

YOUR LOGO GOES HERE

---

# DIGITAL SECURITY PROGRAM (DSP)

---

ACME Business Consulting, Inc.

**DSP**  
Digital Security Program

**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>NOTICE – REFERENCED FRAMEWORKS &amp; SUPPORTING PRACTICES</b>	<b>25</b>
<b>DIGITAL SECURITY PROGRAM (DSP) OVERVIEW</b>	<b>26</b>
INTRODUCTION	26
PURPOSE	26
SCOPE & APPLICABILITY	27
POLICY OVERVIEW	27
VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES	27
EXCEPTION TO STANDARDS	27
UPDATES TO POLICIES & STANDARDS	27
KEY TERMINOLOGY	28
<b>CYBERSECURITY &amp; DATA PROTECTION PROGRAM STRUCTURE</b>	<b>30</b>
MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION	30
POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE	30
<b>CYBERSECURITY &amp; DATA PROTECTION (GOV) POLICY &amp; STANDARDS</b>	<b>32</b>
<b>GOV-01: CYBERSECURITY &amp; DATA PROTECTION GOVERNANCE PROGRAM</b>	<b>32</b>
GOV-01.1: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM   STEERING COMMITTEE & PROGRAM OVERSIGHT	32
GOV-01.2: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM   STATUS REPORTING TO GOVERNING BODY	32
<b>GOV-02: PUBLISHING CYBERSECURITY &amp; DATA PROTECTION DOCUMENTATION</b>	<b>33</b>
GOV-02.1: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION   EXCEPTION MANAGEMENT	33
<b>GOV-03: PERIODIC REVIEW &amp; UPDATE OF CYBERSECURITY &amp; DATA PROTECTION PROGRAM</b>	<b>34</b>
<b>GOV-04: ASSIGNED CYBERSECURITY &amp; DATA PROTECTION RESPONSIBILITIES</b>	<b>34</b>
GOV-04.1: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES   ACCOUNTABILITY STRUCTURE	34
GOV-04.2: ASSIGNED CYBERSECURITY & DATA PROTECTION RESPONSIBILITIES   AUTHORITATIVE CHAIN OF COMMAND	34
<b>GOV-05: MEASURES OF PERFORMANCE</b>	<b>35</b>
GOV-05.1: MEASURES OF PERFORMANCE   KEY PERFORMANCE INDICATORS (KPIs)	35
GOV-05.2: MEASURES OF PERFORMANCE   KEY RISK INDICATORS (KRIs)	35
<b>GOV-06: CONTACTS WITH AUTHORITIES</b>	<b>36</b>
<b>GOV-07: CONTACTS WITH GROUPS &amp; ASSOCIATIONS</b>	<b>36</b>
<b>GOV-08: DEFINED BUSINESS CONTEXT &amp; MISSION</b>	<b>36</b>
<b>GOV-09: DEFINED CONTROL OBJECTIVES</b>	<b>36</b>
<b>GOV-10: DATA GOVERNANCE</b>	<b>37</b>
<b>GOV-11: PURPOSE VALIDATION</b>	<b>37</b>
<b>GOV-12: FORCED TECHNOLOGY TRANSFER (FTT)</b>	<b>37</b>
<b>GOV-13: STATE-SPONSORED ESPIONAGE</b>	<b>38</b>
<b>GOV-14: BUSINESS AS USUAL (BAU) SECURE PRACTICES</b>	<b>39</b>
<b>GOV-15: OPERATIONALIZING CYBERSECURITY &amp; DATA PROTECTION PRACTICES</b>	<b>39</b>
GOV-15.1: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES   SELECT CONTROLS	39
GOV-15.2: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES   IMPLEMENT CONTROLS	39
GOV-15.3: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES   ASSESS CONTROLS	40
GOV-15.4: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES   AUTHORIZE SYSTEMS, APPLICATIONS & SERVICES	40
GOV-15.5: OPERATIONALIZING CYBERSECURITY & DATA PROTECTION PRACTICES   MONITOR CONTROLS	40
<b>ARTIFICIAL INTELLIGENCE AND AUTONOMOUS TECHNOLOGIES (AAT)</b>	<b>41</b>
<b>AAT-01: ARTIFICIAL INTELLIGENCE (AI) &amp; AUTONOMOUS TECHNOLOGIES GOVERNANCE</b>	<b>41</b>
AAT-01.1: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE   AI & AUTONOMOUS TECHNOLOGIES-RELATED LEGAL REQUIREMENTS DEFINITION	42
AAT-01.2: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE   TRUSTWORTHY AI & AUTONOMOUS TECHNOLOGIES	42
AAT-01.3: ARTIFICIAL INTELLIGENCE (AI) & AUTONOMOUS TECHNOLOGIES GOVERNANCE   AI & AUTONOMOUS TECHNOLOGIES VALUE SUSTAINMENT	43
<b>AAT-02: SITUATIONAL AWARENESS OF AI &amp; AUTONOMOUS TECHNOLOGIES</b>	<b>43</b>
AAT-02.1: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES   AI & AUTONOMOUS TECHNOLOGIES RISK MAPPING	43
AAT-02.2: SITUATIONAL AWARENESS OF AI & AUTONOMOUS TECHNOLOGIES   AI & AUTONOMOUS TECHNOLOGIES INTERNAL CONTROLS	43
<b>AAT-03: AI &amp; AUTONOMOUS TECHNOLOGIES CONTEXT DEFINITION</b>	<b>44</b>

