

Your Logo
Will Be
Placed Here

DIGITAL SECURITY PROGRAM (DSP)

ACME Business Consulting, LLC



INTERNAL USE

Access Limited to Internal Use Only

***IT IS PROHIBITED TO DISCLOSE THIS DOCUMENT TO THIRD-PARTIES
WITHOUT AN EXECUTED NON-DISCLOSURE AGREEMENT (NDA)***

TABLE OF CONTENTS

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES	19
DIGITAL SECURITY PROGRAM (DSP) OVERVIEW	20
INTRODUCTION	20
PURPOSE	20
SCOPE & APPLICABILITY	21
POLICY OVERVIEW	21
VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES	21
EXCEPTION TO STANDARDS	21
UPDATES TO POLICIES & STANDARDS	21
KEY TERMINOLOGY	22
INFORMATION SECURITY PROGRAM STRUCTURE	24
MANAGEMENT DIRECTION FOR INFORMATION SECURITY	24
POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	24
SECURITY & PRIVACY GOVERNANCE (GOV)	25
GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM	25
GOV-02: PUBLISHING SECURITY & PRIVACY POLICIES	25
GOV-03: PERIODIC REVIEW & UPDATE OF SECURITY & PRIVACY DOCUMENTATION	25
GOV-04: ASSIGNED SECURITY & PRIVACY RESPONSIBILITIES	26
GOV-05: MEASURES OF PERFORMANCE	26
GOV-05(A): MEASURES OF PERFORMANCE KEY PERFORMANCE INDICATORS (KPIs)	26
GOV-05(B): MEASURES OF PERFORMANCE KEY RISK INDICATORS (KRIs)	26
GOV-06: CONTACTS WITH AUTHORITIES	27
GOV-07: CONTACTS WITH SECURITY GROUPS & ASSOCIATIONS	27
GOV-08: DEFINED BUSINESS CONTEXT & MISSION	27
GOV-09: DEFINED CONTROL OBJECTIVES	27
ASSET MANAGEMENT (AST)	29
AST-01: ASSET GOVERNANCE	29
AST-01(A): ASSET GOVERNANCE ASSET-SERVICE DEPENDENCIES	29
AST-01(B): ASSET GOVERNANCE STAKEHOLDER IDENTIFICATION & INVOLVEMENT	29
AST-02: ASSET INVENTORIES	29
AST-02(A): ASSET INVENTORIES UPDATES DURING INSTALLATIONS / REMOVALS	30
AST-02(B): ASSET INVENTORIES AUTOMATED UNAUTHORIZED COMPONENT DETECTION	30
AST-02(C): ASSET INVENTORIES COMPONENT DUPLICATION AVOIDANCE	30
AST-02(D): ASSET INVENTORIES APPROVED DEVIATIONS	31
AST-02(E): ASSET INVENTORIES NETWORK ACCESS CONTROL (NAC)	31
AST-02(F): ASSET INVENTORIES DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING	31
AST-02(G): ASSET INVENTORIES SOFTWARE LICENSING RESTRICTIONS	31
AST-02(H): ASSET INVENTORIES DATA ACTION MAPPING	31
AST-02(I): ASSET INVENTORIES CONFIGURATION MANAGEMENT DATABASE (CMDB)	32
AST-03: ASSIGNING OWNERSHIP OF ASSETS	32
AST-03(A): ASSIGNING OWNERSHIP OF ASSETS ACCOUNTABILITY INFORMATION	32
AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	33
AST-05: SECURITY OF ASSETS & MEDIA	33
AST-06: UNATTENDED END-USER EQUIPMENT	33
AST-06(A): UNATTENDED END-USER EQUIPMENT ASSET STORAGE IN AUTOMOBILES	33
AST-07: KIOSKS & POINT OF SALE (POS) DEVICES	34
AST-08: TAMPER PROTECTION & DETECTION	34
AST-09: SECURE DISPOSAL OR RE-USE OF EQUIPMENT	35
AST-10: RETURN OF ASSETS	35
AST-11: REMOVAL OF ASSETS	35
AST-12: USE OF PERSONAL DEVICES	35
AST-13: USE OF THIRD-PARTY DEVICES	36
AST-14: USAGE PARAMETERS	36
AST-15: TAMPER PROTECTION	36
AST-15(A): TAMPER PROTECTION INSPECTION OF SYSTEMS, COMPONENTS & DEVICES	37
AST-16: BRING YOUR OWN DEVICE (BYOD) USAGE	37

BUSINESS CONTINUITY & DISASTER RECOVERY (BCD)**38**

BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)	38
BCD-01(A): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH RELATED PLANS	38
BCD-01(B): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) COORDINATE WITH EXTERNAL SERVICE PROVIDERS	39
BCD-01(C): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) TRANSFER TO ALTERNATE PROCESSING / STORAGE SITE	39
BCD-01(D): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS) RECOVERY TIME / POINT OBJECTIVES	39
BCD-02: IDENTIFY CRITICAL ASSETS	40
BCD-02(A): IDENTIFY CRITICAL ASSETS RESUME ALL MISSIONS & BUSINESS FUNCTIONS	40
BCD-02(B): IDENTIFY CRITICAL ASSETS CONTINUE ESSENTIAL MISSION & BUSINESS FUNCTIONS	40
BCD-02(C): IDENTIFY CRITICAL ASSETS RESUME ESSENTIAL MISSION & BUSINESS FUNCTIONS	41
BCD-03: CONTINGENCY TRAINING	41
BCD-03(A): CONTINGENCY TRAINING SIMULATED EVENTS	41
BCD-03(B): CONTINGENCY TRAINING AUTOMATED TRAINING ENVIRONMENTS	41
BCD-04: CONTINGENCY PLAN TESTING & EXERCISES	41
BCD-04(A): CONTINGENCY PLAN TESTING & EXERCISES COORDINATED TESTING WITH RELATED PLANS	42
BCD-04(B): CONTINGENCY PLAN TESTING & EXERCISES ALTERNATE STORAGE & PROCESSING SITES	42
BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	42
BCD-06: CONTINGENCY PLANNING & UPDATES	42
BCD-07: ALTERNATIVE SECURITY MEASURES	43
BCD-08: ALTERNATE STORAGE SITE	43
BCD-08(A): ALTERNATE STORAGE SITE SEPARATION FROM PRIMARY SITE	43
BCD-08(B): ALTERNATE STORAGE SITE ACCESSIBILITY	43
BCD-09: ALTERNATE PROCESSING SITE	44
BCD-09(A): ALTERNATE PROCESSING SITE SEPARATION FROM PRIMARY SITE	44
BCD-09(B): ALTERNATE PROCESSING SITE ACCESSIBILITY	44
BCD-09(C): ALTERNATE PROCESSING SITE PRIORITY OF SERVICE	44
BCD-09(D): ALTERNATE PROCESSING SITE PREPARATION FOR USE	45
BCD-09(E): ALTERNATE PROCESSING SITE INABILITY TO RETURN TO PRIMARY SITE	45
BCD-10: TELECOMMUNICATIONS SERVICES AVAILABILITY	45
BCD-10(A): TELECOMMUNICATIONS SERVICES AVAILABILITY PRIORITY OF SERVICE PROVISIONS	45
BCD-10(B): TELECOMMUNICATIONS SERVICES AVAILABILITY SEPARATION OF PRIMARY / ALTERNATE PROVIDERS	46
BCD-10(C): TELECOMMUNICATIONS SERVICES AVAILABILITY PROVIDER CONTINGENCY PLAN	46
BCD-11: DATA BACKUPS	46
BCD-11(A): DATA BACKUPS TESTING FOR RELIABILITY & INTEGRITY	48
BCD-11(B): DATA BACKUPS SEPARATE STORAGE FOR CRITICAL INFORMATION	48
BCD-11(C): DATA BACKUPS INFORMATION SYSTEM IMAGING	48
BCD-11(D): DATA BACKUPS CRYPTOGRAPHIC PROTECTION	48
BCD-11(E): DATA BACKUPS TEST RESTORATION USING SAMPLING	49
BCD-11(F): DATA BACKUPS TRANSFER TO ALTERNATE STORAGE SITE	49
BCD-11(G): DATA BACKUPS REDUNDANT SECONDARY SYSTEM	49
BCD-11(H): DATA BACKUPS DUAL AUTHORIZATION	49
BCD-12: INFORMATION SYSTEM RECOVERY & RECONSTITUTION	50
BCD-12(A): INFORMATION SYSTEM RECOVERY & RECONSTITUTION TRANSACTION RECOVERY	50
BCD-12(B): INFORMATION SYSTEM RECOVERY & RECONSTITUTION FAILOVER CAPABILITY	50
BCD-12(C): INFORMATION SYSTEM RECOVERY & RECONSTITUTION ELECTRONIC DISCOVERY (eDISCOVERY)	50
BCD-12(D): INFORMATION SYSTEM RECOVERY & RECONSTITUTION RESTORE WITHIN TIME PERIOD	50
BCD-13: BACKUP & RESTORATION HARDWARE PROTECTION	51

CAPACITY & PERFORMANCE PLANNING (CAP)**52**

CAP-01: CAPACITY & PERFORMANCE MANAGEMENT	52
CAP-02: RESOURCE PRIORITY	52
CAP-03: CAPACITY PLANNING	52

CHANGE MANAGEMENT (CHG)**53**

CHG-01: CHANGE MANAGEMENT PROGRAM	53
CHG-02: CONFIGURATION CHANGE CONTROL	53
CHG-02(A): CONFIGURATION CHANGE CONTROL PROHIBITION OF CHANGES	54
CHG-02(B): CONFIGURATION CHANGE CONTROL TEST, VALIDATE & DOCUMENT CHANGES	54
CHG-02(C): CONFIGURATION CHANGE CONTROL SECURITY REPRESENTATIVE FOR CHANGE	54
CHG-02(D): CONFIGURATION CHANGE CONTROL AUTOMATED SECURITY RESPONSE	54

CHG-02(E): CONFIGURATION CHANGE CONTROL CRYPTOGRAPHIC MANAGEMENT	54
CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES	55
CHG-04: ACCESS RESTRICTION FOR CHANGE	55
CHG-04(A): ACCESS RESTRICTIONS FOR CHANGE AUTOMATED ACCESS ENFORCEMENT / AUDITING	55
CHG-04(B): ACCESS RESTRICTIONS FOR CHANGE SIGNED COMPONENTS	55
CHG-04(C): ACCESS RESTRICTIONS FOR CHANGE DUAL AUTHORIZATION FOR CHANGE	56
CHG-04(D): ACCESS RESTRICTIONS FOR CHANGE LIMIT PRODUCTION / OPERATIONAL PRIVILEGES (INCOMPATIBLE ROLES)	56
CHG-04(E): ACCESS RESTRICTIONS FOR CHANGE LIBRARY PRIVILEGES	56
CHG-05: STAKEHOLDER NOTIFICATION OF CHANGES	56
CHG-06: SECURITY FUNCTIONALITY VERIFICATION	57
CHG-06(A): SECURITY FUNCTIONALITY VERIFICATION REPORT VERIFICATION RESULTS	57
CLD SECURITY (CLD)	58
CLD-01: CLOUD SERVICES	58
CLD-02: CLOUD SECURITY ARCHITECTURE	58
CLD-03: SECURITY MANAGEMENT SUBNET	59
CLD-04: APPLICATION & PROGRAM INTERFACE (API) SECURITY	59
CLD-05: VIRTUAL MACHINE IMAGES	59
CLD-06: MULTI-TENANT ENVIRONMENTS	59
CLD-07: DATA HANDLING & PORTABILITY	60
CLD-08: STANDARDIZED VIRTUALIZATION FORMATS	60
CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS	60
CLD-10: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS	60
CLD-11: CLOUD ACCESS POINT (CAP)	61
COMPLIANCE (CPL)	62
CPL-01: STATUTORY, REGULATORY & CONTRACTUAL COMPLIANCE	62
CPL-02: SECURITY CONTROLS OVERSIGHT	62
CPL-02(A): SECURITY CONTROLS OVERSIGHT INTERNAL AUDIT FUNCTION	63
CPL-03: SECURITY ASSESSMENTS	63
CPL-03(A): SECURITY ASSESSMENTS INDEPENDENT ASSESSORS	64
CPL-03(B): SECURITY ASSESSMENTS FUNCTIONAL REVIEW OF SECURITY CONTROLS	64
CPL-04: AUDIT ACTIVITIES	64
CONFIGURATION MANAGEMENT (CFG)	65
CFG-01: CONFIGURATION MANAGEMENT PROGRAM	65
CFG-01(A): CONFIGURATION MANAGEMENT PROGRAM ASSIGNMENT OF RESPONSIBILITY	65
CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS	65
CFG-02(A): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS REVIEWS & UPDATES	66
CFG-02(B): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS AUTOMATED CENTRAL MANAGEMENT & VERIFICATION	67
CFG-02(C): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS RETENTION OF PREVIOUS CONFIGURATIONS	67
CFG-02(D): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS DEVELOPMENT & TEST ENVIRONMENTS	67
CFG-02(E): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS	68
CFG-02(F): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS NETWORK DEVICE CONFIGURATION FILE SYNCHRONIZATION	68
CFG-02(G): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS APPROVED DEVIATIONS	68
CFG-02(H): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS RESPOND TO UNAUTHORIZED CHANGES	68
CFG-02(I): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS BASELINE TAILORING	69
CFG-03: LEAST FUNCTIONALITY	69
CFG-03(A): LEAST FUNCTIONALITY PERIODIC REVIEW	70
CFG-03(B): LEAST FUNCTIONALITY PREVENT PROGRAM EXECUTION	70
CFG-03(C): LEAST FUNCTIONALITY UNAUTHORIZED OR AUTHORIZED SOFTWARE (BLACKLISTING OR WHITELISTING)	70
CFG-03(D): LEAST FUNCTIONALITY SPLIT TUNNELING	70
CFG-04: SOFTWARE USAGE RESTRICTIONS	71
CFG-04(A): SOFTWARE USAGE RESTRICTIONS OPEN SOURCE SOFTWARE	71
CFG-04(B): SOFTWARE USAGE RESTRICTIONS UNSUPPORTED INTERNET BROWSERS & EMAIL CLIENTS	71
CFG-05: USER-INSTALLED SOFTWARE	72
CFG-05(A): USER-INSTALLED SOFTWARE UNAUTHORIZED INSTALLATION ALERTS	72

CONTINUOUS MONITORING (MON)**73****MON-01: CONTINUOUS MONITORING****73***MON-01(A): CONTINUOUS MONITORING | INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)*

74

MON-01(B): CONTINUOUS MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

74

MON-01(C): CONTINUOUS MONITORING | INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC

74

MON-01(D): CONTINUOUS MONITORING | SYSTEM GENERATED ALERTS

74

MON-01(E): CONTINUOUS MONITORING | WIRELESS INTRUSION DETECTION SYSTEM (WIDS)

75

MON-01(F): CONTINUOUS MONITORING | HOST-BASED DEVICES

75

MON-01(G): CONTINUOUS MONITORING | FILE INTEGRITY MONITORING (FIM)

