

Your Logo  
Will Be  
Placed Here

---

# STANDARDIZED OPERATING PROCEDURES (SOP)

---

**ACME Business Consulting, Inc.**

**SCF** | SECURE  
CONTROLS  
FRAMEWORK



**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

<b>OVERVIEW, INSTRUCTIONS &amp; EXAMPLE</b>	<b>19</b>
KEY TERMINOLOGY	19
OVERVIEW	19
CUSTOMIZATION GUIDANCE	19
VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES	19
PROCEDURES DOCUMENTATION	20
NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK	21
EXAMPLE	21
SUPPORTING POLICIES & STANDARDS	24
<b>KNOWN COMPLIANCE REQUIREMENTS</b>	<b>25</b>
STATUTORY REQUIREMENTS	25
REGULATORY REQUIREMENTS	25
CONTRACTUAL REQUIREMENTS	25
<b>DIGITAL SECURITY GOVERNANCE (GOV) PROCEDURES</b>	<b>26</b>
P-GOV-01: DIGITAL SECURITY GOVERNANCE PROGRAM	26
P-GOV-02: PUBLISHING SECURITY & PRIVACY POLICIES	26
P-GOV-03: PERIODIC REVIEW & UPDATE OF CYBERSECURITY DOCUMENTATION	27
P-GOV-04: ASSIGNED SECURITY & PRIVACY RESPONSIBILITIES	28
P-GOV-05: MEASURES OF PERFORMANCE	28
P-GOV-05(A): MEASURES OF PERFORMANCE   KEY PERFORMANCE INDICATORS (KPDs)	29
P-GOV-05(B): MEASURES OF PERFORMANCE   KEY RISK INDICATORS (KRIs)	30
P-GOV-06: CONTACTS WITH AUTHORITIES	30
P-GOV-07: CONTACTS WITH SECURITY GROUPS & ASSOCIATIONS	31
P-GOV-08: DEFINED BUSINESS CONTEXT & MISSION	32
P-GOV-09: DEFINED CONTROL OBJECTIVES	32
<b>ASSET MANAGEMENT (AST) PROCEDURES</b>	<b>33</b>
P-AST-01: ASSET GOVERNANCE	33
P-AST-01(A): ASSET GOVERNANCE   ASSET-SERVICE DEPENDENCIES	33
P-AST-01(B): ASSET GOVERNANCE   STAKEHOLDER IDENTIFICATION & INVOLVEMENT	34
P-AST-02: ASSET INVENTORIES	34
P-AST-02(A): ASSET INVENTORIES   UPDATES DURING INSTALLATIONS / REMOVALS	35
P-AST-02(B): ASSET INVENTORIES   AUTOMATED UNAUTHORIZED COMPONENT DETECTION	35
P-AST-02(C): ASSET INVENTORIES   COMPONENT DUPLICATION AVOIDANCE	36
P-AST-02(D): ASSET INVENTORIES   APPROVED DEVIATIONS	36
P-AST-02(E): ASSET INVENTORIES   NETWORK ACCESS CONTROL (NAC)	37
P-AST-02(F): ASSET INVENTORIES   DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING	38
P-AST-02(G): ASSET INVENTORIES   SOFTWARE LICENSING RESTRICTIONS	38
P-AST-02(H): ASSET INVENTORIES   DATA ACTION MAPPING	39
P-AST-02(I): ASSET INVENTORIES   CONFIGURATION MANAGEMENT DATABASE (CMDB)	40
P-AST-03: ASSIGNING OWNERSHIP OF ASSETS	40
P-AST-03(A): ASSIGNING OWNERSHIP OF ASSETS   ACCOUNTABILITY INFORMATION	41
P-AST-04: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)	41
P-AST-05: SECURITY OF ASSETS & MEDIA	42
P-AST-06: UNATTENDED END-USER EQUIPMENT	43
P-AST-06(A): UNATTENDED END-USER EQUIPMENT   ASSET STORAGE IN AUTOMOBILES	43
P-AST-07: KIOSKS & POINT OF SALE (POS) DEVICES	44
P-AST-08: TAMPER PROTECTION & DETECTION	45
P-AST-09: SECURE DISPOSAL OR RE-USE OF EQUIPMENT	46
P-AST-10: RETURN OF ASSETS	46
P-AST-11: REMOVAL OF ASSETS	47
P-AST-12: USE OF PERSONAL DEVICES	48
P-AST-13: USE OF THIRD-PARTY DEVICES	48
P-AST-14: USAGE PARAMETERS	49
P-AST-15: TAMPER PROTECTION	50

<i>P-AST-15(A): TAMPER RESISTANCE   INSPECTION OF SYSTEMS, COMPONENTS &amp; DEVICES</i>	50
<b>P-AST-16: BRING YOUR OWN DEVICE (BYOD) USAGE</b>	<b>51</b>
<b>BUSINESS CONTINUITY &amp; DISASTER RECOVERY (BCD) PROCEDURES</b>	<b>53</b>
<b>P-BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)</b>	<b>53</b>
<i>P-BCD-01(A): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   COORDINATE WITH RELATED PLANS</i>	53
<i>P-BCD-01(B): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   COORDINATE WITH EXTERNAL SERVICE PROVIDERS</i>	54
<i>P-BCD-01(C): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   TRANSFER TO ALTERNATE PROCESSING / STORAGE SITE</i>	55
<i>P-BCD-01(D): BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   RECOVERY TIME / POINT OBJECTIVES</i>	55
<b>P-BCD-02: IDENTIFY CRITICAL ASSETS</b>	<b>55</b>
<i>P-BCD-02(A): IDENTIFY CRITICAL ASSETS   RESUME ALL MISSIONS &amp; BUSINESS FUNCTIONS</i>	56
<i>P-BCD-02(B): IDENTIFY CRITICAL ASSETS   CONTINUE ESSENTIAL MISSION &amp; BUSINESS FUNCTIONS</i>	57
<i>P-BCD-02(C): IDENTIFY CRITICAL ASSETS   RESUME ESSENTIAL MISSION &amp; BUSINESS FUNCTIONS</i>	57
<b>P-BCD-03: CONTINGENCY TRAINING</b>	<b>58</b>
<i>P-BCD-03(A): CONTINGENCY TRAINING   SIMULATED EVENTS</i>	59
<i>P-BCD-03(B): CONTINGENCY TRAINING   AUTOMATED TRAINING ENVIRONMENTS</i>	59
<b>P-BCD-04: CONTINGENCY PLAN TESTING &amp; EXERCISES</b>	<b>60</b>
<i>P-BCD-04(A): CONTINGENCY PLAN TESTING   COORDINATED TESTING WITH RELATED PLANS</i>	60
<i>P-BCD-04(B): CONTINGENCY PLAN TESTING &amp; EXERCISES   ALTERNATE STORAGE &amp; PROCESSING SITES</i>	61
<b>P-BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) &amp; LESSONS LEARNED</b>	<b>61</b>
<b>P-BCD-06: CONTINGENCY PLANNING &amp; UPDATES</b>	<b>62</b>
<b>P-BCD-07: ALTERNATIVE SECURITY MEASURES</b>	<b>63</b>
<b>P-BCD-08: ALTERNATE STORAGE SITE</b>	<b>63</b>
<i>P-BCD-08(A): ALTERNATE STORAGE SITE   SEPARATION FROM PRIMARY SITE</i>	64
<i>P-BCD-08(B): ALTERNATE STORAGE SITE   ACCESSIBILITY</i>	65
<b>P-BCD-09: ALTERNATE PROCESSING SITE</b>	<b>65</b>
<i>P-BCD-09(A): ALTERNATE PROCESSING SITE   SEPARATION FROM PRIMARY SITE</i>	66
<i>P-BCD-09(B): ALTERNATE PROCESSING SITE   ACCESSIBILITY</i>	67
<i>P-BCD-09(C): ALTERNATE PROCESSING SITE   PRIORITY OF SERVICE</i>	67
<i>P-BCD-09(D): ALTERNATE PROCESSING SITE   PREPARATION FOR USE</i>	68
<i>P-BCD-09(E): ALTERNATE PROCESSING SITE   INABILITY TO RETURN TO PRIMARY SITE</i>	68
<b>P-BCD-10: TELECOMMUNICATIONS SERVICES AVAILABILITY</b>	<b>69</b>
<i>P-BCD-10(A): TELECOMMUNICATIONS SERVICES   PRIORITY OF SERVICE PROVISIONS</i>	69
<i>P-BCD-10(B): TELECOMMUNICATIONS SERVICES AVAILABILITY   SEPARATION OF PRIMARY / ALTERNATE PROVIDERS</i>	70
<i>P-BCD-10(C): TELECOMMUNICATIONS SERVICES AVAILABILITY   PROVIDER CONTINGENCY PLAN</i>	70
<b>P-BCD-11: DATA BACKUPS</b>	<b>71</b>
<i>P-BCD-11(A): DATA BACKUPS   TESTING FOR RELIABILITY &amp; INTEGRITY</i>	72
<i>P-BCD-11(B): DATA BACKUPS   SEPARATE STORAGE FOR CRITICAL INFORMATION</i>	72
<i>P-BCD-11(C): DATA BACKUPS   INFORMATION SYSTEM IMAGING</i>	73
<i>P-BCD-11(D): DATA BACKUPS   CRYPTOGRAPHIC PROTECTION</i>	73
<i>P-BCD-11(E): DATA BACKUPS   TEST RESTORATION USING SAMPLING</i>	74
<i>P-BCD-11(F): DATA BACKUPS   TRANSFER TO ALTERNATE STORAGE SITE</i>	74
<i>P-BCD-11(G): DATA BACKUPS   REDUNDANT SECONDARY SYSTEM</i>	75
<i>P-BCD-11(H): DATA BACKUPS   DUAL AUTHORIZATION</i>	75
<b>P-BCD-12: INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION</b>	<b>76</b>
<i>P-BCD-12(A): INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION   TRANSACTION RECOVERY</i>	76
<i>P-BCD-12(B): INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION   FAILOVER CAPABILITY</i>	77
<i>P-BCD-12(C): INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION   ELECTRONIC DISCOVERY (eDISCOVERY)</i>	78
<i>P-BCD-12(D): INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION   RESTORE WITHIN TIME PERIOD</i>	78
<b>P-BCD-13: BACKUP &amp; RESTORATION HARDWARE PROTECTION</b>	<b>79</b>
<b>CAPACITY &amp; PERFORMANCE PLANNING (CAP) PROCEDURES</b>	<b>80</b>
<b>P-CAP-01: CAPACITY &amp; PERFORMANCE MANAGEMENT</b>	<b>80</b>
<b>P-CAP-02: RESOURCE PRIORITY</b>	<b>80</b>
<b>P-CAP-03: CAPACITY PLANNING</b>	<b>81</b>
<b>CHANGE MANAGEMENT (CHG) PROCEDURES</b>	<b>82</b>
<b>P-CHG-01: CHANGE MANAGEMENT PROGRAM</b>	<b>82</b>
<b>P-CHG-02: CONFIGURATION CHANGE CONTROL</b>	<b>82</b>

<i>P-CHG-02(A): CONFIGURATION CHANGE CONTROL   PROHIBITION OF CHANGES</i>	83
<i>P-CHG-02(B): CONFIGURATION CHANGE CONTROL   TEST, VALIDATE &amp; DOCUMENT CHANGES</i>	84
<i>P-CHG-02(C): CONFIGURATION CHANGE CONTROL   SECURITY REPRESENTATIVE FOR CHANGE</i>	84
<i>P-CHG-02(D): CONFIGURATION CHANGE CONTROL   AUTOMATED SECURITY RESPONSE</i>	85
<i>P-CHG-02(E): CONFIGURATION CHANGE CONTROL   CRYPTOGRAPHIC MANAGEMENT</i>	85
<b>P-CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES</b>	<b>86</b>
<b>P-CHG-04: ACCESS RESTRICTION FOR CHANGE</b>	<b>86</b>
<i>P-CHG-04(A): ACCESS RESTRICTIONS FOR CHANGE   AUTOMATED ACCESS ENFORCEMENT / AUDITING</i>	87
<i>P-CHG-04(B): ACCESS RESTRICTIONS FOR CHANGE   SIGNED COMPONENTS</i>	88
<i>P-CHG-04(C): ACCESS RESTRICTIONS FOR CHANGE   DUAL AUTHORIZATION FOR CHANGE</i>	88
<i>P-CHG-04(D): ACCESS RESTRICTIONS FOR CHANGE   LIMIT PRODUCTION / OPERATIONAL PRIVILEGES (INCOMPATIBLE ROLES)</i>	89
<i>P-CHG-04(E): ACCESS RESTRICTIONS FOR CHANGE   LIBRARY PRIVILEGES</i>	90
<b>P-CHG-05: STAKEHOLDER NOTIFICATION OF CHANGES</b>	<b>90</b>
<b>P-CHG-06: SECURITY FUNCTIONALITY VERIFICATION</b>	<b>91</b>
<i>P-CHG-06(A): SECURITY FUNCTIONALITY VERIFICATION   REPORT VERIFICATION RESULTS</i>	91
<b>CLD SECURITY (CLD) PROCEDURES</b>	<b>93</b>
<b>P-CLD-01: CLOUD SERVICES</b>	<b>93</b>
<b>P-CLD-02: CLOUD SECURITY ARCHITECTURE</b>	<b>93</b>
<b>P-CLD-03: SECURITY MANAGEMENT SUBNET</b>	<b>94</b>
<b>P-CLD-04: APPLICATION &amp; PROGRAM INTERFACE (APD) SECURITY</b>	<b>95</b>
<b>P-CLD-05: VIRTUAL MACHINE IMAGES</b>	<b>96</b>
<b>P-CLD-06: MULTI-TENANT ENVIRONMENTS</b>	<b>96</b>
<b>P-CLD-07: DATA HANDLING &amp; PORTABILITY</b>	<b>97</b>
<b>P-CLD-08: STANDARDIZED VIRTUALIZATION FORMATS</b>	<b>98</b>
<b>P-CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS</b>	<b>98</b>
<b>P-CLD-10: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS</b>	<b>99</b>
<b>P-CLD-11: CLOUD ACCESS POINT (CAP)</b>	<b>100</b>
<b>COMPLIANCE (CPL) PROCEDURES</b>	<b>101</b>
<b>P-CPL-01: STATUTORY, REGULATORY &amp; CONTRACTUAL COMPLIANCE</b>	<b>101</b>
<b>P-CPL-02: SECURITY CONTROLS OVERSIGHT</b>	<b>101</b>
<i>P-CPL-02(A): SECURITY CONTROLS OVERSIGHT   INTERNAL AUDIT FUNCTION</i>	102
<b>P-CPL-03: SECURITY ASSESSMENTS</b>	<b>103</b>
<i>P-CPL-03(A): SECURITY ASSESSMENTS   INDEPENDENT ASSESSORS</i>	103
<i>P-CPL-03(B): SECURITY ASSESSMENTS   FUNCTIONAL REVIEW OF SECURITY CONTROLS</i>	104
<b>P-CPL-04: AUDIT ACTIVITIES</b>	<b>105</b>
<b>CONFIGURATION MANAGEMENT (CFG) PROCEDURES</b>	<b>106</b>
<b>P-CFG-01: CONFIGURATION MANAGEMENT PROGRAM</b>	<b>106</b>
<b>P-CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS</b>	<b>106</b>
<i>P-CFG-02(A): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   REVIEWS &amp; UPDATES</i>	108
<i>P-CFG-02(B): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   AUTOMATED CENTRAL MANAGEMENT &amp; VERIFICATION</i>	109
<i>P-CFG-02(C): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   RETENTION OF PREVIOUS CONFIGURATIONS</i>	110
<i>P-CFG-02(D): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   DEVELOPMENT &amp; TEST ENVIRONMENTS</i>	110
<i>P-CFG-02(E): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS</i>	111
<i>P-CFG-02(F): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   NETWORK DEVICE CONFIGURATION FILE SYNCHRONIZATION</i>	112
<i>P-CFG-02(G): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   APPROVED DEVIATIONS</i>	112
<i>P-CFG-02(H): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   RESPOND TO UNAUTHORIZED CHANGES</i>	113
<i>P-CFG-02(I): SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   BASELINE TAILORING</i>	114
<b>P-CFG-03: LEAST FUNCTIONALITY</b>	<b>114</b>
<i>P-CFG-03(A): LEAST FUNCTIONALITY   PERIODIC REVIEW</i>	115
<i>P-CFG-03(B): LEAST FUNCTIONALITY   PREVENT PROGRAM EXECUTION</i>	116
<i>P-CFG-03(C): LEAST FUNCTIONALITY   UNAUTHORIZED OR AUTHORIZED SOFTWARE (BLACKLISTING OR WHITELISTING)</i>	116
<i>P-CFG-03(D): LEAST FUNCTIONALITY   SPLIT TUNNELING</i>	117
<b>P-CFG-04: SOFTWARE USAGE RESTRICTIONS</b>	<b>117</b>
<i>P-CFG-04(A): SOFTWARE USAGE RESTRICTIONS   OPEN SOURCE SOFTWARE</i>	118

