07.1: PREDICTABLE FAILURE ANALYSIS TECHNOLOGY LIFECYCLE MANAGEMENT	481
SEA-07.2: PREDICTABLE FAILURE ANALYSIS FAIL SECURE	482
SEA-07.3: PREDICTABLE FAILURE ANALYSIS FAIL SAFE	482
SEA-08: NON-PERSISTENCE	482
SEA-08.1: NON-PERSISTENCE REFRESH FROM TRUSTED SOURCES	483
SEA-09: INFORMATION OUTPUT FILTERING	483
SEA-09.1: INFORMATION OUTPUT FILTERING LIMIT PERSONAL DATA (PD) DISSEMINATION	483
SEA-10: MEMORY PROTECTION	483
SEA-11: HONEYPOTS	484
SEA-12: HONEYCLIENTS	484
SEA-13: HETEROGENEITY	484
SEA-13.1: HETEROGENEITY VIRTUALIZATION TECHNIQUES	485
SEA-14: CONCEALMENT & MISDIRECTION	485
SEA-14.1: CONCEALMENT & MISDIRECTION RANDOMNESS	485
SEA-14.2: CONCEALMENT & MISDIRECTION CHANGE PROCESSING & STORAGE LOCATIONS	486
SEA-15: DISTRIBUTED PROCESSING & STORAGE	486
SEA-16: NON-MODIFIABLE EXECUTABLE PROGRAMS	486
SEA-17: SECURE LOG-ON PROCEDURES	486
SEA-18: SYSTEM USE NOTIFICATION (LOGON BANNER)	487
SEA-18.1: SYSTEM USE NOTIFICATION STANDARDIZED MICROSOFT WINDOWS BANNER	487
SEA-18.2: SYSTEM USE NOTIFICATION TRUNCATED BANNER	487
SEA-19: PREVIOUS LOGON NOTIFICATION	488
SEA-20: CLOCK SYNCHRONIZATION	488
SEA-21: APPLICATION CONTAINER	488
SEA-22: PRIVILEGED ENVIRONMENTS	489
SECURITY OPERATIONS (OPS) POLICY & STANDARDS	490
OPS-01: OPERATIONS SECURITY	490
OPS-01.1: OPERATIONS SECURITY STANDARDIZED OPERATING PROCEDURES (SOP)	490
OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)	491
OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)	491
OPS-04: SECURITY OPERATIONS CENTER (SOC)	491
OPS-05: SECURE PRACTICES GUIDELINES	492
OPS-06: SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)	492
OPS-07: SHADOW INFORMATION TECHNOLOGY DETECTION	492
SECURITY AWARENESS & TRAINING (SAT) POLICY & STANDARDS	493
SAT-01: CYBERSECURITY & DATA PROTECTION-MINDED WORKFORCE	493
SAT-01.1: CYBERSECURITY & DATA PROTECTION-MINDED WORKFORCE MAINTAINING WORKFORCE DEVELOPMENT RELEVANCY	494
SAT-02: CYBERSECURITY & DATA PROTECTION AWARENESS TRAINING	494
SAT-02.1: CYBERSECURITY & DATA PROTECTION AWARENESS TRAINING SIMULATED CYBER ATTACK SCENARIO TRAINING	495
SAT-02.2: CYBERSECURITY & DATA PROTECTION AWARENESS TRAINING SOCIAL ENGINEERING & MINING	495
SAT-03: CYBERSECURITY & DATA PROTECTION ROLE-BASED TRAINING	496
SAT-03.1: CYBERSECURITY & DATA PROTECTION TRAINING PRACTICAL EXERCISES	497
SAT-03.2: CYBERSECURITY & DATA PROTECTION TRAINING SUSPICIOUS COMMUNICATIONS & ANOMALOUS SYSTEM BEHAVIOR	497
SAT-03.3: CYBERSECURITY & DATA PROTECTION TRAINING SENSITIVE / REGULATED DATA STORAGE, HANDLING & PROCESSING	498
SAT-03.4: CYBERSECURITY & DATA PROTECTION TRAINING VENDOR SECURITY TRAINING	498
SAT-03.5: CYBERSECURITY & DATA PROTECTION TRAINING PRIVILEGED USERS	498
SAT-03.6: CYBERSECURITY & DATA PROTECTION TRAINING CYBER THREAT ENVIRONMENT	498
SAT-03.7: CYBERSECURITY & DATA PROTECTION TRAINING CONTINUING PROFESSIONAL EDUCATION (CPE) - CYBERSECURITY & DATA PRIVACY PERSONNEL	499
SAT-03.8: CYBERSECURITY & DATA PROTECTION TRAINING CONTINUING PROFESSIONAL EDUCATION (CPE) - DEVOPS PERSONNEL	499
SAT-03.9: CYBERSECURITY & DATA PROTECTION TRAINING COUNTERINTELLIGENCE TRAINING	499
SAT-04: CYBERSECURITY & DATA PROTECTION TRAINING RECORDS	499
SAT-05: CYBERSECURITY KNOWLEDGE SHARING	500
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) POLICY & STANDARDS	501
TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION	501

TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION PRODUCT MANAGEMENT	501
TDA-01.2: TECHNOLOGY DEVELOPMENT & ACQUISITION INTEGRITY MECHANISMS FOR SOFTWARE/FIRMWARE UPDATES	502
TDA-01.3: TECHNOLOGY DEVELOPMENT & ACQUISITION MALWARE TESTING PRIOR TO RELEASE	502
TDA-01.4: TECHNOLOGY DEVELOPMENT & ACQUISITION DEVSECOPS	503
TDA-02: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS	503
TDA-02.1: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS PORTS, PROTOCOLS & SERVICES IN USE	503
TDA-02.2: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS INFORMATION ASSURANCE ENABLED PRODUCTS	504
TDA-02.3: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS DEVELOPMENT METHODS, TECHNIQUES & PROCESSES	504
TDA-02.4: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS PRE-ESTABLISHED SECURITY CONFIGURATIONS	504
TDA-02.5: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS IDENTIFICATION & JUSTIFICATION OF PORTS, PROTOCOLS & SERVICES	505
TDA-02.6: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS USE OF INSECURE PORTS, PROTOCOLS & SERVICES	505
TDA-02.7: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS CYBERSECURITY & DATA PRIVACY REPRESENTATIVES FOR PRODUCT CHANGES	506
TDA-02.8: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS MINIMIZING ATTACK SURFACES	506
TDA-02.9: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS ONGOING PRODUCT SECURITY SUPPORT	506
TDA-02.10: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS PRODUCT TESTING & REVIEWS	506
TDA-02.11: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS DISCLOSURE OF VULNERABILITIES	507
TDA-02.12: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS PRODUCTS WITH DIGITAL ELEMENTS	507
TDA-02.13: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS REPORTING EXPLOITABLE VULNERABILITIES	507
TDA-02.14: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS LOGGING SYNTAX	507
TDA-03: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS	508
TDA-03.1: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS SUPPLIER DIVERSITY	508
TDA-04: DOCUMENTATION REQUIREMENTS	508
TDA-04.1: DOCUMENTATION REQUIREMENTS FUNCTIONAL PROPERTIES	509
TDA-04.2: DOCUMENTATION REQUIREMENTS SOFTWARE BILL OF MATERIALS (SBOM)	509
TDA-05: DEVELOPER ARCHITECTURE & DESIGN	510
TDA-05.1: DEVELOPER ARCHITECTURE & DESIGN PHYSICAL DIAGNOSTIC & TEST INTERFACES	510
TDA-05.2: DEVELOPER ARCHITECTURE & DESIGN DIAGNOSTIC & TEST INTERFACE MONITORING	511
TDA-06: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP)	511
TDA-06.1: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) CRITICALITY ANALYSIS	512
TDA-06.2: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) THREAT MODELING	513
TDA-06.3: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) SOFTWARE ASSURANCE MATURITY MODEL (SAMM)	513
TDA-06.4: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) SUPPORTING TOOLCHAIN	513
TDA-06.5: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) SOFTWARE DESIGN REVIEW	513
TDA-06.6: SECURE SOFTWARE DEVELOPMENT PRACTICES (SSDP) SOFTWARE DEVELOPMENT ROOT CAUSE ANALYSIS	513
TDA-07: SECURE DEVELOPMENT ENVIRONMENTS	514
TDA-08: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS	514
TDA-08.1: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS SECURE MIGRATION PRACTICES	514
TDA-09: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT	515
TDA-09.1: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT CONTINUOUS MONITORING PLAN	515
TDA-09.2: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT STATIC CODE ANALYSIS	516
TDA-09.3: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT DYNAMIC CODE ANALYSIS	516
TDA-09.4: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT MALFORMED INPUT TESTING	516
TDA-09.5: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT APPLICATION PENETRATION TESTING	517
TDA-09.6: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT SECURE SETTINGS BY DEFAULT	517
TDA-09.7: CYBERSECURITY & DATA PROTECTION TESTING THROUGHOUT DEVELOPMENT MANUAL CODE REVIEW	517
TDA-10: USE OF LIVE DATA	517
TDA-10.1: USE OF LIVE DATA TEST DATA INTEGRITY	518
TDA-11: PRODUCT TAMPERING AND COUNTERFEITING (PTC)	518
TDA-11.1: PRODUCT TAMPERING AND COUNTERFEITING (PTC) ANTI-COUNTERFEIT TRAINING	518
TDA-11.2: PRODUCT TAMPERING AND COUNTERFEITING (PTC) COMPONENT DISPOSAL	518
TDA-12: CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	519
TDA-13: DEVELOPER SCREENING	519
TDA-14: DEVELOPER CONFIGURATION MANAGEMENT	519
TDA-14.1: DEVELOPER CONFIGURATION MANAGEMENT SOFTWARE/FIRMWARE INTEGRITY VERIFICATION	520
TDA-14.2: DEVELOPER CONFIGURATION MANAGEMENT HARDWARE INTEGRITY VERIFICATION	520
TDA-15: DEVELOPER THREAT ANALYSIS & FLAW REMEDIATION	520