75

MON-01(H): CONTINUOUS MONITORING | REVIEWS & UPDATES

75

MON-01(I): CONTINUOUS MONITORING | PROXY LOGGING

76

MON-01(J): CONTINUOUS MONITORING | DEACTIVATED ACCOUNT ACTIVITY

76

MON-01(K): CONTINUOUS MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS

76

MON-01(L): CONTINUOUS MONITORING | AUTOMATED ALERTS

76

MON-01(M): CONTINUOUS MONITORING | ANALYZE TRAFFIC / EVENT PATTERNS

76

MON-01(N): CONTINUOUS MONITORING | INDIVIDUALS POSING GREATER RISK

77

MON-01(O): CONTINUOUS MONITORING | PRIVILEGED USER OVERSIGHT

77

MON-01(P): CONTINUOUS MONITORING | ANALYZE & PRIORITIZE MONITORING REQUIREMENTS

77

MON-02: CENTRALIZED EVENT LOG COLLECTION**77***MON-02(A): CENTRALIZED SECURITY EVENT LOG COLLECTION | CORRELATE MONITORING INFORMATION*

78

MON-02(B): CENTRALIZED SECURITY EVENT LOG COLLECTION | CENTRAL REVIEW & ANALYSIS

78

MON-02(C): CENTRALIZED SECURITY EVENT LOG COLLECTION | INTEGRATION OF SCANNING & OTHER MONITORING INFORMATION

79

MON-02(D): CENTRALIZED SECURITY EVENT LOG COLLECTION | CORRELATION WITH PHYSICAL MONITORING

79

MON-02(E): CENTRALIZED SECURITY EVENT LOG COLLECTION | PERMITTED ACTIONS

79

MON-02(F): CENTRALIZED SECURITY EVENT LOG COLLECTION | AUDIT LEVEL ADJUSTMENT

79

MON-02(G): CENTRALIZED SECURITY EVENT LOG COLLECTION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL

80

MON-02(H): CENTRALIZED SECURITY EVENT LOG COLLECTION | CHANGES BY AUTHORIZED INDIVIDUALS

80

MON-03: CONTENT OF AUDIT RECORDS**80***MON-03(A): CONTENT OF AUDIT RECORDS | SENSITIVE AUDIT INFORMATION*

81

MON-03(B): CONTENT OF AUDIT RECORDS | AUDIT TRAILS

81

MON-03(C): CONTENT OF AUDIT RECORDS | PRIVILEGED FUNCTIONS LOGGING

81

MON-03(D): CONTENT OF AUDIT RECORDS | VERBOSITY LOGGING FOR BOUNDARY DEVICES

81

MON-03(E): CONTENT OF AUDIT RECORDS | LIMIT PERSONAL DATA (PD) IN AUDIT RECORDS

82

MON-03(F): CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT

82

MON-04: AUDIT STORAGE CAPACITY**82****MON-05: RESPONSE TO AUDIT PROCESSING FAILURES****82***MON-05(A): RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS OF AUDIT FAILURE*

83

MON-05(B): RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY ALERTING

83

MON-06: MONITORING REPORTING**83***MON-06(A): MONITORING REPORTING | QUERY PARAMETER AUDITS OF PERSONAL DATA (PD)*

83

MON-06(B): MONITORING REPORTING | TREND ANALYSIS REPORTING

84

MON-07: TIME STAMPS**84***MON-07(A): TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*

84

MON-08: PROTECTION OF AUDIT INFORMATION**84***MON-08(A): PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*

85

MON-08(B): PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS

85

MON-08(C): PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION OF AUDIT INFORMATION

85

MON-08(D): PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION

86

MON-09: NON-REPUDIATION**86****MON-10: AUDIT RECORD RETENTION****86****MON-11: MONITORING FOR INFORMATION DISCLOSURE****87***MON-11(A): MONITORING FOR INFORMATION DISCLOSURE | ANALYZE TRAFFIC FOR COVERT EXFILTRATION)*

87

MON-11(B): MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED NETWORK SERVICES

87

MON-11(C): MONITORING FOR INFORMATION DISCLOSURE | MONITORING FOR INDICATORS OF COMPROMISE (IOC)

87

MON-12: SESSION AUDIT**87****MON-13: ALTERNATE AUDIT CAPABILITY****88**

MON-14: Cross-Organizational Monitoring	88
<i>MON-14(A): Cross-Organizational Monitoring Sharing of Audit Information</i>	88
MON-15: Covert Channel Analysis	89
MON-16 Anomalous Behavior	89
<i>MON-16(A): Anomalous Behavior Insider Threats</i>	89
<i>MON-16(B): Anomalous Behavior Third-Party Threats</i>	89
<i>MON-16(C): Anomalous Behavior Unauthorized Activities</i>	90
<u>Cryptographic Protections (CRY)</u>	<u>91</u>
CRY-01: Use of Cryptographic Controls	91
<i>CRY-01(A): Use of Cryptographic Controls Alternate Physical Protection</i>	91
<i>CRY-01(B): Use of Cryptographic Controls Export-Controlled Technology</i>	92
<i>CRY-01(C): Use of Cryptographic Controls Pre / Post Transmission Handling</i>	92
<i>CRY-01(D): Use of Cryptographic Controls Conceal / Randomize Communications</i>	92
CRY-02: Cryptographic Module Authentication	92
CRY-03: Transmission Confidentiality	92
CRY-04: Transmission Integrity	93
CRY-05: Encrypting Data At Rest	93
<i>CRY-05(A): Encrypting Data At Rest Storage Media</i>	94
<i>CRY-05(B): Encrypting Data At Rest Offline Storage</i>	94
CRY-06: Non-Console Administrative Access	94
CRY-07: Wireless Access Authentication & Encryption	95
CRY-08: Public Key Infrastructure (PKI)	95
<i>CRY-08(A): Public Key Infrastructure (PKI) Availability</i>	95
CRY-09: Cryptographic Key Management	95
<i>CRY-09(A): Cryptographic Key Management Symmetric Keys</i>	96
<i>CRY-09(B): Cryptographic Key Management Asymmetric Keys</i>	97
<i>CRY-09(C): Cryptographic Key Management Cryptographic Key Loss or Change</i>	97
<i>CRY-09(D): Cryptographic Key Management Control & Distribution of Cryptographic Keys</i>	97
<i>CRY-09(E): Cryptographic Key Management Assigned Owners</i>	97
CRY-10: Transmission of Security & Privacy Attributes	98
<u>Data Classification & Handling (DCH)</u>	<u>99</u>
DCH-01: Data Protection	99
<i>DCH-01(A): Data Protection Data Stewardship</i>	99
DCH-02: Data & Asset Classification	99
DCH-03: Media Access	100
<i>DCH-03(A): Media Access Disclosure of Information</i>	100
<i>DCH-03(B): Media Access Masking Displayed Data</i>	100
DCH-04: Media Marking	100
<i>DCH-04(A): Media Marking Automated Marking</i>	101
DCH-05: Security Attributes	101
<i>DCH-05(A): Security Attributes Dynamic Attribute Association</i>	101
<i>DCH-05(B): Security Attributes Attribute Value Changes by Authorized Individuals</i>	101
<i>DCH-05(C): Security Attributes Maintenance of Attribute Associations by System</i>	101
<i>DCH-05(D): Security Attributes Association of Attributes by Authorized Individuals</i>	102
<i>DCH-05(E): Security Attributes Attribute Displays for Output Devices</i>	102
<i>DCH-05(F): Security Attributes Data Subject Attribute Associations</i>	102
<i>DCH-05(G): Security Attributes Consistent Attribute Interpretation</i>	102
<i>DCH-05(H): Security Attributes Identity Association Techniques & Technologies</i>	102
<i>DCH-05(I): Security Attributes Attribute Reassignment</i>	103
<i>DCH-05(J): Security Attributes Attribute Configuration by Authorized Individuals</i>	103
<i>DCH-05(K): Security Attributes Audit Changes</i>	103
DCH-06: Media Storage	103
<i>DCH-06(A): Media Storage Physically Secure All Media</i>	104
<i>DCH-06(B): Media Storage Sensitive Data Inventories</i>	104
<i>DCH-06(C): Media Storage Periodic Scans for Sensitive Data</i>	104
<i>DCH-06(D): Media Storage Making Sensitive Data Unreadable in Storage</i>	104
<i>DCH-06(E): Media Storage Storing Authentication Data</i>	105
DCH-07: Media Transportation	105

<i>DCH-07(A): MEDIA TRANSPORTATION CUSTODIANS</i>	106
<i>DCH-07(B): MEDIA TRANSPORTATION ENCRYPTING DATA IN STORAGE MEDIA</i>	106
DCH-08: PHYSICAL MEDIAL DISPOSAL	106
DCH-09: DIGITAL MEDIA SANITIZATION	106
<i>DCH-09(A): MEDIA SANITIZATION MEDIA SANITIZATION DOCUMENTATION</i>	107
<i>DCH-09(B): MEDIA SANITIZATION EQUIPMENT TESTING</i>	107
<i>DCH-09(C): MEDIA SANITIZATION DESTRUCTION OF PERSONAL DATA (PD)</i>	107
<i>DCH-09(D): MEDIA SANITIZATION NON-DESTRUCTIVE TECHNIQUES</i>	107
<i>DCH-09(E): MEDIA SANITIZATION DUAL AUTHORIZATION</i>	108
DCH-10: MEDIA USE	108
<i>DCH-10(A): MEDIA USE LIMITATIONS ON USE</i>	108
<i>DCH-10(B): MEDIA USE PROHIBIT USE WITHOUT OWNER</i>	108
DCH-11: MEDIA DOWNGRADING	109
DCH-12: REMOVABLE MEDIA SECURITY	109
DCH-13: USE OF EXTERNAL INFORMATION SYSTEMS	109
<i>DCH-13(A): USE OF EXTERNAL INFORMATION SYSTEMS LIMITS OF AUTHORIZED USE</i>	109
<i>DCH-13(B): USE OF EXTERNAL INFORMATION SYSTEMS PORTABLE STORAGE DEVICES</i>	110
<i>DCH-13(C): USE OF EXTERNAL INFORMATION SYSTEMS PROTECTING SENSITIVE DATA ON EXTERNAL SYSTEMS</i>	110
<i>DCH-13(D): USE OF EXTERNAL INFORMATION SYSTEMS NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES</i>	110
DCH-14: INFORMATION SHARING	111
<i>DCH-14(A): INFORMATION SHARING INFORMATION SEARCH & RETRIEVAL</i>	112
DCH-15: PUBLICLY ACCESSIBLE CONTENT	112
DCH-16: DATA MINING PROTECTION	112
DCH-17: AD-HOC TRANSFERS	112
DCH-18: MEDIA & DATA RETENTION	113
<i>DCH-18(A): MEDIA & DATA RETENTION LIMIT PERSONAL DATA (PD) ELEMENTS IN TESTING, TRAINING & RESEARCH</i>	114
<i>DCH-18(B): MEDIA & DATA RETENTION MINIMIZE PERSONAL DATA (PD)</i>	114
<i>DCH-18(C): MEDIA & DATA RETENTION TEMPORARY FILES CONTAINING PERSONAL DATA</i>	114
DCH-19: GEOGRAPHIC LOCATION OF DATA	114
DCH-20: ARCHIVED DATA SETS	115
DCH-21: INFORMATION DISPOSAL	115
DCH-22: DATA QUALITY OPERATIONS	115
<i>DCH-22(A): DATA QUALITY OPERATIONS UPDATING & CORRECTING PERSONAL DATA (PD)</i>	115
<i>DCH-22(B): DATA QUALITY OPERATIONS DATA TAGS</i>	116
<i>DCH-22(C): DATA QUALITY OPERATIONS PERSONAL DATA (PD) COLLECTION</i>	116
DCH-23: DE-IDENTIFICATION (ANONYMIZATION)	116
<i>DCH-23(A): DE-IDENTIFICATION (ANONYMIZATION) COLLECTION</i>	116
<i>DCH-23(B): DE-IDENTIFICATION (ANONYMIZATION) ARCHIVING</i>	116
<i>DCH-23(C): DE-IDENTIFICATION (ANONYMIZATION) RELEASE</i>	117
<i>DCH-23(D): DE-IDENTIFICATION (ANONYMIZATION) REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS</i>	117
<i>DCH-23(E): DE-IDENTIFICATION (ANONYMIZATION) STATISTICAL DISCLOSURE CONTROL</i>	117
<i>DCH-23(F): DE-IDENTIFICATION (ANONYMIZATION) DIFFERENTIAL PRIVACY</i>	117
<i>DCH-23(G): DE-IDENTIFICATION (ANONYMIZATION) VALIDATED SOFTWARE</i>	118
<i>DCH-23(H): DE-IDENTIFICATION (ANONYMIZATION) MOTIVATED INTRUDER</i>	118
DCH-24: INFORMATION LOCATION	118
<i>DCH-24(A): INFORMATION LOCATION AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION</i>	118
DCH-25: TRANSFER OF PERSONAL INFORMATION	119
EMBEDDED TECHNOLOGY (EMB)	120
EMB-01: EMBEDDED TECHNOLOGY SECURITY PROGRAM	120
EMB-02: INTERNET OF THINGS (IoT)	120
EMB-03: OPERATIONAL TECHNOLOGY (OT)	120
ENDPOINT SECURITY (END)	122
END-01: ENDPOINT SECURITY	122
END-02: ENDPOINT PROTECTION MEASURES	122
END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	122
<i>END-03(A): PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS UNAUTHORIZED INSTALLATION ALERTS</i>	123