P-CFG-04(B): SOFTWARE USAGE RESTRICTIONS   UNSUPPORTED INTERNET BROWSERS & EMAIL CLIENTS	119
<b>P-CFG-05: USER-INSTALLED SOFTWARE</b>	<b>119</b>
P-CFG-05(A): USER-INSTALLED SOFTWARE   UNAUTHORIZED INSTALLATION ALERTS	120
P-CFG-05(B): USER-INSTALLED SOFTWARE   PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	121
<b>CONTINUOUS MONITORING (MON) PROCEDURES</b>	<b>122</b>
<b>P-MON-01: CONTINUOUS MONITORING</b>	<b>122</b>
P-MON-01(A): CONTINUOUS MONITORING   INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)	123
P-MON-01(B): CONTINUOUS MONITORING   AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	124
P-MON-01(C): CONTINUOUS MONITORING   INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC	124
P-MON-01(D): CONTINUOUS MONITORING   SYSTEM GENERATED ALERTS	125
P-MON-01(E): CONTINUOUS MONITORING   WIRELESS INTRUSION DETECTION SYSTEM (WIDS)	126
P-MON-01(F): CONTINUOUS MONITORING   HOST-BASED DEVICES	126
P-MON-01(G): CONTINUOUS MONITORING   FILE INTEGRITY MONITORING (FIM)	127
P-MON-01(H): CONTINUOUS MONITORING   REVIEWS & UPDATES	128
P-MON-01(I): CONTINUOUS MONITORING   PROXY LOGGING	128
P-MON-01(J): CONTINUOUS MONITORING   DEACTIVATED ACCOUNT ACTIVITY	129
P-MON-01(K): CONTINUOUS MONITORING   AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	129
P-MON-01(L): CONTINUOUS MONITORING   AUTOMATED ALERTS	130
P-MON-01(M): CONTINUOUS MONITORING   ANALYZE TRAFFIC / EVENT PATTERNS	130
P-MON-01(N): CONTINUOUS MONITORING   INDIVIDUALS POSING GREATER RISK	130
P-MON-01(O): CONTINUOUS MONITORING   PRIVILEGED USER OVERSIGHT	131
P-MON-01(P): CONTINUOUS MONITORING   ANALYZE & PRIORITIZE MONITORING REQUIREMENTS	131
<b>P-MON-02: CENTRALIZED EVENT LOG COLLECTION</b>	<b>132</b>
P-MON-02(A): CENTRALIZED SECURITY EVENT LOG COLLECTION   CORRELATE MONITORING INFORMATION	133
P-MON-02(B): CENTRALIZED SECURITY EVENT LOG COLLECTION   CENTRAL REVIEW & ANALYSIS	133
P-MON-02(C): CENTRALIZED SECURITY EVENT LOG COLLECTION   INTEGRATION OF SCANNING & OTHER MONITORING INFORMATION	134
P-MON-02(D): CENTRALIZED SECURITY EVENT LOG COLLECTION   CORRELATION WITH PHYSICAL MONITORING	134
P-MON-02(E): CENTRALIZED SECURITY EVENT LOG COLLECTION   PERMITTED ACTIONS	134
P-MON-02(F): CENTRALIZED SECURITY EVENT LOG COLLECTION   AUDIT LEVEL ADJUSTMENT	135
P-MON-02(G): CENTRALIZED SECURITY EVENT LOG COLLECTION   SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL	135
P-MON-02(H): CENTRALIZED SECURITY EVENT LOG COLLECTION   CHANGES BY AUTHORIZED INDIVIDUALS	136
<b>P-MON-03: CONTENT OF AUDIT RECORDS</b>	<b>136</b>
P-MON-03(A): CONTENT OF AUDIT RECORDS   SENSITIVE AUDIT INFORMATION	137
P-MON-03(B): CONTENT OF AUDIT RECORDS   AUDIT TRAILS	138
P-MON-03(C): CONTENT OF AUDIT RECORDS   PRIVILEGED FUNCTIONS LOGGING	138
P-MON-03(D): CONTENT OF AUDIT RECORDS   VERBOSITY LOGGING FOR BOUNDARY DEVICES	139
P-MON-03(E): CONTENT OF AUDIT RECORDS   LIMIT PERSONAL DATA (PD) IN AUDIT RECORDS	140
P-MON-03(F): CONTENT OF AUDIT RECORDS   CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	140
<b>P-MON-04: AUDIT STORAGE CAPACITY</b>	<b>141</b>
<b>P-MON-05: RESPONSE TO AUDIT PROCESSING FAILURES</b>	<b>141</b>
P-MON-05(A): RESPONSE TO AUDIT PROCESSING FAILURES   REAL-TIME ALERTS	142
P-MON-05(B): RESPONSE TO AUDIT PROCESSING FAILURES   AUDIT STORAGE CAPACITY ALERTING	142
<b>P-MON-06: MONITORING REPORTING</b>	<b>143</b>
P-MON-06(A): MONITORING REPORTING   QUERY PARAMETER AUDITS OF PERSONAL DATA (PD)	144
P-MON-06(B): MONITORING REPORTING   TREND ANALYSIS REPORTING	145
<b>P-MON-07: TIME STAMPS</b>	<b>145</b>
P-MON-07(A): TIME STAMPS   SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	146
<b>P-MON-08: PROTECTION OF AUDIT INFORMATION</b>	<b>146</b>
P-MON-08(A): PROTECTION OF AUDIT INFORMATION   AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS	147
P-MON-08(B): PROTECTION OF AUDIT INFORMATION   ACCESS BY SUBSET OF PRIVILEGED USERS	148
P-MON-08(C): PROTECTION OF AUDIT INFORMATION   CRYPTOGRAPHIC PROTECTION OF AUDIT INFORMATION	148
P-MON-08(D): PROTECTION OF AUDIT INFORMATION   DUAL AUTHORIZATION	149
<b>P-MON-09: NON-REPUDIATION</b>	<b>149</b>
<b>P-MON-10: AUDIT RECORD RETENTION</b>	<b>150</b>
<b>P-MON-11: MONITORING FOR INFORMATION DISCLOSURE</b>	<b>151</b>
P-MON-11(A): MONITORING FOR INFORMATION DISCLOSURE   ANALYZE TRAFFIC FOR COVERT EXFILTRATION)	151
P-MON-11(B): MONITORING FOR INFORMATION DISCLOSURE   UNAUTHORIZED NETWORK SERVICES	152

<i>P-MON-11(c): MONITORING FOR INFORMATION DISCLOSURE   MONITORING FOR INDICATORS OF COMPROMISE (IOC)</i>	152
<b>P-MON-12: SESSION AUDIT</b>	<b>152</b>
<b>P-MON-13: ALTERNATE AUDIT CAPABILITY</b>	<b>153</b>
<b>P-MON-14: CROSS-ORGANIZATIONAL MONITORING</b>	<b>154</b>
<i>P-MON-14(A): CROSS-ORGANIZATIONAL MONITORING   SHARING OF AUDIT INFORMATION</i>	154
<b>P-MON-15: COVERT CHANNEL ANALYSIS</b>	<b>155</b>
<b>P-MON-16: ANOMALOUS BEHAVIOR</b>	<b>155</b>
<i>P-MON-16(A): ANOMALOUS BEHAVIOR   INSIDER THREATS</i>	156
<i>P-MON-16(B): ANOMALOUS BEHAVIOR   THIRD-PARTY THREATS</i>	157
<i>P-MON-16(C): ANOMALOUS BEHAVIOR   UNAUTHORIZED ACTIVITIES</i>	157
<b>CRYPTOGRAPHIC PROTECTIONS (CRY) PROCEDURES</b>	<b>159</b>
<b>P-CRY-01: USE OF CRYPTOGRAPHIC CONTROLS</b>	<b>159</b>
<i>P-CRY-01(A): USE OF CRYPTOGRAPHIC CONTROLS   ALTERNATE PHYSICAL PROTECTION</i>	159
<i>P-CRY-01(B): USE OF CRYPTOGRAPHIC CONTROLS   EXPORT-CONTROLLED TECHNOLOGY</i>	160
<i>P-CRY-01(C): USE OF CRYPTOGRAPHIC CONTROLS   PRE / POST TRANSMISSION HANDLING</i>	161
<i>P-CRY-01(D): USE OF CRYPTOGRAPHIC CONTROLS   CONCEAL / RANDOMIZE COMMUNICATIONS</i>	161
<b>P-CRY-02: CRYPTOGRAPHIC MODULE AUTHENTICATION</b>	<b>161</b>
<b>P-CRY-03: TRANSMISSION CONFIDENTIALITY</b>	<b>162</b>
<b>P-CRY-04: TRANSMISSION INTEGRITY</b>	<b>163</b>
<b>P-CRY-05: ENCRYPTING DATA AT REST</b>	<b>164</b>
<i>P-CRY-05(A): ENCRYPTING DATA AT REST   STORAGE MEDIA</i>	164
<i>P-CRY-05(B): ENCRYPTING DATA AT REST   OFFLINE STORAGE</i>	165
<b>P-CRY-06: NON-CONSOLE ADMINISTRATIVE ACCESS</b>	<b>165</b>
<b>P-CRY-07: WIRELESS ACCESS AUTHENTICATION &amp; ENCRYPTION</b>	<b>166</b>
<b>P-CRY-08: PUBLIC KEY INFRASTRUCTURE (PKI)</b>	<b>167</b>
<i>P-CRY-08(A): PUBLIC KEY INFRASTRUCTURE (PKI)   AVAILABILITY</i>	167
<b>P-CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT</b>	<b>168</b>
<i>P-CRY-09(A): CRYPTOGRAPHIC KEY MANAGEMENT   SYMMETRIC KEYS</i>	169
<i>P-CRY-09(B): CRYPTOGRAPHIC KEY MANAGEMENT   ASYMMETRIC KEYS</i>	170
<i>P-CRY-09(C): CRYPTOGRAPHIC KEY MANAGEMENT   CRYPTOGRAPHIC KEY LOSS OR CHANGE</i>	170
<i>P-CRY-09(D): CRYPTOGRAPHIC KEY MANAGEMENT   CONTROL &amp; DISTRIBUTION OF CRYPTOGRAPHIC KEYS</i>	171
<i>P-CRY-09(E): CRYPTOGRAPHIC KEY MANAGEMENT   ASSIGNED OWNERS</i>	172
<b>P-CRY-10: TRANSMISSION OF SECURITY &amp; PRIVACY ATTRIBUTES</b>	<b>172</b>
<b>DATA CLASSIFICATION &amp; HANDLING (DCH) PROCEDURES</b>	<b>174</b>
<b>P-DCH-01: DATA PROTECTION</b>	<b>174</b>
<i>P-DCH-01(A): DATA PROTECTION   DATA STEWARDSHIP</i>	174
<b>P-DCH-02: DATA &amp; ASSET CLASSIFICATION</b>	<b>175</b>
<b>P-DCH-03: MEDIA ACCESS</b>	<b>176</b>
<i>P-DCH-03(A): MEDIA ACCESS   DISCLOSURE OF INFORMATION</i>	177
<i>P-DCH-03(B): MEDIA ACCESS   MASKING DISPLAYED DATA</i>	177
<b>P-DCH-04: MEDIA MARKING</b>	<b>178</b>
<i>P-DCH-04(A): MEDIA MARKING   AUTOMATED MARKING</i>	178
<b>P-DCH-05: SECURITY ATTRIBUTES</b>	<b>179</b>
<i>P-DCH-05(A): SECURITY ATTRIBUTES   DYNAMIC ATTRIBUTE ASSOCIATION</i>	180
<i>P-DCH-05(B): SECURITY ATTRIBUTES   ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS</i>	180
<i>P-DCH-05(C): SECURITY ATTRIBUTES   MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM</i>	181
<i>P-DCH-05(D): SECURITY ATTRIBUTES   ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS</i>	182
<i>P-DCH-05(E): SECURITY ATTRIBUTES   ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES</i>	182
<i>P-DCH-05(F): SECURITY ATTRIBUTES   MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION</i>	183
<i>P-DCH-05(G): SECURITY ATTRIBUTES   CONSISTENT ATTRIBUTE INTERPRETATION</i>	184
<i>P-DCH-05(H): SECURITY ATTRIBUTES   ASSOCIATION TECHNIQUES &amp; TECHNOLOGIES</i>	184
<i>P-DCH-05(I): SECURITY ATTRIBUTES   ATTRIBUTE REASSIGNMENT</i>	185
<i>P-DCH-05(J): SECURITY ATTRIBUTES   ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS</i>	185
<i>P-DCH-05(K): SECURITY ATTRIBUTES   AUDIT CHANGES</i>	186
<b>P-DCH-06: MEDIA STORAGE</b>	<b>187</b>
<i>P-DCH-06(A): MEDIA STORAGE   PHYSICALLY SECURE ALL MEDIA</i>	187
<i>P-DCH-06(B): MEDIA STORAGE   SENSITIVE DATA INVENTORIES</i>	188

<i>P-DCH-06(c): MEDIA STORAGE   PERIODIC SCANS FOR SENSITIVE DATA</i>	189
<i>P-DCH-06(d): MEDIA STORAGE   MAKING SENSITIVE DATA UNREADABLE IN STORAGE</i>	189
<i>P-DCH-06(e): MEDIA STORAGE   STORING AUTHENTICATION DATA</i>	190
<b>P-DCH-07: MEDIA TRANSPORTATION</b>	<b>191</b>
<i>P-DCH-07(a): MEDIA TRANSPORTATION   CUSTODIANS</i>	192
<i>P-DCH-07(b): MEDIA TRANSPORTATION   ENCRYPTING DATA IN STORAGE MEDIA</i>	192
<b>P-DCH-08: PHYSICAL MEDIAL DISPOSAL</b>	<b>193</b>
<b>P-DCH-09: DIGITAL MEDIA SANITIZATION</b>	<b>194</b>
<i>P-DCH-09(a): MEDIA SANITIZATION   MEDIA SANITIZATION DOCUMENTATION</i>	194
<i>P-DCH-09(b): MEDIA SANITIZATION   EQUIPMENT TESTING</i>	195
<i>P-DCH-09(c): MEDIA SANITIZATION   DESTRUCTION OF PERSONAL DATA (PD)</i>	195
<i>P-DCH-09(d): MEDIA SANITIZATION   NON-DESTRUCTIVE TECHNIQUES</i>	196
<i>P-DCH-09(e): MEDIA SANITIZATION   DUAL AUTHORIZATION</i>	196
<b>P-DCH-10: MEDIA USE</b>	<b>197</b>
<i>P-DCH-10(a): MEDIA USE   LIMITATIONS ON USE</i>	197
<i>P-DCH-10(b): MEDIA USE   PROHIBIT USE WITHOUT OWNER</i>	198
<b>P-DCH-11: MEDIA DOWNGRADING</b>	<b>199</b>
<b>P-DCH-12: REMOVABLE MEDIA SECURITY</b>	<b>199</b>
<b>P-DCH-13: USE OF EXTERNAL INFORMATION SYSTEMS</b>	<b>200</b>
<i>P-DCH-13(a): USE OF EXTERNAL INFORMATION SYSTEMS   LIMITS OF AUTHORIZED USE</i>	200
<i>P-DCH-13(b): USE OF EXTERNAL INFORMATION SYSTEMS   PORTABLE STORAGE DEVICES</i>	201
<i>P-DCH-13(c): USE OF EXTERNAL INFORMATION SYSTEMS   PROTECTING SENSITIVE INFORMATION ON EXTERNAL SYSTEMS</i>	202
<i>P-DCH-13(d): USE OF EXTERNAL INFORMATION SYSTEMS   NON-ORGANIZATIONALLY OWNED SYSTEMS / COMPONENTS / DEVICES</i>	203
<b>P-DCH-14: INFORMATION SHARING</b>	<b>204</b>
<i>P-DCH-14(a): INFORMATION SHARING   INFORMATION SEARCH &amp; RETRIEVAL</i>	204
<b>P-DCH-15: PUBLICLY ACCESSIBLE CONTENT</b>	<b>205</b>
<b>P-DCH-16: DATA MINING PROTECTION</b>	<b>205</b>
<b>P-DCH-17: AD-HOC TRANSFERS</b>	<b>206</b>
<b>P-DCH-18: MEDIA &amp; DATA RETENTION</b>	<b>207</b>
<i>P-DCH-18(a): MEDIA &amp; DATA RETENTION   LIMIT PERSONAL DATA (PD) ELEMENTS IN TESTING, TRAINING &amp; RESEARCH</i>	208
<i>P-DCH-18(b): MEDIA &amp; DATA RETENTION   MINIMIZE PERSONAL DATA (PD)</i>	209
<i>P-DCH-18(c): MEDIA &amp; DATA RETENTION   TEMPORARY FILES CONTAINING PERSONAL DATA</i>	209
<b>P-DCH-19: GEOGRAPHIC LOCATION OF DATA</b>	<b>210</b>
<b>P-DCH-20: ARCHIVED DATA SETS</b>	<b>210</b>
<b>P-DCH-21: INFORMATION DISPOSAL</b>	<b>211</b>
<b>P-DCH-22: DATA QUALITY OPERATIONS</b>	<b>212</b>
<i>P-DCH-22(a): DATA QUALITY OPERATIONS   UPDATING &amp; CORRECTING PERSONAL DATA (PD)</i>	213
<i>P-DCH-22(b): DATA QUALITY OPERATIONS   DATA TAGS</i>	213
<i>P-DCH-22(c): DATA QUALITY OPERATIONS   PERSONAL DATA (PD) COLLECTION</i>	214
<b>P-DCH-23: DE-IDENTIFICATION</b>	<b>215</b>
<i>P-DCH-23(a): DE-IDENTIFICATION   COLLECTION</i>	215
<i>P-DCH-23(b): DE-IDENTIFICATION   ARCHIVING</i>	216
<i>P-DCH-23(c): DE-IDENTIFICATION   RELEASE</i>	216
<i>P-DCH-23(d): DE-IDENTIFICATION   REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS</i>	217
<i>P-DCH-23(e): DE-IDENTIFICATION   STATISTICAL DISCLOSURE CONTROL</i>	218
<i>P-DCH-23(f): DE-IDENTIFICATION   DIFFERENTIAL PRIVACY</i>	218
<i>P-DCH-23(g): DE-IDENTIFICATION   VALIDATED SOFTWARE</i>	219
<i>P-DCH-23(h): DE-IDENTIFICATION   MOTIVATED INTRUDER</i>	220
<b>P-DCH-24: INFORMATION LOCATION</b>	<b>220</b>
<i>P-DCH-24(a): INFORMATION LOCATION   AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION</i>	221
<b>P-DCH-25: TRANSFER OF PERSONAL INFORMATION</b>	<b>222</b>
<b>EMBEDDED TECHNOLOGY (EMB) PROCEDURES</b>	<b>223</b>
<b>P-EMB-01: EMBEDDED TECHNOLOGY SECURITY PROGRAM</b>	<b>223</b>
<b>P-EMB-02: INTERNET OF THINGS (IoT)</b>	<b>224</b>
<b>P-EMB-03: OPERATIONAL TECHNOLOGY (OT)</b>	<b>224</b>
<b>ENDPOINT SECURITY (END) PROCEDURES</b>	<b>226</b>