<i>AAT-03.1: AI &amp; AUTONOMOUS TECHNOLOGIES CONTEXT DEFINITION   AI &amp; AUTONOMOUS TECHNOLOGIES MISSION AND GOALS DEFINITION</i>	44
<b>AAT-04: AI &amp; AUTONOMOUS TECHNOLOGIES BUSINESS CASE</b>	<b>44</b>
<i>AAT-04.1: AI &amp; AUTONOMOUS TECHNOLOGIES BUSINESS CASE   AI &amp; AUTONOMOUS TECHNOLOGIES POTENTIAL BENEFITS ANALYSIS</i>	45
<i>AAT-04.2: AI &amp; AUTONOMOUS TECHNOLOGIES BUSINESS CASE   AI &amp; AUTONOMOUS TECHNOLOGIES POTENTIAL COSTS ANALYSIS</i>	45
<i>AAT-04.3: AI &amp; AUTONOMOUS TECHNOLOGIES BUSINESS CASE   AI &amp; AUTONOMOUS TECHNOLOGIES TARGETED APPLICATION SCOPE</i>	45
<i>AAT-04.4: AI &amp; AUTONOMOUS TECHNOLOGIES BUSINESS CASE   AI &amp; AUTONOMOUS TECHNOLOGIES COST / BENEFIT MAPPING</i>	45
<b>AAT-05: AI &amp; AUTONOMOUS-SPECIFIC TRAINING</b>	<b>45</b>
<b>AAT-06: AI &amp; AUTONOMOUS TECHNOLOGIES FAIRNESS &amp; BIAS</b>	<b>46</b>
<b>AAT-07: AI &amp; AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS</b>	<b>46</b>
<i>AAT-07.1: AI &amp; AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS   AI &amp; AUTONOMOUS TECHNOLOGIES IMPACT CHARACTERIZATION</i>	46
<i>AAT-07.2: AI &amp; AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS   AI &amp; AUTONOMOUS TECHNOLOGIES LIKELIHOOD &amp; IMPACT RISK ANALYSIS</i>	47
<i>AAT-07.3: AI &amp; AUTONOMOUS TECHNOLOGIES RISK MANAGEMENT DECISIONS   AI &amp; AUTONOMOUS TECHNOLOGIES CONTINUOUS IMPROVEMENTS</i>	47
<b>AAT-08: ASSIGNED RESPONSIBILITIES FOR AI &amp; AUTONOMOUS TECHNOLOGIES</b>	<b>47</b>
<b>AAT-09: AI &amp; AUTONOMOUS TECHNOLOGIES RISK PROFILING</b>	<b>47</b>
<b>AAT-10: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)</b>	<b>48</b>
<i>AAT-10.1: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV TRUSTWORTHINESS ASSESSMENT</i>	48
<i>AAT-10.2: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV TOOLS</i>	48
<i>AAT-10.3: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV TRUSTWORTHINESS DEMONSTRATION</i>	49
<i>AAT-10.4: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV SAFETY DEMONSTRATION</i>	49
<i>AAT-10.5: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV RESILIENCY ASSESSMENT</i>	49
<i>AAT-10.6: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV TRANSPARENCY &amp; ACCOUNTABILITY ASSESSMENT</i>	49
<i>AAT-10.7: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV PRIVACY ASSESSMENT</i>	49
<i>AAT-10.8: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV FAIRNESS &amp; BIAS ASSESSMENT</i>	50
<i>AAT-10.9: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI &amp; AUTONOMOUS TECHNOLOGIES MODEL VALIDATION</i>	50
<i>AAT-10.10: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV RESULTS EVALUATION</i>	50
<i>AAT-10.11: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV EFFECTIVENESS</i>	50
<i>AAT-10.12: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV COMPARABLE DEPLOYMENT SETTINGS</i>	50
<i>AAT-10.13: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   AI TEVV POST-DEPLOYMENT MONITORING</i>	51
<i>AAT-10.14: ARTIFICIAL INTELLIGENCE TEST, EVALUATION, VALIDATION &amp; VERIFICATION (AI TEVV)   UPDATING AI &amp; AUTONOMOUS TECHNOLOGIES</i>	51
<b>AAT-11: ROBUST STAKEHOLDER ENGAGEMENT FOR AI &amp; AUTONOMOUS TECHNOLOGIES</b>	<b>51</b>
<i>AAT-11.1: ROBUST STAKEHOLDER ENGAGEMENT FOR AI &amp; AUTONOMOUS TECHNOLOGIES   AI &amp; AUTONOMOUS TECHNOLOGIES STAKEHOLDER FEEDBACK INTEGRATION</i>	51
<i>AAT-11.2: ROBUST STAKEHOLDER ENGAGEMENT FOR AI &amp; AUTONOMOUS TECHNOLOGIES   AI &amp; AUTONOMOUS TECHNOLOGIES ONGOING ASSESSMENTS</i>	52
<i>AAT-11.3: ROBUST STAKEHOLDER ENGAGEMENT FOR AI &amp; AUTONOMOUS TECHNOLOGIES   AI &amp; AUTONOMOUS TECHNOLOGIES END USER FEEDBACK</i>	52
<i>AAT-11.4: ROBUST STAKEHOLDER ENGAGEMENT FOR AI &amp; AUTONOMOUS TECHNOLOGIES   AI &amp; AUTONOMOUS TECHNOLOGIES INCIDENT &amp; ERROR REPORTING</i>	52

<b>AAT-12: AI &amp; AUTONOMOUS TECHNOLOGIES INTELLECTUAL PROPERTY INFRINGEMENT PROTECTIONS</b>	<b>52</b>
<b>AAT-13: AI &amp; AUTONOMOUS TECHNOLOGIES STAKEHOLDER DIVERSITY</b>	<b>53</b>
AAT-13.1: AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER DIVERSITY   AI & AUTONOMOUS TECHNOLOGIES STAKEHOLDER COMPETENCIES	53
<b>AAT-14: AI &amp; AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS</b>	<b>53</b>
AAT-14.1: AI & AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS   AI & AUTONOMOUS TECHNOLOGIES IMPLEMENTATION TASKS DEFINITION	53
AAT-14.2: AI & AUTONOMOUS TECHNOLOGIES REQUIREMENTS DEFINITIONS   AI & AUTONOMOUS TECHNOLOGIES KNOWLEDGE LIMITS	53
<b>AAT-15: AI &amp; AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS</b>	<b>54</b>
AAT-15.1: AI & AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS   AI & AUTONOMOUS TECHNOLOGIES NEGATIVE RESIDUAL RISKS	54
AAT-15.2: AI & AUTONOMOUS TECHNOLOGIES VIABILITY DECISIONS   RESPONSIBILITY TO SUPERSEDE, DEACTIVATE AND/OR DISENGAGE AI & AUTONOMOUS TECHNOLOGIES	54
<b>AAT-16: AI &amp; AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING</b>	<b>54</b>
AAT-16.1: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   AI & AUTONOMOUS TECHNOLOGIES MEASUREMENT APPROACHES	55
AAT-16.2: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   MEASURING AI & AUTONOMOUS TECHNOLOGIES EFFECTIVENESS	55
AAT-16.3: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   UNMEASURABLE AI & AUTONOMOUS TECHNOLOGIES RISKS	55
AAT-16.4: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   EFFICACY OF AI & AUTONOMOUS TECHNOLOGIES MEASUREMENT	56
AAT-16.5: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   AI & AUTONOMOUS TECHNOLOGIES DOMAIN EXPERT REVIEWS	56
AAT-16.6: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   AI & AUTONOMOUS TECHNOLOGIES PERFORMANCE CHANGES	56
AAT-16.7: AI & AUTONOMOUS TECHNOLOGIES PRODUCTION MONITORING   PRE-TRAINED AI & AUTONOMOUS TECHNOLOGIES MODELS	56
<b>AAT-17: AI &amp; AUTONOMOUS TECHNOLOGIES HARM PREVENTION</b>	<b>57</b>
AAT-17.1: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION   AI & AUTONOMOUS TECHNOLOGIES HUMAN SUBJECT PROTECTIONS	57
AAT-17.2: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION   AI & AUTONOMOUS TECHNOLOGIES ENVIRONMENTAL IMPACT & SUSTAINABILITY	58
AAT-17.3: AI & AUTONOMOUS TECHNOLOGIES HARM PREVENTION   PREVIOUSLY UNKNOWN AI & AUTONOMOUS TECHNOLOGIES THREATS & RISKS	58
<b>AAT-18: AI &amp; AUTONOMOUS TECHNOLOGIES RISK TRACKING APPROACHES</b>	<b>59</b>
AAT-18.1: AI & AUTONOMOUS TECHNOLOGIES RISK TRACKING APPROACHES   AI & AUTONOMOUS TECHNOLOGIES RISK RESPONSE	59
<b>ASSET MANAGEMENT (AST) POLICY &amp; STANDARDS</b>	<b>60</b>
<b>AST-01: ASSET GOVERNANCE</b>	<b>60</b>
AST-01.1: ASSET GOVERNANCE   ASSET-SERVICE DEPENDENCIES	60
AST-01.2: ASSET GOVERNANCE   STAKEHOLDER IDENTIFICATION & INVOLVEMENT	61
AST-01.3: ASSET GOVERNANCE   STANDARDIZED NAMING CONVENTION	61
<b>AST-02: ASSET INVENTORIES</b>	<b>61</b>
AST-02.1: ASSET INVENTORIES   UPDATES DURING INSTALLATIONS/REMOVALS	62
AST-02.2: ASSET INVENTORIES   AUTOMATED UNAUTHORIZED COMPONENT DETECTION	62
AST-02.3: ASSET INVENTORIES   COMPONENT DUPLICATION AVOIDANCE	62
AST-02.4: ASSET INVENTORIES   APPROVED BASELINE DEVIATIONS	63
AST-02.5: ASSET INVENTORIES   NETWORK ACCESS CONTROL (NAC)	63
AST-02.6: ASSET INVENTORIES   DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) SERVER LOGGING	63
AST-02.7: ASSET INVENTORIES   SOFTWARE LICENSING RESTRICTIONS	63
AST-02.8: ASSET INVENTORIES   DATA ACTION MAPPING	63
AST-02.9: ASSET INVENTORIES   CONFIGURATION MANAGEMENT DATABASE (CMDB)	64
AST-02.10: ASSET INVENTORIES   AUTOMATED LOCATION TRACKING	64
AST-02.11: ASSET INVENTORIES   COMPONENT ASSIGNMENT	64
<b>AST-03: ASSET OWNERSHIP ASSIGNMENT</b>	<b>64</b>
AST-03.1: ASSET OWNERSHIP ASSIGNMENT   ACCOUNTABILITY INFORMATION	65