<i>END-03(B): PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS ACCESS RESTRICTION FOR CHANGE</i>	123
END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)	123
<i>END-04(A): MALICIOUS CODE PROTECTION (ANTI-MALWARE) AUTOMATIC UPDATES</i>	124
<i>END-04(B): MALICIOUS CODE PROTECTION (ANTI-MALWARE) DOCUMENTED PROTECTION MEASURES</i>	124
<i>END-04(C): MALICIOUS CODE PROTECTION (ANTI-MALWARE) CENTRALIZED MANAGEMENT</i>	124
<i>END-04(D): MALICIOUS CODE PROTECTION (ANTI-MALWARE) NONSIGNATURE-BASED DETECTION</i>	124
<i>END-04(E): MALICIOUS CODE PROTECTION (ANTI-MALWARE) MALWARE PROTECTION MECHANISM TESTING</i>	124
<i>END-04(F): MALICIOUS CODE PROTECTION (ANTI-MALWARE) EVOLVING MALWARE THREATS</i>	125
<i>END-04(G): MALICIOUS CODE PROTECTION (ANTI-MALWARE) ALWAYS ON PROTECTION</i>	125
END-05: SOFTWARE FIREWALL	125
END-06: FILE INTEGRITY MONITORING (FIM)	126
<i>END-06(A): FILE INTEGRITY MONITORING (FIM) INTEGRITY CHECKS</i>	126
<i>END-06(B): FILE INTEGRITY MONITORING (FIM) INTEGRATION OF DETECTION & RESPONSE</i>	127
<i>END-06(C): FILE INTEGRITY MONITORING (FIM) AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS</i>	127
<i>END-06(D): FILE INTEGRITY MONITORING (FIM) AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS</i>	127
<i>END-06(E): FILE INTEGRITY MONITORING (FIM) VERIFY BOOT PROCESS</i>	127
<i>END-06(F): FILE INTEGRITY MONITORING (FIM) PROTECTION OF BOOT FIRMWARE</i>	128
<i>END-06(G): FILE INTEGRITY MONITORING (FIM) BINARY OR MACHINE-EXECUTABLE CODE</i>	128
END-07: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS / HIPS)	128
END-08: PHISHING & SPAM PROTECTION	128
<i>END-08(A): PHISHING & SPAM PROTECTION CENTRAL MANAGEMENT</i>	129
<i>END-08(B): PHISHING & SPAM PROTECTION AUTOMATIC UPDATES</i>	129
END-09: TRUSTED PATH	129
END-10: MOBILE CODE	129
END-11: THIN NODES	130
END-12: PORT & INPUT / OUTPUT (I/O) DEVICE ACCESS	130
END-13: SENSOR CAPABILITY	131
<i>END-13(A): SENSOR CAPABILITY AUTHORIZED USE</i>	131
<i>END-13(B): SENSOR CAPABILITY NOTICE OF COLLECTION</i>	131
<i>END-13(C): SENSOR CAPABILITY COLLECTION MINIMIZATION</i>	131
END-14: COLLABORATIVE COMPUTING DEVICES	132
<i>END-14(A): COLLABORATIVE COMPUTING DEVICES DISABLING / REMOVAL IN SECURE WORK AREAS</i>	132
<i>END-14(B): COLLABORATIVE COMPUTING DEVICES EXPLICITLY INDICATE CURRENT PARTICIPANTS</i>	132
END-15: HYPERVISOR ACCESS	132
END-16: SECURITY FUNCTION ISOLATION	132
<i>END-16(A): SECURITY FUNCTION ISOLATION HOST-BASED SECURITY FUNCTION ISOLATION</i>	133
HUMAN RESOURCES SECURITY (HRS)	134
HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT	134
HRS-02: POSITION CATEGORIZATION	134
<i>HRS-02(A): POSITION CATEGORIZATION USERS WITH ELEVATED PRIVILEGES</i>	134
HRS-03: ROLES & RESPONSIBILITIES	135
<i>HRS-03(A): ROLES & RESPONSIBILITIES USER AWARENESS</i>	135
<i>HRS-03(B): ROLES & RESPONSIBILITIES COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS</i>	135
HRS-04: PERSONNEL SCREENING	135
<i>HRS-04(A): PERSONNEL SCREENING ROLES WITH SPECIAL PROTECTION MEASURES</i>	136
<i>HRS-04(B): PERSONNEL SCREENING FORMAL INDOCTRINATION</i>	136
HRS-05: TERMS OF EMPLOYMENT	136
<i>HRS-05(A): TERMS OF EMPLOYMENT RULES OF BEHAVIOR</i>	136
<i>HRS-05(B): TERMS OF EMPLOYMENT SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS</i>	137
<i>HRS-05(C): TERMS OF EMPLOYMENT USE OF COMMUNICATIONS TECHNOLOGY</i>	137
<i>HRS-05(D): TERMS OF EMPLOYMENT USE OF CRITICAL TECHNOLOGIES</i>	137
<i>HRS-05(E): TERMS OF EMPLOYMENT USE OF MOBILE DEVICES</i>	138
HRS-06: ACCESS AGREEMENTS	138
<i>HRS-06(A): ACCESS AGREEMENTS CONFIDENTIALITY AGREEMENTS</i>	138
<i>HRS-06(B): ACCESS AGREEMENTS POST-EMPLOYMENT OBLIGATIONS</i>	138
HRS-07: PERSONNEL SANCTIONS	139
<i>HRS-07(A): PERSONNEL SANCTIONS WORKPLACE INVESTIGATIONS</i>	139
HRS-08: PERSONNEL TRANSFER	140

HRS-09: PERSONNEL TERMINATION	140
<i>HRS-09(A): PERSONNEL TERMINATION ASSET COLLECTION</i>	140
<i>HRS-09(B): PERSONNEL TERMINATION HIGH-RISK TERMINATIONS</i>	141
<i>HRS-09(C): PERSONNEL TERMINATION POST-EMPLOYMENT REQUIREMENTS</i>	141
<i>HRS-09(D): PERSONNEL TERMINATION AUTOMATED EMPLOYMENT STATUS NOTIFICATION</i>	141
HRS-10: THIRD-PARTY PERSONNEL SECURITY	141
HRS-11: SEPARATION OF DUTIES	142
HRS-12: INCOMPATIBLE ROLES	142
<i>HRS-12(A): INCOMPATIBLE ROLES TWO-PERSON RULE</i>	142
HRS-13: IDENTIFY CRITICAL SKILLS & GAPS	142
<i>HRS-13(A): IDENTIFY CRITICAL SKILLS & GAPS REMEDIATE IDENTIFIED SKILLS DEFICIENCIES</i>	143
<i>HRS-13(B): IDENTIFY CRITICAL SKILLS & GAPS IDENTIFY VITAL CYBERSECURITY & PRIVACY STAFF</i>	143
<i>HRS-13(C): IDENTIFY CRITICAL SKILLS & GAPS ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & PRIVACY STAFF</i>	143
<i>HRS-13(D): IDENTIFY CRITICAL SKILLS & GAPS PERFORM SUCCESSION PLANNING</i>	143
IDENTIFICATION & AUTHENTICATION (IAC)	145
IAC-01: IDENTITY & ACCESS MANAGEMENT (IAM)	145
IAC-02: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS	145
<i>IAC-02(A): IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS GROUP AUTHENTICATION</i>	145
<i>IAC-02(B): IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS NETWORK ACCESS TO PRIVILEGED ACCOUNTS</i>	
- REPLAY RESISTANT	146
<i>IAC-02(C): IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS ACCEPTANCE OF PIV CREDENTIALS</i>	146
<i>IAC-02(D): IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS OUT-OF-BAND AUTHENTICATION (OOBA)</i>	146
IAC-03: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS	146
<i>IAC-03(A): IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF PIV CREDENTIALS</i>	
FROM OTHER ORGANIZATIONS	147
<i>IAC-03(B): IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS ACCEPTANCE OF THIRD-PARTY</i>	
CREDENTIALS	147
<i>IAC-03(C): IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS USE OF FICAM-ISSUED PROFILES</i>	147
<i>IAC-03(D): IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS DISASSOCIABILITY</i>	147
IAC-04: IDENTIFICATION & AUTHENTICATION FOR DEVICES	148
<i>IAC-04(A): IDENTIFICATION & AUTHENTICATION FOR DEVICES DEVICE ATTESTATION</i>	148
IAC-05: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES	148
<i>IAC-05(A): IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES INFORMATION EXCHANGE</i>	148
IAC-06: MULTIFACTOR AUTHENTICATION (MFA)	149
<i>IAC-06(A): MULTI-FACTOR AUTHENTICATION (MFA) NETWORK ACCESS TO PRIVILEGED ACCOUNTS</i>	149
<i>IAC-06(B): MULTI-FACTOR AUTHENTICATION (MFA) NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS</i>	149
<i>IAC-06(C): MULTI-FACTOR AUTHENTICATION (MFA) LOCAL ACCESS TO PRIVILEGED ACCOUNTS</i>	149
<i>IAC-06(D): MULTI-FACTOR AUTHENTICATION (MFA) OUT OF BAND (OOB) FACTOR</i>	149
IAC-07: USER PROVISIONING & DE-PROVISIONING	150
<i>IAC-07(A): USER PROVISIONING & DE-PROVISIONING CHANGE OF ROLES & DUTIES</i>	150
<i>IAC-07(B): USER PROVISIONING & DE-PROVISIONING TERMINATION OF EMPLOYMENT</i>	150
IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)	151
IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)	151
<i>IAC-09(A): IDENTIFIER MANAGEMENT USER IDENTITY (ID) MANAGEMENT</i>	151
<i>IAC-09(B): IDENTIFIER MANAGEMENT IDENTITY USER STATUS</i>	152
<i>IAC-09(C): IDENTIFIER MANAGEMENT DYNAMIC MANAGEMENT</i>	152
<i>IAC-09(D): IDENTIFIER MANAGEMENT CROSS-ORGANIZATION MANAGEMENT</i>	152
<i>IAC-09(E): IDENTIFIER MANAGEMENT PRIVILEGED ACCOUNT IDENTIFIERS</i>	152
<i>IAC-09(F): IDENTIFIER MANAGEMENT PAIRWISE PSEUDONYMOUS IDENTIFIERS (PPID)</i>	153
IAC-10: AUTHENTICATOR MANAGEMENT (PASSWORDS)	153
<i>IAC-10(A): AUTHENTICATOR MANAGEMENT PASSWORD-BASED AUTHENTICATION</i>	153
<i>IAC-10(B): AUTHENTICATOR MANAGEMENT PKI-BASED AUTHENTICATION</i>	155
<i>IAC-10(C): AUTHENTICATOR MANAGEMENT IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION</i>	155
<i>IAC-10(D): AUTHENTICATOR MANAGEMENT AUTOMATED SUPPORT FOR PASSWORD STRENGTH</i>	156
<i>IAC-10(E): AUTHENTICATOR MANAGEMENT PROTECTION OF AUTHENTICATORS</i>	156
<i>IAC-10(F): AUTHENTICATOR MANAGEMENT NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS</i>	156
<i>IAC-10(G): AUTHENTICATOR MANAGEMENT HARDWARE TOKEN-BASED AUTHENTICATION</i>	156
<i>IAC-10(H): AUTHENTICATOR MANAGEMENT VENDOR-SUPPLIED DEFAULTS</i>	157

IAC-10(i): AUTHENTICATOR MANAGEMENT MULTIPLE INFORMATION SYSTEM ACCOUNTS	157
IAC-10(j): AUTHENTICATOR MANAGEMENT EXPIRATION OF CACHED AUTHENTICATORS	157
IAC-11: AUTHENTICATOR FEEDBACK	157
IAC-12: CRYPTOGRAPHIC MODULE AUTHENTICATION	157
IAC-13: ADAPTIVE IDENTIFICATION & AUTHENTICATION	158
IAC-14: RE-AUTHENTICATION	158
IAC-15: ACCOUNT MANAGEMENT	158
IAC-15(A): ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT	159
IAC-15(B): ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	160
IAC-15(C): ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS	160
IAC-15(D): ACCOUNT MANAGEMENT AUTOMATED AUDIT ACTIONS	160
IAC-15(E): ACCOUNT MANAGEMENT RESTRICTIONS ON SHARED GROUPS / ACCOUNTS	160
IAC-15(F): ACCOUNT MANAGEMENT ACCOUNT DISABLING FOR HIGH RISK INDIVIDUALS	160
IAC-15(G): ACCOUNT MANAGEMENT SYSTEM ACCOUNTS	160
IAC-15(H): ACCOUNT MANAGEMENT USAGE CONDITIONS	161
IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)	161
IAC-16(A): PRIVILEGED ACCOUNT MANAGEMENT (PAM) PRIVILEGED ACCOUNT INVENTORIES	161
IAC-17: PERIODIC REVIEW OF USER PRIVILEGES	161
IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT	162
IAC-19: CREDENTIAL SHARING	162
IAC-20: ACCESS ENFORCEMENT	163
IAC-20(A): ACCESS ENFORCEMENT ACCESS TO SENSITIVE DATA	163
IAC-20(B): ACCESS ENFORCEMENT DATABASE ACCESS	163
IAC-20(C): ACCESS ENFORCEMENT USE OF PRIVILEGED UTILITY PROGRAMS	163
IAC-20(D): ACCESS ENFORCEMENT DEDICATED ADMINISTRATIVE MACHINES	164
IAC-20(E): ACCESS ENFORCEMENT DUAL AUTHORIZATION FOR PRIVILEGED COMMANDS	164
IAC-21: LEAST PRIVILEGE	164
IAC-21(A): LEAST PRIVILEGE AUTHORIZE ACCESS TO SECURITY FUNCTIONS	164
IAC-21(B): LEAST PRIVILEGE NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS	165
IAC-21(C): LEAST PRIVILEGE PRIVILEGED ACCOUNTS	165
IAC-21(D): LEAST PRIVILEGE AUDITING USE OF PRIVILEGED FUNCTIONS	165
IAC-21(E): LEAST PRIVILEGE PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	165
IAC-21(F): LEAST PRIVILEGE NETWORK ACCESS TO PRIVILEGED COMMANDS	166
IAC-21(G): LEAST PRIVILEGE PRIVILEGE LEVELS FOR CODE EXECUTION	166
IAC-22: ACCOUNT LOCKOUT	166
IAC-23: CONCURRENT SESSION CONTROL	166
IAC-24: SESSION LOCK	167
IAC-24(A): SESSION LOCK PATTERN-HIDING DISPLAYS	167
IAC-25: SESSION TERMINATION	167
IAC-25(A): SESSION TERMINATION USER-INITIATED LOGOUTS / MESSAGE DISPLAYS	167
IAC-26: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHORIZATION	168
IAC-27: REFERENCE MONITOR	168
IAC-28: IDENTITY PROOFING	168
IAC-28(A): IDENTITY PROOFING SUPERVISOR AUTHORIZATION	169
IAC-28(B): IDENTITY PROOFING IDENTITY EVIDENCE	169
IAC-28(C): IDENTITY PROOFING IDENTITY EVIDENCE VALIDATION & VERIFICATION	169
IAC-28(D): IDENTITY PROOFING IN-PERSON VALIDATION & VERIFICATION	169
IAC-28(E): IDENTITY PROOFING ADDRESS CONFIRMATION	169
INCIDENT RESPONSE (IRO)	171
IRO-01: INCIDENTS RESPONSE OPERATIONS	171
IRO-02: INCIDENT HANDLING	171
IRO-02(A): INCIDENT HANDLING AUTOMATED INCIDENT HANDLING PROCESSES	172
IRO-02(B): INCIDENT HANDLING INSIDER THREAT PROGRAM	172
IRO-02(C): INCIDENT HANDLING DYNAMIC RECONFIGURATION	173
IRO-02(D): INCIDENT HANDLING CONTINUITY OF OPERATIONS	173
IRO-02(E): INCIDENT HANDLING CORRELATION WITH EXTERNAL ORGANIZATIONS	174
IRO-03: INDICATORS OF COMPROMISE (IOC)	175
IRO-04: INCIDENT RESPONSE PLAN (IRP)	175