<b>P-END-01: WORKSTATION SECURITY</b>	<b>226</b>
<b>P-END-02: ENDPOINT PROTECTION MEASURES</b>	<b>227</b>
<b>P-END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS</b>	<b>228</b>
<i>P-END-03(A): PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS   UNAUTHORIZED INSTALLATION ALERTS</i>	228
<i>P-END-03(B): PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS   ACCESS RESTRICTION FOR CHANGE</i>	229
<b>P-END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)</b>	<b>229</b>
<i>P-END-04(A): MALICIOUS CODE PROTECTION   AUTOMATIC UPDATES</i>	230
<i>P-END-04(B): MALICIOUS CODE PROTECTION   DOCUMENTED PROTECTION MEASURES</i>	231
<i>P-END-04(C): MALICIOUS CODE PROTECTION   CENTRALIZED MANAGEMENT</i>	231
<i>P-END-04(D): MALICIOUS CODE PROTECTION   HEURISTIC / NONSIGNATURE-BASED DETECTION</i>	232
<i>P-END-04(E): MALICIOUS CODE PROTECTION   MALWARE PROTECTION MECHANISM TESTING</i>	233
<i>P-END-04(F): MALICIOUS CODE PROTECTION   EVOLVING MALWARE THREATS</i>	233
<i>P-END-04(G): MALICIOUS CODE PROTECTION   ALWAYS ON PROTECTION</i>	234
<b>P-END-05: SOFTWARE FIREWALL</b>	<b>235</b>
<b>P-END-06: FILE INTEGRITY MONITORING (FIM)</b>	<b>235</b>
<i>P-END-06(A): FILE INTEGRITY MONITORING   INTEGRITY CHECKS</i>	236
<i>P-END-06(B): FILE INTEGRITY MONITORING   INTEGRATION OF DETECTION &amp; RESPONSE</i>	237
<i>P-END-06(C): FILE INTEGRITY MONITORING (FIM)   AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS</i>	238
<i>P-END-06(D): FILE INTEGRITY MONITORING (FIM)   AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS</i>	238
<i>P-END-06(E): FILE INTEGRITY MONITORING (FIM)   VERIFY BOOT PROCESS</i>	238
<i>P-END-06(F): FILE INTEGRITY MONITORING (FIM)   PROTECTION OF BOOT FIRMWARE</i>	239
<i>P-END-06(G): FILE INTEGRITY MONITORING (FIM)   BINARY OR MACHINE-EXECUTABLE CODE</i>	239
<b>P-END-07: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS / HIPS)</b>	<b>239</b>
<b>P-END-08: PHISHING &amp; SPAM PROTECTION</b>	<b>240</b>
<i>P-END-08(A): PHISHING &amp; SPAM PROTECTION   CENTRAL MANAGEMENT</i>	241
<i>P-END-08(B): PHISHING &amp; SPAM PROTECTION   AUTOMATIC UPDATES</i>	241
<b>P-END-09: TRUSTED PATH</b>	<b>242</b>
<b>P-END-10: MOBILE CODE</b>	<b>242</b>
<b>P-END-11: THIN NODES</b>	<b>243</b>
<b>P-END-12: PORT &amp; I / O DEVICE ACCESS</b>	<b>244</b>
<b>P-END-13: SENSOR CAPABILITY</b>	<b>245</b>
<i>P-END-13(A): SENSOR CAPABILITY   AUTHORIZED USE</i>	245
<i>P-END-13(B): SENSOR CAPABILITY   NOTICE OF COLLECTION</i>	246
<i>P-END-13(C): SENSOR CAPABILITY   COLLECTION MINIMIZATION</i>	247
<b>P-END-14: COLLABORATIVE COMPUTING DEVICES</b>	<b>247</b>
<i>P-END-14(A): COLLABORATIVE COMPUTING DEVICES   DISABLING / REMOVAL IN SECURE WORK AREAS</i>	248
<i>P-END-14(B): COLLABORATIVE COMPUTING DEVICES   EXPLICITLY INDICATE CURRENT PARTICIPANTS</i>	248
<b>P-END-15: HYPERVISOR ACCESS</b>	<b>249</b>
<b>P-END-16: SECURITY FUNCTION ISOLATION</b>	<b>249</b>
<i>P-END-16(A): SECURITY FUNCTION ISOLATION   HOST-BASED SECURITY FUNCTION ISOLATION</i>	250
<b>HUMAN RESOURCES SECURITY (HRS) PROCEDURES</b>	<b>252</b>
<b>P-HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT</b>	<b>252</b>
<b>P-HRS-02: POSITION CATEGORIZATION</b>	<b>252</b>
<i>P-HRS-02(A): POSITION CATEGORIZATION   USERS WITH ELEVATED PRIVILEGES</i>	253
<b>P-HRS-03: ROLES &amp; RESPONSIBILITIES</b>	<b>254</b>
<i>P-HRS-03(A): ROLES &amp; RESPONSIBILITIES   USER AWARENESS</i>	254
<i>P-HRS-03(B): ROLES &amp; RESPONSIBILITIES   COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS</i>	255
<b>P-HRS-04: PERSONNEL SCREENING</b>	<b>256</b>
<i>P-HRS-04(A): PERSONNEL SCREENING   ROLES WITH SPECIAL PROTECTION MEASURES</i>	257
<i>P-HRS-04(B): PERSONNEL SCREENING   FORMAL INDOCTRINATION</i>	257
<b>P-HRS-05: TERMS OF EMPLOYMENT</b>	<b>258</b>
<i>P-HRS-05(A): TERMS OF EMPLOYMENT   RULES OF BEHAVIOR</i>	258
<i>P-HRS-05(B): TERMS OF EMPLOYMENT   SOCIAL MEDIA &amp; SOCIAL NETWORKING RESTRICTIONS</i>	259
<i>P-HRS-05(C): TERMS OF EMPLOYMENT   USE OF COMMUNICATIONS TECHNOLOGY</i>	260
<i>P-HRS-05(D): TERMS OF EMPLOYMENT   USE OF CRITICAL TECHNOLOGIES</i>	260
<i>P-HRS-05(E): TERMS OF EMPLOYMENT   USE OF MOBILE DEVICES</i>	261
<b>P-HRS-06: ACCESS AGREEMENTS</b>	<b>262</b>
<i>P-HRS-06(A): ACCESS AGREEMENTS   CONFIDENTIALITY AGREEMENTS</i>	262



<i>P-HRS-06(B): ACCESS AGREEMENTS   POST-EMPLOYMENT OBLIGATIONS</i>	263
<b>P-HRS-07: PERSONNEL SANCTIONS</b>	<b>263</b>
<i>P-HRS-07(A): PERSONNEL SANCTIONS   WORKPLACE INVESTIGATIONS</i>	264
<b>P-HRS-08: PERSONNEL TRANSFER</b>	<b>265</b>
<b>P-HRS-09: PERSONNEL TERMINATION</b>	<b>266</b>
<i>P-HRS-09(A): PERSONNEL TERMINATION   ASSET COLLECTION</i>	267
<i>P-HRS-09(B): PERSONNEL TERMINATION   HIGH-RISK TERMINATIONS</i>	267
<i>P-HRS-09(C): PERSONNEL TERMINATION   POST-EMPLOYMENT REQUIREMENTS</i>	268
<i>P-HRS-09(D): PERSONNEL TERMINATION   AUTOMATED EMPLOYMENT STATUS NOTIFICATION</i>	269
<b>P-HRS-10: THIRD-PARTY PERSONNEL SECURITY</b>	<b>269</b>
<b>P-HRS-11: SEPARATION OF DUTIES</b>	<b>270</b>
<b>P-HRS-12: INCOMPATIBLE ROLES</b>	<b>271</b>
<i>P-HRS-12(A): INCOMPATIBLE ROLES   TWO-PERSON RULE</i>	271
<b>P-HRS-13: IDENTIFY CRITICAL SKILLS &amp; GAPS</b>	<b>272</b>
<i>P-HRS-13(A): IDENTIFY CRITICAL SKILLS &amp; GAPS   REMEDIATE IDENTIFIED SKILLS DEFICIENCIES</i>	272
<i>P-HRS-13(B): IDENTIFY CRITICAL SKILLS &amp; GAPS   IDENTIFY VITAL CYBERSECURITY &amp; PRIVACY STAFF</i>	272
<i>P-HRS-13(C): IDENTIFY CRITICAL SKILLS &amp; GAPS   ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY &amp; PRIVACY STAFF</i>	273
<i>P-HRS-13(D): IDENTIFY CRITICAL SKILLS &amp; GAPS   PERFORM SUCCESSION PLANNING</i>	273
<b>IDENTIFICATION &amp; AUTHENTICATION (IAC) PROCEDURES</b>	<b>275</b>
<b>P-IAC-01: IDENTITY &amp; ACCESS MANAGEMENT (IAM)</b>	<b>275</b>
<b>P-IAC-02: IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS</b>	<b>275</b>
<i>P-IAC-02(A): IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS   GROUP AUTHENTICATION</i>	276
<i>P-IAC-02(B): IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS   NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT</i>	277
<i>P-IAC-02(C): IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS   ACCEPTANCE OF PIV CREDENTIALS</i>	277
<i>P-IAC-02(D): IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS   OUT-OF-BAND AUTHENTICATION (OOBA)</i>	278
<b>P-IAC-03: IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS</b>	<b>278</b>
<i>P-IAC-03(A): IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   ACCEPTANCE OF PIV CREDENTIALS FROM OTHER ORGANIZATIONS</i>	279
<i>P-IAC-03(B): IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   ACCEPTANCE OF THIRD-PARTY CREDENTIALS</i>	280
<i>P-IAC-03(C): IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   USE OF FICAM-ISSUED PROFILES</i>	280
<i>P-IAC-03(D): IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   DISASSOCIABILITY</i>	281
<b>P-IAC-04: IDENTIFICATION &amp; AUTHENTICATION FOR DEVICES</b>	<b>282</b>
<i>P-IAC-04(A): IDENTIFICATION &amp; AUTHENTICATION FOR DEVICES   DEVICE ATTESTATION</i>	282
<b>P-IAC-05: IDENTIFICATION &amp; AUTHENTICATION FOR THIRD PARTY SYSTEMS &amp; SERVICES</b>	<b>283</b>
<i>P-IAC-05(A): IDENTIFICATION &amp; AUTHENTICATION FOR THIRD PARTY SYSTEMS &amp; SERVICES   INFORMATION EXCHANGE</i>	283
<b>P-IAC-06: MULTIFACTOR AUTHENTICATION (MFA)</b>	<b>284</b>
<i>P-IAC-06(A): MULTI-FACTOR AUTHENTICATION (MFA)   NETWORK ACCESS TO PRIVILEGED ACCOUNTS</i>	284
<i>P-IAC-06(B): MULTI-FACTOR AUTHENTICATION (MFA)   NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS</i>	285
<i>P-IAC-06(C): MULTI-FACTOR AUTHENTICATION (MFA)   LOCAL ACCESS TO PRIVILEGED ACCOUNTS</i>	286
<i>P-IAC-06(D): MULTI-FACTOR AUTHENTICATION (MFA)   OUT OF BAND (OOB) FACTOR</i>	286
<b>P-IAC-07: USER PROVISIONING &amp; DE-PROVISIONING</b>	<b>287</b>
<i>P-IAC-07(A): USER PROVISIONING &amp; DE-PROVISIONING   CHANGE OF ROLES &amp; DUTIES</i>	287
<i>P-IAC-07(B): USER PROVISIONING &amp; DE-PROVISIONING   TERMINATION OF EMPLOYMENT</i>	288
<b>P-IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)</b>	<b>289</b>
<b>P-IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)</b>	<b>289</b>
<i>P-IAC-09(A): IDENTIFIER MANAGEMENT   USER IDENTITY (ID) MANAGEMENT</i>	291
<i>P-IAC-09(B): IDENTIFIER MANAGEMENT   IDENTITY USER STATUS</i>	292
<i>P-IAC-09(C): IDENTIFIER MANAGEMENT   DYNAMIC MANAGEMENT</i>	292
<i>P-IAC-09(D): IDENTIFIER MANAGEMENT   CROSS-ORGANIZATION MANAGEMENT</i>	293
<i>P-IAC-09(E): IDENTIFIER MANAGEMENT   PRIVILEGED ACCOUNT IDENTIFIERS</i>	294
<i>P-IAC-09(F): IDENTIFIER MANAGEMENT   PAIRWISE PSEUDONYMOUS IDENTIFIERS (PPID)</i>	295
<b>P-IAC-10: AUTHENTICATOR MANAGEMENT (PASSWORDS)</b>	<b>296</b>
<i>P-IAC-10(A): AUTHENTICATOR MANAGEMENT   PASSWORD-BASED AUTHENTICATION</i>	297
<i>P-IAC-10(B): AUTHENTICATOR MANAGEMENT   PKI-BASED AUTHENTICATION</i>	297
<i>P-IAC-10(C): AUTHENTICATOR MANAGEMENT   IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION</i>	298
<i>P-IAC-10(D): AUTHENTICATOR MANAGEMENT   AUTOMATED SUPPORT FOR PASSWORD STRENGTH</i>	298