AST-03.2: ASSET OWNERSHIP ASSIGNMENT   PROVENANCE	65
<b>AST-04: NETWORK DIAGRAMS &amp; DATA FLOW DIAGRAMS (DFDs)</b>	<b>66</b>
AST-04.1: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)   ASSET SCOPE CLASSIFICATION	67
AST-04.2: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)   CONTROL APPLICABILITY BOUNDARY GRAPHICAL REPRESENTATION	67
AST-04.3: NETWORK DIAGRAMS & DATA FLOW DIAGRAMS (DFDs)   COMPLIANCE-SPECIFIC ASSET IDENTIFICATION	67
<b>AST-05: SECURITY OF ASSETS &amp; MEDIA</b>	<b>68</b>
AST-05.1: SECURITY OF ASSETS & MEDIA   MANAGEMENT APPROVAL FOR EXTERNAL MEDIA TRANSFER	68
<b>AST-06: UNATTENDED END-USER EQUIPMENT</b>	<b>68</b>
AST-06.1: UNATTENDED END-USER EQUIPMENT   ASSET STORAGE IN AUTOMOBILES	69
<b>AST-07: KIOSKS &amp; POINT OF INTERACTION (POI) DEVICES</b>	<b>69</b>
<b>AST-08: TAMPER DETECTION</b>	<b>69</b>
<b>AST-09: SECURE DISPOSAL, DESTRUCTION OR RE-USE OF EQUIPMENT</b>	<b>70</b>
<b>AST-10: RETURN OF ASSETS</b>	<b>70</b>
<b>AST-11: REMOVAL OF ASSETS</b>	<b>71</b>
<b>AST-12: USE OF PERSONAL DEVICES</b>	<b>71</b>
<b>AST-13: USE OF THIRD-PARTY DEVICES</b>	<b>71</b>
<b>AST-14: USAGE PARAMETERS</b>	<b>72</b>
AST-14.1: USAGE PARAMETERS   BLUETOOTH & WIRELESS DEVICES	72
AST-14.2: USAGE PARAMETERS   INFRARED COMMUNICATIONS	72
<b>AST-15: TAMPER PROTECTION</b>	<b>73</b>
AST-15.1: TAMPER PROTECTION   INSPECTION OF SYSTEMS, COMPONENTS & DEVICES	73
<b>AST-16: BRING YOUR OWN DEVICE (BYOD) USAGE</b>	<b>73</b>
<b>AST-17: PROHIBITED EQUIPMENT &amp; SERVICES</b>	<b>74</b>
<b>AST-18: ROOTS OF TRUST PROTECTION</b>	<b>75</b>
<b>AST-19: TELECOMMUNICATIONS EQUIPMENT</b>	<b>75</b>
<b>AST-20: VIDEO TELECONFERENCE (VTC) SECURITY</b>	<b>75</b>
<b>AST-21: VOICE OVER INTERNET PROTOCOL (VOIP) SECURITY</b>	<b>76</b>
<b>AST-22: MICROPHONES &amp; WEB CAMERAS</b>	<b>76</b>
<b>AST-23: MULTI-FUNCTION DEVICES (MFD)</b>	<b>76</b>
<b>AST-24: TRAVEL-ONLY DEVICES</b>	<b>77</b>
<b>AST-25: RE-IMAGING DEVICES AFTER TRAVEL</b>	<b>77</b>
<b>AST-26: SYSTEM ADMINISTRATIVE PROCESSES</b>	<b>77</b>
<b>AST-27: JUMP SERVER</b>	<b>78</b>
<b>AST-28: DATABASE ADMINISTRATIVE PROCESSES</b>	<b>78</b>
AST-28.1: DATABASE ADMINISTRATIVE PROCESSES   DATABASE MANAGEMENT SYSTEM (DBMS)	78
<b>AST-29: RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY</b>	<b>79</b>
AST-29.1: RADIO FREQUENCY IDENTIFICATION (RFID) SECURITY   CONTACTLESS ACCESS CONTROL SYSTEMS	79
<b>AST-30: DECOMMISSIONING</b>	<b>80</b>
<b>AST-31: ASSET CATEGORIZATION</b>	<b>81</b>
AST-31.1: ASSET CATEGORIZATION   CATEGORIZE ARTIFICIAL INTELLIGENCE (AI)-RELATED TECHNOLOGIES	81
<b>BUSINESS CONTINUITY &amp; DISASTER RECOVERY (BCD) POLICY &amp; STANDARDS</b>	<b>82</b>
<b>BCD-01: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)</b>	<b>82</b>
BCD-01.1: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   COORDINATE WITH RELATED PLANS	82
BCD-01.2: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   COORDINATE WITH EXTERNAL SERVICE PROVIDERS	83
BCD-01.3: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   TRANSFER TO ALTERNATE PROCESSING/STORAGE SITE	83
BCD-01.4: BUSINESS CONTINUITY MANAGEMENT SYSTEM (BCMS)   RECOVERY TIME/POINT OBJECTIVES (RTO/RPO)	83
<b>BCD-02: IDENTIFY CRITICAL ASSETS</b>	<b>84</b>
BCD-02.1: IDENTIFY CRITICAL ASSETS   RESUME ALL MISSIONS & BUSINESS FUNCTIONS	84
BCD-02.2: IDENTIFY CRITICAL ASSETS   CONTINUE ESSENTIAL MISSION & BUSINESS FUNCTIONS	84
BCD-02.3: IDENTIFY CRITICAL ASSETS   RESUME ESSENTIAL MISSION & BUSINESS FUNCTIONS	85
BCD-02.4: IDENTIFY CRITICAL ASSETS   DATA STORAGE LOCATION REVIEWS	85
<b>BCD-03: CONTINGENCY TRAINING</b>	<b>85</b>
BCD-03.1: CONTINGENCY TRAINING   SIMULATED EVENTS	86
BCD-03.2: CONTINGENCY TRAINING   AUTOMATED TRAINING ENVIRONMENTS	86
<b>BCD-04: CONTINGENCY PLAN TESTING &amp; EXERCISES</b>	<b>86</b>
BCD-04.1: CONTINGENCY PLAN TESTING & EXERCISES   COORDINATED TESTING WITH RELATED PLANS	86
BCD-04.2: CONTINGENCY PLAN TESTING & EXERCISES   ALTERNATE STORAGE & PROCESSING SITES	87