<i>IRO-04(A): INCIDENT RESPONSE PLAN (IRP) PERSONAL DATA (PD) PROCESSES</i>	176
<i>IRO-04(B): INCIDENT RESPONSE PLAN (IRP) IRP UPDATE</i>	176
IRO-05: INCIDENT RESPONSE TRAINING	176
<i>IRO-05(A): INCIDENT RESPONSE TRAINING SIMULATED INCIDENTS</i>	177
<i>IRO-05(B): INCIDENT RESPONSE TRAINING AUTOMATED INCIDENT RESPONSE TRAINING ENVIRONMENTS</i>	177
IRO-06: INCIDENT RESPONSE TESTING	177
<i>IRO-06(A): INCIDENT RESPONSE TESTING COORDINATION WITH RELATED PLANS</i>	177
IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)	178
IRO-08: CHAIN OF CUSTODY & FORENSICS	178
IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS	178
<i>IRO-09(A): SITUATIONAL AWARENESS FOR INCIDENTS AUTOMATED TRACKING, DATA COLLECTION & ANALYSIS</i>	178
IRO-10: INCIDENT STAKEHOLDER REPORTING	179
<i>IRO-10(A): INCIDENT STAKEHOLDER REPORTING AUTOMATED REPORTING</i>	179
<i>IRO-10(B): INCIDENT STAKEHOLDER REPORTING CYBER INCIDENT REPORTING FOR COVERED DEFENSE INFORMATION (CDI)</i>	179
<i>IRO-10(C): INCIDENT STAKEHOLDER REPORTING VULNERABILITIES RELATED TO INCIDENTS</i>	180
<i>IRO-10(D): INCIDENT STAKEHOLDER REPORTING SUPPLY CHAIN COORDINATION</i>	180
IRO-11: INCIDENT REPORTING ASSISTANCE	180
<i>IRO-11(A): INCIDENT REPORTING ASSISTANCE AUTOMATION SUPPORT OF AVAILABILITY OF INFORMATION / SUPPORT</i>	181
<i>IRO-11(B): INCIDENT REPORTING ASSISTANCE COORDINATION WITH EXTERNAL PROVIDERS</i>	181
IRO-12: INFORMATION SPILLAGE RESPONSE	181
<i>IRO-12(A): INFORMATION SPILLAGE RESPONSE RESPONSIBLE PERSONNEL</i>	181
<i>IRO-12(B): INFORMATION SPILLAGE RESPONSE TRAINING</i>	182
<i>IRO-12(C): INFORMATION SPILLAGE RESPONSE POST-SPILL OPERATIONS</i>	182
<i>IRO-12(D): INFORMATION SPILLAGE RESPONSE EXPOSURE TO UNAUTHORIZED PERSONNEL</i>	182
IRO-13: ROOT CAUSE ANALYSIS (RCA) & LESSONS LEARNED	182
IRO-14: REGULATORY & LAW ENFORCEMENT CONTACTS	182
IRO-15: DETONATION CHAMBERS (SANDBOXES)	183
INFORMATION ASSURANCE (IAO)	184
IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS	184
IAO-02: SECURITY ASSESSMENTS	184
<i>IAO-02(A): SECURITY ASSESSMENTS INDEPENDENT ASSESSORS</i>	184
<i>IAO-02(B): SECURITY ASSESSMENTS SPECIALIZED ASSESSMENTS</i>	185
<i>IAO-02(C): SECURITY ASSESSMENTS THIRD-PARTY ASSESSMENTS</i>	185
IAO-03: SYSTEM SECURITY PLANS (SSP)	185
<i>IAO-03(A): SYSTEM SECURITY PLAN (SSP) PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i>	186
<i>IAO-03(B): SYSTEM SECURITY PLAN (SSP) ADEQUATE SECURITY FOR COVERED DEFENSE INFORMATION (CDI)</i>	186
IAO-04: THREAT ANALYSIS & FLAW REMEDIATION DURING DEVELOPMENT	187
IAO-05: PLAN OF ACTION & MILESTONES (POA&M)	187
IAO-06: TECHNICAL VERIFICATION	188
IAO-07: SECURITY AUTHORIZATION	188
MAINTENANCE (MNT)	189
MNT-01: MAINTENANCE OPERATIONS	189
MNT-02: CONTROLLED MAINTENANCE	189
<i>MNT-02(A): CONTROLLED MAINTENANCE AUTOMATED MAINTENANCE ACTIVITIES</i>	190
MNT-03: TIMELY MAINTENANCE	190
<i>MNT-03(A): TIMELY MAINTENANCE PREVENTATIVE MAINTENANCE</i>	190
<i>MNT-03(B): TIMELY MAINTENANCE PREDICTIVE MAINTENANCE</i>	190
<i>MNT-03(C): TIMELY MAINTENANCE AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE</i>	191
MNT-04: MAINTENANCE TOOLS	191
<i>MNT-04(A): MAINTENANCE TOOLS INSPECT TOOLS</i>	191
<i>MNT-04(B): MAINTENANCE TOOLS INSPECT MEDIA</i>	191
<i>MNT-04(C): MAINTENANCE TOOLS PREVENT UNAUTHORIZED REMOVAL</i>	192
<i>MNT-04(D): MAINTENANCE TOOLS RESTRICT TOOL USE</i>	192
MNT-05: NON-LOCAL MAINTENANCE	192
<i>MNT-05(A): NON-LOCAL MAINTENANCE AUDITING</i>	193
<i>MNT-05(B): NON-LOCAL MAINTENANCE NOTIFICATION OF NON-LOCAL MAINTENANCE</i>	193
<i>MNT-05(C): NON-LOCAL MAINTENANCE CRYPTOGRAPHIC PROTECTION</i>	193
<i>MNT-05(D): NON-LOCAL MAINTENANCE REMOTE DISCONNECT VERIFICATION</i>	193

MNT-05(E): NON-LOCAL MAINTENANCE PRE-APPROVAL OF NON-LOCAL MAINTENANCE	193
MNT-05(F): NON-LOCAL MAINTENANCE COMPARABLE SECURITY & SANITIZATION	194
MNT-06: MAINTENANCE PERSONNEL	194
MNT-06(A): MAINTENANCE PERSONNEL MAINTENANCE PERSONNEL WITHOUT APPROPRIATE ACCESS	194
MNT-06(B): MAINTENANCE PERSONNEL NON-SYSTEM RELATED MAINTENANCE	195
MOBILE DEVICE MANAGEMENT (MDM)	196
MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES	196
MDM-02: ACCESS CONTROL FOR MOBILE DEVICES	196
MDM-03: FULL DEVICE & CONTAINER-BASED ENCRYPTION	197
MDM-04: TAMPER PROTECTION & DETECTION	197
MDM-05: REMOTE PURGING	198
MDM-06: PERSONALLY-OWNED MOBILE DEVICES	198
MDM-07: ORGANIZATION-OWNED MOBILE DEVICES	199
MDM-08: MOBILE DEVICE DATA RETENTION LIMITATIONS	199
NETWORK SECURITY (NET)	200
NET-01: NETWORK SECURITY MANAGEMENT	200
NET-02: LAYERED DEFENSES	200
NET-02(A): LAYERED DEFENSES DENIAL OF SERVICE (DOS) PROTECTION	200
NET-02(B): LAYERED DEFENSES GUEST NETWORKS	200
NET-03: BOUNDARY PROTECTION	201
NET-03(A): BOUNDARY PROTECTION ACCESS POINTS	202
NET-03(B): BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES	202
NET-03(C): BOUNDARY PROTECTION PREVENT DISCOVERY OF INTERNAL INFORMATION	202
NET-03(D): BOUNDARY PROTECTION PERSONAL DATA (PD)	202
NET-03(E): BOUNDARY PROTECTION PREVENT UNAUTHORIZED EXFILTRATION	203
NET-03(F): BOUNDARY PROTECTION DYNAMIC ISOLATION & SEGREGATION (SANDBOXING)	203
NET-03(G): BOUNDARY PROTECTION ISOLATION OF INFORMATION SYSTEM COMPONENTS (DMZ)	203
NET-03(H): BOUNDARY PROTECTION SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	204
NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)	204
NET-04(A): DATA FLOW ENFORCEMENT DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION	205
NET-04(B): DATA FLOW ENFORCEMENT OBJECT SECURITY ATTRIBUTES	205
NET-04(C): DATA FLOW ENFORCEMENT CONTENT CHECK FOR ENCRYPTED DATA	205
NET-04(D): DATA FLOW ENFORCEMENT EMBEDDED DATA TYPES	205
NET-04(E): DATA FLOW ENFORCEMENT METADATA	205
NET-04(F): DATA FLOW ENFORCEMENT HUMAN REVIEWS	206
NET-04(G): DATA FLOW ENFORCEMENT SECURITY POLICY FILTERS	206
NET-04(H): DATA FLOW ENFORCEMENT DATA TYPE IDENTIFIERS	206
NET-04(I): DATA FLOW ENFORCEMENT DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS	207
NET-04(J): DATA FLOW ENFORCEMENT DETECTION OF UNSANCTIONED INFORMATION	207
NET-04(K): DATA FLOW ENFORCEMENT APPROVED SOLUTIONS	207
NET-05: SYSTEM INTERCONNECTIONS	208
NET-05(A): SYSTEM INTERCONNECTIONS EXTERNAL SYSTEM CONNECTIONS	208
NET-05(B): SYSTEM INTERCONNECTIONS INTERNAL SYSTEM CONNECTIONS	208
NET-06: NETWORK SEGMENTATION	209
NET-06(A): SECURITY FUNCTION ISOLATION SECURITY MANAGEMENT SUBNETS	209
NET-06(B): SECURITY FUNCTION ISOLATION VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION	209
NET-07: NETWORK DISCONNECT	209
NET-08: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS / NIPS)	210
NET-08(A): NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS / NIPS) DMZ NETWORKS	210
NET-08(B): NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS / NIPS) WIRELESS INTRUSION DETECTION / PREVENTION SYSTEMS (WIDS / WIPS)	210
NET-09: SESSION AUTHENTICITY	210
NET-09(A): SESSION AUTHENTICITY INVALIDATE SESSION IDENTIFIERS AT LOGOUT	211
NET-10 DOMAIN NAME SERVICE (DNS) RESOLUTION	211
NET-10(A): DOMAIN NAME SERVICE (DNS) RESOLUTION ARCHITECTURE & PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	211
NET-10(B): DOMAIN NAME SERVICE (DNS) RESOLUTION SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	212

NET-11: OUT-OF-BAND CHANNELS	212
NET-12: SAFEGUARDING DATA OVER OPEN NETWORKS	212
NET-12(A): SAFEGUARDING DATA OVER OPEN NETWORKS WIRELESS LINK PROTECTION	212
NET-12(B): SAFEGUARDING DATA OVER OPEN NETWORKS END-USER MESSAGING TECHNOLOGIES	213
NET-13: ELECTRONIC MESSAGING	213
NET-14: REMOTE ACCESS	213
NET-14(A): REMOTE ACCESS AUTOMATED MONITORING & CONTROL	214
NET-14(B): REMOTE ACCESS PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION	214
NET-14(C): REMOTE ACCESS MANAGED ACCESS CONTROL POINTS	214
NET-14(D): REMOTE ACCESS PRIVILEGED COMMANDS & ACCESS	214
NET-14(E): REMOTE ACCESS TELECOMMUTING	215
NET-14(F): REMOTE ACCESS THIRD-PARTY REMOTE ACCESS GOVERNANCE	215
NET-14(G): REMOTE ACCESS ENDPOINT SECURITY VALIDATION	215
NET-14(H): REMOTE ACCESS EXPEDITIOUS DISCONNECT / DISABLE CAPABILITY	215
NET-15: WIRELESS NETWORKING	215
NET-15(A): WIRELESS ACCESS AUTHENTICATION & ENCRYPTION	216
NET-15(B): WIRELESS ACCESS DISABLE WIRELESS NETWORKING	216
NET-15(C): WIRELESS ACCESS RESTRICT CONFIGURATION BY USERS	216
NET-15(D): WIRELESS ACCESS WIRELESS BOUNDARIES	216
NET-15(E): WIRELESS ACCESS ROGUE WIRELESS DETECTION	217
NET-16: INTRANETS	217
NET-17: DATA LOSS PREVENTION (DLP)	217
NET-18: CONTENT FILTERING	218
NET-18(A): CONTENT FILTERING ROUTE TRAFFIC TO PROXY SERVERS	218
PHYSICAL & ENVIRONMENTAL SECURITY (PES)	219
PES-01: PHYSICAL & ENVIRONMENTAL PROTECTIONS	219
PES-02: PHYSICAL ACCESS AUTHORIZATIONS	219
PES-02(A): PHYSICAL ACCESS AUTHORIZATIONS ROLE-BASED PHYSICAL ACCESS	219
PES-03: PHYSICAL ACCESS CONTROL	220
PES-03(A): PHYSICAL ACCESS CONTROL CONTROLLED INGRESS & EGRESS POINTS	220
PES-03(B): PHYSICAL ACCESS CONTROL LOCKABLE PHYSICAL CASINGS	221
PES-03(C): PHYSICAL ACCESS CONTROL PHYSICAL ACCESS LOGS	221
PES-03(D): PHYSICAL ACCESS CONTROL ACCESS TO INFORMATION SYSTEMS	221
PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES	222
PES-04(A): PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES WORKING IN SECURE AREAS	222
PES-05: MONITORING PHYSICAL ACCESS	222
PES-05(A): MONITORING PHYSICAL ACCESS INTRUSION ALARMS / SURVEILLANCE EQUIPMENT	223
PES-05(B): MONITORING PHYSICAL ACCESS MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS	223
PES-06: VISITOR CONTROL	223
PES-06(A): VISITOR CONTROL DISTINGUISH VISITORS FROM ON-SITE PERSONNEL	224
PES-06(B): VISITOR CONTROL IDENTIFICATION REQUIREMENT	224
PES-06(C): VISITOR CONTROL RESTRICT UNESCORTED ACCESS	224
PES-06(D): VISITOR CONTROL AUTOMATED RECORDS MANAGEMENT & REVIEW	224
PES-07: SUPPORTING UTILITIES	224
PES-07(A): SUPPORTING UTILITIES AUTOMATIC VOLTAGE CONTROLS	225
PES-07(B): SUPPORTING UTILITIES EMERGENCY SHUTOFF	225
PES-07(C): SUPPORTING UTILITIES EMERGENCY POWER	225
PES-07(D): SUPPORTING UTILITIES EMERGENCY LIGHTING	225
PES-07(E): SUPPORTING UTILITIES WATER DAMAGE PROTECTION	225
PES-07(F): SUPPORTING UTILITIES AUTOMATION SUPPORT FOR WATER DAMAGE PROTECTION	226
PES-08: FIRE PROTECTION	226
PES-08(A): FIRE PROTECTION FIRE DETECTION DEVICES	226
PES-08(B): FIRE PROTECTION FIRE SUPPRESSION DEVICES	226
PES-08(C): FIRE PROTECTION AUTOMATIC FIRE SUPPRESSION	226
PES-09: TEMPERATURE & HUMIDITY CONTROLS	227
PES-09(A): TEMPERATURE & HUMIDITY CONTROLS MONITORING WITH ALARMS / NOTIFICATIONS	227
PES-10: DELIVERY & REMOVAL	227
PES-11: ALTERNATE WORK SITE	227