<i>P-IAC-10(E): AUTHENTICATOR MANAGEMENT   PROTECTION OF AUTHENTICATORS</i>	299
<i>P-IAC-10(F): AUTHENTICATOR MANAGEMENT   NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS</i>	300
<i>P-IAC-10(G): AUTHENTICATOR MANAGEMENT   HARDWARE TOKEN-BASED AUTHENTICATION</i>	300
<i>P-IAC-10(H): AUTHENTICATOR MANAGEMENT   VENDOR-SUPPLIED DEFAULTS</i>	301
<i>P-IAC-10(I): AUTHENTICATOR MANAGEMENT   MULTIPLE INFORMATION SYSTEM ACCOUNTS</i>	302
<i>P-IAC-10(J): AUTHENTICATOR MANAGEMENT   EXPIRATION OF CACHED AUTHENTICATORS</i>	302
<b>P-IAC-11: AUTHENTICATOR FEEDBACK</b>	<b>302</b>
<b>P-IAC-12: CRYPTOGRAPHIC MODULE AUTHENTICATION</b>	<b>303</b>
<b>P-IAC-13: ADAPTIVE IDENTIFICATION &amp; AUTHENTICATION</b>	<b>304</b>
<b>P-IAC-14: RE-AUTHENTICATION</b>	<b>304</b>
<b>P-IAC-15: ACCOUNT MANAGEMENT</b>	<b>305</b>
<i>P-IAC-15(A): ACCOUNT MANAGEMENT   AUTOMATED SYSTEM ACCOUNT MANAGEMENT</i>	306
<i>P-IAC-15(B): ACCOUNT MANAGEMENT   REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS</i>	307
<i>P-IAC-15(C): ACCOUNT MANAGEMENT   DISABLE INACTIVE ACCOUNTS</i>	307
<i>P-IAC-15(D): ACCOUNT MANAGEMENT   AUTOMATED AUDIT ACTIONS</i>	308
<i>P-IAC-15(E): ACCOUNT MANAGEMENT   RESTRICTIONS ON SHARED GROUPS / ACCOUNTS</i>	308
<i>P-IAC-15(F): ACCOUNT MANAGEMENT   ACCOUNT DISABLING FOR HIGH RISK INDIVIDUALS</i>	309
<i>P-IAC-15(G): ACCOUNT MANAGEMENT   SYSTEM ACCOUNTS</i>	310
<i>P-IAC-15(H): ACCOUNT MANAGEMENT   USAGE CONDITIONS</i>	310
<b>P-IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)</b>	<b>311</b>
<i>P-IAC-16(A): PRIVILEGED ACCOUNT MANAGEMENT (PAM)   PRIVILEGED ACCOUNT INVENTORIES</i>	311
<b>P-IAC-17: PERIODIC REVIEW</b>	<b>312</b>
<b>P-IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT</b>	<b>313</b>
<b>P-IAC-19: CREDENTIAL SHARING</b>	<b>313</b>
<b>P-IAC-20: ACCESS ENFORCEMENT</b>	<b>314</b>
<i>P-IAC-20(A): ACCESS ENFORCEMENT   ACCESS TO SENSITIVE DATA</i>	315
<i>P-IAC-20(B): ACCESS ENFORCEMENT   DATABASE ACCESS</i>	316
<i>P-IAC-20(C): ACCESS ENFORCEMENT   USE OF PRIVILEGED UTILITY PROGRAMS</i>	316
<i>P-IAC-20(D): ACCESS ENFORCEMENT   DEDICATED ADMINISTRATIVE MACHINES</i>	317
<i>P-IAC-20(E): ACCESS ENFORCEMENT   DUAL AUTHORIZATION FOR PRIVILEGED COMMANDS</i>	318
<b>P-IAC-21: LEAST PRIVILEGE</b>	<b>318</b>
<i>P-IAC-21(A): LEAST PRIVILEGE   AUTHORIZE ACCESS TO SECURITY FUNCTIONS</i>	319
<i>P-IAC-21(B): LEAST PRIVILEGE   NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS</i>	320
<i>P-IAC-21(C): LEAST PRIVILEGE   PRIVILEGED ACCOUNTS</i>	320
<i>P-IAC-21(D): LEAST PRIVILEGE   AUDITING USE OF PRIVILEGED FUNCTIONS</i>	321
<i>P-IAC-21(E): LEAST PRIVILEGE   PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS</i>	322
<i>P-IAC-21(F): LEAST PRIVILEGE   NETWORK ACCESS TO PRIVILEGED COMMANDS</i>	322
<i>P-IAC-21(G): LEAST PRIVILEGE   PRIVILEGE LEVELS FOR CODE EXECUTION</i>	323
<b>P-IAC-22: ACCOUNT LOCKOUT</b>	<b>323</b>
<b>P-IAC-23: CONCURRENT SESSION CONTROL</b>	<b>324</b>
<b>P-IAC-24: SESSION LOCK</b>	<b>324</b>
<i>P-IAC-24(A): SESSION LOCK   PATTERN-HIDING DISPLAYS</i>	325
<b>P-IAC-25: SESSION TERMINATION</b>	<b>326</b>
<b>P-IAC-26: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHORIZATION</b>	<b>326</b>
<b>P-IAC-27: REFERENCE MONITOR</b>	<b>327</b>
<b>P-IAC-28: IDENTITY PROOFING</b>	<b>327</b>
<i>P-IAC-28(A): IDENTITY PROOFING   SUPERVISOR AUTHORIZATION</i>	328
<i>P-IAC-28(B): IDENTITY PROOFING   IDENTITY EVIDENCE</i>	329
<i>P-IAC-28(C): IDENTITY PROOFING   IDENTITY EVIDENCE VALIDATION &amp; VERIFICATION</i>	329
<i>P-IAC-28(D): IDENTITY PROOFING   IN-PERSON VALIDATION &amp; VERIFICATION</i>	330
<i>P-IAC-28(E): IDENTITY PROOFING   ADDRESS CONFIRMATION</i>	331
<b>INCIDENT RESPONSE (IRO) PROCEDURES</b>	<b>332</b>
<b>P-IRO-01: INCIDENTS RESPONSE OPERATIONS</b>	<b>332</b>
<b>P-IRO-02: INCIDENT HANDLING</b>	<b>332</b>
<i>P-IRO-02(A): INCIDENT HANDLING   AUTOMATED INCIDENT HANDLING PROCESSES</i>	333
<i>P-IRO-02(B): INCIDENT HANDLING   IDENTITY THEFT PROTECTION PROGRAM (ITPP)</i>	334
<i>P-IRO-02(C): INCIDENT HANDLING   DYNAMIC RECONFIGURATION</i>	335
<i>P-IRO-02(D): INCIDENT HANDLING   CONTINUITY OF OPERATIONS</i>	335

<i>P-IRO-02(E): INCIDENT HANDLING   CORRELATION WITH EXTERNAL ORGANIZATIONS</i>	337
<b>P-IRO-03: INDICATORS OF COMPROMISE (IOC)</b>	<b>337</b>
<b>P-IRO-04: INCIDENT RESPONSE PLAN (IRP)</b>	<b>338</b>
<i>P-IRO-04(A): INCIDENT RESPONSE PLAN (IRP)   PERSONAL DATA (PD) PROCESSES</i>	339
<i>P-IRO-04(B): INCIDENT RESPONSE PLAN (IRP)   IRP UPDATE</i>	339
<b>P-IRO-05: INCIDENT RESPONSE TRAINING</b>	<b>340</b>
<i>P-IRO-05(A): INCIDENT RESPONSE TRAINING   SIMULATED INCIDENTS</i>	341
<i>P-IRO-05(B): INCIDENT RESPONSE TRAINING   AUTOMATED INCIDENT RESPONSE TRAINING ENVIRONMENTS</i>	341
<b>P-IRO-06: INCIDENT RESPONSE TESTING</b>	<b>341</b>
<i>P-IRO-06(A): INCIDENT RESPONSE TESTING   COORDINATION WITH RELATED PLANS</i>	342
<b>P-IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)</b>	<b>342</b>
<b>P-IRO-08: CHAIN OF CUSTODY &amp; FORENSICS</b>	<b>343</b>
<b>P-IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS</b>	<b>344</b>
<i>P-IRO-09(A): SITUATIONAL AWARENESS FOR INCIDENTS   AUTOMATED TRACKING, DATA COLLECTION &amp; ANALYSIS</i>	345
<b>P-IRO-10: INCIDENT REPORTING</b>	<b>345</b>
<i>P-IRO-10(A): INCIDENT REPORTING   AUTOMATED REPORTING</i>	346
<i>P-IRO-10(B): INCIDENT REPORTING   CYBER INCIDENT REPORTING FOR COVERED DEFENSE INFORMATION (CDI)</i>	346
<i>P-IRO-10(C): INCIDENT REPORTING   VULNERABILITIES RELATED TO INCIDENTS</i>	347
<i>P-IRO-10(D): INCIDENT REPORTING   SUPPLY CHAIN COORDINATION</i>	348
<b>P-IRO-11: INCIDENT REPORTING ASSISTANCE</b>	<b>349</b>
<i>P-IRO-11(A): INCIDENT REPORTING ASSISTANCE   AUTOMATION SUPPORT OF AVAILABILITY OF INFORMATION / SUPPORT</i>	350
<i>P-IRO-11(B): INCIDENT REPORTING ASSISTANCE   COORDINATION WITH EXTERNAL PROVIDERS</i>	350
<b>P-IRO-12: INFORMATION SPILLAGE RESPONSE</b>	<b>351</b>
<i>P-IRO-12(A): INFORMATION SPILLAGE RESPONSE   RESPONSIBLE PERSONNEL</i>	352
<i>P-IRO-12(B): INFORMATION SPILLAGE RESPONSE   TRAINING</i>	352
<i>P-IRO-12(C): INFORMATION SPILLAGE RESPONSE   POST-SPILL OPERATIONS</i>	353
<i>P-IRO-12(D): INFORMATION SPILLAGE RESPONSE   EXPOSURE TO UNAUTHORIZED PERSONNEL</i>	353
<b>P-IRO-13: ROOT CAUSE ANALYSIS (RCA) &amp; LESSONS LEARNED</b>	<b>354</b>
<b>P-IRO-14: REGULATORY &amp; LAW ENFORCEMENT CONTACTS</b>	<b>355</b>
<b>P-IRO-15: DETONATION CHAMBERS</b>	<b>355</b>
<b>INFORMATION ASSURANCE (IAO) PROCEDURES</b>	<b>357</b>
<b>P-IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS</b>	<b>357</b>
<b>P-IAO-02: SECURITY ASSESSMENTS</b>	<b>358</b>
<i>P-IAO-02(A): SECURITY ASSESSMENTS   INDEPENDENT ASSESSORS</i>	358
<i>P-IAO-02(B): SECURITY ASSESSMENTS   SPECIALIZED ASSESSMENTS</i>	359
<i>P-IAO-02(C): SECURITY ASSESSMENTS   EXTERNAL ORGANIZATIONS</i>	360
<b>P-IAO-03: SYSTEM SECURITY PLANS (SSP)</b>	<b>360</b>
<i>P-IAO-03(A): PL-02(A): SYSTEM SECURITY PLAN   PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES</i>	362
<i>P-IAO-03(B): PL-02(B): SYSTEM SECURITY PLAN   ADEQUATE SECURITY FOR COVERED DEFENSE INFORMATION (CDI)</i>	362
<b>P-IAO-04: THREAT ANALYSIS &amp; FLAW REMEDIATION DURING DEVELOPMENT</b>	<b>363</b>
<b>P-IAO-05: PLAN OF ACTION &amp; MILESTONES (POA&amp;M)</b>	<b>364</b>
<b>P-IAO-06: TECHNICAL VERIFICATION</b>	<b>365</b>
<b>P-IAO-07: SECURITY AUTHORIZATION</b>	<b>365</b>
<b>MAINTENANCE (MNT) PROCEDURES</b>	<b>367</b>
<b>P-MNT-01: MAINTENANCE OPERATIONS</b>	<b>367</b>
<b>P-MNT-02: CONTROLLED MAINTENANCE</b>	<b>367</b>
<i>P-MNT-02(A): CONTROLLED MAINTENANCE   AUTOMATED MAINTENANCE ACTIVITIES</i>	368
<b>P-MNT-03: TIMELY MAINTENANCE</b>	<b>368</b>
<i>P-MNT-03(A): TIMELY MAINTENANCE   PREVENTATIVE MAINTENANCE</i>	369
<i>P-MNT-03(B): TIMELY MAINTENANCE   PREDICTIVE MAINTENANCE</i>	370
<i>P-MNT-03(C): TIMELY MAINTENANCE   AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE</i>	370
<b>P-MNT-04: MAINTENANCE TOOLS</b>	<b>371</b>
<i>P-MNT-04(A): MAINTENANCE TOOLS   INSPECT TOOLS</i>	371
<i>P-MNT-04(B): MAINTENANCE TOOLS   INSPECT MEDIA</i>	372
<i>P-MNT-04(C): MAINTENANCE TOOLS   PREVENT UNAUTHORIZED REMOVAL</i>	372
<i>P-MNT-04(D): MAINTENANCE TOOLS   RESTRICT TOOL USE</i>	373
<b>P-MNT-05: NON-LOCAL MAINTENANCE</b>	<b>373</b>

<i>P-MNT-05(A): NON-LOCAL MAINTENANCE   AUDITING</i>	374
<i>P-MNT-05(B): NON-LOCAL MAINTENANCE   NOTIFICATION OF NON-LOCAL MAINTENANCE</i>	374
<i>P-MNT-05(C): NON-LOCAL MAINTENANCE   CRYPTOGRAPHIC PROTECTION</i>	375
<i>P-MNT-05(D): NON-LOCAL MAINTENANCE   REMOTE DISCONNECT VERIFICATION</i>	376
<i>P-MNT-05(E): NON-LOCAL MAINTENANCE   PRE-APPROVAL OF NON-LOCAL MAINTENANCE</i>	376
<i>P-MNT-05(F): NON-LOCAL MAINTENANCE   COMPARABLE SECURITY &amp; SANITIZATION</i>	377
<b>P-MNT-06: MAINTENANCE PERSONNEL</b>	<b>377</b>
<i>P-MNT-06(A): MAINTENANCE PERSONNEL   MAINTENANCE PERSONNEL WITHOUT APPROPRIATE ACCESS</i>	378
<i>P-MNT-06(B): MAINTENANCE PERSONNEL   NON-SYSTEM RELATED MAINTENANCE</i>	379
<b>MOBILE DEVICE MANAGEMENT (MDM) PROCEDURES</b>	<b>380</b>
<b>P-MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES</b>	<b>380</b>
<b>P-MDM-02: ACCESS CONTROL FOR MOBILE DEVICES</b>	<b>380</b>
<b>P-MDM-03: FULL DEVICE &amp; CONTAINER-BASED ENCRYPTION</b>	<b>382</b>
<b>P-MDM-04: TAMPER PROTECTION &amp; DETECTION</b>	<b>382</b>
<b>P-MDM-05: REMOTE PURGING</b>	<b>383</b>
<b>P-MDM-06: PERSONALLY-OWNED MOBILE DEVICES</b>	<b>383</b>
<b>P-MDM-07: ORGANIZATION-OWNED MOBILE DEVICES</b>	<b>385</b>
<b>P-MDM-08: MOBILE DEVICE DATA RETENTION LIMITATIONS</b>	<b>385</b>
<b>NETWORK SECURITY (NET) PROCEDURES</b>	<b>387</b>
<b>P-NET-01: NETWORK SECURITY MANAGEMENT</b>	<b>387</b>
<b>P-NET-02: LAYERED DEFENSES</b>	<b>387</b>
<i>P-NET-02(A): LAYERED DEFENSES   DENIAL OF SERVICE (DOS) PROTECTION</i>	388
<i>P-NET-02(B): LAYERED DEFENSES   GUEST NETWORKS</i>	389
<b>P-NET-03: BOUNDARY PROTECTION</b>	<b>390</b>
<i>P-NET-03(A): BOUNDARY PROTECTION   ACCESS POINTS</i>	391
<i>P-NET-03(B): BOUNDARY PROTECTION   EXTERNAL TELECOMMUNICATIONS SERVICES</i>	391
<i>P-NET-03(C): BOUNDARY PROTECTION   INTERNAL NETWORK ADDRESS SPACE</i>	392
<i>P-NET-03(D): BOUNDARY PROTECTION   PERSONAL DATA (PD)</i>	393
<i>P-NET-03(E): BOUNDARY PROTECTION   PREVENT UNAUTHORIZED EXFILTRATION</i>	393
<i>P-NET-03(F): BOUNDARY PROTECTION   DYNAMIC ISOLATION &amp; SEGREGATION (SANDBOXING)</i>	394
<i>P-NET-03(G): BOUNDARY PROTECTION   ISOLATION OF INFORMATION SYSTEM COMPONENTS (DMZ)</i>	394
<i>P-NET-03(H): BOUNDARY PROTECTION   SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS</i>	395
<b>P-NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)</b>	<b>395</b>
<i>P-NET-04(A): DATA FLOW ENFORCEMENT   DENY TRAFFIC BY DEFAULT &amp; ALLOW TRAFFIC BY EXCEPTION</i>	396
<i>P-NET-04(B): DATA FLOW ENFORCEMENT   OBJECT SECURITY ATTRIBUTES</i>	397
<i>P-NET-04(C): DATA FLOW ENFORCEMENT   CONTENT CHECK FOR ENCRYPTED DATA</i>	397
<i>P-NET-04(D): DATA FLOW ENFORCEMENT   EMBEDDED DATA TYPES</i>	398
<i>P-NET-04(E): DATA FLOW ENFORCEMENT   METADATA</i>	398
<i>P-NET-04(F): DATA FLOW ENFORCEMENT   HUMAN REVIEWS</i>	399
<i>P-NET-04(G): DATA FLOW ENFORCEMENT   SECURITY POLICY FILTERS</i>	400
<i>P-NET-04(H): DATA FLOW ENFORCEMENT   DATA TYPE IDENTIFIERS</i>	400
<i>P-NET-04(I): DATA FLOW ENFORCEMENT   DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS</i>	401
<i>P-NET-04(J): DATA FLOW ENFORCEMENT   DETECTION OF UNSANCTIONED INFORMATION</i>	401
<i>P-NET-04(K): DATA FLOW ENFORCEMENT   APPROVED SOLUTIONS</i>	402
<b>P-NET-05: SYSTEM INTERCONNECTIONS</b>	<b>402</b>
<i>P-NET-05(A): SYSTEM INTERCONNECTIONS   EXTERNAL SYSTEM CONNECTIONS</i>	403
<i>P-NET-05(B): SYSTEM INTERCONNECTIONS   INTERNAL SYSTEM CONNECTIONS</i>	404
<b>P-NET-06: NETWORK SEGMENTATION</b>	<b>404</b>
<i>P-NET-06(A): SECURITY FUNCTION ISOLATION   SECURITY MANAGEMENT SUBNETS</i>	405
<i>P-NET-06(B): SECURITY FUNCTION ISOLATION   VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION</i>	406
<b>P-NET-07: NETWORK DISCONNECT</b>	<b>407</b>
<b>P-NET-08: NETWORK INTRUSION DETECTION &amp; PREVENTION SYSTEMS (NIDS / NIPS)</b>	<b>408</b>
<i>P-NET-08(A): NETWORK INTRUSION DETECTION &amp; PREVENTION SYSTEMS (NIDS / NIPS)   DMZ NETWORKS</i>	408
<i>P-NET-08(B): NETWORK INTRUSION DETECTION &amp; PREVENTION SYSTEMS (NIDS / NIPS)   WIRELESS INTRUSION DETECTION / PREVENTION SYSTEMS (WIDS / WIPS)</i>	409
<b>P-NET-09: SESSION AUTHENTICITY</b>	<b>410</b>
<i>P-NET-09(A): SESSION AUTHENTICITY   INVALIDATE SESSION IDENTIFIERS AT LOGOUT</i>	410