TDA-16: DEVELOPER-PROVIDED TRAINING	521
TDA-17: UNSUPPORTED TECHNOLOGY ASSETS, APPLICATIONS AND/OR SERVICES (TAAS)	521
<i>TDA-17.1: UNSUPPORTED SYSTEMS ALTERNATE SOURCES FOR CONTINUED SUPPORT</i>	521
TDA-18: INPUT DATA VALIDATION	521
TDA-19: ERROR HANDLING	522
TDA-20: ACCESS TO PROGRAM SOURCE CODE	522
<i>TDA-20.1: ACCESS TO PROGRAM SOURCE CODE SOFTWARE RELEASE INTEGRITY VERIFICATION</i>	522
<i>TDA-20.2: ACCESS TO PROGRAM SOURCE CODE ARCHIVING SOFTWARE RELEASES</i>	523
<i>TDA-20.3: ACCESS TO PROGRAM SOURCE CODE SOFTWARE ESCROW</i>	523
<i>TDA-20.4: ACCESS TO PROGRAM SOURCE CODE APPROVED CODE</i>	523
TDA-21: PRODUCT CONFORMITY GOVERNANCE	523
TDA-22: TECHNICAL DOCUMENTATION ARTIFACTS	523
<i>TDA-22.1: TECHNICAL DOCUMENTATION ARTIFACTS PRODUCT-SPECIFIC RISK ASSESSMENT ARTIFACTS</i>	524
THIRD-PARTY MANAGEMENT (TPM) POLICY & STANDARDS	525
TPM-01: THIRD-PARTY MANAGEMENT	525
<i>TPM-01.1: THIRD-PARTY MANAGEMENT THIRD-PARTY INVENTORIES</i>	526
TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS	526
TPM-03: SUPPLY CHAIN RISK MANAGEMENT (SCRM)	526
<i>TPM-03.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) ACQUISITION STRATEGIES, TOOLS & METHODS</i>	527
<i>TPM-03.2: SUPPLY CHAIN RISK MANAGEMENT (SCRM) LIMIT POTENTIAL HARM</i>	527
<i>TPM-03.3: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES</i>	527
<i>TPM-03.4: SUPPLY CHAIN RISK MANAGEMENT (SCRM) ADEQUATE SUPPLY</i>	527
TPM-04: THIRD-PARTY SERVICES	528
<i>TPM-04.1: THIRD-PARTY SERVICES THIRD-PARTY RISK ASSESSMENTS & APPROVALS</i>	528
<i>TPM-04.2: THIRD-PARTY SERVICES EXTERNAL CONNECTIVITY REQUIREMENTS - IDENTIFICATION OF PORTS, PROTOCOLS & SERVICES</i>	529
<i>TPM-04.3: THIRD-PARTY SERVICES CONFLICT OF INTERESTS</i>	529
<i>TPM-04.4: THIRD-PARTY SERVICES THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS</i>	530
TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	530
<i>TPM-05.1: THIRD-PARTY CONTRACT REQUIREMENTS SECURITY COMPROMISE NOTIFICATION AGREEMENTS</i>	531
<i>TPM-05.2: THIRD-PARTY CONTRACT REQUIREMENTS CONTRACT FLOW-DOWN REQUIREMENTS</i>	531
<i>TPM-05.3: THIRD-PARTY CONTRACT REQUIREMENTS THIRD-PARTY AUTHENTICATION PRACTICES</i>	532
<i>TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX</i>	532
<i>TPM-05.5: THIRD-PARTY CONTRACT REQUIREMENTS THIRD-PARTY SCOPE REVIEW</i>	533
<i>TPM-05.6: THIRD-PARTY CONTRACT REQUIREMENTS FIRST-PARTY DECLARATION (1PD)</i>	533
<i>TPM-05.7: THIRD-PARTY CONTRACT REQUIREMENTS BREAK CLAUSES</i>	534
<i>TPM-05.8: THIRD-PARTY CONTRACT REQUIREMENTS THIRD-PARTY ATTESTATION (3PA)</i>	534
TPM-06: THIRD-PARTY PERSONNEL SECURITY	534
TPM-07: MONITORING FOR THIRD-PARTY INFORMATION DISCLOSURE	535
TPM-08: REVIEW OF THIRD-PARTY SERVICES	535
TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION	535
TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES	536
TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	536
THREAT MANAGEMENT (THR) POLICY & STANDARDS	537
THR-01: THREAT AWARENESS PROGRAM	537
THR-02: INDICATORS OF EXPOSURE (IOE)	537
THR-03: THREAT INTELLIGENCE FEEDS	538
<i>THR-03.1: THREAT INTELLIGENCE FEEDS THREAT INTELLIGENCE REPORTING</i>	538
THR-04: INSIDER THREAT PROGRAM	539
THR-05: INSIDER THREAT AWARENESS	539
THR-06: VULNERABILITY DISCLOSURE PROGRAM (VDP)	539
<i>THR-06.1: VULNERABILITY DISCLOSURE PROGRAM (VDP) SECURITY DISCLOSURE CONTACT INFORMATION</i>	539
THR-07: THREAT HUNTING	540
THR-08: TAINTING	540
THR-09: THREAT CATALOG	541
THR-10: THREAT ANALYSIS	541