PES-12: EQUIPMENT SITING & PROTECTION	228
<i>PES-12(A): EQUIPMENT SITING & PROTECTION ACCESS CONTROL FOR TRANSMISSION MEDIUM</i>	228
<i>PES-12(B): EQUIPMENT SITING & PROTECTION ACCESS CONTROL FOR OUTPUT DEVICES</i>	228
PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS	229
PES-14: ASSET MONITORING AND TRACKING	229
PES-15: ELECTROMAGNETIC PULSE (EMP) PROTECTION	229
PES-16: COMPONENT MARKING	230
PRIVACY (PRI)	231
PRI-01: PRIVACY PROGRAM	231
<i>PRI-01(A): PRIVACY PROGRAM CHIEF PRIVACY OFFICER (CPO)</i>	231
<i>PRI-01(B): PRIVACY PROGRAM PRIVACY ACT STATEMENTS [DEPRECATED – WITHDRAWN FROM DSP]</i>	231
<i>PRI-01(C): PRIVACY PROGRAM DISSEMINATION OF PRIVACY PROGRAM INFORMATION</i>	231
<i>PRI-01(D): PRIVACY PROGRAM DATA PROTECTION OFFICER (DPO)</i>	231
PRI-02: PRIVACY NOTICE	232
<i>PRI-02(A): PRIVACY NOTICE PURPOSE SPECIFICATION</i>	232
<i>PRI-02(B): PRIVACY NOTICE AUTOMATED DATA MANAGEMENT PROCESSES</i>	232
<i>PRI-02(C): PRIVACY NOTICE COMPUTER MATCHING AGREEMENTS (CMA)</i>	233
PRI-03: CHOICE & CONSENT	233
<i>PRI-03(A): CHOICE & CONSENT ATTRIBUTE MANAGEMENT</i>	233
<i>PRI-03(B): CHOICE & CONSENT JUST-IN-TIME NOTICE & UPDATED CONSENT</i>	233
<i>PRI-03(C): CHOICE & CONSENT PROHIBITION OF SELLING PERSONAL DATA</i>	233
PRI-04: COLLECTION	234
<i>PRI-04(A): COLLECTION AUTHORITY TO COLLECT, USE, MAINTAIN & SHARE PERSONAL DATA (PD)</i>	234
PRI-05: USE, RETENTION & DISPOSAL	234
<i>PRI-05(A): USE, RETENTION & DISPOSAL INTERNAL USE</i>	234
<i>PRI-05(B): USE, RETENTION & DISPOSAL DATA INTEGRITY</i>	234
<i>PRI-05(C): USE, RETENTION & DISPOSAL DATA MASKING</i>	235
<i>PRI-05(D): USE, RETENTION & DISPOSAL USAGE RESTRICTIONS OF PERSONAL DATA (PD)</i>	235
<i>PRI-05(E): USE, RETENTION & DISPOSAL INVENTORY OF PERSONAL DATA (PD)</i>	235
<i>PRI-05(F): USE, RETENTION & DISPOSAL PERSONAL DATA (PD) INVENTORY AUTOMATION SUPPORT</i>	235
PRI-06: DATA SUBJECT ACCESS	236
<i>PRI-06(A): DATA SUBJECT ACCESS REDRESS INACCURATE INFORMATION</i>	236
<i>PRI-06(B): DATA SUBJECT ACCESS NOTICE OF CORRECTION OR PROCESSING CHANGE</i>	236
<i>PRI-06(C): DATA SUBJECT ACCESS APPEAL ADVERSE DECISION</i>	236
<i>PRI-06(D): DATA SUBJECT ACCESS USER FEEDBACK MANAGEMENT</i>	236
<i>PRI-06(E): DATA SUBJECT ACCESS RIGHT TO ERASURE</i>	237
<i>PRI-06(F): DATA SUBJECT ACCESS DATA PORTABILITY</i>	237
<i>PRI-06(G): DATA SUBJECT ACCESS PERSONAL DATA EXPORTABILITY</i>	237
PRI-07: INFORMATION SHARING WITH THIRD PARTIES	237
<i>PRI-07(A): INFORMATION SHARING WITH THIRD PARTIES PRIVACY REQUIREMENTS FOR CONTRACTORS & SERVICE PROVIDERS</i>	238
<i>PRI-07(B): INFORMATION SHARING WITH THIRD PARTIES JOINT PROCESSING OF PERSONAL DATA</i>	238
<i>PRI-07(C): INFORMATION SHARING WITH THIRD PARTIES OBLIGATION TO INFORM THIRD PARTIES</i>	238
<i>PRI-07(D): INFORMATION SHARING WITH THIRD PARTIES REJECT UNAUTHORIZED DISCLOSURE REQUESTS</i>	238
PRI-08: TESTING, TRAINING & MONITORING	239
PRI-09: PERSONAL DATA LINEAGE	239
PRI-10: DATA QUALITY MANAGEMENT	240
<i>PRI-10(A): DATA QUALITY MANAGEMENT AUTOMATION</i>	240
<i>PRI-10(B): DATA QUALITY MANAGEMENT DATA ANALYTICS BIAS</i>	240
PRI-11: DATA TAGGING	240
PRI-12: UPDATING PERSONAL DATA (PD)	241
PRI-13: DATA MANAGEMENT BOARD	241
PRI-14: PRIVACY RECORDS & REPORTING	241
<i>PRI-14(A): PRIVACY RECORDS & REPORTING ACCOUNTING OF DISCLOSURES</i>	242
<i>PRI-14(B): PRIVACY RECORDS & REPORTING NOTIFICATION OF DISCLOSURE REQUEST TO DATA SUBJECT</i>	242
PRI-15: REGISTER DATABASE	242
PROJECT & RESOURCE MANAGEMENT (PRM)	243
PRM-01: SECURITY PORTFOLIO MANAGEMENT	243

PRM-01(A): SECURITY PORTFOLIO MANAGEMENT STRATEGIC PLAN & OBJECTIVES	243
PRM-01(B): SECURITY PORTFOLIO MANAGEMENT TARGETED CAPABILITY MATURITY LEVELS	243
PRM-02: SECURITY & PRIVACY RESOURCE MANAGEMENT	243
PRM-03: ALLOCATION OF RESOURCES	244
PRM-04: SECURITY & PRIVACY IN PROJECT MANAGEMENT	244
PRM-05: SECURITY & PRIVACY REQUIREMENTS DEFINITION	244
PRM-06: BUSINESS PROCESS DEFINITION	245
PRM-07: SECURE DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT	245
PRM-08: MANAGE ORGANIZATIONAL KNOWLEDGE	245
RISK MANAGEMENT (RSK)	246
RSK-01: RISK MANAGEMENT PROGRAM	246
RSK-01(A): RISK MANAGEMENT PROGRAM (RMP) RISK FRAMING	246
RSK-02: RISK-BASED SECURITY CATEGORIZATION	247
RSK-03: RISK IDENTIFICATION	247
RSK-04: RISK ASSESSMENT	247
RSK-04(A): RISK ASSESSMENT RISK REGISTER	248
RSK-05: RISK RANKING	248
RSK-06: RISK REMEDIATION	248
RSK-06(A): RISK REMEDIATION RISK RESPONSE	248
RSK-07: RISK ASSESSMENT UPDATE	249
RSK-08: BUSINESS IMPACT ANALYSIS (BIAS)	249
RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM)	249
RSK-09(A): SUPPLY CHAIN RISK MANAGEMENT (SCRM) SUPPLY CHAIN RISK ASSESSMENT	250
RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)	250
SECURE ENGINEERING & ARCHITECTURE (SEA)	252
SEA-01: SECURE ENGINEERING PRINCIPLES	252
SEA-01(A): SECURE ENGINEERING PRINCIPLES CENTRALIZED MANAGEMENT OF CYBERSECURITY & PRIVACY CONTROLS	253
SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE	253
SEA-02(A): ALIGNMENT WITH ENTERPRISE ARCHITECTURE STANDARDIZED TERMINOLOGY	253
SEA-03: DEFENSE-IN-DEPTH (DID) ARCHITECTURE	253
SEA-03(A): DEFENSE-IN-DEPTH (DID) ARCHITECTURE SYSTEM PARTITIONING	254
SEA-03(B): DEFENSE-IN-DEPTH (DID) ARCHITECTURE APPLICATION PARTITIONING	254
SEA-04: PROCESS ISOLATION	254
SEA-04(A): PROCESS ISOLATION SECURITY FUNCTION ISOLATION	255
SEA-04(B): PROCESS ISOLATION HARDWARE SEPARATION	255
SEA-04(C): PROCESS ISOLATION THREAD SEPARATION	255
SEA-05: INFORMATION IN SHARED RESOURCES	256
SEA-06: PREVENT PROGRAM EXECUTION	256
SEA-07: PREDICTABLE FAILURE ANALYSIS	256
SEA-07(A): PREDICTABLE FAILURE ANALYSIS TECHNOLOGY LIFECYCLE MANAGEMENT	256
SEA-07(B): PREDICTABLE FAILURE ANALYSIS FAIL SECURE	257
SEA-07(C): PREDICTABLE FAILURE ANALYSIS FAIL SAFE	257
SEA-08: NON-PERSISTENCE	257
SEA-08(A): NON-PERSISTENCE REFRESH FROM TRUSTED SOURCES	258
SEA-09: INFORMATION OUTPUT FILTERING	258
SEA-09(A): INFORMATION OUTPUT FILTERING LIMIT PERSONAL DATA (PD) DISSEMINATION	258
SEA-10: MEMORY PROTECTION	258
SEA-11: HONEYPOTS	259
SEA-12: HONEYCLIENTS	259
SEA-13: HETEROGENEITY	259
SEA-13(A): HETEROGENEITY VIRTUALIZATION TECHNIQUES	260
SEA-14: CONCEALMENT & MISDIRECTION	260
SEA-14(A): CONCEALMENT & MISDIRECTION RANDOMNESS	260
SEA-14(B): CONCEALMENT & MISDIRECTION CHANGE PROCESSING & STORAGE LOCATIONS	261
SEA-15: DISTRIBUTED PROCESSING & STORAGE	261
SEA-16: NON-MODIFIABLE EXECUTABLE PROGRAMS	261
SEA-17: SECURE LOG-ON PROCEDURES	261
SEA-18: SYSTEM USE NOTIFICATION (LOGON BANNER)	262

SEA-18(A): SYSTEM USE NOTIFICATION STANDARDIZED MICROSOFT WINDOWS BANNER	262
SEA-18(B): SYSTEM USE NOTIFICATION TRUNCATED BANNER	262
SEA-19: PREVIOUS LOGON NOTIFICATION	263
SEA-20: CLOCK SYNCHRONIZATION	263
SECURITY OPERATIONS (OPS)	264
OPS-01: OPERATIONS SECURITY	264
<i>OPS-01(A): OPERATIONS SECURITY STANDARDIZED OPERATING PROCEDURES (SOP)</i>	264
OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)	265
OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)	265
OPS-04: SECURITY OPERATIONS CENTER (SOC)	265
SECURITY AWARENESS & TRAINING (SAT)	266
SAT-01: SECURITY & PRIVACY-MINDED WORKFORCE	266
SAT-02: SECURITY & PRIVACY AWARENESS	267
<i>SAT-02(A): SECURITY AWARENESS PRACTICAL EXERCISES</i>	267
<i>SAT-02(B): SECURITY AWARENESS SOCIAL ENGINEERING & MINING</i>	267
SAT-03: SECURITY & PRIVACY TRAINING	267
<i>SAT-03(A): SECURITY & PRIVACY TRAINING PRACTICAL EXERCISES</i>	268
<i>SAT-03(B): SECURITY & PRIVACY TRAINING SUSPICIOUS COMMUNICATIONS & ANOMALOUS SYSTEM BEHAVIOR</i>	268
<i>SAT-03(C): SECURITY & PRIVACY TRAINING SENSITIVE INFORMATION STORAGE, HANDLING & PROCESSING</i>	268
<i>SAT-03(D): SECURITY & PRIVACY TRAINING VENDOR SECURITY TRAINING</i>	268
<i>SAT-03(E): SECURITY & PRIVACY TRAINING PRIVILEGED USERS</i>	269
SAT-04: SECURITY & PRIVACY TRAINING RECORDS	269
TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA)	270
TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION	270
<i>TDA-01(A): TECHNOLOGY DEVELOPMENT & ACQUISITION PRODUCT MANAGEMENT</i>	270
<i>TDA-01(B): TECHNOLOGY DEVELOPMENT & ACQUISITION INTEGRITY MECHANISMS FOR SOFTWARE / FIRMWARE UPDATES</i>	271
<i>TDA-01(C): TECHNOLOGY DEVELOPMENT & ACQUISITION MALWARE TESTING PRIOR TO RELEASE</i>	271
TDA-02: SECURITY REQUIREMENTS	271
<i>TDA-02(A): SECURITY REQUIREMENTS PORTS, PROTOCOLS & SERVICES IN USE</i>	271
<i>TDA-02(B): SECURITY REQUIREMENTS USE OF APPROVED PIV PRODUCTS</i>	272
<i>TDA-02(C): SECURITY REQUIREMENTS DEVELOPMENT METHODS, TECHNIQUES & PROCESSES</i>	272
TDA-03: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS	272
<i>TDA-03(A): COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS SUPPLIER DIVERSITY</i>	272
TDA-04: DOCUMENTATION REQUIREMENTS	272
<i>TDA-04(A): DOCUMENTATION REQUIREMENTS FUNCTIONAL PROPERTIES</i>	273
TDA-05: DEVELOPER ARCHITECTURE & DESIGN	273
TDA-06: SECURE CODING	274
<i>TDA-06(A): SECURE CODING CRITICALITY ANALYSIS</i>	274
TDA-07: SECURE DEVELOPMENT ENVIRONMENTS	275
TDA-08: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS	275
TDA-09: SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT	275
<i>TDA-09(A): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT CONTINUOUS MONITORING PLAN</i>	276
<i>TDA-09(B): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT STATIC CODE ANALYSIS</i>	276
<i>TDA-09(C): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT DYNAMIC CODE ANALYSIS</i>	276
<i>TDA-09(D): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT MALFORMED INPUT TESTING</i>	277
<i>TDA-09(E): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT APPLICATION PENETRATION TESTING</i>	277
TDA-10: USE OF LIVE DATA	277
<i>TDA-10(A): USE OF LIVE DATA TEST DATA INTEGRITY</i>	278
TDA-11: COMPONENT AUTHENTICITY	278
<i>TDA-11(A): COMPONENT AUTHENTICITY ANTI-COUNTERFEIT TRAINING</i>	278
<i>TDA-11(B): COMPONENT AUTHENTICITY COMPONENT DISPOSAL</i>	278
TDA-12: CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	279
TDA-13: DEVELOPER SCREENING	279
TDA-14: DEVELOPER CONFIGURATION MANAGEMENT	279
<i>TDA-14(A): DEVELOPER CONFIGURATION MANAGEMENT SOFTWARE / FIRMWARE INTEGRITY VERIFICATION</i>	279
TDA-15: DEVELOPER THREAT ANALYSIS & FLAW REMEDIATION	280
TDA-16: DEVELOPER-PROVIDED TRAINING	280