<b>P-NET-10 DOMAIN NAME SERVICE (DNS) RESOLUTION</b>	<b>411</b>
<i>P-NET-10(A): DOMAIN NAME SERVICE (DNS) RESOLUTION   ARCHITECTURE &amp; PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE</i>	411
<i>P-NET-10(B): DOMAIN NAME SERVICE (DNS) RESOLUTION   SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)</i>	412
<b>P-NET-11: OUT-OF-BAND CHANNELS</b>	<b>413</b>
<b>P-NET-12: SAFEGUARDING DATA OVER OPEN NETWORKS</b>	<b>413</b>
<i>P-NET-12(A): SAFEGUARDING DATA OVER OPEN NETWORKS   WIRELESS LINK PROTECTION</i>	414
<i>P-NET-12(B): SAFEGUARDING DATA OVER OPEN NETWORKS   END-USER MESSAGING TECHNOLOGIES</i>	415
<b>P-NET-13: ELECTRONIC MESSAGING</b>	<b>416</b>
<b>P-NET-14: REMOTE ACCESS</b>	<b>417</b>
<i>P-NET-14(A): REMOTE ACCESS   AUTOMATED MONITORING &amp; CONTROL</i>	417
<i>P-NET-14(B): REMOTE ACCESS   PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION</i>	418
<i>P-NET-14(C): REMOTE ACCESS   MANAGED ACCESS CONTROL POINTS</i>	419
<i>P-NET-14(D): REMOTE ACCESS   PRIVILEGED COMMANDS &amp; ACCESS</i>	419
<i>P-NET-14(E): REMOTE ACCESS   TELECOMMUTING</i>	420
<i>P-NET-14(F): REMOTE ACCESS   THIRD-PARTY REMOTE ACCESS GOVERNANCE</i>	420
<i>P-NET-14(G): REMOTE ACCESS   ENDPOINT SECURITY VALIDATION</i>	421
<i>P-NET-14(H): REMOTE ACCESS   EXPEDITIOUS DISCONNECT / DISABLE CAPABILITY</i>	422
<b>P-NET-15: WIRELESS NETWORKING</b>	<b>422</b>
<i>P-NET-15(A): WIRELESS ACCESS   AUTHENTICATION &amp; ENCRYPTION</i>	423
<i>P-NET-15(B): WIRELESS ACCESS   DISABLE WIRELESS NETWORKING</i>	424
<i>P-NET-15(C): WIRELESS ACCESS   RESTRICT CONFIGURATION BY USERS</i>	424
<i>P-NET-15(D): WIRELESS ACCESS   WIRELESS BOUNDARIES</i>	425
<i>P-NET-15(E): WIRELESS ACCESS   ROGUE WIRELESS DETECTION</i>	426
<b>P-NET-16: INTRANETS</b>	<b>426</b>
<b>P-NET-17: DATA LOSS PREVENTION (DLP)</b>	<b>427</b>
<b>P-NET-18: CONTENT FILTERING</b>	<b>428</b>
<i>P-NET-18(A): CONTENT FILTERING   ROUTE TRAFFIC TO PROXY SERVERS</i>	428
<b>PHYSICAL &amp; ENVIRONMENTAL SECURITY (PES) PROCEDURES</b>	<b>430</b>
<b>P-PES-01: PHYSICAL &amp; ENVIRONMENTAL PROTECTIONS</b>	<b>430</b>
<b>P-PES-02: PHYSICAL ACCESS AUTHORIZATIONS</b>	<b>430</b>
<i>P-PES-02(A): PHYSICAL ACCESS AUTHORIZATIONS   ROLE-BASED PHYSICAL ACCESS</i>	431
<b>P-PES-03: PHYSICAL ACCESS CONTROL</b>	<b>432</b>
<i>P-PES-03(A): PHYSICAL ACCESS CONTROL   CONTROLLED INGRESS &amp; EGRESS POINTS</i>	432
<i>P-PES-03(B): PHYSICAL ACCESS CONTROL   LOCKABLE PHYSICAL CASINGS</i>	433
<i>P-PES-03(C): PHYSICAL ACCESS CONTROL   PHYSICAL ACCESS LOGS</i>	434
<i>P-PES-03(D): PHYSICAL ACCESS CONTROL   ACCESS TO INFORMATION SYSTEMS</i>	434
<b>P-PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS &amp; FACILITIES</b>	<b>435</b>
<i>P-PES-04(A): PHYSICAL SECURITY OF OFFICES, ROOMS &amp; FACILITIES   WORKING IN SECURE AREAS</i>	436
<b>P-PES-05: MONITORING PHYSICAL ACCESS</b>	<b>436</b>
<i>P-PES-05(A): MONITORING PHYSICAL ACCESS   INTRUSION ALARMS / SURVEILLANCE EQUIPMENT</i>	437
<i>P-PES-05(B): MONITORING PHYSICAL ACCESS   MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS</i>	438
<b>P-PES-06: VISITOR CONTROL</b>	<b>438</b>
<i>P-PES-06(A): VISITOR CONTROL   DISTINGUISH VISITORS FROM ON-SITE PERSONNEL</i>	439
<i>P-PES-06(B): VISITOR CONTROL   IDENTIFICATION REQUIREMENT</i>	440
<i>P-PES-06(C): VISITOR CONTROL   RESTRICT UNESCORTED ACCESS</i>	440
<i>P-PES-06(D): VISITOR CONTROL   AUTOMATED RECORDS MANAGEMENT &amp; REVIEW</i>	441
<b>P-PES-07: SUPPORTING UTILITIES</b>	<b>441</b>
<i>P-PES-07(A): SUPPORTING UTILITIES   AUTOMATIC VOLTAGE CONTROLS</i>	442
<i>P-PES-07(B): SUPPORTING UTILITIES   EMERGENCY SHUTOFF</i>	443
<i>P-PES-07(C): SUPPORTING UTILITIES   EMERGENCY POWER</i>	443
<i>P-PES-07(D): SUPPORTING UTILITIES   EMERGENCY LIGHTING</i>	444
<i>P-PES-07(E): SUPPORTING UTILITIES   WATER DAMAGE PROTECTION</i>	445
<i>P-PES-07(F): SUPPORTING UTILITIES   AUTOMATION SUPPORT FOR WATER DAMAGE PROTECTION</i>	445
<b>P-PES-08: FIRE PROTECTION</b>	<b>446</b>
<i>P-PES-08(A): FIRE PROTECTION   FIRE DETECTION DEVICES</i>	446
<i>P-PES-08(B): FIRE PROTECTION   FIRE SUPPRESSION DEVICES</i>	447

<i>P-PES-08(c): FIRE PROTECTION   AUTOMATIC FIRE SUPPRESSION</i>	447
<b>P-PES-09: TEMPERATURE &amp; HUMIDITY CONTROLS</b>	<b>448</b>
<i>P-PES-09(A): TEMPERATURE &amp; HUMIDITY CONTROLS   MONITORING WITH ALARMS / NOTIFICATIONS</i>	448
<b>P-PES-10: DELIVERY &amp; REMOVAL</b>	<b>449</b>
<b>P-PES-11: ALTERNATE WORK SITE</b>	<b>450</b>
<b>P-PES-12: EQUIPMENT SITING &amp; PROTECTION</b>	<b>450</b>
<i>P-PES-12(A): EQUIPMENT SITING &amp; PROTECTION   ACCESS CONTROL FOR TRANSMISSION MEDIUM</i>	451
<i>P-PES-12(B): EQUIPMENT SITING &amp; PROTECTION   ACCESS CONTROL FOR OUTPUT DEVICES</i>	452
<b>P-PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS</b>	<b>453</b>
<b>P-PES-14: ASSET MONITORING AND TRACKING</b>	<b>453</b>
<b>P-PES-15: ELECTROMAGNETIC PULSE (EMP) PROTECTION</b>	<b>454</b>
<b>P-PES-16: COMPONENT MARKING</b>	<b>455</b>
<b>PRIVACY (PRI) PROCEDURES</b>	<b>456</b>
<b>P-PRI-01: PRIVACY PROGRAM</b>	<b>456</b>
<i>P-PRI-01(A): PRIVACY PROGRAM   CHIEF PRIVACY OFFICER (CPO)</i>	456
<i>P-PRI-01(B): PRIVACY PROGRAM   PRIVACY ACT STATEMENTS</i>	457
<i>P-PRI-01(C): PRIVACY PROGRAM   DISSEMINATION OF PRIVACY PROGRAM INFORMATION</i>	457
<i>P-PRI-01(D): PRIVACY PROGRAM   DATA PROTECTION OFFICER (DPO)</i>	458
<b>P-PRI-02: PRIVACY NOTICE</b>	<b>459</b>
<i>P-PRI-02(A): PRIVACY NOTICE   PURPOSE SPECIFICATION</i>	459
<i>P-PRI-02(B): PRIVACY NOTICE   AUTOMATED DATA MANAGEMENT PROCESSES</i>	460
<i>P-PRI-02(C): PRIVACY NOTICE   COMPUTER MATCHING AGREEMENTS (CMA)</i>	461
<b>P-PRI-03: CHOICE &amp; CONSENT</b>	<b>461</b>
<i>P-PRI-03(A): CHOICE &amp; CONSENT   ATTRIBUTE MANAGEMENT</i>	462
<i>P-PRI-03(B): CHOICE &amp; CONSENT   JUST-IN-TIME NOTICE &amp; CONSENT</i>	462
<i>P-PRI-03(C): CHOICE &amp; CONSENT   PROHIBITION OF SELLING PERSONAL DATA</i>	463
<b>P-PRI-04: COLLECTION</b>	<b>463</b>
<i>P-PRI-04(A): COLLECTION   AUTHORITY TO COLLECT</i>	464
<b>P-PRI-05: USE, RETENTION &amp; DISPOSAL</b>	<b>465</b>
<i>P-PRI-05(A): USE, RETENTION &amp; DISPOSAL   INTERNAL USE</i>	465
<i>P-PRI-05(B): USE, RETENTION &amp; DISPOSAL   DATA INTEGRITY</i>	466
<i>P-PRI-05(C): USE, RETENTION &amp; DISPOSAL   DATA MASKING</i>	467
<i>P-PRI-05(D): USE, RETENTION &amp; DISPOSAL   USAGE RESTRICTIONS OF PERSONAL DATA (PD)</i>	467
<i>P-PRI-05(E): USE, RETENTION &amp; DISPOSAL   INVENTORY OF PERSONAL DATA (PD)</i>	468
<i>P-PRI-05(F): USE, RETENTION &amp; DISPOSAL   PERSONAL DATA (PD) INVENTORY AUTOMATION SUPPORT</i>	468
<b>P-PRI-06: DATA SUBJECT ACCESS</b>	<b>469</b>
<i>P-PRI-06(A): DATA SUBJECT ACCESS   REDRESS INACCURATE INFORMATION</i>	470
<i>P-PRI-06(B): DATA SUBJECT ACCESS   NOTICE OF CORRECTION OF AMENDMENT</i>	471
<i>P-PRI-06(C): DATA SUBJECT ACCESS   APPEAL ADVERSE DECISION</i>	471
<i>P-PRI-06(D): DATA SUBJECT ACCESS   USER FEEDBACK MANAGEMENT</i>	472
<i>P-PRI-06(E): DATA SUBJECT ACCESS   RIGHT TO ERASURE</i>	472
<i>P-PRI-06(F): DATA SUBJECT ACCESS   DATA PORTABILITY</i>	473
<i>P-PRI-06(G): DATA SUBJECT ACCESS   PERSONAL DATA EXPORTABILITY</i>	474
<b>P-PRI-07: INFORMATION SHARING WITH THIRD PARTIES</b>	<b>474</b>
<i>P-PRI-07(A): INFORMATION SHARING WITH THIRD PARTIES   PRIVACY REQUIREMENTS FOR CONTRACTORS &amp; SERVICE PROVIDERS</i>	475
<i>P-PRI-07(B): INFORMATION SHARING WITH THIRD PARTIES   JOINT PROCESSING OF PERSONAL DATA</i>	476
<i>P-PRI-07(C): INFORMATION SHARING WITH THIRD PARTIES   OBLIGATION TO INFORM THIRD PARTIES</i>	476
<i>P-PRI-07(D): INFORMATION SHARING WITH THIRD PARTIES   REJECT UNAUTHORIZED DISCLOSURE REQUESTS</i>	476
<b>P-PRI-08: TESTING, TRAINING &amp; MONITORING</b>	<b>477</b>
<b>P-PRI-09: PERSONAL DATA LINEAGE</b>	<b>477</b>
<b>P-PRI-10: DATA QUALITY MANAGEMENT</b>	<b>478</b>
<i>P-PRI-10(A): DATA QUALITY MANAGEMENT   AUTOMATION</i>	479
<i>P-PRI-10(B): DATA QUALITY MANAGEMENT   DATA ANALYTICS BIAS</i>	479
<b>P-PRI-11: DATA TAGGING</b>	<b>480</b>
<b>P-PRI-12: UPDATING PERSONAL DATA (PD)</b>	<b>480</b>
<b>P-PRI-13: DATA MANAGEMENT BOARD</b>	<b>481</b>
<b>P-PRI-14: PRIVACY REPORTING</b>	<b>482</b>