THR-11: BEHAVIORAL BASELINING	542
VULNERABILITY & PATCH MANAGEMENT (VPM) POLICY & STANDARDS	543
VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	543
<i>VPM-01.1: VULNERABILITY & PATCH MANAGEMENT PROGRAM ATTACK SURFACE SCOPE</i>	543
VPM-02: VULNERABILITY REMEDIATION PROCESS	544
VPM-03: VULNERABILITY RANKING	544
<i>VPM-03.1: VULNERABILITY RANKING VULNERABILITY EXPLOITATION ANALYSIS</i>	544
VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES	545
<i>VPM-04.1: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES STABLE VERSIONS</i>	545
<i>VPM-04.2: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES FLAW REMEDIATION WITH PERSONAL DATA (PD)</i>	546
<i>VPM-04.3: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES DEFERRED PATCHING DECISIONS</i>	546
VPM-05: SOFTWARE & FIRMWARE PATCHING	546
<i>VPM-05.1: SOFTWARE & FIRMWARE PATCHING CENTRALIZED MANAGEMENT OF FLAW REMEDIATION PROCESSES</i>	549
<i>VPM-05.2: SOFTWARE & FIRMWARE PATCHING AUTOMATED REMEDIATION STATUS</i>	549
<i>VPM-05.3: SOFTWARE & FIRMWARE PATCHING TIME TO REMEDIATE/BENCHMARKS FOR CORRECTIVE ACTION</i>	550
<i>VPM-05.4: SOFTWARE & FIRMWARE PATCHING AUTOMATED SOFTWARE & FIRMWARE UPDATES</i>	550
<i>VPM-05.5: SOFTWARE & FIRMWARE PATCHING REMOVAL OF PREVIOUS VERSIONS</i>	550
<i>VPM-05.6: SOFTWARE & FIRMWARE PATCHING PRE-DEPLOYMENT PATCH TESTING</i>	550
<i>VPM-05.7: SOFTWARE & FIRMWARE PATCHING OUT-OF-CYCLE PATCHING</i>	551
<i>VPM-05.8: SOFTWARE & FIRMWARE PATCHING SOFTWARE PATCH INTEGRITY</i>	551
VPM-06: VULNERABILITY SCANNING	551
<i>VPM-06.1: VULNERABILITY SCANNING UPDATE TOOL CAPABILITY</i>	552
<i>VPM-06.2: VULNERABILITY SCANNING BREADTH/DEPTH OF COVERAGE</i>	552
<i>VPM-06.3: VULNERABILITY SCANNING PRIVILEGED ACCESS</i>	553
<i>VPM-06.4: VULNERABILITY SCANNING TREND ANALYSIS</i>	553
<i>VPM-06.5: VULNERABILITY SCANNING REVIEW HISTORICAL EVENT LOGS</i>	553
<i>VPM-06.6: VULNERABILITY SCANNING EXTERNAL VULNERABILITY ASSESSMENT SCANS</i>	553
<i>VPM-06.7: VULNERABILITY SCANNING INTERNAL VULNERABILITY ASSESSMENT SCANS</i>	554
<i>VPM-06.8: VULNERABILITY SCANNING ACCEPTABLE DISCOVERABLE INFORMATION</i>	554
<i>VPM-06.9: VULNERABILITY SCANNING CORRELATE SCANNING INFORMATION</i>	554
VPM-07: PENETRATION TESTING	555
<i>VPM-07.1: PENETRATION TESTING INDEPENDENT PENETRATION AGENT OR TEAM</i>	555
VPM-08: TECHNICAL SURVEILLANCE COUNTERMEASURES SECURITY	556
VPM-09: REVIEWING VULNERABILITY SCANNER USAGE	556
VPM-10: RED TEAM EXERCISES	556
WEB SECURITY (WEB) POLICY & STANDARDS	557
WEB-01: WEB SECURITY	557
<i>WEB-01.1: WEB SECURITY UNAUTHORIZED CODE</i>	557
WEB-02: USE OF DEMILITARIZED ZONES (DMZs)	558
WEB-03: WEB APPLICATION FIREWALL (WAF)	558
WEB-04: CLIENT-FACING WEB SERVICES	559
WEB-05: COOKIE MANAGEMENT	559
WEB-06: STRONG CUSTOMER AUTHENTICATION (SCA)	559
WEB-07: WEB SECURITY STANDARD	560
WEB-08: WEB APPLICATION FRAMEWORK	560
WEB-09: VALIDATION & SANITIZATION	560
WEB-10: SECURE WEB TRAFFIC	560
WEB-11: OUTPUT ENCODING	561
WEB-12: WEB BROWSER SECURITY	561
WEB-13: WEBSITE CHANGE DETECTION	561
WEB-14: PUBLICLY ACCESSIBLE CONTENT REVIEWS	562
GLOSSARY: ACRONYMS & DEFINITIONS	563
ACRONYMS	563
DEFINITIONS	564
RECORD OF CHANGES	565

SECURITY, COMPLIANCE & RESILIENCE PROGRAM (SCRP) OVERVIEW

MANAGEMENT COMMITMENT

The **Security, Compliance & Resilience Program (SCRP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Business Consulting, Inc. (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with ACME's Technology Assets, Applications, Services and/or Data (TAASD). Therefore, it is the responsibility of both ACME personnel and third-parties to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, cybersecurity and data protection measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of TAASD. This also includes protection against accidental loss or destruction. The protection of TAASD must include safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **CONFIDENTIALITY** – This addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- **INTEGRITY** – This addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **AVAILABILITY** – This addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **SAFETY** – This addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

PURPOSE

The purpose of the Security, Compliance & Resilience Program (SCRP) is to:

- Create a leading practice-based Security, Compliance & Resilience Management System (SCRMS);
- Protect the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME data and systems;
- Protect ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensure the effectiveness of cybersecurity and data protection controls over data and systems that support ACME's operations; and
- Provide for the development, review and maintenance of the cybersecurity and data protection controls required to protect ACME's data and systems.

The formation of these cybersecurity policies is driven by many factors, with the key factor being a risk. These policies set the ground rules under which ACME operates and safeguards its data and systems to both reduce risk and minimize the effect of potential incidents.

These policies, including their related control objectives, standards, procedures and guidelines, are necessary to support the management of information risks in daily operations. The development of policies provides due care to ensure ACME personnel understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help ACME comply with current and future legal obligations to ensure long-term due diligence in protecting the confidentiality, integrity and availability of ACME data.

SCOPE & APPLICABILITY

These policies, standards and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards and guidelines apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME data.

PEOPLE, PROCESSES, TECHNOLOGY, DATA & FACILITIES (PPTDF) CONTROL APPLICABILITY

Control scoping does not mean all controls apply uniformly to every asset, individual or facility. This misunderstanding of applicability vs scoping is one of the biggest hurdles that organizations face, since there is a common misconception that if something is “in scope” then every control will be applicable across the entire boundary of the assessment. This is an incorrect assumption. When looking at the breath of controls that an organization is obligated to comply with, the controls are often administrative, technical or physical in nature. This means that there may be controls that are not applicable to certain systems, applications and/or processes.

Example 1: Network firewall

- A network firewall is a technology asset where specific other controls would be applicable, such as Multi-Factor Authentication (MFA), access control, secure baseline configurations and patch management.
- A network firewall is a device. Therefore, a network firewall is **not** capable of undergoing end user training, completing a Non-Disclosure Agreement (NDA) or conducting incident response exercises.

Example 2: User awareness training

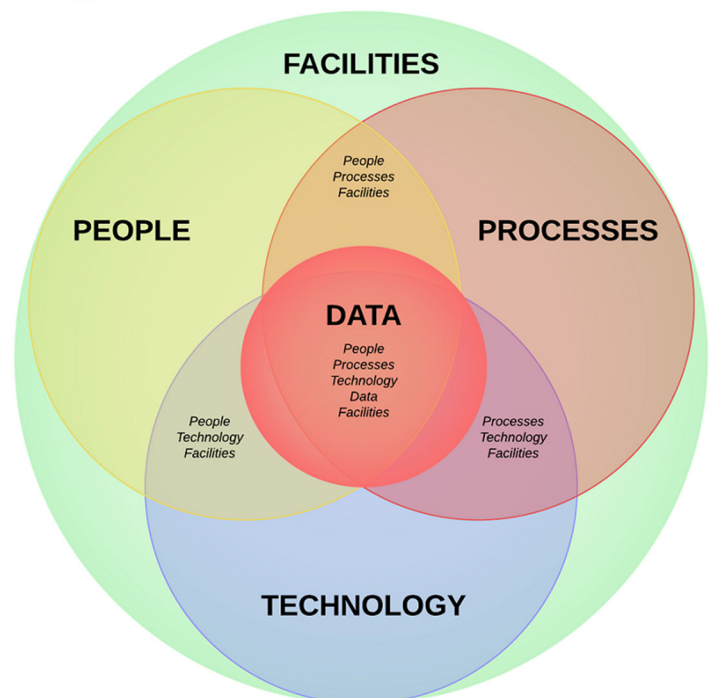
- User awareness training focuses on personnel, such as employees and applicable third parties, who will interact with the organization's systems and data. NDAs, threat intelligence awareness and acceptable use notifications apply to individuals.
- An individual is not a device. Therefore, an individual is **not** capable of having a secure baseline configuration applied, be scanned by a vulnerability assessment tool, or have missing patches installed.