TDA-17: UNSUPPORTED SYSTEMS	280
<i>TDA-17(A): UNSUPPORTED SYSTEMS ALTERNATE SOURCES FOR CONTINUED SUPPORT</i>	281
TDA-18: INPUT DATA VALIDATION	281
TDA-19: ERROR HANDLING	281
TDA-20: ACCESS TO PROGRAM SOURCE CODE	282
THIRD-PARTY MANAGEMENT (TPM)	283
TPM-01: THIRD-PARTY MANAGEMENT	283
TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS	283
TPM-03: SUPPLY CHAIN PROTECTION	283
<i>TPM-03(A): SUPPLY CHAIN PROTECTION ACQUISITION STRATEGIES, TOOLS & METHODS</i>	284
<i>TPM-03(B): SUPPLY CHAIN PROTECTION LIMIT POTENTIAL HARM</i>	284
<i>TPM-03(C): SUPPLY CHAIN PROTECTION PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES</i>	284
TPM-04: THIRD-PARTY SERVICES	285
<i>TPM-04(A): THIRD-PARTY SERVICES THIRD-PARTY RISK ASSESSMENTS & APPROVALS</i>	285
<i>TPM-04(B): THIRD-PARTY SERVICES IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS & SERVICES</i>	286
<i>TPM-04(C): THIRD-PARTY SERVICES CONFLICT OF INTERESTS</i>	286
<i>TPM-04(D): THIRD-PARTY SERVICES THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS</i>	286
TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS	287
TPM-06: THIRD-PARTY PERSONNEL SECURITY	287
TPM-07: MONITORING FOR THIRD-PARTY INFORMATION DISCLOSURE	288
TPM-08: REVIEW OF THIRD-PARTY SERVICES	288
TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION	288
TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES	288
TPM-11: THIRD-PARTY INCIDENT RESPONSE & RECOVERY CAPABILITIES	289
THREAT MANAGEMENT (THR)	290
THR-01: THREAT AWARENESS PROGRAM	290
THR-02: INDICATORS OF EXPOSURE (IOE)	290
THR-03: THREAT INTELLIGENCE FEEDS	290
THR-04: INSIDER THREAT PROGRAM	291
THR-05: INSIDER THREAT AWARENESS	291
VULNERABILITY & PATCH MANAGEMENT (VPM)	292
VPM-01: VULNERABILITY & PATCH MANAGEMENT PROGRAM	292
<i>VPM-01(A): VULNERABILITY & PATCH MANAGEMENT PROGRAM ESTABLISH VULNERABILITY MANAGEMENT SCOPE</i>	292
VPM-02: VULNERABILITY REMEDIATION PROCESS	292
VPM-03: VULNERABILITY RANKING	292
VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES	293
<i>VPM-04(A): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES STABLE VERSIONS</i>	293
<i>VPM-04(B): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES FLAW REMEDIATION WITH PERSONAL DATA (PD)</i>	293
VPM-05: SOFTWARE PATCHING	294
<i>VPM-05(A): SOFTWARE PATCHING CENTRALIZED MANAGEMENT</i>	294
<i>VPM-05(B): SOFTWARE PATCHING AUTOMATED REMEDIATION STATUS</i>	295
<i>VPM-05(C): SOFTWARE PATCHING TIME TO REMEDIATE / BENCHMARKS FOR CORRECTIVE ACTION</i>	295
<i>VPM-05(D): SOFTWARE PATCHING AUTOMATED SOFTWARE & FIRMWARE UPDATES</i>	295
<i>VPM-05(E): SOFTWARE PATCHING REMOVAL OF PREVIOUS VERSIONS</i>	295
VPM-06: VULNERABILITY SCANNING	296
<i>VPM-06(A): VULNERABILITY SCANNING UPDATE TOOL CAPABILITY</i>	296
<i>VPM-06(B): VULNERABILITY SCANNING BREADTH / DEPTH OF COVERAGE</i>	297
<i>VPM-06(C): VULNERABILITY SCANNING PRIVILEGED ACCESS</i>	297
<i>VPM-06(D): VULNERABILITY SCANNING TREND ANALYSIS</i>	297
<i>VPM-06(E): VULNERABILITY SCANNING REVIEW HISTORICAL AUDIT LOGS</i>	297
<i>VPM-06(F): VULNERABILITY SCANNING EXTERNAL VULNERABILITY ASSESSMENT SCANS</i>	297
<i>VPM-06(G): VULNERABILITY SCANNING INTERNAL VULNERABILITY ASSESSMENT SCANS</i>	298
<i>VPM-06(H): VULNERABILITY SCANNING ACCEPTABLE DISCOVERABLE INFORMATION</i>	298
<i>VPM-06(I): VULNERABILITY SCANNING CORRELATE SCANNING INFORMATION</i>	298
VPM-07: PENETRATION TESTING	298
<i>VPM-07(A): PENETRATION TESTING INDEPENDENT PENETRATION AGENT OR TEAM</i>	299
VPM-08: TECHNICAL SURVEILLANCE COUNTERMEASURES SECURITY	299

VPM-09: REVIEWING VULNERABILITY SCANNER USAGE	299
VPM-10: RED TEAM EXERCISES	300
WEB SECURITY (WEB)	301
WEB-01: WEB SECURITY	301
WEB-02: USE OF DEMILITARIZED ZONES (DMZ)	301
WEB-03: WEB APPLICATION FIREWALL (WAF)	301
WEB-04: CLIENT-FACING WEB SERVICES	302
WEB-05: COOKIE MANAGEMENT	302
WEB-06: STRONG CUSTOMER AUTHENTICATION (SCA)	302
GLOSSARY: ACRONYMS & DEFINITIONS	303
ACRONYMS	303
DEFINITIONS	303
KEY WORD INDEX	304
RECORD OF CHANGES	305

EXAMPLE

NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a data-centric, holistic approach to securely designing, building and maintaining ACME Business Consulting, LLC (ACME)'s systems, applications and services to protect its data, regardless of where it is stored, transmitted or processed. The following external content is a non-exhaustive list of frameworks that either support the implementation of or are referenced by the Digital Security Program (DSP):

- The National Institute of Standards and Technology (NIST):¹
 - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
 - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
 - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
 - NIST SP 800-64: *Security Considerations in Secure Development Life Cycle*
 - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personal Data (PD)*
 - NIST SP 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
 - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
 - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
 - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
 - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
 - NIST Framework for Improving Critical Cybersecurity (Cybersecurity Framework)
- The International Organization for Standardization (ISO):²
 - ISO/IEC 15288: *Systems and Software Engineering -- System Life Cycle Processes*
 - ISO/IEC 22301: *Societal Security – Business Continuity Management Systems – Requirements*
 - ISO/IEC 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
 - ISO/IEC 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personal Data (PD) in Public Clouds Acting as PD Processors*
 - ISO/IEC 27701: *Information Technology - Security Techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines*
- Other influencing frameworks (alphabetical order):
 - AuditScripts. *Open Threat Taxonomy*³
 - Center for Internet Security (CIS) Critical Security Controls (CSC)⁴
 - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)⁵
 - Control Objectives for Information and Related Technologies (COBIT)⁶
 - Defense Information Systems Agency (DISA) Secure Technology Implementation Guides (STIGs)⁷
 - Department of Defense Cybersecurity Maturity Model Certification (CMMC)⁸
 - European Union Regulation 2016/279 (General Data Protection Regulation (EU GDPR))⁹
 - Fair Information Practice Principles (FIPP)¹⁰
 - Generally Accepted Privacy Practices (GAPP)¹¹
 - Open Web Application Security Project (OWASP)¹²
 - Payment Card Industry Data Security Standard (PCI DSS)¹³
 - Privacy by Design (PbD)¹⁴

¹ National Institute of Standards and Technology - <http://csrc.nist.gov/publications/PubsSPs.html>

² International Organization for Standardization - <https://www.iso.org>

³ Open Threat Taxonomy - http://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

⁴ Center for Internet Security - <https://www.cisecurity.org/>

⁵ Cloud Security Alliance - <https://cloudsecurityalliance.org/>

⁶ COBIT - <http://www.isaca.org/COBIT/Pages/default.aspx>

⁷ DoD Information Security Agency - <https://public.cyber.mil/>

⁸ DoD Cybersecurity Maturity Model Certification - <https://www.acq.osd.mil/cmmc/index.html>

⁹ EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

¹⁰ Federal Trade Commission - <https://www.ftc.gov>

¹¹ The American Institute of CPAs - <http://www.aicpa.org>

¹² OWASP - https://www.owasp.org/index.php/Main_Page

¹³ Payment Card Industry Security Standards Council - <https://www.pcisecuritystandards.org/>

¹⁴ Term and principles coined by Dr. Ann Cavoukian - https://www.owasp.org/index.php/Privacy_by_Design

DIGITAL SECURITY PROGRAM (DSP) OVERVIEW

INTRODUCTION

The Digital Security Program (DSP) provides definitive information on the prescribed measures used to establish and enforce the security program at ACME Business Consulting, LLC (ACME).

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective cybersecurity is a team effort involving the participation and support of every ACME user who interacts with data and systems. Therefore, it is the responsibility of every user to know these policies and to conduct their activities accordingly.

Protecting company data and the systems that collect, process and maintain this information is of critical importance. Consequently, the security of systems must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.
- Safety – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

Commensurate with risk, security measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems. This also includes protection against accidental loss or destruction.

PURPOSE

The purpose of the Digital Security Program (DSP) is to prescribe a comprehensive framework for:

- Creating a leading practice-based Information Security Management System (ISMS);
- Protecting the confidentiality, integrity, availability and safety of ACME data and systems;
- Protecting ACME, its employees and its clients from illicit use of ACME systems and data;
- Ensuring the effectiveness of security controls over data and systems that support ACME's operations.
- Recognizing the highly-networked nature of the current computing environment and provide effective company-wide management and oversight of those related cybersecurity risks; and
- Providing for the development, review and maintenance of minimum security 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 users 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.

Some standards apply specifically to persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting ACME business functions shall comply with the standards. ACME departments shall 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 regards 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 shall be effective immediately upon approval by management unless otherwise stated.

POLICY OVERVIEW

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

The DSP 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 DSP requirements.

ACME users are required to 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 are required to submit a business justification for deviation from the standard in question.

UPDATES TO POLICIES & STANDARDS

Updates to the Digital Security Program (DSP) 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.

KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that ACME uses to define common cybersecurity terms.¹⁵ Key terminology to be aware of includes:

Adequate Security. A term describing protective measures that are commensurate with the consequences and probability of loss, misuse or unauthorized access to or modification of information.

Asset: A term describing any data, device, application, service or other component of the environment that supports information-related activities. An asset is a resource with economic value that a ACME owns or controls.

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, are used for the purposes intended and that information regarding the equipment is properly documented.

Cloud Computing. A term describing a technology infrastructure model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It also includes commercial offerings for Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Control: A term describing any management, operational or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help ACME accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align ACME with accepted due diligence and due care requirements.

Cybersecurity / Information Security: A term that covers the protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, Availability and Safety (CIAS) of data.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched or retrieved via electronic networks or other electronic data processing technologies. *Annex 1: Data Classification & Handling Guidelines* provides guidance on data classification and handling restrictions.

Data Controller. A term describing the privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing Personal Data (PD) other than natural persons who use data for personal purposes

Data Principle. A term describing the natural person to whom the Personal Data (PD) relates

Data Processor. A term describing the privacy stakeholder that processes Personal Data (PD) on behalf of and in accordance with the instructions of a PD controller

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation or use.

Information Technology (IT). A term includes computers, ancillary equipment (including imaging peripherals, input, output and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services) and related resources.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

¹⁵ NIST IR 7298 - <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf>

Personal Data / Personal Information (PD): A term describing any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.¹⁶

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Process Owner / Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, process or the data hosted on the asset or process. It does not mean that the asset belongs to the owner in a legal sense. Data / process owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained and used.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include sensitive Personal Data (sPD), Electronic Protected Health Information (ePHI) and all other forms of data classified as Restricted or Confidential in *Annex 1: Data Classification & Handling Guidelines*.

Sensitive Personal Data (sPD) / Sensitive Personal Information (sPI): A term describing personal data, revealing:

- The first name or first initial and last name, in combination with any one or more of the following data elements:¹⁷
 - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN);
 - Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.);
 - Financial account number; or
 - Payment card number (e.g., credit or debit card);
- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade-union membership;
- Physical or mental health;
- Sex life and sexual orientation;
- Genetic data; and / or
- Biometric data.¹⁸

Standard: A term describing formally established requirements in regard to processes, actions and configurations.

System: A term describing an asset; a system or network that can be defined, scoped and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls and mobile devices.

Target Audience: A term describing the intended group for which a control or standard is directed.

¹⁶ European Union General Data Protection Requirement – Article 4(1)

¹⁷ The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - https://www.oregonlegislature.gov/bills_laws/ors/ors646A.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 <http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf>

¹⁸ European Union General Data Protection Requirement – Article 9(1)

MANAGEMENT DIRECTION FOR INFORMATION SECURITY

The objective is to provide management direction and support for cybersecurity in accordance with business requirements and relevant laws and regulations.¹⁹

An Information Security Management System (ISMS) focuses on cybersecurity management and technology-related risks. The governing principle behind ACME's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with leading practices, ACME's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA) or Deming Cycle, approach:

- **Plan:** This phase involves designing the ISMS, assessing IT-related risks and selecting appropriate controls.
- **Do:** This phase involves implementing and operating the appropriate security controls.
- **Check:** This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- **Act:** This involves making changes, where necessary, to bring the ISMS back to optimal performance.

POLICIES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Information security documentation is comprised of five main parts: a core policy; a control objective that identifies desired conditions; measurable standards used to quantify the requirement; procedures that must be followed; and guidelines that are recommended, but not mandatory.

Cybersecurity documentation is comprised of six (6) main parts:

- (1) Core policy that establishes management's intent;
- (2) Control objective that identifies leading practices;
- (3) Standards that provides quantifiable requirements;
- (4) Controls identify desired conditions that are expected to be met;
- (5) Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
- (6) Guidelines are recommended, but not mandatory.

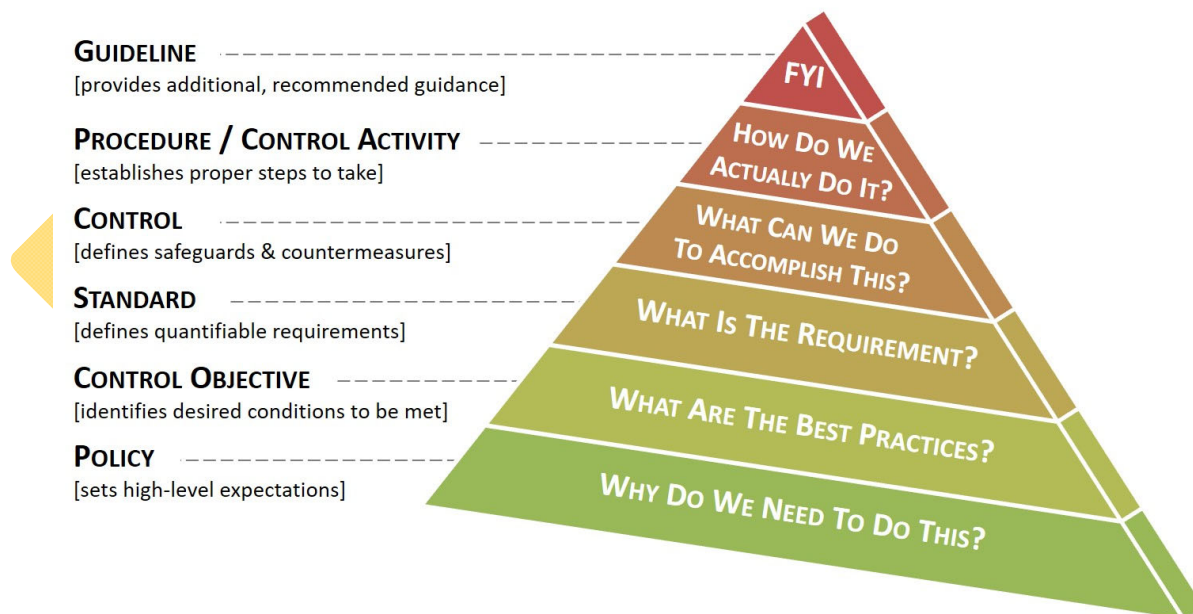


Figure 1: Information Security Documentation Framework

¹⁹ ISO 27002:2013 5.1

SECURITY & PRIVACY GOVERNANCE (GOV)

Management Intent: The purpose of the Security & Privacy Governance (GOV) policy is to specify the development, proactive management and ongoing review of ACME's security and privacy program.