<i>P-PRI-14(A): PRIVACY REPORTING   ACCOUNTING OF DISCLOSURES</i>	483
<i>P-PRI-14(B): PRIVACY RECORDS &amp; REPORTING   NOTIFICATION OF DISCLOSURE REQUEST TO DATA SUBJECT</i>	483
<b>P-PRI-15: REGISTER DATABASE</b>	<b>484</b>
<b>PROJECT &amp; RESOURCE MANAGEMENT (PRM) PROCEDURES</b>	<b>485</b>
<b>P-PRM-01: SECURITY PORTFOLIO MANAGEMENT</b>	<b>485</b>
<i>P-PRM-01(A): SECURITY PORTFOLIO MANAGEMENT   STRATEGIC PLAN &amp; OBJECTIVES</i>	485
<i>P-PRM-01(B): SECURITY PORTFOLIO MANAGEMENT   TARGETED CAPABILITY MATURITY LEVELS</i>	486
<b>P-PRM-02: INFORMATION SECURITY RESOURCE MANAGEMENT</b>	<b>487</b>
<b>P-PRM-03: ALLOCATION OF RESOURCES</b>	<b>487</b>
<b>P-PRM-04: SECURITY &amp; PRIVACY IN PROJECT MANAGEMENT</b>	<b>488</b>
<b>P-PRM-05: SECURITY &amp; PRIVACY REQUIREMENTS DEFINITION</b>	<b>489</b>
<b>P-PRM-06: BUSINESS PROCESS DEFINITION</b>	<b>489</b>
<b>P-PRM-07: SECURE DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT</b>	<b>490</b>
<b>P-PRM-08: MANAGE ORGANIZATIONAL KNOWLEDGE</b>	<b>491</b>
<b>RISK MANAGEMENT (RSK) PROCEDURES</b>	<b>492</b>
<b>P-RSK-01: RISK MANAGEMENT PROGRAM</b>	<b>492</b>
<i>P-RSK-01(A): RISK MANAGEMENT PROGRAM (RMP)   RISK FRAMING</i>	492
<b>P-RSK-02: RISK-BASED SECURITY CATEGORIZATION</b>	<b>493</b>
<b>P-RSK-03: RISK IDENTIFICATION</b>	<b>494</b>
<b>P-RSK-04: RISK ASSESSMENT</b>	<b>494</b>
<i>P-RSK-04(A): RISK ASSESSMENT   RISK REGISTER</i>	495
<b>P-RSK-05: RISK RANKING</b>	<b>496</b>
<b>P-RSK-06: RISK REMEDIATION</b>	<b>497</b>
<i>P-RSK-06(A): RISK REMEDIATION   RISK RESPONSE</i>	497
<b>P-RSK-07: RISK ASSESSMENT UPDATE</b>	<b>498</b>
<b>P-RSK-08: BUSINESS IMPACT ANALYSIS (BIA)</b>	<b>498</b>
<b>P-RSK-09: SUPPLY CHAIN RISK MANAGEMENT PLAN</b>	<b>499</b>
<i>P-RSK-09(A): SUPPLY CHAIN RISK MANAGEMENT PLAN   SUPPLY CHAIN RISK ASSESSMENT</i>	500
<b>P-RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)</b>	<b>501</b>
<b>SECURE ENGINEERING &amp; ARCHITECTURE (SEA) PROCEDURES</b>	<b>503</b>
<b>P-SEA-01: SECURE ENGINEERING PRINCIPLES</b>	<b>503</b>
<i>P-SEA-01(A): SECURE ENGINEERING PRINCIPLES   CENTRALIZED MANAGEMENT OF CYBERSECURITY &amp; PRIVACY CONTROLS</i>	504
<b>P-SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE</b>	<b>505</b>
<i>P-SEA-02(A): ALIGNMENT WITH ENTERPRISE ARCHITECTURE   STANDARDIZED TERMINOLOGY</i>	505
<b>P-SEA-03: DEFENSE-IN-DEPTH (DID) ARCHITECTURE</b>	<b>506</b>
<i>P-SEA-03(A): DEFENSE-IN-DEPTH (DID) ARCHITECTURE   SYSTEM PARTITIONING</i>	507
<i>P-SEA-03(B): DEFENSE-IN-DEPTH (DID) ARCHITECTURE   APPLICATION PARTITIONING</i>	507
<b>P-SEA-04: PROCESS ISOLATION</b>	<b>508</b>
<i>P-SEA-04(A): PROCESS ISOLATION   SECURITY FUNCTION ISOLATION</i>	509
<i>P-SEA-04(B): PROCESS ISOLATION   HARDWARE SEPARATION</i>	510
<i>P-SEA-04(C): PROCESS ISOLATION   THREAD SEPARATION</i>	510
<b>P-SEA-05: INFORMATION IN SHARED RESOURCES</b>	<b>511</b>
<b>P-SEA-06: PREVENT PROGRAM EXECUTION</b>	<b>511</b>
<b>P-SEA-07: PREDICTABLE FAILURE ANALYSIS</b>	<b>512</b>
<i>P-SEA-07(A): PREDICTABLE FAILURE ANALYSIS   TECHNOLOGY LIFECYCLE MANAGEMENT</i>	513
<i>P-SEA-07(B): PREDICTABLE FAILURE ANALYSIS   FAIL SECURE</i>	513
<i>P-SEA-07(C): PREDICTABLE FAILURE ANALYSIS   FAIL SAFE</i>	514
<b>P-SEA-08: NON-PERSISTENCE</b>	<b>515</b>
<i>P-SEA-08(A): NON-PERSISTENCE   REFRESH FROM TRUSTED SOURCES</i>	515
<b>P-SEA-09: INFORMATION OUTPUT FILTERING</b>	<b>516</b>
<i>P-SEA-09(A): INFORMATION OUTPUT FILTERING   LIMIT PERSONAL DATA (PD) DISSEMINATION</i>	516
<b>P-SEA-10: MEMORY PROTECTION</b>	<b>517</b>
<b>P-SEA-11: HONEYPOTS</b>	<b>518</b>
<b>P-SEA-12: HONEYCLIENTS</b>	<b>518</b>
<b>P-SEA-13: HETEROGENEITY</b>	<b>519</b>
<i>P-SEA-13(A): HETEROGENEITY   VIRTUALIZATION TECHNIQUES</i>	520
<b>P-SEA-14: CONCEALMENT &amp; MISDIRECTION</b>	<b>520</b>

P-SEA-14(A): CONCEALMENT & MISDIRECTION   RANDOMNESS	521
P-SEA-14(B): CONCEALMENT & MISDIRECTION   CHANGE PROCESSING & STORAGE LOCATIONS	521
<b>P-SEA-15: DISTRIBUTED PROCESSING &amp; STORAGE</b>	<b>522</b>
<b>P-SEA-16: NON-MODIFIABLE EXECUTABLE PROGRAMS</b>	<b>522</b>
<b>P-SEA-17: SECURE LOG-ON PROCEDURES</b>	<b>523</b>
<b>P-SEA-18: SYSTEM USE NOTIFICATION (LOGON BANNER)</b>	<b>524</b>
P-SEA-18(A): SYSTEM USE NOTIFICATION   STANDARDIZED MICROSOFT WINDOWS BANNER	524
P-SEA-18(B): SYSTEM USE NOTIFICATION   TRUNCATED BANNER	525
<b>P-SEA-19: PREVIOUS LOGON NOTIFICATION</b>	<b>526</b>
<b>P-SEA-20: CLOCK SYNCHRONIZATION</b>	<b>526</b>
<b>SECURITY OPERATIONS (OPS) PROCEDURES</b>	<b>528</b>
<b>P-OPS-01: OPERATIONS SECURITY</b>	<b>528</b>
P-OPS-01(A): OPERATIONS SECURITY   STANDARDIZED OPERATING PROCEDURES (SOP)	528
<b>P-OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)</b>	<b>529</b>
<b>P-OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)</b>	<b>530</b>
<b>P-OPS-04: SECURITY OPERATIONS CENTER (SOC)</b>	<b>531</b>
<b>SECURITY AWARENESS &amp; TRAINING (SAT) PROCEDURES</b>	<b>532</b>
<b>P-SAT-01: SECURITY &amp; PRIVACY-MINDED WORKFORCE</b>	<b>532</b>
<b>P-SAT-02: SECURITY &amp; PRIVACY AWARENESS</b>	<b>532</b>
P-SAT-02(A): SECURITY AWARENESS   PRACTICAL EXERCISES	533
P-SAT-02(B): SECURITY AWARENESS   SOCIAL ENGINEERING & MINING	534
<b>P-SAT-03: SECURITY &amp; PRIVACY TRAINING</b>	<b>535</b>
P-SAT-03(A): SECURITY & PRIVACY TRAINING   PRACTICAL EXERCISES	535
P-SAT-03(B): SECURITY & PRIVACY TRAINING   SUSPICIOUS COMMUNICATIONS & ANOMALOUS SYSTEM BEHAVIOR	536
P-SAT-03(C): SECURITY & PRIVACY TRAINING   SENSITIVE INFORMATION STORAGE, HANDLING & PROCESSING	537
P-SAT-03(D): SECURITY & PRIVACY TRAINING   VENDOR SECURITY TRAINING	537
P-SAT-03(E): SECURITY & PRIVACY TRAINING   PRIVILEGED USERS	538
<b>P-SAT-04: SECURITY &amp; PRIVACY TRAINING RECORDS</b>	<b>539</b>
<b>TECHNOLOGY DEVELOPMENT &amp; ACQUISITION (TDA) PROCEDURES</b>	<b>540</b>
<b>P-TDA-01: TECHNOLOGY DEVELOPMENT &amp; ACQUISITION</b>	<b>540</b>
P-TDA-01(A): TECHNOLOGY DEVELOPMENT & ACQUISITION   PRODUCT MANAGEMENT	540
P-TDA-01(B): TECHNOLOGY DEVELOPMENT & ACQUISITION   INTEGRITY MECHANISMS FOR SOFTWARE / FIRMWARE UPDATES	541
P-TDA-01(C): TECHNOLOGY DEVELOPMENT & ACQUISITION   MALWARE TESTING PRIOR TO RELEASE	542
<b>P-TDA-02: SECURITY REQUIREMENTS</b>	<b>543</b>
P-TDA-02(A): SECURITY REQUIREMENTS   PORTS, PROTOCOLS & SERVICES IN USE	543
P-TDA-02(B): SECURITY REQUIREMENTS   USE OF APPROVED PIV PRODUCTS	544
P-TDA-02(C): SECURITY REQUIREMENTS   DEVELOPMENT METHODS, TECHNIQUES & PROCESSES	544
<b>P-TDA-03: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS</b>	<b>545</b>
P-TDA-03(A): COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS   SUPPLIER DIVERSITY	545
<b>P-TDA-04: DOCUMENTATION REQUIREMENTS</b>	<b>546</b>
P-TDA-04(A): DOCUMENTATION REQUIREMENTS   FUNCTIONAL PROPERTIES	547
<b>P-TDA-05: DEVELOPER ARCHITECTURE &amp; DESIGN</b>	<b>548</b>
<b>P-TDA-06: SECURE CODING</b>	<b>549</b>
P-TDA-06(A): SECURE CODING   CRITICALITY ANALYSIS	550
<b>P-TDA-07: SECURE DEVELOPMENT ENVIRONMENTS</b>	<b>550</b>
<b>P-TDA-08: SEPARATION OF DEVELOPMENT, TESTING &amp; OPERATIONAL ENVIRONMENTS</b>	<b>551</b>
<b>P-TDA-09: SECURITY &amp; PRIVACY TESTING THROUGHOUT DEVELOPMENT</b>	<b>552</b>
P-TDA-09(A): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT   CONTINUOUS MONITORING PLAN	553
P-TDA-09(B): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT   STATIC CODE ANALYSIS	553
P-TDA-09(C): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT   DYNAMIC CODE ANALYSIS	554
P-TDA-09(D): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT   MALFORMED INPUT TESTING	555
P-TDA-09(E): SECURITY & PRIVACY TESTING THROUGHOUT DEVELOPMENT   APPLICATION PENETRATION TESTING	555
<b>P-TDA-10: USE OF LIVE DATA</b>	<b>556</b>
P-TDA-10(A): USE OF LIVE DATA   TEST DATA INTEGRITY	557
<b>P-TDA-11: COMPONENT AUTHENTICITY</b>	<b>557</b>
P-TDA-11(A): COMPONENT AUTHENTICITY   ANTI-COUNTERFEIT TRAINING	558



<i>P-TDA-11(B): COMPONENT AUTHENTICITY   COMPONENT DISPOSAL</i>	559
<b>P-TDA-12: CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS</b>	<b>559</b>
<b>P-TDA-13: DEVELOPER SCREENING</b>	<b>560</b>
<b>P-TDA-14: DEVELOPER CONFIGURATION MANAGEMENT</b>	<b>561</b>
<i>P-TDA-14(A): DEVELOPER CONFIGURATION MANAGEMENT   SOFTWARE / FIRMWARE INTEGRITY VERIFICATION</i>	562
<b>P-TDA-15: DEVELOPER THREAT ANALYSIS &amp; FLAW REMEDIATION</b>	<b>562</b>
<b>P-TDA-16: DEVELOPER-PROVIDED TRAINING</b>	<b>563</b>
<b>P-TDA-17: UNSUPPORTED SYSTEMS</b>	<b>564</b>
<i>P-TDA-17(A): UNSUPPORTED SYSTEMS   ALTERNATE SOURCES FOR CONTINUED SUPPORT</i>	565
<b>P-TDA-18: INPUT DATA VALIDATION</b>	<b>565</b>
<b>P-TDA-19: ERROR HANDLING</b>	<b>566</b>
<b>P-TDA-20: ACCESS TO PROGRAM SOURCE CODE</b>	<b>567</b>
<b>THIRD-PARTY MANAGEMENT (TPM) PROCEDURES</b>	<b>568</b>
<b>P-TPM-01: THIRD-PARTY MANAGEMENT</b>	<b>568</b>
<b>P-TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS</b>	<b>568</b>
<b>P-TPM-03: SUPPLY CHAIN PROTECTION</b>	<b>569</b>
<i>P-TPM-03(A): SUPPLY CHAIN PROTECTION   ACQUISITION STRATEGIES, TOOLS &amp; METHODS</i>	570
<i>P-TPM-03(B): SUPPLY CHAIN PROTECTION   LIMIT POTENTIAL HARM</i>	571
<i>P-TPM-03(C): SUPPLY CHAIN PROTECTION   PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES</i>	571
<b>P-TPM-04: THIRD-PARTY SERVICES</b>	<b>572</b>
<i>P-TPM-04(A): THIRD-PARTY SERVICES   THIRD-PARTY RISK ASSESSMENTS &amp; APPROVALS</i>	573
<i>P-TPM-04(B): THIRD-PARTY SERVICES   IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS &amp; SERVICES</i>	573
<i>P-TPM-04(C): THIRD-PARTY SERVICES   CONFLICT OF INTERESTS</i>	574
<i>P-TPM-04(D): THIRD-PARTY SERVICES   THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS</i>	575
<b>P-TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS</b>	<b>575</b>
<b>P-TPM-06: THIRD-PARTY PERSONNEL SECURITY</b>	<b>576</b>
<b>P-TPM-07: MONITORING FOR THIRD-PARTY INFORMATION DISCLOSURE</b>	<b>577</b>
<b>P-TPM-08: REVIEW OF THIRD-PARTY SERVICES</b>	<b>578</b>
<b>P-TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION</b>	<b>578</b>
<b>P-TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES</b>	<b>579</b>
<b>P-TPM-11: THIRD-PARTY INCIDENT RESPONSE &amp; RECOVERY CAPABILITIES</b>	<b>580</b>
<b>THREAT MANAGEMENT (THR) PROCEDURES</b>	<b>581</b>
<b>P-THR-01: THREAT AWARENESS PROGRAM</b>	<b>581</b>
<b>P-THR-02: INDICATORS OF EXPOSURE (IOE)</b>	<b>581</b>
<b>P-THR-03: THREAT INTELLIGENCE FEEDS</b>	<b>582</b>
<b>P-THR-04: INSIDER THREAT PROGRAM</b>	<b>583</b>
<b>P-THR-05: INSIDER THREAT AWARENESS</b>	<b>584</b>
<b>VULNERABILITY &amp; PATCH MANAGEMENT (VPM) PROCEDURES</b>	<b>585</b>
<b>P-VPM-01: VULNERABILITY &amp; PATCH MANAGEMENT PROGRAM</b>	<b>585</b>
<i>P-VPM-01(A): VULNERABILITY &amp; PATCH MANAGEMENT PROGRAM   ESTABLISH VULNERABILITY MANAGEMENT SCOPE</i>	585
<b>P-VPM-02: VULNERABILITY REMEDIATION PROCESS</b>	<b>586</b>
<b>P-VPM-03: VULNERABILITY RANKING</b>	<b>587</b>
<b>P-VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES</b>	<b>587</b>
<i>P-VPM-04(A): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES   STABLE VERSIONS</i>	588
<i>P-VPM-04(B): CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES   FLAW REMEDIATION WITH PERSONAL DATA (PD)</i>	589
<b>P-VPM-05: SOFTWARE PATCHING</b>	<b>589</b>
<i>P-VPM-05(A): SOFTWARE PATCHING   CENTRALIZED MANAGEMENT</i>	590
<i>P-VPM-05(B): SOFTWARE PATCHING   AUTOMATED REMEDIATION STATUS</i>	591
<i>P-VPM-05(C): SOFTWARE PATCHING   TIME TO REMEDIATE / BENCHMARKS FOR CORRECTIVE ACTION</i>	592
<i>P-VPM-05(D): SOFTWARE PATCHING   AUTOMATED SOFTWARE &amp; FIRMWARE UPDATES</i>	592
<i>P-VPM-05(E): SOFTWARE PATCHING   REMOVAL OF PREVIOUS VERSIONS</i>	593
<b>P-VPM-06: VULNERABILITY SCANNING</b>	<b>593</b>
<i>P-VPM-06(A): VULNERABILITY SCANNING   UPDATE TOOL CAPABILITY</i>	594
<i>P-VPM-06(B): VULNERABILITY SCANNING   BREADTH / DEPTH OF COVERAGE</i>	594
<i>P-VPM-06(C): VULNERABILITY SCANNING   PRIVILEGED ACCESS</i>	595
<i>P-VPM-06(D): VULNERABILITY SCANNING   TREND ANALYSIS</i>	596
<i>P-VPM-06(E): VULNERABILITY SCANNING   REVIEW HISTORICAL AUDIT LOGS</i>	596