<b>BCD-05: CONTINGENCY PLAN ROOT CAUSE ANALYSIS (RCA) &amp; LESSONS LEARNED</b>	<b>87</b>
<b>BCD-06: CONTINGENCY PLANNING &amp; UPDATES</b>	<b>87</b>
<b>BCD-07: ALTERNATIVE SECURITY MEASURES</b>	<b>87</b>
<b>BCD-08: ALTERNATE STORAGE SITE</b>	<b>88</b>
BCD-08.1: ALTERNATE STORAGE SITE   SEPARATION FROM PRIMARY SITE	88
BCD-08.2: ALTERNATE STORAGE SITE   ACCESSIBILITY	88
<b>BCD-09: ALTERNATE PROCESSING SITE</b>	<b>88</b>
BCD-09.1: ALTERNATE PROCESSING SITE   SEPARATION FROM PRIMARY SITE	89
BCD-09.2: ALTERNATE PROCESSING SITE   ACCESSIBILITY	89
BCD-09.3: ALTERNATE PROCESSING SITE   ALTERNATE SITE PRIORITY OF SERVICE	89
BCD-09.4: ALTERNATE PROCESSING SITE   PREPARATION FOR USE	89
BCD-09.5: ALTERNATE PROCESSING SITE   INABILITY TO RETURN TO PRIMARY SITE	90
<b>BCD-10: TELECOMMUNICATIONS SERVICES AVAILABILITY</b>	<b>90</b>
BCD-10.1: TELECOMMUNICATIONS SERVICES AVAILABILITY   TELECOMMUNICATIONS PRIORITY OF SERVICE PROVISIONS	90
BCD-10.2: TELECOMMUNICATIONS SERVICES AVAILABILITY   SEPARATION OF PRIMARY/ALTERNATE PROVIDERS	90
BCD-10.3: TELECOMMUNICATIONS SERVICES AVAILABILITY   PROVIDER CONTINGENCY PLAN	91
BCD-10.4: TELECOMMUNICATIONS SERVICES AVAILABILITY   ALTERNATE COMMUNICATIONS PATHS	91
<b>BCD-11: DATA BACKUPS</b>	<b>91</b>
BCD-11.1: DATA BACKUPS   TESTING FOR RELIABILITY & INTEGRITY	93
BCD-11.2: DATA BACKUPS   SEPARATE STORAGE FOR CRITICAL INFORMATION	94
BCD-11.3: DATA BACKUPS   INFORMATION SYSTEM IMAGING	94
BCD-11.4: DATA BACKUPS   CRYPTOGRAPHIC PROTECTION	94
BCD-11.5: DATA BACKUPS   TEST RESTORATION USING SAMPLING	94
BCD-11.6: DATA BACKUPS   TRANSFER TO ALTERNATE STORAGE SITE	95
BCD-11.7: DATA BACKUPS   REDUNDANT SECONDARY SYSTEM	95
BCD-11.8: DATA BACKUPS   DUAL AUTHORIZATION FOR BACKUP MEDIA DESTRUCTION	95
BCD-11.9: DATA BACKUPS   BACKUP ACCESS	95
BCD-11.10: DATA BACKUPS   BACKUP MODIFICATION AND/OR DESTRUCTION	96
<b>BCD-12: INFORMATION SYSTEM RECOVERY &amp; RECONSTITUTION</b>	<b>96</b>
BCD-12.1: INFORMATION SYSTEM RECOVERY & RECONSTITUTION   TRANSACTION RECOVERY	96
BCD-12.2: INFORMATION SYSTEM RECOVERY & RECONSTITUTION   FAILOVER CAPABILITY	96
BCD-12.3: INFORMATION SYSTEM RECOVERY & RECONSTITUTION   ELECTRONIC DISCOVERY (eDISCOVERY)	96
BCD-12.4: INFORMATION SYSTEM RECOVERY & RECONSTITUTION   RESTORE WITHIN TIME PERIOD	97
<b>BCD-13: BACKUP &amp; RESTORATION HARDWARE PROTECTION</b>	<b>97</b>
<b>BCD-14: ISOLATED RECOVERY ENVIRONMENT</b>	<b>97</b>
<b>BCD-15: RESERVE HARDWARE</b>	<b>97</b>
<b>BCD-16: AI &amp; AUTONOMOUS TECHNOLOGIES INCIDENTS</b>	<b>98</b>
<b>CAPACITY &amp; PERFORMANCE PLANNING (CAP) POLICY &amp; STANDARDS</b>	<b>99</b>
<b>CAP-01: CAPACITY &amp; PERFORMANCE MANAGEMENT</b>	<b>99</b>
<b>CAP-02: RESOURCE PRIORITY</b>	<b>99</b>
<b>CAP-03: CAPACITY PLANNING</b>	<b>99</b>
<b>CAP-04: PERFORMANCE MONITORING</b>	<b>100</b>
<b>CHANGE MANAGEMENT (CHG) POLICY &amp; STANDARDS</b>	<b>101</b>
<b>CHG-01: CHANGE MANAGEMENT PROGRAM</b>	<b>101</b>
<b>CHG-02: CONFIGURATION CHANGE CONTROL</b>	<b>102</b>
CHG-02.1: CONFIGURATION CHANGE CONTROL   PROHIBITION OF CHANGES	102
CHG-02.2: CONFIGURATION CHANGE CONTROL   TEST, VALIDATE & DOCUMENT CHANGES	102
CHG-02.3: CONFIGURATION CHANGE CONTROL   CYBERSECURITY & DATA PRIVACY REPRESENTATIVE FOR ASSET LIFECYCLE CHANGES	103
CHG-02.4: CONFIGURATION CHANGE CONTROL   AUTOMATED SECURITY RESPONSE	103
CHG-02.5: CONFIGURATION CHANGE CONTROL   CRYPTOGRAPHIC MANAGEMENT	103
<b>CHG-03: SECURITY IMPACT ANALYSIS FOR CHANGES</b>	<b>104</b>
<b>CHG-04: ACCESS RESTRICTION FOR CHANGE</b>	<b>104</b>
CHG-04.1: ACCESS RESTRICTIONS FOR CHANGE   AUTOMATED ACCESS ENFORCEMENT/AUDITING	104
CHG-04.2: ACCESS RESTRICTIONS FOR CHANGE   SIGNED COMPONENTS	105
CHG-04.3: ACCESS RESTRICTIONS FOR CHANGE   DUAL AUTHORIZATION FOR CHANGE	105
CHG-04.4: ACCESS RESTRICTIONS FOR CHANGE   LIMIT PRODUCTION/OPERATIONAL PRIVILEGES (INCOMPATIBLE ROLES)	105
CHG-04.5: ACCESS RESTRICTIONS FOR CHANGE   LIBRARY PRIVILEGES	105