Policy: ACME shall protect the confidentiality, integrity, availability and safety of its data and systems, regardless of how its data is created, distributed or stored. Digital 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, in accordance with all statutory, regulatory and contractual obligations.

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

GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide digital security policy, as well as associated standards, controls and procedures.²⁰

Standard: ACME's security program shall be represented in a single document, the Digital Security Program (DSP) that:

- (a) Shall 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 DSP together provide complete coverage for all cybersecurity and privacy-related controls employed within the organization.

GOV-02: PUBLISHING SECURITY & PRIVACY POLICIES

Control Objective: The organization establishes, publishes, maintains and disseminates security and privacy policies.²¹

Standard: ACME's security and privacy policies and standards shall be represented in a consolidated document, the Digital Security Program (DSP) that shall be:

- (a) Endorsed by executive management; and
- (b) Disseminated to the appropriate parties to ensure all ACME personnel understand their applicable requirements.

Guidelines: An organization's cybersecurity policies create the roadmap for implementing cybersecurity and privacy measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

GOV-03: PERIODIC REVIEW & UPDATE OF SECURITY & PRIVACY DOCUMENTATION

Control Objective: The organization reviews its security and privacy policies, standards and procedures at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.²²

Standard: ACME's business leadership (or other accountable business role or function) shall review the Digital Security Program (DSP) at planned intervals or as a result of changes to the organization (e.g., mergers, acquisitions, partnerships, new products, etc.) to ensure its continuing alignment with the security strategy, risk posture, effectiveness, accuracy, relevance and applicability to statutory, regulatory and / or contractual compliance obligations.

Guidelines: Updates to the DSP 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.

²⁰ NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.1

²¹ NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.1 | NIST CSF v1.1 ID.GV-1

²² NIST 800-53 rev4 PM-1 | ISO 27002:2013 5.1.2

CHANGE MANAGEMENT (CHG)

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security 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.

Policy: All technology changes to production environments must follow a standard process to reduce the risk associated with change. ACME requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network.

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

CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide change management policy, as well as associated standards, controls and procedures.⁸⁴

Standard: Data/process owners and asset custodians are required to test, validate and document changes to systems before implementing the changes on the production network.

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 privacy or any combination thereof.

CHG-02: CONFIGURATION CHANGE CONTROL

Control Objective: The organization follows change control processes and procedures for all changes to system components. The organization.⁸⁵

- Determines the types of changes to systems that are configuration controlled;
- Approves configuration-controlled changes to systems with explicit consideration for security impact analyses;
- Documents approved configuration-controlled changes to systems;
- Retains and reviews records of configuration-controlled changes to systems;
- Audits activities associated with configuration-controlled changes to systems; and
- Coordinates and provides oversight for configuration change control activities through an organization-defined configuration change control element (e.g., committee, board) that convenes on a routine basis.

Standard: Data/process owners and asset custodians are required to follow 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 PANs) 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;
 3. Functionality testing to verify that the change does not adversely impact the security of the system; and
- (f) Back-out procedures.
- (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

⁸⁴ NIST 800-53 rev4 CM-3 | ISO 27002:2013 12.1.2

⁸⁵ NIST 800-53 rev4 CM-3 | ISO 27002:2013 14.2.2 | NIST 800-171 rev1 3.4.3 | NIST CSF v1.1 PR.IP-3

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(A): CONFIGURATION CHANGE CONTROL | PROHIBITION OF CHANGES

Control Objective: The organization prohibits changes to systems until designated approvals are received.⁸⁶

Standard: Data/process owners and asset custodians are prohibited from implementing a change without first obtaining Pre-approval from the Change Control Board (CCB) and notifying all affected parties prior to the implementation of the change.

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

CHG-02(B): CONFIGURATION CHANGE CONTROL | TEST, VALIDATE & DOCUMENT CHANGES

Control Objective: The organization tests, validates and documents changes in a non-production environment before changes are implemented in a production environment.⁸⁷

Standard: Where technically feasible, asset custodians and data / process owners are required to test and validate configuration changes in a test environment, prior to deploying the change in the production environment.

Guidelines: When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. If it is not technically or logistically feasible to test a configuration change, compensating control should be identified and implemented in order to mitigate any negative impact to the production environment from an adverse change event. Compensating controls can include, but is not limited to:

- Images of systems;
- Backups of configurations;
- Viable back out plan;
- After-hours implementation; and
- Pilot / test group rollouts.

CHG-02(C): CONFIGURATION CHANGE CONTROL | SECURITY REPRESENTATIVE FOR CHANGE

Control Objective: The organization includes a cybersecurity representative in the configuration change control review process.⁸⁸

Standard: ACME's cybersecurity personnel are required to represent cybersecurity topics as a representative of ACME's Change Control Board (CCB).

Guidelines: Information security representatives can include, for example, system security officers or system security managers.

CHG-02(D): CONFIGURATION CHANGE CONTROL | AUTOMATED SECURITY RESPONSE

Control Objective: The information system implements organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.⁸⁹

Standard: Where technically feasible and justified by a valid business case, ACME shall:

- (a) Employ automated mechanisms that remediate non-conforming systems to ACME-approved baseline configurations; and
- (b) Alert incident response personnel to the possible security incident that generated the need to revert the configuration.

Guidelines: Security responses include, for example, halting information system processing, halting selected system functions or issuing alerts/notifications to organizational personnel when there is an unauthorized modification of a configuration item.

CHG-02(E): CONFIGURATION CHANGE CONTROL | CRYPTOGRAPHIC MANAGEMENT

Control Objective: The organization ensures that cryptographic mechanisms used to provide organization-defined security safeguards are under configuration management.⁹⁰

⁸⁶ NIST 800-53 rev4 CM-3(1)

⁸⁷ NIST 800-53 rev4 CM-3(2) | ISO 27002:2013 14.2.3

⁸⁸ NIST 800-53 rev4 CM-3(5)

⁸⁹ NIST 800-53 rev4 CM-3(4)

⁹⁰ NIST 800-53 rev4 CM-3(6)

DATA CLASSIFICATION & HANDLING (DCH)

Management Intent: The purpose of the Data Classification & Handling (DCH) policy is to ensure that technology assets 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 data.

Policy: In accordance with all applicable legal requirements, ACME shall protect data in both hardcopy and digital form by limiting access to authorized users and utilize methods of sanitizing or destroying 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 develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide data protection policy, as well as associated standards, controls and procedures.²⁰²

Standard: Data/process owners and asset custodians must:

- (a) In accordance with all applicable statutory, regulatory and contractual compliance obligations, implement and govern controls to protect ACME data wherever it is stored, transmitted and processed;
- (b) Define retention periods for both sensitive and non-sensitive data;
- (c) Dispose of, destroy, erase and / or anonymizes data once it is no longer necessary for business purposes;
- (d) Maintain strict control over the storage and accessibility of media; and
- (e) Maintain inventories of sensitive data under their 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(A): DATA PROTECTION | DATA STEWARDSHIP

Control Objective: The organization designates data with individual stewardship by assigned responsibilities that are defined, documented and communicated.

Standard: At least annually, data / process owner is required to assess the following criteria, as it pertains to their data and / or processes:

- (a) Data classification requirements;
- (b) System criticality;
- (c) Geographical storage and / or processing of the data; and
- (d) Applicable statutory, regulatory and contractual requirements.

Guidelines: A complete inventory of business-critical 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-02: DATA & ASSET CLASSIFICATION

Control Objective: The organization:²⁰³

- Categorizes systems and data in accordance with applicable local, state and Federal laws;
- Documents the security categorization results (including supporting rationale) in the security plan for systems; and
- Ensures the security categorization decision is reviewed and approved by the asset owner.

Standard: Assets must be classified in terms of system criticality and data sensitivity (see [Annex 4: Baseline Security Categorization Guidelines](#)). Data/process owners and asset custodians are required to:

- (a) Categorize the system and data; and
- (b) Where applicable, document the security categorization results (including supporting rationale) for the system.

²⁰² NIST 800-53 rev4 AR-7, DM-2, DM-2(b) & MP-1 | ISO 27002:2013 8.2, 8.3.3 & 18.1.4

²⁰³ ISO 27002:2013 8.2.1 | NIST CSF v1.1 ID.AM-5

Guidelines: Clearly defined authorization boundaries are a prerequisite for effective security categorization decisions. Security categories describe the potential adverse impacts on organizational operations, organizational assets and individuals if organizational information and systems are comprised through a loss of confidentiality, integrity or availability. Security categorization processes carried out by business units, facilitates the development of inventories of information assets mappings to specific system components where information is processed, stored or transmitted.

DCH-03: MEDIA ACCESS

Control Objective: The organization restricts access to types of digital and non-digital media to authorized individuals using organization-defined security measures.²⁰⁴

Standard: Data/process owners and asset custodians are required to restrict access to digital and non-digital media to authorized individuals.

Guidelines: System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external / removable hard drives, flash drives, compact disks and digital video disks. Non-digital media includes, for example, paper and microfilm. For media containing information determined by organizations to be in the public domain, to be publicly releasable or to have limited or no adverse impact on organizations or individuals if accessed by other than authorized personnel, fewer safeguards may be needed. In these situations, physical access controls may provide adequate protection.

DCH-03(A): MEDIA ACCESS | DISCLOSURE OF INFORMATION

Control Objective: The organization limits the disclosure of information to authorized parties.

Standard: ACME personnel, including ACME subcontractors, are prohibited from releasing any information, regardless of medium (e.g., voice, email, film, tape, document, etc.), pertaining to any part of a contract, project or program to anyone outside of ACME. The only exceptions are if:

- (a) The project's contracting officer has given prior written approval; or
- (b) The information is otherwise in the public domain before the date of release.

Guidelines: None

DCH-03(B): MEDIA ACCESS | MASKING DISPLAYED DATA

Control Objective: The organization applies data masking to sensitive information that is displayed or printed.

Standard: Sensitive information that is displayed or printed is required to be masked. This includes, but is not limited to:

- (a) Financial account numbers;
- (b) Social Security Numbers (SSN); and
- (c) Credit or debit Primary Account Numbers (PANs), where no more than the first six (6) / last four (4) digits are allowed to be shown.

Guidelines: Only personnel with a legitimate business need should be able to see more than the first six (6) / last four (4) of the PAN.

DCH-04: MEDIA MARKING

Control Objective: The organization marks media in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats and applicable security requirements.²⁰⁵

Standard: ACME users are required to mark media in accordance with ACME's Data & Asset Classification Standard.

Guidelines: Reference *Annex 1: Data Classification & Handling Guidelines* for examples of data classification and handling.

The term security marking refers to the application / use of human-readable security attributes. The term security labeling refers to the application / use of security attributes with regard to internal data structures within systems. System media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external / removable hard drives, flash drives,

²⁰⁴ NIST 800-53 rev4 MP-2 & MP-2(1) | NIST 800-171 rev1 3.8.1, 3.8.2 & 3.8.3

²⁰⁵ NIST 800-53 rev4 MP-3 | ISO 27002:2013 8.2.2 | NIST 800-171 rev1 3.8.4

Standard: Where technically feasible and justified by a valid business case, ACME shall employ an automatic fire suppression capability in its data center environments where sensitive data and/or critical systems are located.

Guidelines: None

PES-09: TEMPERATURE & HUMIDITY CONTROLS

Control Objective: The organization:⁵⁰⁸

- Maintains temperature and humidity levels within the facility; and
- Monitors temperature and humidity levels.

Standard: In data center environments, asset custodians are required to employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Guidelines: Temperature and humidity controls typically apply to facilities containing concentrations of system resources, for example, data centers, server rooms and mainframe computer rooms.

PES-09(A): TEMPERATURE & HUMIDITY CONTROLS | MONITORING WITH ALARMS / NOTIFICATIONS

Control Objective: The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.⁵⁰⁹

Standard: Where technically feasible, ACME shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

Guidelines: None

PES-10: DELIVERY & REMOVAL

Control Objective: The organization uses controlled access points to isolate information processing facilities for points, such as delivery and loading areas, to avoid unauthorized access.⁵¹⁰

Standard: Systems are prohibited from being removed from ACME facilities without prior, management authorization. Prior to the removal of the system, the following information needs to be captured:

- (a) Make / model / serial # of the asset;
- (b) Owner of the asset;
- (c) Reason the asset is being removed from the facility;
- (d) Company and name of representative removing the asset; and
- (e) Estimated return date for the asset, if applicable.

Guidelines: Effectively enforcing authorizations for entry and exit of system components may require restricting access to delivery areas and possibly isolating the areas from the system and media libraries.

PES-11: ALTERNATE WORK SITE

Control Objective: The organization.⁵¹¹

- Employs organization-defined management, operational and technical system security controls at alternate work sites;
- Assesses as feasible, the effectiveness of security controls at alternate work sites; and
- Provides a means for employees to communicate with cybersecurity personnel in case of security incidents or problems.

Standard: ACME management is required to develop plans regarding alternate work sites that include:

- (a) System security controls at alternate work sites;
- (b) The effectiveness of security controls at alternate work sites; and

⁵⁰⁸ NIST 800-53 rev4 PE-14 |

⁵⁰⁹ NIST 800-53 rev4 PE-14(2)

⁵¹⁰ NIST 800-53 rev4 PE-16 | ISO 27002:2013 11.1.6

⁵¹¹ NIST 800-53 rev4 PE-17 | NIST 800-171 rev1 3.10.6

PRI-06: DATA SUBJECT ACCESS

Control Objective: The organization provides individuals with access to their personal information for review and update.⁵³⁰

Standard: ACME must implement mechanisms to grant identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to the data subject consistent with the entity's privacy commitments and system requirements. If access is denied, the data subject must be informed of the denial and reason for such denial, as required, consistent with ACME's privacy commitments and system requirements.

Guidelines: Access includes timely, simplified and inexpensive access to data. Organizational processes for allowing access to records may differ based on resources, legal requirements or other factors. Legal counsel should be consulted for record request processing.

PRI-06(A): DATA SUBJECT ACCESS | REDRESS INACCURATE INFORMATION

Control Objective: The organization establishes and implements a process for:⁵³¹

- Individuals to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and
- Disseminating corrections or amendments of PD to other authorized users of the PD.

Standard: ACME must implement mechanisms to correct, amend or append personal information based on information provided by the data subjects and communicates such information to third-parties, as committed or required, consistent with ACME's privacy commitments and system requirements. If a request for correction is denied, the data subject must be informed of the denial and reason for such denial consistent with ACME's privacy commitments and system requirements.

Guidelines: Effective redress processes demonstrate organizational commitment to data quality especially in those business functions where inaccurate data may result in inappropriate decisions or denial of benefits and services to individuals. Organizations apply discretion in determining if records are to be corrected or amended, based on the scope of redress requests, the changes sought and the impact of the changes.