<i>P-VPM-06(F): VULNERABILITY SCANNING   EXTERNAL VULNERABILITY ASSESSMENT SCANS</i>	597
<i>P-VPM-06(G): VULNERABILITY SCANNING   INTERNAL VULNERABILITY ASSESSMENT SCANS</i>	598
<i>P-VPM-06(H): VULNERABILITY SCANNING   ACCEPTABLE DISCOVERABLE INFORMATION</i>	598
<i>P-VPM-06(I): VULNERABILITY SCANNING   CORRELATE SCANNING INFORMATION</i>	599
<b>P-VPM-07: PENETRATION TESTING</b>	<b>599</b>
<i>P-VPM-07(A): PENETRATION TESTING   INDEPENDENT PENETRATION AGENT OR TEAM</i>	600
<b>P-VPM-08: TECHNICAL SURVEILLANCE COUNTERMEASURES SECURITY</b>	<b>601</b>
<b>P-VPM-09: REVIEWING VULNERABILITY SCANNER USAGE</b>	<b>601</b>
<b>P-VPM-10: RED TEAM EXERCISES</b>	<b>602</b>
<b>WEB SECURITY (WEB) PROCEDURES</b>	<b>604</b>
<b>P-WEB-01: WEB SECURITY</b>	<b>604</b>
<b>P-WEB-02: USE OF DEMILITARIZED ZONES (DMZ)</b>	<b>604</b>
<b>P-WEB-03: WEB APPLICATION FIREWALL (WAF)</b>	<b>605</b>
<b>P-WEB-04: CLIENT-FACING WEB SERVICES</b>	<b>606</b>
<b>P-WEB-05: COOKIE MANAGEMENT</b>	<b>606</b>
<b>P-WEB-06: STRONG CUSTOMER AUTHENTICATION (SCA)</b>	<b>607</b>
<b>GLOSSARY: ACRONYMS &amp; DEFINITIONS</b>	<b>609</b>
<b>ACRONYMS</b>	<b>609</b>
<b>DEFINITIONS</b>	<b>609</b>
<b>RECORD OF CHANGES</b>	<b>610</b>

EXAMPLE

## OVERVIEW, INSTRUCTIONS & EXAMPLE

### KEY TERMINOLOGY

With the Cybersecurity Standardized Operating Procedures (CSOP), it is important to understand a few key terms:

- **Procedure / Control Activity:** Procedures represent an established way of doing something, such as a series of actions conducted in a specified order or manner. Some organizations refer to procedures as “control activities” and the terms essentially synonymous. In the CSOP, the terms procedure or control activity can be used interchangeably.
- **Process Owner:** This is the name of the individual or team accountable for the procedure being performed. This identifies the *accountable party to ensure the procedure is performed*. This role is more oversight and managerial.
  - Example: The **Security Operations Center (SOC) Supervisor** is accountable for his/her team to collect log files, perform analysis and escalate potential incidents for further investigation.
- **Process Operator:** This is the name of the individual or team responsible to perform the procedure’s tasks. This identifies the *responsible party for actually performing the task*. This role is a “doer” and performs tasks.
  - Example: The **SOC analyst** is responsible for performing daily log reviews, evaluating anomalous activities and responding to potential incidents in accordance with the organization’s Incident Response Plan (IRP).

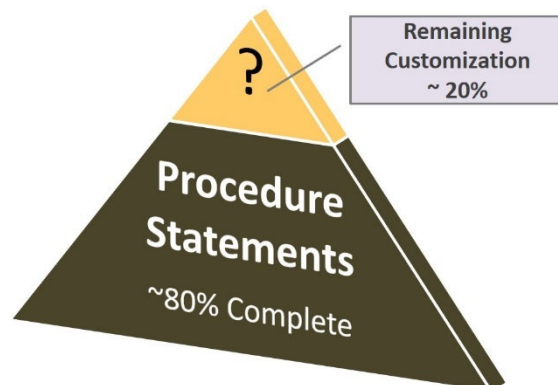
### OVERVIEW

The Cybersecurity Standardized Operating Procedures (CSOP) is a catalog of procedure/control activity statements. These are templates that require slight modification to suit the specific needs of the organization,

#### CUSTOMIZATION GUIDANCE

The content of the CSOP does require a certain level of customization by any organization, since every organization has some difference in available people, processes or technology that can be leveraged to perform these procedures/control activities.

Essentially, we’ve done the heavy lifting in developing the template and pre-populating a significant amount of content. Our target is about 80% of the content as part of the template that would leave the remaining 20% for customization with specifics that only the organization would know, such as the organization calls the change management group the Change Advisory Board (CAB) instead of the Change Control Board (CCB). Those little changes in roles, titles, department naming, technologies in use are all content that just needs to be filled into the template to finalize the procedures/control activities.



#### VALIDATING NEEDS FOR PROCEDURES / CONTROL ACTIVITIES

Procedures are not meant to be documented for the sake of generating paperwork - procedures are meant to satisfy a specific operational need that are complied with:

- If procedures exist and are not tied to a standard, then management should review why the procedure is in place.
- A procedure that lacks a mapping to a standard may indicate “mission creep” and represent an opportunity to reassess the work or cease performing the procedure.

## PROCEDURES DOCUMENTATION

The objective of the CSOP is to provide management direction and support for cybersecurity in accordance with business requirements, as well as relevant laws, regulations and contractual obligations.

Procedures should be both clearly-written and concise.

- Procedure documentation is meant to provide evidence of due diligence that standards are complied with.
- Well-managed procedures are critical to a security program, since procedures represents the specific activities that are performed to protect systems and data.

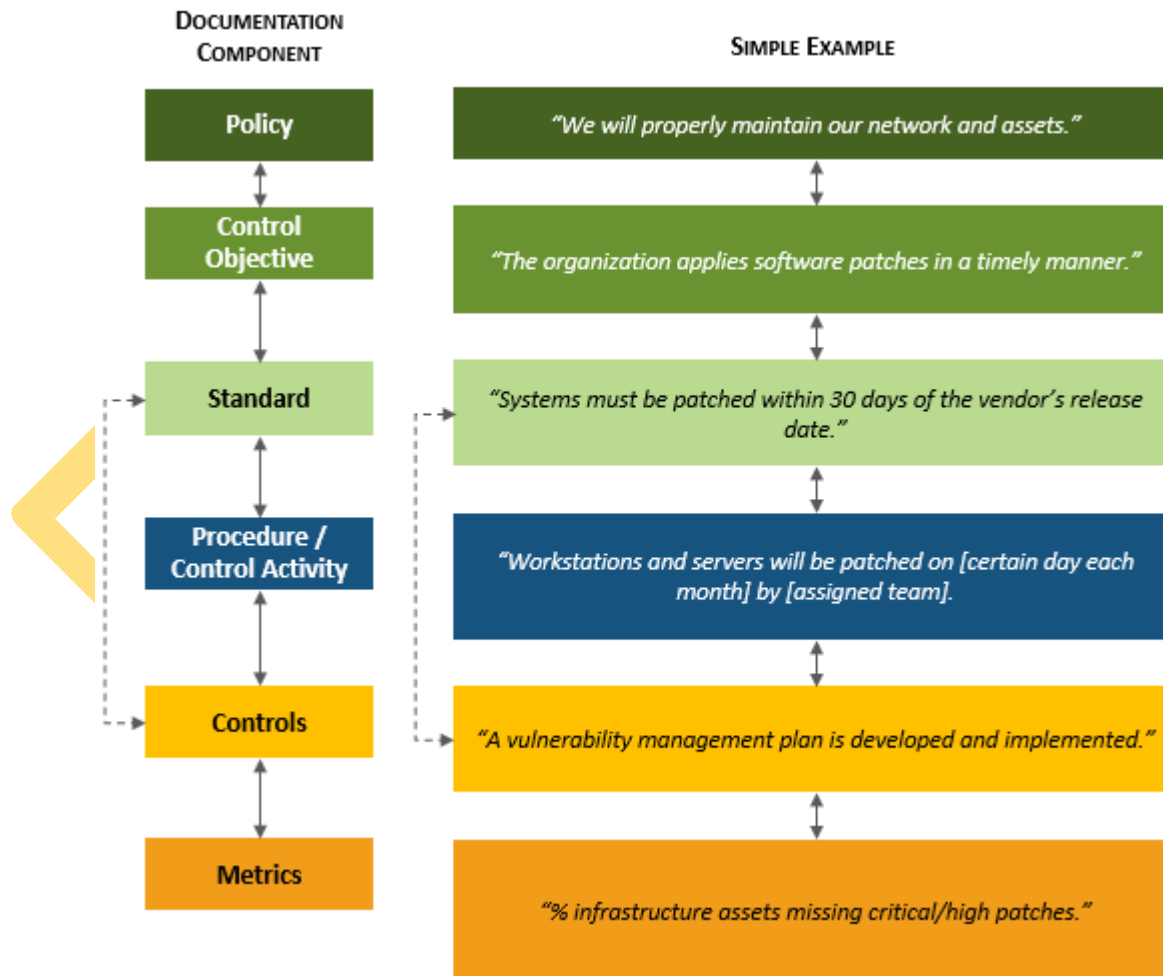
Procedures service a critical function in cybersecurity. Most other documentation produces evidence of due care considerations, but procedures are unique where procedures generate evidence of due diligence.

From a due care and due diligence perspective, it can be thought of this way:

- Certain standards require processes to exist (*due care – evidence demonstrates standards exist*).
- Performing the activities outlined in a procedure and documenting the work that was performed satisfies the intent of the standard (*due diligence – evidence demonstrates the standard is operating effectively*).

The diagram shown below helps visualize the linkages in documentation that involve written procedures:

- CONTROL OBJECTIVES exist to support POLICIES;
- STANDARDS are written to support CONTROL OBJECTIVES;
- PROCEDURES are written to implement the requirements that STANDARDS establish;
- CONTROLS exist as a mechanism to assess/audit both the existence of PROCEDURES / STANDARDS and how well their capabilities are implemented and/or functioning; and
- METRICS exist as a way to measure the performance of CONTROLS.



Documentation Flow Example.

## NIST NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE) CYBERSECURITY WORKFORCE FRAMEWORK

The CSOP leverages the NIST NICE Cybersecurity Workforce Framework.<sup>1</sup> The purpose of this framework is that work roles have an impact on an organization's ability to protect its data, systems and operations. By assigning work roles, it helps direct the work of employees and contractors to minimize assumptions about who is responsible for certain cybersecurity and privacy tasks.

The CSOP uses the work roles identified in the NIST NICE Cybersecurity Workforce Framework to help make assigning the tasks associated with procedures/control activities more efficient and manageable. Keep in mind these are merely recommendations and are fully editable for every organization – this is just a helpful point in the right direction!



NIST NICE Cybersecurity Workforce Framework – Work Categories

### EXAMPLE

This example is a configuration procedure **P-CFG-02 (System Hardening Through Baseline Configurations)**

**PLEASE NOTE THE PROCESS CRITERIA SECTION SHOWN BELOW CAN BE DELETED & IS NOT PART OF THE PROCEDURE**

The process criteria sections exist only to be a useful tool to help build out the procedures by establishing criteria and creating a working space to capture key components that impacts the procedure.

#### Process Criteria:

- **Process Owner:** name of the individual or team accountable for the procedure being performed
  - **Example:** *The process owner for system hardening at ACME is the cybersecurity director, John Doe.*
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks.
  - **Example:** *The process operator for system hardening at ACME is split between several teams:*
    - *Network gear is assigned to network admins.*
    - *Servers are assigned to server admins.*
    - *Laptops, desktops and mobile devices are assign to the End User Computing (EUC) team.*
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
  - **Example:** *Generally, system hardening is an "as needed" process that happens when new operating systems are released or when new technology is purchased. However, there should still be an annual review to ensure that appropriate baseline configurations exist and are current to what is deployed at ACME.*
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
  - **Example:** *The scope affects the entire company. Any deviations to the secure baselines are handled on an individual basis.*
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
  - **Example:** *Baseline configurations, benchmarks and STIGs are located on server XYZ123 in the folder called "Secure Baselines" and it is available for read-only for all users.*
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
  - **Example:** *There are no SLAs associated with baseline configurations.*
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?
  - **Example:** *The following classes of systems and applications are in scope for this procedure:*
    - *Server-Class Systems*
    - *Workstation-Class Systems*
    - *Network Devices*
    - *Databases*

<sup>1</sup> NIST NICE Cybersecurity Workforce Framework - <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

**Control:** Mechanisms exist to develop, document and maintain secure baseline configurations for technology platform that are consistent with industry-accepted system hardening standards. *[control wording comes directly from the Secure Controls Framework (SCF) control #CFG-02. The SCF is a free resource that can be downloaded from <https://www.securecontrolsframework.com>]*

**Procedure / Control Activity:** Systems Security Developer [SP-SYS-001], in conjunction with the Technical Support Specialist [OM-STS-001] and Security Architect [SP-ARC-002]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to ensure baseline system hardening configuration for all ACME-owned or managed assets comply with applicable legal, statutory, and regulatory compliance obligations.
- (2) Where technically feasible, technology platforms align with industry-recommended hardening recommendations, including but not limited to:
  - a. Center for Internet Security (CIS) benchmarks;
  - b. Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs); or
  - c. Original Equipment Manufacturer (OEM) security configuration guides.
- (3) Ensures that system hardening includes, but is not limited to:
  - a. Technology platforms that include, but are not limited to:
    - i. Server-Class Systems
      1. Microsoft Server 2003
      2. Microsoft Server 2008
      3. Microsoft Server 2012
      4. Microsoft Server 2016
      5. Red Hat Enterprise Linux (RHEL)
      6. Unix
      7. Solaris
    - ii. Workstation-Class Systems
      1. Microsoft XP
      2. Microsoft 7
      3. Microsoft 8
      4. Microsoft 10
      5. Apple
      6. Fedora (Linux)
      7. Ubuntu (Linux)
      8. SuSe (Linux)
    - iii. Network Devices
      1. Firewalls
      2. Routers
      3. Load balancers
      4. Virtual Private Network (VPN) concentrators
      5. Wireless Access Points (WAPs)
      6. Wireless controllers
      7. Printers
      8. Multi-Function Devices (MFDs)
    - iv. Mobile Devices
      1. Tablets
      2. Mobile phones
      3. Other portable electronic devices
    - v. Databases
      1. MySQL
      2. Windows SQL Server
      3. Windows SQL Express
      4. Oracle
      5. DB2
  - b. Enforcing least functionality, which includes but is not limited to:
    - i. Allowing only necessary and secure services, protocols, and daemons;
    - ii. Removing all unnecessary functionality, which includes but is not limited to:
      1. Scripts;
      2. Drivers;
      3. Features;

4. Subsystems;
  5. File systems; and
  6. Unnecessary web servers.
- c. Configuring and documenting only the necessary ports, protocols, and services to meet business needs;
  - d. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S-FTP), Transport Layer Security (TLS), or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP;
  - e. Installing and configuring appropriate technical controls, such as:
    - i. Antimalware;
    - ii. Software firewall;
    - iii. Event logging; and
    - iv. File Integrity Monitoring (FIM), as required; and
  - f. As applicable, implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers).
- (4) Documents and validates security parameters are configured to prevent misuse.
  - (5) Authorizes deviations from standard baseline configurations in accordance with ACME's change management processes, prior to deployment, provisioning, or use.
  - (6) Validates and refreshes configurations on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. Unless a technical or business reason exists, standardized images are used to represent hardened versions of the underlying operating system and the applications installed on the system.
  - (7) On at least an annual basis, during the 2nd quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    - a. Distributes copies of the change to key personnel; and
    - b. Communicates the changes and updates to key personnel.
  - (8) If necessary, requests corrective action to address identified deficiencies.
  - (9) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
  - (10) If necessary, documents the results of corrective action and notes findings.
  - (11) If necessary, requests additional corrective action to address unremediated deficiencies.