<b>CHG-05: STAKEHOLDER NOTIFICATION OF CHANGES</b>	<b>106</b>
<b>CHG-06: CYBERSECURITY FUNCTIONALITY VERIFICATION</b>	<b>106</b>
<i>CHG-06.1: CYBERSECURITY FUNCTIONALITY VERIFICATION   REPORT VERIFICATION RESULTS</i>	106
<b>CLD SECURITY (CLD) POLICY &amp; STANDARDS</b>	<b>107</b>
<b>CLD-01: CLOUD SERVICES</b>	<b>107</b>
<i>CLD-01.1: CLOUD SERVICES   CLOUD INFRASTRUCTURE ONBOARDING</i>	107
<i>CLD-01.2: CLOUD SERVICES   CLOUD INFRASTRUCTURE OFFBOARDING</i>	108
<b>CLD-02: CLOUD SECURITY ARCHITECTURE</b>	<b>108</b>
<b>CLD-03: CLOUD INFRASTRUCTURE SECURITY SUBNET</b>	<b>108</b>
<b>CLD-04: APPLICATION &amp; PROGRAM INTERFACE (API) SECURITY</b>	<b>109</b>
<b>CLD-05: VIRTUAL MACHINE IMAGES</b>	<b>109</b>
<b>CLD-06: MULTI-TENANT ENVIRONMENTS</b>	<b>109</b>
<i>CLD-06.1: MULTI-TENANT ENVIRONMENTS   CUSTOMER RESPONSIBILITY MATRIX (CRM)</i>	109
<i>CLD-06.2: MULTI-TENANT ENVIRONMENTS   MULTI-TENANT EVENT LOGGING CAPABILITIES</i>	110
<i>CLD-06.3: MULTI-TENANT ENVIRONMENTS   MULTI-TENANT FORENSICS CAPABILITIES</i>	110
<i>CLD-06.4: MULTI-TENANT ENVIRONMENTS   MULTI-TENANT INCIDENT RESPONSE CAPABILITIES</i>	110
<b>CLD-07: DATA HANDLING &amp; PORTABILITY</b>	<b>111</b>
<b>CLD-08: STANDARDIZED VIRTUALIZATION FORMATS</b>	<b>111</b>
<b>CLD-09 GEOLOCATION REQUIREMENTS FOR PROCESSING, STORAGE AND SERVICE LOCATIONS</b>	<b>111</b>
<b>CLD-10: SENSITIVE DATA IN PUBLIC CLOUD PROVIDERS</b>	<b>111</b>
<b>CLD-11: CLOUD ACCESS POINT (CAP)</b>	<b>112</b>
<b>CLD-12: SIDE CHANNEL ATTACK PREVENTION</b>	<b>112</b>
<b>CLD-13: HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES</b>	<b>112</b>
<i>CLD-13.1: HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES   AUTHORIZED INDIVIDUALS FOR HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES</i>	113
<i>CLD-13.2: HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES   SENSITIVE/REGULATED DATA ON HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES</i>	113
<b>CLD-14: PROHIBITION ON UNVERIFIED HOSTED SYSTEMS, APPLICATIONS &amp; SERVICES</b>	<b>114</b>
<b>COMPLIANCE (CPL) POLICY &amp; STANDARDS</b>	<b>115</b>
<b>CPL-01: STATUTORY, REGULATORY &amp; CONTRACTUAL COMPLIANCE</b>	<b>115</b>
<i>CPL-01.1: STATUTORY, REGULATORY &amp; CONTRACTUAL COMPLIANCE   NON-COMPLIANCE OVERSIGHT</i>	115
<i>CPL-01.2: STATUTORY, REGULATORY &amp; CONTRACTUAL COMPLIANCE   COMPLIANCE SCOPE</i>	115
<b>CPL-02: CYBERSECURITY &amp; DATA PROTECTION CONTROLS OVERSIGHT</b>	<b>116</b>
<i>CPL-02.1: CYBERSECURITY &amp; DATA PROTECTION CONTROLS OVERSIGHT   INTERNAL AUDIT FUNCTION</i>	117
<b>CPL-03: CYBERSECURITY &amp; DATA PROTECTION ASSESSMENTS</b>	<b>117</b>
<i>CPL-03.1: CYBERSECURITY &amp; DATA PROTECTION ASSESSMENTS   INDEPENDENT ASSESSORS</i>	117
<i>CPL-03.2: CYBERSECURITY &amp; DATA PROTECTION ASSESSMENTS   FUNCTIONAL REVIEW OF CYBERSECURITY &amp; DATA PROTECTION CONTROLS</i>	118
<b>CPL-04: AUDIT ACTIVITIES</b>	<b>118</b>
<b>CPL-05: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES</b>	<b>118</b>
<i>CPL-05.1: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES   INVESTIGATION REQUEST NOTIFICATIONS</i>	119
<i>CPL-05.2: LEGAL ASSESSMENT OF INVESTIGATIVE INQUIRES   INVESTIGATION ACCESS RESTRICTIONS</i>	119
<b>CPL-06: GOVERNMENT SURVEILLANCE</b>	<b>119</b>
<b>CONFIGURATION MANAGEMENT (CFG) POLICY &amp; STANDARDS</b>	<b>120</b>
<b>CFG-01: CONFIGURATION MANAGEMENT PROGRAM</b>	<b>120</b>
<i>CFG-01.1: CONFIGURATION MANAGEMENT PROGRAM   ASSIGNMENT OF RESPONSIBILITY</i>	120
<b>CFG-02: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS</b>	<b>121</b>
<i>CFG-02.1: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   REVIEWS &amp; UPDATES</i>	122
<i>CFG-02.2: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   AUTOMATED CENTRAL MANAGEMENT &amp; VERIFICATION</i>	122
<i>CFG-02.3: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   RETENTION OF PREVIOUS CONFIGURATIONS</i>	123
<i>CFG-02.4: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   DEVELOPMENT &amp; TEST ENVIRONMENTS</i>	123
<i>CFG-02.5: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS</i>	123
<i>CFG-02.6: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   NETWORK DEVICE CONFIGURATION FILE SYNCHRONIZATION</i>	124
<i>CFG-02.7: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   APPROVED CONFIGURATION DEVIATIONS</i>	124