Example 3: Incident Response Plan (IRP)

- An IRP is a documented process that guides incident response operations.
- An IRP is not an individual or technology. Therefore, an IRP cannot sign an NDA, have MFA or be patched.

The People, Processes, Technology, Data and Facilities (PPTDF) model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls.

- **People.** Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
- **Processes.** Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
- **Technology.** Control directly applies to Technology Assets, Applications and/or Services (TAAS) (e.g., secure baseline configurations, patching, etc.).
- **Data.** Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
- **Facilities.** Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions must comply with the standards. ACME departments must use these standards or may create a more restrictive standard, but none that are less restrictive, less comprehensive or less compliant than these standards.

These policies do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

ACME's documented roles and responsibilities provides a detailed description of ACME user roles and responsibilities, in regard to cybersecurity-related use obligations.

ACME reserves the right to revoke, change or supplement these policies, standards and guidelines at any time without prior notice. Such changes must be effective immediately upon approval by management unless otherwise stated.

ROLES

As part of ACME's Human Resources (HR) department's function to facilitate the implementation of personnel security controls, HR is required to assign all employees and contractors with one, or more, defined roles. Those roles are designed to manage personnel security risk by:

- Assigning a risk designation to all position; and
- Establishing screening criteria for individuals filling those positions

RESPONSIBILITIES

To ensure an acceptable level of cybersecurity risk, ACME must design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems. The SCRP addresses the policies, standards and guidelines.

Data/process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with the SCRP's policies, standards and guidelines.

ACME personnel must protect and ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of data and systems, regardless of how its data is created, distributed or stored.

- Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system; and
- Security controls must be designed and maintained to ensure compliance with all legal requirements.

VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES

Any ACME user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

EXCEPTION TO STANDARDS

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception, users must submit a business justification for deviation from the standard in question.

UPDATES TO POLICIES & STANDARDS

Updates to the Security, Compliance & Resilience Program (SCRP) will be announced to employees via management updates or email announcements. Changes will be noted in the [Record of Changes](#) to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

CYBERSECURITY & DATA PROTECTION (GOV) POLICY & STANDARDS

Management Intent: The purpose of the Cybersecurity & Data Protection (GOV) policy is to govern a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity and data protection principles that addresses all applicable statutory, regulatory and contractual obligations.

Policy: ACME shall tailor cybersecurity and data protection controls accordingly so that cost-effective controls can be applied commensurately with the risk and sensitivity of the data and technologies in use, ensuring applicable security, compliance and resilience requirements are sufficiently addressed.

ACME shall implement and maintain a maturity-based capability to strengthen the security and resilience of its technology infrastructure and data protection mechanisms against both physical and cyber threats. Security control decisions shall take applicable statutory, regulatory and contractual obligations into account, but ACME acknowledges that being compliant does not equate to being secure, so all stakeholders shall protect the confidentiality, integrity, availability and safety of ACME's technology resources and data, regardless of the geographic location of the data or technology in use.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

Control Objective: The organization facilitates the implementation of cybersecurity and data protection governance controls.²²

Standard: ACME's cybersecurity and data protection policies and standards must be represented in a single document, the Security, Compliance & Resilience Program (SCRP) that:

- (a) Must be reviewed and updated at least annually; and
- (b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

Guidelines: The security plans for individual systems and the organization-wide SCRPs together provide complete coverage for all cybersecurity and data protection-related controls employed within the organization.

GOV-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STEERING COMMITTEE & PROGRAM OVERSIGHT

Control Objective: The organization coordinates cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.²³

Standard: ACME must establish a cybersecurity and data protection steering committee, or advisory board, comprised of key stakeholders from ACME Lines of Business (LOB) and technology-related executives that:

- (a) Meets formally and on a regular basis; and
- (b) Receives briefings from the following:
 1. Chief Information Security Officer (CISO) on matters of cybersecurity;
 2. Chief Privacy Officer (CPO) on matters of data privacy; and
 3. Chief Risk Officer (CRO) on matters of enterprise risk.

Guidelines: To achieve proper situational awareness across the organization, key cybersecurity and data protection leaders must facilitate communication with business stakeholders. This includes translating cybersecurity, data privacy and risk concepts and language into business concepts and language as well as ensuring that business teams consult with cybersecurity and data protection teams to determine appropriate controls measures when planning new business projects.

²² ISO 27001-2013: 4.3, 4.4, 5.1, 6.1.1 | ISO 27002-2022: 5.1, 5.4, 5.37 | NIST SP 800-53 R5: PM-1 | NIST SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV, GV.RM-01, GV.RM-03, GV.RR-01, GV.SC, GV.SC-01, GV.SC-03, GV.SC-09, ID.RA, PR, PR.IR

²³ ISO 27001-2013: 4.3, 6.2, 7.4, 9.3, 10.2 | NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.OV, GV.OV-01, GV.OV-02, GV.OV-03, GV.RM-01, GV.RM-03, GV.RR-01, GV.SC, GV.SC-01, GV.SC-03, GV.SC-09, ID, ID.RA, PR, PR.IR

The steering committee, or advisory board, can best advise the CISO, CPO and CRO on important matters pertaining to the organization to ensure technology, cybersecurity and data protection practices support the overall strategy and mission of the organization.

GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | STATUS REPORTING TO GOVERNING BODY

Control Objective: The organization provides governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to its cybersecurity and data protection program.²⁴

Standard: ACME's Chief Information Security Officer (CISO) must:

- (a) Operate a repeatable process for reporting to ACME's board of directors, or similar oversight function; and
- (b) Provide detailed reporting, along with recommendations, to the oversight body; and
- (c) Document feedback received.

Guidelines: None

GOV-01.3: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM | COMMITMENT TO CONTINUAL IMPROVEMENTS

Control Objective: The organization commits appropriate resources needed for continual improvement of the organization's cybersecurity and data protection program, including:

- (1) Staffing;
- (2) Budget;
- (3) Processes; and
- (4) Technologies.

Standard: ACME must:

- (a) Appropriate necessary resources needed for continual improvement of the organization's cybersecurity and data protection program, including:
 1. Staffing;
 2. Budget;
 3. Processes; and
 4. Technologies.
- (b) Operate a repeatable process for reporting to ACME's board of directors, or similar oversight function, that:
 1. Provides detailed reporting, along with recommendations, to the oversight body; and
 2. Documents feedback received.

Guidelines: None

GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

Control Objective: The organization establishes, maintains and disseminates cybersecurity and data protection policies, standards and procedures.²⁵

Standard: The Security, Compliance & Resilience Program (SCRP) document represents the consolidation of ACME's cybersecurity and data protection policies and standards. The SCRPs are endorsed by ACME's executive management and shall be:

- (a) Disseminated to the appropriate parties to ensure all affected personnel are made aware of and understand their applicable requirements to protect cardholder data;
- (b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the SCRPs, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;
- (c) Enforced by ACME personnel through "business as usual" secure practices in the form of Standardized Operating Procedures (SOP) that shall be developed, enforced and maintained at the control operator level; and

²⁴ NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.OV, GV.OV-01, GV.OV-03, GV.SC, GV.SC-09, ID

²⁵ ISO 27001-2013: 4.3, 5.2, 7.5.1, 7.5.2, 7.5.3 | ISO 27002-2022: 5.1, 5.37 | NIST SP 800-53 R5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1 | NIST SP 800-171 R3: 03.15.01.a | NIST CSF 2.0: GV.PO, GV.PO-01, GV.SC-01, GV.SC-03, ID.RA

CHANGE MANAGEMENT (CHG) POLICY & STANDARDS

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change in a unified effort to prevent business disruptions and unintended outcomes. Without properly documented and implemented change controls, cybersecurity and data protection features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise that affect Technology Assets, Applications, Services and/or Data (TAASD).