PRI-06(B): DATA SUBJECT ACCESS | NOTICE OF CORRECTION OR PROCESSING CHANGE

Control Objective: The organization notifies affected individuals if their Personal Data (PD) has been corrected or amended.

Standard: Where technically feasible and justified by a valid business case, data/process owners are required to notify affected individuals if their Personal Data (PD) has been corrected or amended.

Guidelines: Where Personal Data (PD) is corrected or amended, organizations take steps to ensure that all authorized recipients of such information and the individual with which the information is associated, are informed of the corrected or amended information.

PRI-06(C): DATA SUBJECT ACCESS | APPEAL ADVERSE DECISION

Control Objective: The organization provides an organization-defined process for individuals to appeal an adverse decision and have incorrect information amended.

Standard: Where technically feasible and justified by a valid business case, data/process owners are required to provides a process for individuals to appeal an adverse decision and have incorrect information amended.

Guidelines: The Senior Agency Official for Privacy ensures that practical means and mechanisms exist and are accessible for individuals to seek the correction or amendment of their Personal Data (PD). Redress processes are clearly defined and publicly available. Additionally, redress processes include the provision of responses to individuals of decisions to deny requests for correction or amendment. The responses include the reasons for the decisions, a means to record individual objections to the decisions and finally, a means of requesting reviews of the initial determinations.

PRI-06(D): DATA SUBJECT ACCESS | USER FEEDBACK MANAGEMENT

Control Objective: The organization implements a process for receiving and responding to complaints, concerns or questions from individuals about the organizational privacy practices that includes:⁵³²

- Mechanisms that are easy to use and readily accessible by the public;

⁵³⁰ NIST 800-53 rev4 IP-2

⁵³¹ NIST 800-53 rev4 IP-3

⁵³² NIST 800-53 rev4 IP-4

Guidelines: None

PRM-03: ALLOCATION OF RESOURCES

Control Objective: The organization:⁵⁴²

- Includes a determination of cybersecurity requirements for systems in business process planning;
- Determines, documents and allocates the resources required to protect systems as part of its capital planning and investment control process; and
- Establishes a discrete line item for cybersecurity in organizational programming and budgeting documentation.

Standard: The Chief Information Security Officer (CISO) and his / her designated representatives are responsible for managing and providing oversight for the cybersecurity-related aspects of the planning and service / tool selection process. The CISO is required to:

- (a) Include cybersecurity requirements in business process planning; and
- (b) Allocate resources required to protect its systems and data, as part of its capital planning process.

Guidelines: To apply needed security controls within the Secure Development Life Cycle (SDLC) (including the acquisition process), it requires a basic understanding of cybersecurity, threats, vulnerabilities and risk to critical missions / business functions. Security engineering principles cannot be properly applied if individuals that design, code and test systems and system components (including information technology products that are used to build those systems / components) do not understand security. Therefore, ACME should include qualified cybersecurity personnel in SDLC activities to ensure that security requirements are incorporated into organizational systems.

PRM-04: SECURITY & PRIVACY IN PROJECT MANAGEMENT

Control Objective: The organization:⁵⁴³

- Assesses the security controls in system project management to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system;
- Produces a security assessment report that documents the results of the assessment; and
- Provides the results of the security control assessment, in writing, to the senior cybersecurity official or officially designated representative.

Standard: A formal cybersecurity risk analysis must be performed on all significant development and / or acquisitions, prior to systems being placed into production:

- (a) New systems and applications must be appropriately tested for functionality prior to being placed in production; and
- (b) Data/process owners and asset custodians are required to perform a gap analysis, at least once per year, to determine any deviations from their systems' current state of compliance and that which is required.

Guidelines: Control evaluators should have sufficient independence to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision.

PRM-05: SECURITY & PRIVACY REQUIREMENTS DEFINITION

Control Objective: The organization identifies security requirements for systems, system components and services at pre-defined decision points in the Secure Development Life Cycle (SDLC).⁵⁴⁴

Standard: Asset custodians, conjunction with data / process owners, are required to:

- (a) Identify, define and document security requirements for systems, system components and services; and
- (b) Update security requirements as business processes or other conditions change.

Guidelines: None

⁵⁴² NIST 800-53 rev4 SA-2 | NIST CSF v1.1 ID.BE-3

⁵⁴³ NIST 800-53 rev4 CA-2 | ISO 27002:2013 6.1.5

⁵⁴⁴ NIST 800-53 rev4 SA-14 | ISO 27002:2013 14.1 | NIST CSF v1.1 ID.BE-4 & ID.BE-5

TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA)

Management Intent: The purpose of the Technology Development & Acquisition (TDA) policy is to ensure secure technologies are developed and / or acquired.

Policy: ACME shall implement the principles of “least privilege” and “least functionality in the development and implementation of technology, regardless if it is internally-developed or acquired from a third party. Technology development and acquisition must employ adequate security measures during all phases of the Secure Development Life Cycle (SDLC) to ensure security and privacy-related risks are identified and appropriately remediated.

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

TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION

Control Objective: The organization develops, implements and governs processes and documentation to facilitate the implementation of an enterprise-wide technology development and acquisition policy, as well as associated standards, controls and procedures.⁵⁹⁸

Standard: ACME’s Procurement Department, in conjunction with the Chief Information Security Officer (CISO), is required to develop, implement and govern a formal acquisition program that:

- (a) Incorporates cybersecurity and privacy principles; requirements; and
- (b) Tailors acquisitions, contract tools and procurement methods to ensure compliance with applicable statutory, regulatory and contractual obligations.

Guidelines: None

TDA-01(A): TECHNOLOGY DEVELOPMENT & ACQUISITION | PRODUCT MANAGEMENT

Control Objective: The organization designs and implements products, applications and services to allow for security updates to correct security deficiencies.

Standard: ACME requires that products are designed and implemented to:

- (a) Maintain appropriate documentation on how ACME provides validated software updates / patches throughout the product life cycle to assure its continued security;
- (b) Allow for the application of security updates to the products 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.
- (c) 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.
- (d) Maintain at least one security-related event log that at a minimum contains the following events:
 1. Successful and unsuccessful login attempts;
 2. Change of user authentication credentials;
 3. Changes in the list of valid user accounts (e.g., addition, modification or deletion of accounts); and
 4. Successful and unsuccessful software updates.
- (e) 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: None

⁵⁹⁸ NIST 800-53 PL-1

TDA-01(B): TECHNOLOGY DEVELOPMENT & ACQUISITION | INTEGRITY MECHANISMS FOR SOFTWARE / FIRMWARE UPDATES

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

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(C): TECHNOLOGY DEVELOPMENT & ACQUISITION | MALWARE TESTING PRIOR TO RELEASE

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

Standard: ACME requires that products and updates incorporate malware testing by at least two (2) different malware detection tools in order to identify the existence of any known malware in the final deliverable:

- (a) The malware tool must be applicable to for operating system that the software will be used on.
- (b) All binary code and bytecode must be inspected for malware by automated tools.

Guidelines: None

TDA-02: SECURITY REQUIREMENTS

Control Objective: The organization includes the following requirements and / or specifications, explicitly or by reference, in system acquisitions based on an assessment of risk.⁵⁹⁹

- Security functional requirements / specifications;
- Security-related documentation requirements; and
- Developmental and evaluation-related security requirements.

Standard: Data/process owners and asset custodians are required to take security requirements into account when purchasing systems or outsourcing solutions.

Guidelines: None

TDA-02(A): SECURITY REQUIREMENTS | PORTS, PROTOCOLS & SERVICES IN USE

Control Objective: The organization requires the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.⁶⁰⁰

Standard: ACME requires that developers of systems, system components or services identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended that will be enabled for use in a production environment.

Guidelines: The identification of functions, ports, protocols and services early in the Secure Development Life Cycle (e.g., during the initial requirements definition and design phases) allows organizations to influence the design of the system, system component or system service. This early involvement in the life cycle helps organizations to avoid or minimize the use of functions, ports, protocols or services that pose unnecessarily high risks and understand the trade-offs involved in blocking specific ports, protocols or services (or when requiring system service providers to do so). Early identification of functions, ports, protocols and services avoids costly retrofitting of security controls after the system, system component or system service has been implemented.

⁵⁹⁹ NIST 800-53 rev4 SA-4

⁶⁰⁰ NIST 800-53 rev4 SA-4(9)

- SUPPLEMENTAL DOCUMENTATION -

DIGITAL SECURITY PROGRAM (DSP)

ANNEXES, TEMPLATES & REFERENCES

Version 2020.1



INTERNAL USE

Access Limited to Internal Use Only

TABLE OF CONTENTS

ANNEXES	3
ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES	3
ANNEX 2: DATA CLASSIFICATION EXAMPLES	8
ANNEX 3: DATA RETENTION PERIODS	10
ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES	12
ANNEX 5: RULES OF BEHAVIOR (ACCEPTABLE & UNACCEPTABLE USE)	14
ANNEX 6: GUIDELINES FOR PERSONAL USE OF ORGANIZATIONAL IT RESOURCES	16
ANNEX 7: RISK MANAGEMENT FRAMEWORK (RMF)	17
ANNEX 8: SYSTEM HARDENING	20
ANNEX 9: SAFETY CONSIDERATIONS WITH EMBEDDED TECHNOLOGY	22
ANNEX 10: INDICATORS OF COMPROMISE (IOC)	23
TEMPLATES	26
TEMPLATE 1: MANAGEMENT DIRECTIVE (POLICY AUTHORIZATION)	26
TEMPLATE 2: USER ACKNOWLEDGEMENT FORM	27
TEMPLATE 3: USER EQUIPMENT RECEIPT OF ISSUE	28
TEMPLATE 4: SERVICE PROVIDER NON-DISCLOSURE AGREEMENT (NDA)	29
TEMPLATE 5: INCIDENT RESPONSE PLAN (IRP)	30
TEMPLATE 6: INCIDENT RESPONSE FORM	41
TEMPLATE 7: APPOINTMENT ORDERS (INFORMATION SECURITY OFFICER)	42
TEMPLATE 8: PRIVILEGED USER ACCOUNT REQUEST FORM	43
TEMPLATE 9: CHANGE MANAGEMENT REQUEST FORM	44
TEMPLATE 10: CHANGE CONTROL BOARD (CCB) MEETING MINUTES	46
TEMPLATE 11: PLAN OF ACTION & MILESTONES (POA&M) / RISK REGISTER	47
TEMPLATE 12: PORTS, PROTOCOLS & SERVICES (PPS)	48
TEMPLATE 13: BUSINESS IMPACT ANALYSIS (BIA)	49
TEMPLATE 14: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (BCP)	51
TEMPLATE 15: PRIVACY IMPACT ASSESSMENT (PIA)	55
REFERENCES	57
REFERENCE 1: DSP EXCEPTION REQUEST PROCESS	57
REFERENCE 2: ELECTRONIC DISCOVERY (eDISCOVERY) GUIDELINES	58
REFERENCE 3: TYPES OF SECURITY CONTROLS	59
REFERENCE 4: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	60

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 four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal 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 [Company Name]. • Impact could include negatively affecting [Company Name]'s competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by [Company Name]
	Potential Impact of Loss	<ul style="list-style-type: none"> • MODERATE DAMAGE would occur if Confidential information were to become available to unauthorized parties either internal or external to [Company Name]. • Impact could include negatively affecting [Company Name]'s competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by [Company Name], 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 [Company Name]. • 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.
	Potential Impact of Loss	<ul style="list-style-type: none"> • NO DAMAGE would occur if Public information were to become available to parties either internal or external to [Company Name]. • Impact would not be damaging or a risk to business operations.

LABELING

Labeling is the practice of marking a system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed.** Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material since marketing material is primarily developed for public release.
- **Displayed.** Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.



GENERAL ASSUMPTIONS

- Any information created or received by [Company Name] employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as “Internal Use” at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so, and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

PERSONAL DATA (PD)

PD is any information about an individual maintained by [Company Name] including any information that:

- Can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and
- Is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Sensitive PD (sPD) is always PD, but PD is not always sPD. Examples of PD include, but are not limited to:

- Name
 - Full name;
 - Maiden name;
 - Mother’s maiden name; and
 - Alias(es);
- Personal Identification Numbers
 - Social Security Number (SSN);
 - Passport number;
 - Driver’s license number;
 - Taxpayer Identification Number (TIN), and
 - Financial account or credit card number;
- Address Information
 - Home address; and
 - Personal email address;
- Personal Characteristics
 - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
 - Fingerprints;
 - Handwriting, and

DATA HANDLING GUIDELINES

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	<ul style="list-style-type: none"> ▪ NDA is required prior to access by non-[Company Name] employees. 	<ul style="list-style-type: none"> ▪ NDA is recommended prior to access by non-[Company Name] 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 	<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 ▪ Remote access should be used only when necessary and only with VPN and two-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>
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 individuals 	<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
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Remote wipe must be enabled, if possible 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Remote wipe must be enabled, if possible 	<ul style="list-style-type: none"> ▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible 	<i>No special requirements</i>
Email (with and without attachments)	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Do not forward 	<ul style="list-style-type: none"> ▪ Encryption is required ▪ Do not forward 	<ul style="list-style-type: none"> ▪ Encryption is recommended 	<i>No special requirements</i>
Physical Mail	<ul style="list-style-type: none"> ▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper-resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally 	<ul style="list-style-type: none"> ▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper-resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail 	<ul style="list-style-type: none"> ▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings 	<i>No special requirements</i>
Printer	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Attend printer while printing 	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Attend printer while printing 	<ul style="list-style-type: none"> ▪ Verify destination printer ▪ Retrieve printed material without delay 	<i>No special requirements</i>

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	Confidential	Restricted
Client or Employee Personal Data	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
	Controlled Unclassified Information (CUI)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
Email Address		X			
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			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).*

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the “importance” of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company’s goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to [Company Name], its clients, its partners, or the general public.

The three (3) SC ratings are:

- **SC-1: Mission Critical.** This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of [Company Name]:
 - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
 - Any business interruption would have a significant impact on [Company Name]’s mission.
 - Cannot go down without having a significant impact on [Company Name]’s mission.
 - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
 - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
 - Safety aspects of SC-1 systems, services and data could lead to:
 - Catastrophic hardware failure;
 - Unauthorized physical access to premises; and/or
 - Physical injury to users.
- **SC-2: Business Critical.** This category involves systems, services and data that are determined to be important to the support of [Company Name]’s business operations:
 - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
 - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on [Company Name]’s mission.
 - Loss of availability is difficult to deal with and can only be tolerated for a short time.
 - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
 - The consequences of loss of integrity are unacceptable.
 - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
 - Safety aspects of SC-2 systems could lead to:
 - Loss of privacy; and/or
 - Unwanted harassment.
- **SC-3: Non-Critical.** This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
 - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
 - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on [Company Name]’s mission.
 - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
 - The consequences could include the delay or degradation of services or routine activities.
 - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
 - Safety aspects of SC-3 systems could lead to:
 - Inconvenience;
 - Frustration; and/or
 - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the “level of effort” that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

BASIC ASSURANCE REQUIREMENTS

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

ENHANCED ASSURANCE REQUIREMENTS

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to [Company Name].