CFG-02.8: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   RESPOND TO UNAUTHORIZED CHANGES	124
CFG-02.9: SYSTEM HARDENING THROUGH BASELINE CONFIGURATIONS   BASELINE TAILORING	125
<b>CFG-03: LEAST FUNCTIONALITY</b>	<b>125</b>
CFG-03.1: LEAST FUNCTIONALITY   PERIODIC REVIEW	126
CFG-03.2: LEAST FUNCTIONALITY   PREVENT UNAUTHORIZED SOFTWARE EXECUTION	127
CFG-03.3: LEAST FUNCTIONALITY   UNAUTHORIZED OR AUTHORIZED SOFTWARE (BLACKLISTING OR WHITELISTING)	127
CFG-03.4: LEAST FUNCTIONALITY   SPLIT TUNNELING	127
<b>CFG-04: SOFTWARE USAGE RESTRICTIONS</b>	<b>128</b>
CFG-04.1: SOFTWARE USAGE RESTRICTIONS   OPEN SOURCE SOFTWARE	128
CFG-04.2: SOFTWARE USAGE RESTRICTIONS   UNSUPPORTED INTERNET BROWSERS & EMAIL CLIENTS	129
<b>CFG-05: USER-INSTALLED SOFTWARE</b>	<b>129</b>
CFG-05.1: USER-INSTALLED SOFTWARE   UNAUTHORIZED INSTALLATION ALERTS	129
CFG-05.2: USER-INSTALLED SOFTWARE   PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS	129
<b>CFG-06: CONFIGURATION ENFORCEMENT</b>	<b>130</b>
<b>CFG-07: ZERO-TOUCH PROVISIONING (ZTP)</b>	<b>130</b>
<b>CFG-08: SENSITIVE / REGULATED DATA ACCESS ENFORCEMENT</b>	<b>130</b>
CFG-08.1: SENSITIVE / REGULATED DATA ACCESS ENFORCEMENT   SENSITIVE / REGULATED DATA ACTIONS	131
<b>CONTINUOUS MONITORING (MON) POLICY &amp; STANDARDS</b>	<b>132</b>
<b>MON-01: CONTINUOUS MONITORING</b>	<b>132</b>
MON-01.1: CONTINUOUS MONITORING   INTRUSION DETECTION & PREVENTION SYSTEMS (IDS & IPS)	133
MON-01.2: CONTINUOUS MONITORING   AUTOMATED TOOLS FOR REAL-TIME ANALYSIS	133
MON-01.3: CONTINUOUS MONITORING   INBOUND & OUTBOUND COMMUNICATIONS TRAFFIC	133
MON-01.4: CONTINUOUS MONITORING   SYSTEM GENERATED ALERTS	134
MON-01.5: CONTINUOUS MONITORING   WIRELESS INTRUSION DETECTION SYSTEM (WIDS)	135
MON-01.6: CONTINUOUS MONITORING   HOST-BASED DEVICES	135
MON-01.7: CONTINUOUS MONITORING   FILE INTEGRITY MONITORING (FIM)	135
MON-01.8: CONTINUOUS MONITORING   REVIEWS & UPDATES	136
MON-01.9: CONTINUOUS MONITORING   PROXY LOGGING	136
MON-01.10: CONTINUOUS MONITORING   DEACTIVATED ACCOUNT ACTIVITY	136
MON-01.11: CONTINUOUS MONITORING   AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	137
MON-01.12: CONTINUOUS MONITORING   AUTOMATED ALERTS	137
MON-01.13: CONTINUOUS MONITORING   ALERT THRESHOLD TUNING	137
MON-01.14: CONTINUOUS MONITORING   INDIVIDUALS POSING GREATER RISK	137
MON-01.15: CONTINUOUS MONITORING   PRIVILEGED USER OVERSIGHT	138
MON-01.16: CONTINUOUS MONITORING   ANALYZE & PRIORITIZE MONITORING REQUIREMENTS	138
MON-01.17: CONTINUOUS MONITORING   REAL-TIME SESSION MONITORING	138
<b>MON-02: CENTRALIZED EVENT LOG COLLECTION</b>	<b>139</b>
MON-02.1: CENTRALIZED SECURITY EVENT LOG COLLECTION   CORRELATE MONITORING INFORMATION	140
MON-02.2: CENTRALIZED SECURITY EVENT LOG COLLECTION   CENTRAL REVIEW & ANALYSIS	140
MON-02.3: CENTRALIZED SECURITY EVENT LOG COLLECTION   INTEGRATION OF SCANNING & OTHER MONITORING INFORMATION	140
MON-02.4: CENTRALIZED SECURITY EVENT LOG COLLECTION   CORRELATION WITH PHYSICAL MONITORING	141
MON-02.5: CENTRALIZED SECURITY EVENT LOG COLLECTION   PERMITTED ACTIONS	141
MON-02.6: CENTRALIZED SECURITY EVENT LOG COLLECTION   AUDIT LEVEL ADJUSTMENT	141
MON-02.7: CENTRALIZED SECURITY EVENT LOG COLLECTION   SYSTEM-WIDE/TIME-CORRELATED AUDIT TRAIL	141
MON-02.8: CENTRALIZED SECURITY EVENT LOG COLLECTION   CHANGES BY AUTHORIZED INDIVIDUALS	142
<b>MON-03: CONTENT OF EVENT LOGS</b>	<b>142</b>
MON-03.1: CONTENT OF EVENT LOGS   SENSITIVE AUDIT INFORMATION	143
MON-03.2: CONTENT OF EVENT LOGS   AUDIT TRAILS	143
MON-03.3: CONTENT OF EVENT LOGS   PRIVILEGED FUNCTIONS LOGGING	144
MON-03.4: CONTENT OF EVENT LOGS   VERBOSITY LOGGING FOR BOUNDARY DEVICES	144
MON-03.5: CONTENT OF EVENT LOGS   LIMIT PERSONAL DATA (PD) IN AUDIT RECORDS	144
MON-03.6: CONTENT OF EVENT LOGS   CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT	145
MON-03.7: CONTENT OF EVENT LOGS   DATABASE LOGGING	145
<b>MON-04: EVENT LOG STORAGE CAPACITY</b>	<b>145</b>
<b>MON-05: RESPONSE TO EVENT LOG PROCESSING FAILURES</b>	<b>146</b>
MON-05.1: RESPONSE TO AUDIT PROCESSING FAILURES   REAL-TIME ALERTS OF EVENT LOGGING FAILURE	146
MON-05.2: RESPONSE TO AUDIT PROCESSING FAILURES   EVENT LOG STORAGE CAPACITY ALERTING	146