Policy: ACME shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change affecting production Technology Assets, Applications, Services and/or Data (TAASD).

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of change management controls. ¹⁴⁰

Standard: ACME's Change Management Program requires data/process owners and asset custodians to test, validate and document changes to systems before implementing the changes on the production network. Changes for any production Technology Assets, Applications and/or Services (TAAS) must:

- (a) Be:
 - 1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;
 - 2. Approved by a ACME employee with the appropriate authority and knowledge to understand the impact of the change; and
 - 3. Approved by ACME's Change Control Board (CCB);
- (b) Sufficiently document the following criteria to enable independent review:
 - 1. Reason for, and description of, the change;
 - 2. Security impact;
 - 3. Change approval by authorized parties;
 - 4. Functionality testing to verify the change:
 - i. Did not adversely impact the security of the network; and
 - ii. Performs as expected;
 - 5. For bespoke and custom software changes, all updates are tested for compliance with applicable statutory, regulatory and contractual obligations; and
 - 6. Procedures to address failures and return to a secure state;
- (c) Ensure all applicable statutory, regulatory and contractual requirements are confirmed to be in place on all new or changed systems and networks; and
- (d) As applicable, update affected documentation to include the changes to prevent inconsistencies between network documentation and the actual configuration.

Guidelines: Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security, availability, processing integrity, confidentiality or data privacy or any combination thereof.

Due to the constantly changing state of pre- production environments, they are often less secure than the production environment. Organizations must clearly understand which environments are test environments or development environments and how these environments interact on the level of networks and applications.

¹⁴⁰ ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a | CSF 2.0: ID.RA-07

Pre-production environments include development, testing, User Acceptance Testing (UAT), etc. Even where production infrastructure is used to facilitate testing or development, production environments still need to be separated (logically or physically) from pre-production functionality such that vulnerabilities introduced as a result of pre-production activities do not adversely affect production systems.

CHG-02: CONFIGURATION CHANGE CONTROL

Control Objective: The organization governs the technical configuration change control processes.¹⁴¹

Standard: Data/process owners and asset custodians must follow ACME's change control processes and procedures for all changes to system components:

- (a) Utilize separate environments for development/testing/staging and production;
- (b) Utilize a separation of duties between development/testing/staging and production environments;
- (c) Prohibit the use of production data (e.g., live data) for testing or development;
- (d) Remove test data and accounts before production systems become active/goes into production; and
- (e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following:
 1. Documentation of impact;
 2. Documented change approval by authorized parties; and
 3. Functionality testing to verify that the change does not adversely impact the security of the system;
- (f) Back-out procedures; and
- (g) Upon completion of significant change, all relevant compliance requirements must be implemented on all new or changed systems and networks and documentation updated as applicable.

Guidelines: Configuration change controls for organizational systems involve the systematic proposal, justification, implementation, testing, review and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers and mobile devices), unscheduled/unauthorized changes and changes to remediate vulnerabilities.

CHG-02.1: CONFIGURATION CHANGE CONTROL | PROHIBITION OF CHANGES

Control Objective: The organization prohibits unauthorized changes, unless organization-approved change requests are received.¹⁴²

Standard: To prohibit unauthorized changes, ACME requires:

- (a) Data/process owners and asset custodians to:
 1. Prohibit implementing a change without first obtaining pre-approval from ACME's Change Control Board (CCB); and
 2. Notify all affected parties prior to the implementation of the change; and
- (b) Where technically feasible, ACME must utilize automated mechanisms to:
 1. Document proposed change(s);
 2. Notify affected stakeholders of proposed change(s);
 3. Request change approval;
 4. Highlight proposed changes that have not been approved or disapproved within an organization-defined time period;
 5. Prohibit change(s) until designated approval(s) is/are received;
 6. Document all changes; and
 7. Notify affected stakeholders when approved change(s) are completed.

Guidelines: The scope of affected parties must include any clients, partners or vendors that would be affected by the change.

¹⁴¹ ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a, 03.04.03.b, 03.04.03.c | NIST CSF 2.0: ID.RA-07

¹⁴² NIST SP 800-53 R5: CM-3(1) | NIST SP 800-171 R3: 03.04.02.b, 03.04.03.a | NIST CSF 2.0: ID.RA-07

DATA CLASSIFICATION & HANDLING (DCH) POLICY & STANDARDS

Management Intent: The purpose of the Data Classification & Handling (DCH) policy is to ensure that Technology Assets, Applications, Services and/or Data (TAASD) are properly classified and measures are implemented to protect ACME's data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity and availability of sensitive/regulated data.

Policy: In accordance with all applicable statutory, regulatory and contractual obligations for cybersecurity and data protection, ACME shall implement and maintain appropriate administrative, technical and physical security measures for its Technology Assets, Applications and/or Services (TAAS) to protect the confidentiality, integrity and availability of its data, regardless if the data is in hardcopy or digital form. ACME shall utilize methods of sanitizing or destroying digital and physical media so that data recovery is technically infeasible.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

DCH-01: DATA PROTECTION

Control Objective: The organization facilitates the implementation of data protection controls.²⁸⁸

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement:

- (a) Controls to protect ACME data wherever it is stored, transmitted and processed, in accordance with all applicable statutory, regulatory and contractual compliance obligations;
- (b) Retention periods for both sensitive and non-sensitive/regulated data; and
- (c) Processes to:
 - 1. Dispose of, destroy, erase and/or anonymizes data once it is no longer necessary for business purposes;
 - 2. Maintain strict control over the storage and accessibility of media; and
 - 3. Maintain inventories of sensitive/regulated data under ACME's control.

Guidelines: The objective is to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.

DCH-01.1: DATA PROTECTION | DATA STEWARDSHIP

Control Objective: The organization ensures data stewardship is assigned, documented and communicated.²⁸⁹

Standard: ACME's Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Data Protection Officer (DPO), or their designated representative(s), must:

- (a) Develop and implement data stewardship practices that educate and train stakeholders how to:
 - 1. Physically secure all media with sensitive/regulated data;
 - 2. Maintain strict control over the storage and accessibility of media with sensitive/regulated data; and
 - 3. Maintain strict control over the internal or external distribution of any kind of media with sensitive/regulated data, including the following:
 - i. Classify media so the sensitivity of the data can be determined; and
 - ii. Send the media by secured courier or another delivery method that can be accurately tracked; and
- (b) Require data/process owners and asset custodians to re-assess the following criteria, as it pertains to data stewardship on the Technology Assets, Applications and/or Services (TAAS) under their control:
 - 1. Data classification requirements;
 - 2. System criticality;
 - 3. Geographical storage and/or processing of the data; and

²⁸⁸ ISO 27002-2022: 5.9, 5.10, 5.12, 5.33, 7.1, 8.12 | NIST SP 800-53 R5: MP-1 | NIST SP 800-171 R2: 3.8.1, 3.8.3, NFO - MP-1 | NIST SP 800-171 R3: 03.01.01.d.01, 03.01.01.d.02, 03.08.01 | NIST CSF 2.0: ID.AM-08, PR.DS, PR.DS-01, PR.DS-02, PR.DS-10 | FAR 52.204-21(b)(1)(vii)

²⁸⁹ NIST SP 800-53 R5: SA-4(12) | NIST SP 800-171 R3: 03.08.01, 03.08.05.a | NIST CSF 2.0: ID.AM-08, PR.DS

4. Applicable statutory, regulatory and contractual requirements.

Guidelines: See *Annex 4: Baseline Security Categorization Guidelines* for Safety & Criticality (SC) categorization. A complete inventory of mission-critical (SC1) and business-critical (SC2) assets located at all sites and/or geographical locations and their usage over time should be maintained and updated regularly and assigned ownership by defined roles and responsibilities.