## SUPPORTING POLICIES & STANDARDS

While there are no policies and standards included in the CSOP, the CSOP is designed to provide a 1-1 relationship with ComplianceForge's [Digital Security Program \(DSP\)](#) that contains policies, control objectives, standards and guidelines. It also directly maps to the [Secure Controls Framework \(SCF\)](#) for cybersecurity and privacy controls.

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.

### GUIDELINE

[provides additional, recommended guidance]

### PROCEDURE / CONTROL ACTIVITY

[establishes proper steps to take]

### CONTROL

[defines safeguards & countermeasures]

### STANDARD

[defines quantifiable requirements]

### CONTROL OBJECTIVE

[identifies desired conditions to be met]

### POLICY

[sets high-level expectations]



Cybersecurity Documentation Hierarchy





## **P-GOV-08: DEFINED BUSINESS CONTEXT & MISSION**

**Control:** Mechanisms exist to define the context of its business model and document the mission of the organization.

**Procedure / Control Activity:** Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001]:

- (1) Researches, establishes and documents:
  - a. ACME's business model.
  - b. ACME's corporate mission statement so that cybersecurity-related objectives can be tied back to strategic concerns.
  - c. Strength, Weakness, Opportunities & Threats (SWOT) analysis to define external and internal issues that are relevant and that affect the organization's ability to achieve ACME's mission (e.g., industry drivers, relevant regulations, basis for competition, etc.).
- (2) Prioritizes the objectives and activities necessary to support ACME's corporate mission in a cybersecurity and privacy-specific business plan that takes a multi-year approach to documenting:
  - a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
  - b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
  - c. Resource requirements.
  - d. Cybersecurity and privacy specific:
    - i. Vision.
    - ii. Mission.
    - iii. Strategy.
  - e. Prioritized objectives to accomplish the business plan.
- (3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

## **P-GOV-09: DEFINED CONTROL OBJECTIVES**

**Control:** Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.

**Procedure / Control Activity:** Executive Cyber Leadership [OV-EXL-001], in conjunction with Systems Security Manager [OV-MGT-001]:

- (1) Researches, establishes and documents the appropriate internal control system for both cybersecurity and privacy controls that supports ACME's applicable statutory, regulatory and/or contractual obligations.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

## P-MON-06(b): MONITORING REPORTING | TREND ANALYSIS REPORTING

**Control:** Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

**Procedure / Control Activity:** Procedure / Control Activity: Systems Security Manager [OV-MGT-001], in conjunction with Security Architect [SP-ARC-002] and Executive Cyber Leadership [OV-EXL-001]:

- (1) Develop measures of performance or outcome-based metrics, to enable trend analysis through measuring the effectiveness or efficiency of the cybersecurity program and the security controls employed in support of the program that incorporates:
  - a. Recent threat information regarding the types of threat events that have occurred within the organization or across the federal government;
  - b. Success rates of certain types of cyber attacks;
  - c. Emerging vulnerabilities in information technologies;
  - d. Evolving social engineering techniques;
  - e. Results from multiple security control assessments;
  - f. The effectiveness of configuration settings; and
  - g. Findings from Internal Audit (IA) or third-party assessors.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

## P-MON-07: TIME STAMPS

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?

**Control:** Mechanisms exist to configure systems to use internal system clocks to generate time stamps for audit records.

**Procedure / Control Activity:** System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.
- (2) Enables NTP for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.<sup>7</sup>
- (3) Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
  - a. time.nist.gov 192.43.244.18 [primary].

<sup>7</sup> <http://tycho.usno.navy.mil/ntp.html>

- b. time-nw.nist.gov 131.107.13.100 [alternate].
- (4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (5) If necessary, requests corrective action to address identified deficiencies.
- (6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (7) If necessary, documents the results of corrective action and notes findings.
- (8) If necessary, requests additional corrective action to address unremediated deficiencies.

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

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure’s tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?

**Control:** Mechanisms exist to synchronize internal system clocks with an authoritative time source.

**Procedure / Control Activity:** System Administrator [OM-ADM-001], in conjunction with Systems Security Analyst [OM-ANA-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times, and ensure that the following is implemented for acquiring, distributing, and storing time.
- (2) Enables NTP is the Internet standard protocol for client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.<sup>8</sup>
- (3) Utilizes The official NIST or USNO Internet Time Service (ITS) for system time synchronization:
  - a. time.nist.gov 192.43.244.18 [primary].
  - b. time-nw.nist.gov 131.107.13.100 [alternate].
- (4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (5) If necessary, requests corrective action to address identified deficiencies.
- (6) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (7) If necessary, documents the results of corrective action and notes findings.
- (8) If necessary, requests additional corrective action to address unremediated deficiencies.

**P-MON-08: PROTECTION OF AUDIT INFORMATION**

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure’s tasks

<sup>8</sup> <http://tycho.usno.navy.mil/ntp.html>

### **P-HRS-13: IDENTIFY CRITICAL SKILLS & GAPS**

Control: Mechanisms exist to evaluate the critical cybersecurity and privacy skills needed to support the organization's mission and identify gaps that exist.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Conducts a critical skills inventory that:
  - a. Analyzes the appropriate skills that are required to support the organization's mission and business functions;
  - b. Documents competencies necessary to define critical skills;
  - c. Inventories the current technology staff for the identified critical skills;
  - d. Documents the gap that exists in current versus needed critical skills;
  - e. Proposes a solution to address the critical skills shortfall.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

### **P-HRS-13(A): IDENTIFY CRITICAL SKILLS & GAPS | REMEDIATE IDENTIFIED SKILLS DEFICIENCIES**

Control: Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Remediate critical skills deficiencies by:
  - a. Resourcing new hires;
  - b. Outsourcing the responsibilities to a competent third-party;
  - c. Reassigning and training existing staff; and/or
  - d. Creating new positions with higher level skill requirements.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

### **P-HRS-13(B): IDENTIFY CRITICAL SKILLS & GAPS | IDENTIFY VITAL CYBERSECURITY & PRIVACY STAFF**

Control: Mechanisms exist to identify vital cybersecurity & privacy staff.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Identifies the objectives and activities necessary to support ACME's corporate mission:
  - a. Current maturity capability levels associated with cybersecurity and privacy-related People, Processes and Technologies (PPT).
  - b. Target maturity capability levels associated with cybersecurity and privacy-related PPT.
  - c. Resource requirements.
  - d. Cybersecurity and privacy specific:
    - i. Vision.
    - ii. Mission.
    - iii. Strategy.

- e. Prioritized objectives to accomplish the business plan.
- (2) Identifies critical staff by:
  - a. Identifying vital cybersecurity & privacy staff;
  - b. Documenting the role, function, responsibility and reasons that supports their designation as vital;
  - c. Where possible, identifying staff that can backfill vital roles.
- (3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

**P-HRS-13(c): IDENTIFY CRITICAL SKILLS & GAPS | ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & PRIVACY STAFF**

**Control:** Mechanisms exist to establish redundancy for vital cybersecurity & privacy staff.

**Procedure / Control Activity:** The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Conducts a critical skills inventory that:
  - a. Analyzes the appropriate skills that are required to support the organization's mission and business functions;
  - b. Documents competencies necessary to define critical skills;
  - c. Inventories the current technology staff for the identified critical skills;
  - d. Documents the gap that exists in current versus needed critical skills;
- (2) Designates roles that require redundancy.
- (3) Identifies a primary and alternate staff member for vital cybersecurity & privacy roles.
- (4) Proposes a solution to address any redundancy shortfalls.
- (5) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (6) If necessary, requests corrective action to address identified deficiencies.
- (7) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (8) If necessary, documents the results of corrective action and notes findings.
- (9) If necessary, requests additional corrective action to address unremediated deficiencies.

**P-HRS-13(d): IDENTIFY CRITICAL SKILLS & GAPS | PERFORM SUCCESSION PLANNING**

**Control:** Mechanisms exist to perform succession planning for vital cybersecurity & privacy roles.

**Procedure / Control Activity:** The Human Resources (HR) department, in conjunction with Systems Security Manager [OV-MGT-001], Cyber Workforce Developer and Manager [OV-SPP-001] and Cyber Legal Advisor [OV-LGA-001]:

- (1) Manages succession planning as an extensive and systematic activity that:
  - a. Maintains documented roles and responsibilities for vital cybersecurity & privacy staff positions;
  - b. Works with senior leaders who responsible those vital cybersecurity & privacy staff positions to develop succession plans;
  - c. Works with identified staff members to provide training and/or guidance on steps needed to successfully move into the new role if succession plans must be implemented to help ensure a smooth transition.
- (2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (3) If necessary, requests corrective action to address identified deficiencies.
- (4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (5) If necessary, documents the results of corrective action and notes findings.
- (6) If necessary, requests additional corrective action to address unremediated deficiencies.

**P-IRO-02(c): INCIDENT HANDLING | DYNAMIC RECONFIGURATION**

**Control:** Automated mechanisms exist to dynamically reconfigure information system components as part of the incident response capability.

**Procedure / Control Activity:** System Administrator [OM-ADM-001], in conjunction with Asset Owner [XX-AST-001], Crisis Management Specialist [XX-CON-001], Disaster Recovery Team Leader [XX-CON-003] and Business Continuity Team Leader [XX-CON-005]:

- (1) Develops specific use cases where dynamic reconfiguration is appropriate that includes:
  - a. Stopping an active attack;
  - b. Misdirecting attackers; and
  - c. Isolating systems, thus limiting the extent of the damage from breaches or compromises.
- (2) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms to employ automated mechanisms that enable dynamic reconfiguration of systems as part of incident response remediation actions that includes:
  - a. Changes to router or firewall Access Control Lists (ACLs);
  - b. Intrusion Detection / Prevention System (IDS/IPS) parameters.
- (3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

**P-IRO-02(d): INCIDENT HANDLING | CONTINUITY OF OPERATIONS**

**Control:** Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.

**Procedure / Control Activity:** Systems Security Manager [OV-MGT-001], in conjunction with Systems Security Analyst [OM-ANA-001], Integrated Security Incident Response Team (ISIRT) Leader [XX-CIR-02] and Cyber Defense Incident Responder [PR-CIR-001]:

- (1) Leverages the Integrated Incident Response Program (IIRP) to categorize cybersecurity incidents based on each category’s potential to escalate and different handling procedures:

#	Threat	Category	Category Description
0	Training	Simulated Incident (Training & Exercises)	This category is used during exercises and approved testing of internal/external network defenses or responses.
1	Illegal Content or Activities	Illegal Content	This category is used for any data that is illegal to have in possession. This includes illegal content such as <u>child pornography</u> or <u>classified information on unclassified systems</u> .
2		Criminal Conduct	This category is used for any incident that would be considered criminal conduct. This includes <u>embezzlement</u> , <u>corporate espionage</u> , <u>terrorism/national security threats</u> , <u>fraud</u> , <u>violence</u> or other conduct that would constitute a <u>criminal felony or misdemeanor charge</u> .
3	Safety	Technology Compromise	This category is used for any incident that has <u>safety implications</u> from the compromise of the technology to be used in a manner it was not designed for. This includes categories of technologies that includes <u>Operational Technology (OT)</u> and <u>Internet of Things (IoT)</u> .

4	Confidentiality	Breach of Sensitive Data	<p>This category is used for any incident that has involves the <u>unauthorized disclosure or compromise of sensitive data</u>.</p> <p>This includes sensitive <u>Personal Data (PD)</u> and <u>Intellectual Property (IP)</u>.</p>
5	Nefarious Activity	Malware	<p>This category is used for malware-related incidents.</p> <p>Any software code intentionally created or introduced into multiple systems for the distinct purpose of causing hard or loss to the computer system, its data or other resources (e.g., spyware, adware, viruses, Trojans, worms, etc.).</p>
6		Host / Application Compromise	<p>This is a <u>known or suspected compromise</u> that is not directly related to malware.</p> <p>A successful event of this nature means the <u>attacker has total control over the host or application</u> and access to any and all data stored on it or on systems that trust the compromised host or application.</p> <p>This may be from a <u>privilege escalation attack</u>.</p>
7		Denial of Service (DoS)	<p>This is a known or suspected <u>Denial of Service (DoS) attack</u>.</p> <p>A successful event of this nature means the attacker(s) successfully denied access to either the entire network, a portion of the network or to critical service(s) / website(s).</p>
8	Lost / Stolen Asset	Lost / Stolen IT Asset	<p>This category is used to respond to any <u>lost or stolen IT equipment</u> (e.g., laptops, tablets, computers, servers, media, tapes, etc.)</p>
9	Poor Security Practice	Poor Security Practice	<p>This category is used for any suspected incident involving <u>misconfigurations, poor cybersecurity practices &amp; policy violations</u>.</p>
10	Unknown / Other	Unknown / Other (Under Investigation)	<p>This category is used if the <u>situation is unclear and categorization cannot be made</u>.</p> <p>This is meant to be a "placeholder" category until the threat or situation is investigated and a final determination has been made, so that the incident can be properly categorized.</p>

- (2) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to implement appropriate administrative and technical mechanisms to employ the IIRP to ensure users understand the different categories of incidents and the actions required to be taken, per ACME's Incident Response Plan (IRP).
- (3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

### P-PES-03(c): PHYSICAL ACCESS CONTROL | PHYSICAL ACCESS LOGS

**Process Criteria:** (this process criteria section (yellow text field) can be deleted, but it will be useful in populating a System Security Plan (SSP) or other system-related documentation – it is meant to be a useful tool to help build the procedure by establishing criteria and creating a working space to capture key components that impacts the procedure)

- **Process Owner:** name of the individual or team accountable for the procedure being performed
- **Process Operator:** name of the individual or team responsible to perform the procedure's tasks
- **Occurrence:** how often does the procedure need to be conducted? is it something that needs to be performed annually, semi-annually, quarterly, monthly, bi-weekly, weekly, daily, continuous or as needed?
- **Scope of Impact:** what is the potential impact of the procedure? does it affect a system, application, process, team, department, user, client, vendor, geographic region or the entire company?
- **Location of Additional Documentation:** if applicable, is there a server, link or other repository where additional documentation is stored or can be found
- **Performance Target:** if applicable, is there a Service Level Agreement (SLA) or targeted timeline for the process to be completed?
- **Technology in Use:** if applicable, what is the name of the application/system/service used to perform the procedure?

**Control:** Physical access control mechanisms exist to generate a log entry for each access through controlled ingress and egress points.

**Procedure / Control Activity:** Physical Security Specialist [XX-PES-001]:

- (1) Uses vendor-recommended settings and industry-recognized secure practices that enable the implementation of appropriate physical, administrative and technical mechanisms to configure access control systems to log the following information:
  - a. Physical location of the access;
  - b. Direction of access, if possible (e.g., ingress or egress);
  - c. Identity of the person accessing the location; and
  - d. Indication of success or failure.
- (2) Uses a visitor log to maintain a physical audit trail of visitor activity:
  - a. At a minimum, document the visitor's name, the company represented, and the onsite personnel authorizing physical access; and
  - b. Retain this log for a minimum of three months, unless otherwise restricted by law.
- (3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
  - a. Distributes copies of the change to key personnel; and
  - b. Communicates the changes and updates to key personnel.
- (4) If necessary, requests corrective action to address identified deficiencies.
- (5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
- (6) If necessary, documents the results of corrective action and notes findings.
- (7) If necessary, requests additional corrective action to address unremediated deficiencies.

### P-PES-03(d): PHYSICAL ACCESS CONTROL | ACCESS TO INFORMATION SYSTEMS

**Control:** Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive data, in addition to the physical access controls for the facility.

**Procedure / Control Activity:** Asset Owner [XX-AST-001], in conjunction with Physical Security Specialist [XX-PES-001] and Physical Security Manager [XX-PES-002]:

- (1) Implements appropriate administrative, physical and technical means to enforce physical access authorizations to information systems in addition to the physical access controls.
- (2) Develops unique physical security zones to determine specific areas that are more vulnerable to unauthorized use, theft or viewing of data where enhanced physical safeguards should be implemented:
  - a. Facilities management implements physical access authorization mechanisms to secure workspaces, such as:
    - i. Proximity badges; or
    - ii. Personalized PIN pad
  - b. Line supervisors and manage facilitate "clean desk" requirements for all work areas to ensure media containing sensitive data is properly secured when the workspace is not occupied, including:
    - i. Filing cabinets, lockable drawers / overhead cabinets, storage rooms and any other storage unit containing sensitive data will be locked when not in use; and