<b>MON-06: MONITORING REPORTING</b>	<b>147</b>
MON-06.1: MONITORING REPORTING   QUERY PARAMETER AUDITS OF PERSONAL DATA	147
MON-06.2: MONITORING REPORTING   TREND ANALYSIS REPORTING	147
<b>MON-07: TIME STAMPS</b>	<b>148</b>
MON-07.1: TIME STAMPS   SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE	148
<b>MON-08: PROTECTION OF EVENT LOGS</b>	<b>148</b>
MON-08.1: PROTECTION OF EVENT LOGS   EVENT LOG BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS	149
MON-08.2: PROTECTION OF EVENT LOGS   ACCESS BY SUBSET OF PRIVILEGED USERS	149
MON-08.3: PROTECTION OF EVENT LOGS   CRYPTOGRAPHIC PROTECTION OF EVENT LOG INFORMATION	149
MON-08.4: PROTECTION OF EVENT LOGS   DUAL AUTHORIZATION FOR EVENT LOG MOVEMENT	149
<b>MON-09: NON-REPUDIATION</b>	<b>150</b>
MON-09.1: NON-REPUDIATION   IDENTITY BINDING	150
<b>MON-10: EVENT LOG RETENTION</b>	<b>151</b>
<b>MON-11: MONITORING FOR INFORMATION DISCLOSURE</b>	<b>151</b>
MON-11.1: MONITORING FOR INFORMATION DISCLOSURE   ANALYZE TRAFFIC FOR COVERT EXFILTRATION	151
MON-11.2: MONITORING FOR INFORMATION DISCLOSURE   UNAUTHORIZED NETWORK SERVICES	151
MON-11.3: MONITORING FOR INFORMATION DISCLOSURE   MONITORING FOR INDICATORS OF COMPROMISE (IOC)	152
<b>MON-12: SESSION AUDIT</b>	<b>152</b>
<b>MON-13: ALTERNATE EVENT LOGGING CAPABILITY</b>	<b>152</b>
<b>MON-14: CROSS-ORGANIZATIONAL MONITORING</b>	<b>153</b>
MON-14.1: CROSS-ORGANIZATIONAL MONITORING   SHARING OF EVENT LOGS	153
<b>MON-15: COVERT CHANNEL ANALYSIS</b>	<b>153</b>
<b>MON-16: ANOMALOUS BEHAVIOR</b>	<b>154</b>
MON-16.1: ANOMALOUS BEHAVIOR   INSIDER THREATS	154
MON-16.2: ANOMALOUS BEHAVIOR   THIRD-PARTY THREATS	154
MON-16.3: ANOMALOUS BEHAVIOR   UNAUTHORIZED ACTIVITIES	154
MON-16.4: ANOMALOUS BEHAVIOR   ACCOUNT CREATION AND MODIFICATION LOGGING	154
<b>CRYPTOGRAPHIC PROTECTIONS (CRY) POLICY &amp; STANDARDS</b>	<b>156</b>
<b>CRY-01: USE OF CRYPTOGRAPHIC CONTROLS</b>	<b>156</b>
CRY-01.1: USE OF CRYPTOGRAPHIC CONTROLS   ALTERNATE PHYSICAL PROTECTION	157
CRY-01.2: USE OF CRYPTOGRAPHIC CONTROLS   EXPORT-CONTROLLED TECHNOLOGY	157
CRY-01.3: USE OF CRYPTOGRAPHIC CONTROLS   PRE/POST TRANSMISSION HANDLING	157
CRY-01.4: USE OF CRYPTOGRAPHIC CONTROLS   CONCEAL/RANDOMIZE COMMUNICATIONS	157
CRY-01.5: USE OF CRYPTOGRAPHIC CONTROLS   CRYPTOGRAPHIC CIPHER SUITES AND PROTOCOLS INVENTORY	158
<b>CRY-02: CRYPTOGRAPHIC MODULE AUTHENTICATION</b>	<b>158</b>
<b>CRY-03: TRANSMISSION CONFIDENTIALITY</b>	<b>158</b>
<b>CRY-04: TRANSMISSION INTEGRITY</b>	<b>159</b>
<b>CRY-05: ENCRYPTING DATA AT REST</b>	<b>159</b>
CRY-05.1: ENCRYPTING DATA AT REST   STORAGE MEDIA	160
CRY-05.2: ENCRYPTING DATA AT REST   OFFLINE STORAGE	160
CRY-05.3: ENCRYPTING DATA AT REST   DATABASE ENCRYPTION	160
<b>CRY-06: NON-CONSOLE ADMINISTRATIVE ACCESS</b>	<b>161</b>
<b>CRY-07: WIRELESS ACCESS AUTHENTICATION &amp; ENCRYPTION</b>	<b>161</b>
<b>CRY-08: PUBLIC KEY INFRASTRUCTURE (PKI)</b>	<b>162</b>
CRY-08.1: PUBLIC KEY INFRASTRUCTURE (PKI)   AVAILABILITY	162
<b>CRY-09: CRYPTOGRAPHIC KEY MANAGEMENT</b>	<b>162</b>
CRY-09.1: CRYPTOGRAPHIC KEY MANAGEMENT   SYMMETRIC KEYS	164
CRY-09.2: CRYPTOGRAPHIC KEY MANAGEMENT   ASYMMETRIC KEYS	164
CRY-09.3: CRYPTOGRAPHIC KEY MANAGEMENT   CRYPTOGRAPHIC KEY LOSS OR CHANGE	164
CRY-09.4: CRYPTOGRAPHIC KEY MANAGEMENT   CONTROL & DISTRIBUTION OF CRYPTOGRAPHIC KEYS	165
CRY-09.5: CRYPTOGRAPHIC KEY MANAGEMENT   ASSIGNED OWNERS	165
CRY-09.6: CRYPTOGRAPHIC KEY MANAGEMENT   THIRD-PARTY CRYPTOGRAPHIC KEYS	166
CRY-09.7: CRYPTOGRAPHIC KEY MANAGEMENT   EXTERNAL SYSTEM CRYPTOGRAPHIC KEY CONTROL	166
<b>CRY-10: TRANSMISSION OF CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES</b>	<b>166</b>
<b>CRY-11: CERTIFICATE AUTHORITIES</b>	<b>166</b>
<b>DATA CLASSIFICATION &amp; HANDLING (DCH) POLICY &amp; STANDARDS</b>	<b>167</b>
<b>DCH-01: DATA PROTECTION</b>	<b>167</b>
DCH-01.1: DATA PROTECTION   DATA STEWARDSHIP	167