DCH-01.2: DATA PROTECTION | SENSITIVE/REGULATED DATA PROTECTION

Control Objective: The organization protects sensitive/regulated data wherever it is processed and/or stored.²⁹⁰

Standard: Data/process owners and asset custodians must protect sensitive/regulated data from being stored in cleartext, where it is human-readable in storage media by:

- (a) Configuring Technology Assets, Applications and/or Services (TAAS) to render sensitive/regulated data unreadable anywhere it is processed and/or stored by using any of the following approaches:
 1. One-way hashes based on strong cryptography of the sensitive/regulated data;
 2. Truncation;
 3. Index tokens; and
 4. Strong cryptography;
- (b) Reviewing the following data sources to ensure that sensitive/regulated data is not retained in a human-readable format:
 1. Incoming transaction data;
 2. All logs (e.g., transaction, history, debugging, error);
 3. History files;
 4. Trace files;
 5. Database schemas;
 6. Contents of databases, and on-premises and cloud data stores; and
 7. Any existing memory/crash dump files;
- (c) Rendering sensitive/regulated data unreadable anywhere it is stored; and
- (d) Not tying user accounts to decryption keys.

Guidelines: The removal of cleartext sensitive/regulated data is a defense in depth control designed to protect the data if an unauthorized individual gains access to stored data by taking advantage of a vulnerability or misconfiguration of an entity's primary access control.

Sources for information about index tokens include:

- PCI SSC's Tokenization Product Security Guidelines
- ANSI X9.119-2-2017: Retail Financial Services
- Requirements For Protection Of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems

DCH-01.3: DATA PROTECTION | SENSITIVE / REGULATED MEDIA RECORDS

Control Objective: The organization ensures media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.²⁹¹

Standard: Where technically feasible, ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement a metadata tracking and reporting capability for sensitive/regulated data that:

- (a) Categorizes media records according to defined data classification categories;
- (b) Identifies assets that contain sensitive/regulated data;
- (c) Configures system event logging to provide appropriate situational awareness on activities associated with logical access to assets that contain sensitive/regulated data; and
- (d) Provides the ability to determine the potential impact in the event of a data loss incident for identified sensitive/regulated data.

²⁹⁰ NIST SP 800-171 R2: 3.10.6 | NIST SP 800-171 R3: 03.01.01.d.01, 03.01.01.d.02, 03.01.02, 03.01.20.a, 03.01.20.b, 03.01.20.c.01, 03.01.20.d, 03.06.05.d, 03.08.01, 03.08.02, 03.08.05.a, 03.17.01.c | NIST CSF 2.0: PR.DS | FAR 52.204-21(b)(1)

²⁹¹ NIST SP 800-171 R3: 03.08.05.c | NIST CSF 2.0: PR.DS

TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) POLICY & STANDARDS

Management Intent: The purpose of the Technology Development & Acquisition (TDA) policy is to ensure technologies are developed and/or acquired according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws that could affect ACME's Technology Assets, Applications, Services and/or Data (TAASD).

Policy: ACME shall implement and maintain secure development practices to strengthen the security and resilience of its developed technologies, regardless if the Technology Asset, Application and/or Service (TAAS) is internally-developed or acquired from a third-party provider. To reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses, TAAS shall be developed according to a Secure Software Development Framework (SSDF) and tested throughout development to ensure secure development practices are implemented.

Supporting Documentation: This policy is supported by the following control objectives, standards and guidelines.

TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION

Control Objective: The organization facilitates the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.⁸⁷³

Standard: ACME's Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement processes to govern a formal Technical Development & Acquisition (TDA) program that:

- (a) Ensures acquisition strategies, contract tools and procurement methods:
 - 1. Identify supply chain risks;
 - 2. Protect against supply chain risks; and
 - 3. Mitigate supply chain risks;
- (b) Incorporates cybersecurity and data protection principles into the asset's lifecycle; and
- (c) Tailors acquisitions, contract tools and procurement methods to ensure compliance with applicable statutory, regulatory and contractual obligations.

Guidelines: The acquisition process provides an important vehicle for protecting the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, the insertion of counterfeits, the insertion of malicious software or backdoors, and poor development practices throughout the system life cycle.

Organizations also consider providing incentives for suppliers to implement controls, promote transparency in their processes and security practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security requirements of the organization. Contracts may specify documentation protection requirements.

TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION | PRODUCT MANAGEMENT

Control Objective: The organization designs and implements product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:⁸⁷⁴

- (1) Improve functionality;
- (2) Enhance security and resiliency capabilities;
- (3) Correct security deficiencies; and

⁸⁷³ ISO 27002-2022: 8.25, 8.30 | NIST SP 800-53 R5: PL-1, SA-1, SA-4, SA-23 | NIST SP 800-171 R2: NFO - SA-4 | NIST SP 800-171 R3: 03.12.01, 03.12.03, 03.14.01.a, 03.16.01, 03.17.02 | NIST CSF 2.0: ID.RA-09, PR.PS-06

⁸⁷⁴ NIST SP 800-53 R5: SA-23 | NIST SP 800-171 R3: 03.12.03 | NIST CSF 2.0: GV.SC-09, PR.PS-06

- (4) Conform with applicable statutory, regulatory and/or contractual obligations.

Standard: ACME's Technology Assets, Applications and/or Services (TAAS) must be proactively managed to:

- (a) Govern the design, development and production of TAAS across the System Development Life Cycle (SDLC) to:
 - 1. Improve functionality;
 - 2. Enhance security and resiliency capabilities;
 - 3. Correct security deficiencies; and
 - 4. Conform with applicable statutory, regulatory and/or contractual obligations; and
- (b) Maintain appropriate documentation on how ACME provides validated software updates/patches throughout the product life cycle to assure its continued security;
- (c) Allow for the application of security updates to the product's software and firmware:
 - 1. Processes must support reverting to a previously-installed version if the update fails; and
 - 2. The roll-back would revert to the most recent installed version.
- (d) Verify the authenticity and integrity of any software update through cryptographic means, prior to the installation of the update:
 - 1. Product updates must be possible in an offline environment; and
 - 2. Offline updates must also support the same authenticity and integrity validation process.
- (e) Build security features into TAAS, including:
 - 1. Maintaining situational awareness through an event log that, at a minimum, contains the following events:
 - i. Successful and unsuccessful login attempts;
 - ii. Change of user authentication credentials;
 - iii. Changes in the list of valid user accounts (e.g., addition, modification or deletion of accounts); and
 - iv. Successful and unsuccessful software updates; and
 - 2. Prevent tampering of security-related event logs through transmitting logs to an external data storage location or security store the logs in non-volatile memory that prevents non-privileged users from deleting, moving or altering log file contents; and
- (f) Enable secure decommissioning of the product by allowing users to securely purge or erase (e.g., zeroization) all user-defined data that includes:
 - 1. Configuration data; and
 - 2. Sensitive data.

Guidelines: It is often necessary for a system or system component that supports mission-essential services or functions to be enhanced to maximize the trustworthiness of the resource. Sometimes this enhancement is done at the design level. In other instances, it is done post-design, either through modifications of the system in question or by augmenting the system with additional components. For example, supplemental authentication or non-repudiation functions may be added to the system to enhance the identity of critical resources to other resources that depend on the organization-defined resources.

TDA-01.2: TECHNOLOGY DEVELOPMENT & ACQUISITION | INTEGRITY MECHANISMS FOR SOFTWARE/FIRMWARE UPDATES

Control Objective: The organization utilizes integrity validation mechanisms for security updates.⁸⁷⁵

Standard: ACME requires that products incorporate integrity mechanisms for software/firmware updates that include:

- (a) Using a ACME code signing digital certificate to sign the software/firmware components; and
- (b) Generating and publishing a Keyed-Hash Message Authentication Code (HMAC) value to provide assurance of the integrity of the following components:
 - 1. Binaries;
 - 2. Executables; and
 - 3. Libraries.

Guidelines: None

TDA-01.3: TECHNOLOGY DEVELOPMENT & ACQUISITION | MALWARE TESTING PRIOR TO RELEASE

Control Objective: The organization utilizes at least one (1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update.

⁸⁷⁵ NIST CSF 2.0: ID.RA-09

- SUPPLEMENTAL DOCUMENTATION -

**SECURITY, COMPLIANCE & RESILIENCE PROGRAM
ANNEXES, TEMPLATES & REFERENCES**

INTERNAL USE

Access Limited to Internal Use Only

TABLE OF CONTENTS

ANNEXES	4
ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES	4
<i>DATA CLASSIFICATION</i>	4
<i>LABELING</i>	6
<i>GENERAL ASSUMPTIONS</i>	6
<i>PERSONAL DATA (PD)</i>	6
<i>SENSITIVE PERSONAL DATA (SPD)</i>	7
<i>DATA HANDLING GUIDELINES</i>	8
ANNEX 2: DATA CLASSIFICATION EXAMPLES	11
ANNEX 3: DATA RETENTION SCHEDULE	13
ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES	15
<i>SAFETY & CRITICALITY</i>	15
<i>BASIC ASSURANCE REQUIREMENTS</i>	16
<i>ENHANCED ASSURANCE REQUIREMENTS</i>	16
ANNEX 5: RULES OF BEHAVIOR (ACCEPTABLE & UNACCEPTABLE USE)	17
<i>ACCEPTABLE USE</i>	17
<i>PROHIBITED USE</i>	17
<i>ADDITIONAL RULES FOR SECURITY & PRIVILEGED USERS</i>	18
ANNEX 6: GUIDELINES FOR PERSONAL USE OF ORGANIZATIONAL IT RESOURCES	19
ANNEX 7: RISK MANAGEMENT FRAMEWORK (RMF)	20
<i>RISK MANAGEMENT OVERVIEW</i>	20
<i>RISK MANAGEMENT FRAMEWORK (RMF)</i>	20
<i>ASSESSING RISK</i>	22
ANNEX 8: SYSTEM HARDENING	23
<i>SERVER-CLASS SYSTEMS</i>	23
<i>WORKSTATION-CLASS SYSTEMS</i>	23
<i>NETWORK DEVICES</i>	23
<i>MOBILE DEVICES</i>	23
<i>DATABASES</i>	24
ANNEX 9: SAFETY CONSIDERATIONS WITH EMBEDDED TECHNOLOGY	25
<i>MISSION CRITICAL (SC-1)</i>	25
<i>BUSINESS CRITICAL (SC-2)</i>	25
<i>NON-CRITICAL (SC-3) & BUSINESS SUPPORTING (SC-4)</i>	25
ANNEX 10: INDICATORS OF COMPROMISE (IOC)	26
TEMPLATES	29
TEMPLATE 1: MANAGEMENT DIRECTIVE (POLICY AUTHORIZATION)	29
TEMPLATE 2: USER ACKNOWLEDGEMENT FORM	30
TEMPLATE 3: USER EQUIPMENT RECEIPT OF ISSUE	31
TEMPLATE 4: SERVICE PROVIDER NON-DISCLOSURE AGREEMENT (NDA)	32
TEMPLATE 5: INCIDENT RESPONSE PLAN (IRP)	33
<i>PLAN OBJECTIVES</i>	33
<i>INCIDENT DISCOVERY</i>	33
<i>COMMON EFFECTS OF ATTACKS</i>	36
<i>INCIDENT RESPONSE STAGES</i>	37
<i>INCIDENT CATEGORIES</i>	38
<i>ESCALATION LEVEL CONSIDERATIONS</i>	40
<i>INCIDENT RESPONSE PROCESS</i>	41
<i>INCIDENT RESPONSE TEAM (24X7)</i>	43
<i>INCIDENT RESPONSE TEAM CAPABILITIES</i>	43
<i>INCIDENT NOTIFICATION REQUIREMENTS</i>	43
<i>POST INCIDENT REQUIREMENTS</i>	44
TEMPLATE 6: INCIDENT RESPONSE FORM	45
TEMPLATE 7: APPOINTMENT ORDERS (INFORMATION SECURITY OFFICER)	45
TEMPLATE 8: PRIVILEGED USER ACCOUNT REQUEST FORM	47
TEMPLATE 9: CHANGE MANAGEMENT REQUEST FORM	48
TEMPLATE 10: CHANGE CONTROL BOARD (CCB) MEETING MINUTES	50

TEMPLATE 11: PLAN OF ACTION & MILESTONES (POA&M) / RISK REGISTER	51
TEMPLATE 12: PORTS, PROTOCOLS & SERVICES (PPS)	52
TEMPLATE 13: BUSINESS IMPACT ANALYSIS (BIA)	53
TEMPLATE 14: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (BCP)	55
<i>DISASTER RECOVERY PLAN (DRP)</i>	55
<i>BUSINESS CONTINUITY PLAN (BCP)</i>	56
<i>CRITICAL EQUIPMENT</i>	58
<i>ALTERNATE WORK SITE</i>	58
<i>ASSUMED RISK & MAXIMUM DOWNTIME REQUIREMENTS</i>	58
TEMPLATE 15: DATA PROTECTION IMPACT ASSESSMENT (DPIA)	59

REFERENCES

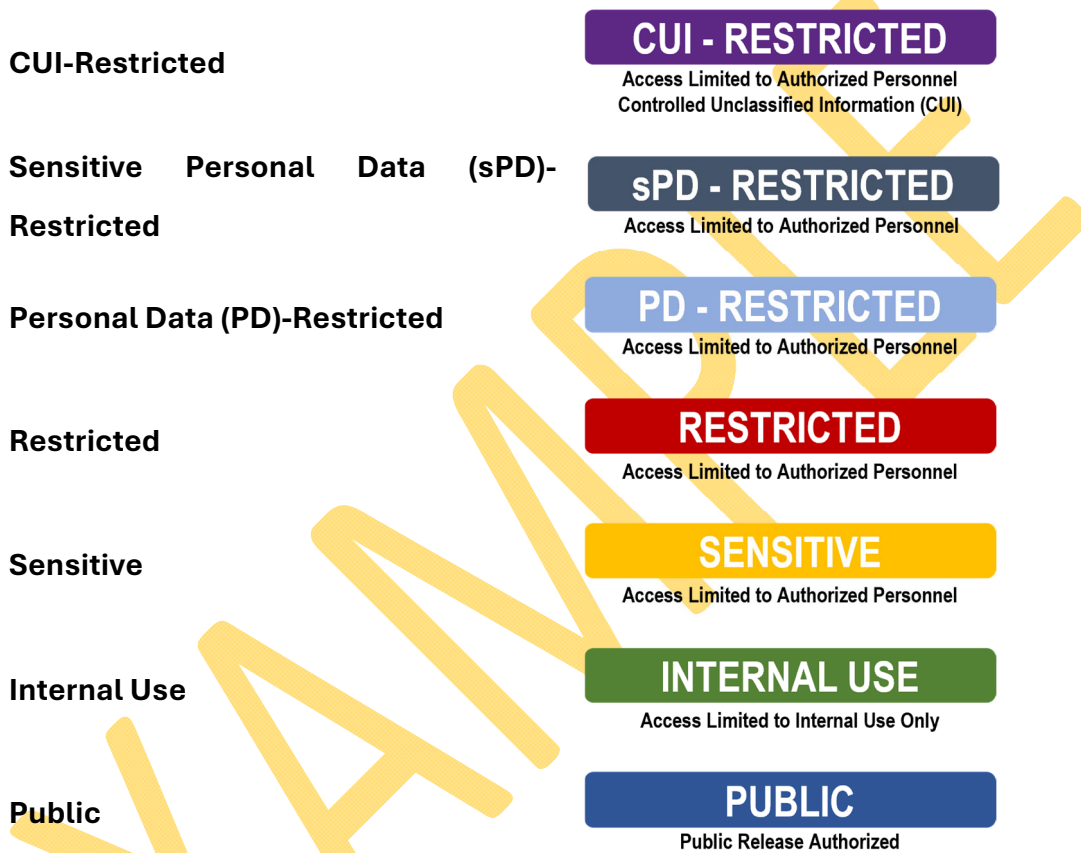
REFERENCE 1: EXCEPTION REQUEST PROCESS	61
REFERENCE 2: ELECTRONIC DISCOVERY (EDISCOVERY) GUIDELINES	62
<i>FEDERAL RULES OF CIVIL PROCEDURE (FCRP)</i>	62
<i>LEGAL HOLD</i>	62
<i>ELECTRONIC DISCOVERY</i>	62
REFERENCE 3: TYPES OF SECURITY CONTROLS	63
<i>PREVENTATIVE CONTROLS</i>	63
<i>DETECTIVE CONTROLS</i>	63
<i>CORRECTIVE CONTROLS</i>	63
<i>RECOVERY CONTROLS</i>	63
<i>DIRECTIVE CONTROLS</i>	63
<i>DETERRENT CONTROLS</i>	63
<i>COMPENSATING CONTROLS</i>	63
REFERENCE 4: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	64
<i>CYBERSECURITY PROGRAM - PLAN</i>	64
<i>CYBERSECURITY PROGRAM - DO</i>	64
<i>CYBERSECURITY PROGRAM - CHECK</i>	64
<i>CYBERSECURITY PROGRAM - ACT</i>	64

EXAMPLE

ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES

DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following seven (7) sensitivity levels:



Classification		Data Sensitivity Description
Controlled Unclassified Information (CUI) - Restricted	Definition	CUI-Restricted information is U.S. Government regulated data that is highly-sensitive business information and the level of protection is dictated externally by both NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI-Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if CUI-Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME’s competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company’s reputation.

Sensitive Personal Data (sPD) Restricted	Definition	Sensitive Personal Data (sPD) is a subset of Personal Data (PD) that is highly-sensitive information about individuals (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. sPD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the sPD is authorized to be stored, processed and/or transmitted.
	Potential Impact of Loss	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if sPD Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME’s competitive position, violating statutory, regulatory and/or contractual requirements, damaging the company’s reputation and posing a risk to identified individuals (e.g., identity theft, stalking, harassment, etc.).
Personal Data (PD) Restricted	Definition	Personal Data (PD) Restricted that is information that can identify an individual (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. The difference between sPD Restricted and PD Restricted is that PD Restricted information is publicly-available information (e.g., social media, news, court filings, etc.). PD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the PD Restricted is authorized to be stored, processed and/or transmitted, unless it is publicly-available information.
	Potential Impact of Loss	<ul style="list-style-type: none"> · MODERATE DAMAGE would occur if PD Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME’s competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company’s reputation.
Restricted	Definition	Restricted information is highly-valuable, highly-sensitive business information and the level of protection is generally dictated externally by statutory, regulatory and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	<ul style="list-style-type: none"> · SIGNIFICANT DAMAGE would occur if Restricted information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME’s competitive position, violating regulatory requirements, damaging the company’s reputation, violating contractual requirements and posing an identity theft risk.
Sensitive	Definition	Sensitive information is highly-valuable, sensitive business information and the level of protection is dictated internally by ACME.
	Potential Impact of Loss	<ul style="list-style-type: none"> · MODERATE DAMAGE would occur if Sensitive information were to become available to unauthorized parties either internal or external to ACME. · Impact could include negatively affecting ACME’s competitive position, damaging the company’s reputation and violating contractual requirements.
Internal Use	Definition	Internal Use information is information originated or owned by ACME or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company’s business interests.
	Potential Impact of Loss	<ul style="list-style-type: none"> · MINIMAL or NO DAMAGE would occur if Internal Use information were to become available to unauthorized parties either internal or external to ACME. · Impact could include damaging the company’s reputation and violating contractual requirements.
Public	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.

DATA HANDLING GUIDELINES

Note: For U.S. Government regulated data, the following requirements supersede ACME data handling guidelines:

- For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handling:
 - 48 CFR 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))
- For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handling:
 - 32 CFR Part 170
 - DoD Instruction 5200.48
 - NIST SP 800-171

Handling Controls	CUI - RESTRICTED	Restricted	Sensitive	Internal Use	Public
Non-Disclosure Agreement (NDA)	<ul style="list-style-type: none"> ▪ NDA is required prior to access by non-employees. 	<ul style="list-style-type: none"> ▪ NDA is required prior to access by non-employees. 	<ul style="list-style-type: none"> ▪ NDA is recommended prior to access by non-employees. 	<i>No NDA requirements</i>	<i>No NDA requirements</i>
Internal Network Transmission (wired & wireless)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<i>No special requirements</i>	<i>No special requirements</i>
External Network Transmission (wired & wireless)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited 	<ul style="list-style-type: none"> ▪ Encryption is recommended 	<i>No special requirements</i>
Data At Rest (file servers, databases, archives, etc.)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups 	<ul style="list-style-type: none"> ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups

ANNEX 2: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

Data Class	Sensitive Data Elements	Public	Internal Use	Sensitive	Restricted	PD - Restricted	sPD - Restricted	CUJ - Restricted
Non-Public Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Social Security Number (SSN)						X	
	Employer Identification Number (EIN)						X	
	Driver's License (DL) Number						X	
	Financial Account Number						X	
	Payment Card Number (credit or debit)						X	
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)						X	
	Geolocation Information (e.g., precise geographic location and/or history)						X	
	Race / Ethnicity						X	
	Religious Affiliation						X	
	Union Membership						X	
	Philosophical Beliefs						X	
	Private Communications (e.g., contents of private mail, emails and text messages)						X	
	Genetic Information						X	
	Biometrics						X	
	Health Information						X	
	Sexual Orientation						X	
	Birth Date						X	
	First & Last Name						X	
	Age						X	
	Phone Number						X	
Home Address						X		
Gender						X		
Email Address						X		
Publicly Available Consumer, Client or Employee Personal Data That Can Uniquely Identify An Individual	Geolocation Information (e.g., precise geographic location and/or history)					X		
	Race / Ethnicity					X		
	Religious Affiliation					X		
	Union Membership					X		
	Philosophical Beliefs					X		
	Private Communications (e.g., contents of private mail, emails and text messages)					X		
	Health Information					X		
	Sexual Orientation					X		
	Birth Date					X		

ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. This basis is called an Assurance Level (AL).

SAFETY & CRITICALITY

One component of assessing risk is to understand the criticality of systems and data. By having a clear understanding of the Safety & Criticality Level (SC) for an asset, system, application, service or data, determining potential impact will be more accurate.

There are four (4) SC levels:

1. Mission Critical (SC1);
2. Business Critical (SC2);
3. Non-Critical (SC3); and
4. Business Supporting (SC4).

MISSION CRITICAL (SC1)

Mission Critical (SC1) assets handle information that is determined to be vital to the operations or mission effectiveness of ACME.

The impact of a SC1 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide business stoppage with significant revenue impact can be anything that creates a significant impact on ACME's ability to perform its mission;
- Public, wide-spread damage to ACME's reputation;
- Direct, negative & long-term impact on customer satisfaction; and
- Risk to human health or the environment.

Examples of SC1 systems, applications and services include, but are not limited to:

- *Enterprise Resource Management (ERM) system (e.g., SAP)*
- *Active Directory (AD)*
- *Ability to process Point of Sale (PoS) or eCommerce payments*

BUSINESS CRITICAL (SC2)

Business Critical (SC2) assets handle information that is important to the support of ACME's primary operations.

The impact of a SC2 system, or its data, being unavailable includes, but is not limited to:

- Enterprise-wide delay or degradation in providing important support services that may seriously impact mission effectiveness or the ability to operate;
- Department-level business stoppage with direct or indirect revenue impact; and
- Direct, negative & short-term impact on customer satisfaction.

Examples of SC2 systems, applications and services include, but are not limited to:

- *Email (e.g., Exchange)*
- *Payroll systems*
- *Corporate website functionality*
- *Corporate mobile device application functionality*
- *HVAC systems*
- *Customer support / call center functionality*

NON-CRITICAL (SC3)

Non-Critical (SC3) assets handle information that is necessary for the conduct of day-to-day business, but they are not mission critical in the short-term.

The impact of a SC3 system, or its data, being unavailable includes, but is not limited to:

- Widespread delays or degradation of services or routine activities;
- Widespread employee productivity degradation;