<i>DCH-01.2: DATA PROTECTION   SENSITIVE/REGULATED DATA PROTECTION</i>	168
<i>DCH-01.3: DATA PROTECTION   SENSITIVE / REGULATED MEDIA RECORDS</i>	168
<i>DCH-01.4: DATA PROTECTION   DEFINING ACCESS AUTHORIZATIONS FOR SENSITIVE / REGULATED DATA</i>	168
<b>DCH-02: DATA &amp; ASSET CLASSIFICATION</b>	<b>169</b>
<i>DCH-02.1: DATA &amp; ASSET CLASSIFICATION   HIGHEST CLASSIFICATION LEVEL</i>	169
<b>DCH-03: MEDIA ACCESS</b>	<b>169</b>
<i>DCH-03.1: MEDIA ACCESS   DISCLOSURE OF INFORMATION</i>	170
<i>DCH-03.2: MEDIA ACCESS   MASKING DISPLAYED DATA</i>	170
<i>DCH-03.3: MEDIA ACCESS   CONTROLLED RELEASE</i>	170
<b>DCH-04: MEDIA MARKING</b>	<b>171</b>
<i>DCH-04.1: MEDIA MARKING   AUTOMATED MARKING</i>	171
<b>DCH-05: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES</b>	<b>171</b>
<i>DCH-05.1: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   DYNAMIC ATTRIBUTE ASSOCIATION</i>	172
<i>DCH-05.2: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS</i>	172
<i>DCH-05.3: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM</i>	172
<i>DCH-05.4: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS</i>	172
<i>DCH-05.5: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES</i>	172
<i>DCH-05.6: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   DATA SUBJECT ATTRIBUTE ASSOCIATIONS</i>	173
<i>DCH-05.7: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   CONSISTENT ATTRIBUTE INTERPRETATION</i>	173
<i>DCH-05.8: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   IDENTITY ASSOCIATION TECHNIQUES &amp; TECHNOLOGIES</i>	173
<i>DCH-05.9: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   ATTRIBUTE REASSIGNMENT</i>	173
<i>DCH-05.10: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS</i>	174
<i>DCH-05.11: CYBERSECURITY &amp; DATA PRIVACY ATTRIBUTES   AUDIT CHANGES</i>	174
<b>DCH-06: MEDIA STORAGE</b>	<b>174</b>
<i>DCH-06.1: MEDIA STORAGE   PHYSICALLY SECURE ALL MEDIA</i>	175
<i>DCH-06.2: MEDIA STORAGE   SENSITIVE DATA INVENTORIES</i>	175
<i>DCH-06.3: MEDIA STORAGE   PERIODIC SCANS FOR SENSITIVE DATA</i>	175
<i>DCH-06.4: MEDIA STORAGE   MAKING SENSITIVE DATA UNREADABLE IN STORAGE</i>	175
<i>DCH-06.5: MEDIA STORAGE   STORING AUTHENTICATION DATA</i>	176
<b>DCH-07: MEDIA TRANSPORTATION</b>	<b>177</b>
<i>DCH-07.1: MEDIA TRANSPORTATION   CUSTODIANS</i>	177
<i>DCH-07.2: MEDIA TRANSPORTATION   ENCRYPTING DATA IN STORAGE MEDIA</i>	177
<b>DCH-08: PHYSICAL MEDIA DISPOSAL</b>	<b>178</b>
<b>DCH-09: SYSTEM MEDIA SANITIZATION</b>	<b>178</b>
<i>DCH-09.1: SYSTEM MEDIA SANITIZATION   SYSTEM MEDIA SANITIZATION DOCUMENTATION</i>	179
<i>DCH-09.2: SYSTEM MEDIA SANITIZATION   EQUIPMENT TESTING</i>	179
<i>DCH-09.3: SYSTEM MEDIA SANITIZATION   SANITIZATION OF PERSONAL DATA (PD)</i>	179
<i>DCH-09.4: SYSTEM MEDIA SANITIZATION   FIRST TIME USE SANITIZATION</i>	180
<i>DCH-09.5: SYSTEM MEDIA SANITIZATION   DUAL AUTHORIZATION FOR SENSITIVE DATA DESTRUCTION</i>	180
<b>DCH-10: MEDIA USE</b>	<b>180</b>
<i>DCH-10.1: MEDIA USE   LIMITATIONS ON USE</i>	181
<i>DCH-10.2: MEDIA USE   PROHIBIT USE WITHOUT OWNER</i>	181
<b>DCH-11: DATA RECLASSIFICATION</b>	<b>181</b>
<b>DCH-12: REMOVABLE MEDIA SECURITY</b>	<b>181</b>
<b>DCH-13: USE OF EXTERNAL INFORMATION SYSTEMS</b>	<b>182</b>
<i>DCH-13.1: USE OF EXTERNAL INFORMATION SYSTEMS   LIMITS OF AUTHORIZED USE</i>	183
<i>DCH-13.2: USE OF EXTERNAL INFORMATION SYSTEMS   PORTABLE STORAGE DEVICES</i>	183
<i>DCH-13.3: USE OF EXTERNAL INFORMATION SYSTEMS   PROTECTING SENSITIVE DATA ON EXTERNAL SYSTEMS</i>	183
<i>DCH-13.4: USE OF EXTERNAL INFORMATION SYSTEMS   NON-ORGANIZATIONALLY OWNED SYSTEMS/COMPONENTS/DEVICES</i>	183
<b>DCH-14: INFORMATION SHARING</b>	<b>184</b>
<i>DCH-14.1: INFORMATION SHARING   INFORMATION SEARCH &amp; RETRIEVAL</i>	185
<i>DCH-14.2: INFORMATION SHARING   TRANSFER AUTHORIZATIONS</i>	185
<i>DCH-14.3: INFORMATION SHARING   DATA ACCESS MAPPING</i>	185
<b>DCH-15: PUBLICLY ACCESSIBLE CONTENT</b>	<b>186</b>
<b>DCH-16: DATA MINING PROTECTION</b>	<b>186</b>
<b>DCH-17: AD-HOC TRANSFERS</b>	<b>186</b>
<b>DCH-18: MEDIA &amp; DATA RETENTION</b>	<b>186</b>
<i>DCH-18.1: MEDIA &amp; DATA RETENTION   LIMIT PERSONAL DATA (PD) ELEMENTS IN TESTING, TRAINING &amp; RESEARCH</i>	188

DCH-18.2: MEDIA & DATA RETENTION   MINIMIZE PERSONAL DATA (PD)	188
DCH-18.3: MEDIA & DATA RETENTION   TEMPORARY FILES CONTAINING PERSONAL DATA	188
<b>DCH-19: GEOGRAPHIC LOCATION OF DATA</b>	<b>189</b>
<b>DCH-20: ARCHIVED DATA SETS</b>	<b>189</b>
<b>DCH-21: INFORMATION DISPOSAL</b>	<b>189</b>
<b>DCH-22: DATA QUALITY OPERATIONS</b>	<b>190</b>
DCH-22.1: DATA QUALITY OPERATIONS   UPDATING & CORRECTING PERSONAL DATA (PD)	190
DCH-22.2: DATA QUALITY OPERATIONS   DATA TAGS	190
DCH-22.3: DATA QUALITY OPERATIONS   PRIMARY SOURCE PERSONAL DATA (PD) COLLECTION	190
<b>DCH-23: DE-IDENTIFICATION (ANONYMIZATION)</b>	<b>190</b>
DCH-23.1: DE-IDENTIFICATION (ANONYMIZATION)   DE-IDENTIFY DATASET UPON COLLECTION	191
DCH-23.2: DE-IDENTIFICATION (ANONYMIZATION)   ARCHIVING	191
DCH-23.3: DE-IDENTIFICATION (ANONYMIZATION)   RELEASE	191
DCH-23.4: DE-IDENTIFICATION (ANONYMIZATION)   REMOVAL, MASKING, ENCRYPTION, HASHING OR REPLACEMENT OF DIRECT IDENTIFIERS	191
DCH-23.5: DE-IDENTIFICATION (ANONYMIZATION)   STATISTICAL DISCLOSURE CONTROL	192
DCH-23.6: DE-IDENTIFICATION (ANONYMIZATION)   DIFFERENTIAL DATA PRIVACY	192
DCH-23.7: DE-IDENTIFICATION (ANONYMIZATION)   AUTOMATED DE-IDENTIFICATION OF SENSITIVE DATA	192
DCH-23.8: DE-IDENTIFICATION (ANONYMIZATION)   MOTIVATED INTRUDER	192
DCH-23.9: DE-IDENTIFICATION (ANONYMIZATION)   CODE NAMES	193
<b>DCH-24: INFORMATION LOCATION</b>	<b>193</b>
DCH-24.1: INFORMATION LOCATION   AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION	193
<b>DCH-25: TRANSFER OF SENSITIVE AND/OR REGULATED DATA</b>	<b>194</b>
DCH-25.1: TRANSFER OF SENSITIVE AND/OR REGULATED DATA   TRANSFER ACTIVITY LIMITS	194
<b>DCH-26: DATA LOCALIZATION</b>	<b>194</b>
<b>EMBEDDED TECHNOLOGY (EMB) POLICY &amp; STANDARDS</b>	<b>195</b>
<b>EMB-01: EMBEDDED TECHNOLOGY SECURITY PROGRAM</b>	<b>195</b>
<b>EMB-02: INTERNET OF THINGS (IOT)</b>	<b>195</b>
<b>EMB-03: OPERATIONAL TECHNOLOGY (OT)</b>	<b>195</b>
<b>EMB-04: INTERFACE SECURITY</b>	<b>196</b>
<b>EMB-05: EMBEDDED TECHNOLOGY CONFIGURATION MONITORING</b>	<b>196</b>
<b>EMB-06: PREVENT ALTERATIONS</b>	<b>197</b>
<b>EMB-07: EMBEDDED TECHNOLOGY MAINTENANCE</b>	<b>197</b>
<b>EMB-08: RESILIENCE TO OUTAGES</b>	<b>197</b>
<b>EMB-09: POWER LEVEL MONITORING</b>	<b>197</b>
<b>EMB-10: EMBEDDED TECHNOLOGY REVIEWS</b>	<b>198</b>
<b>EMB-11: MESSAGE QUEUING TELEMETRY TRANSPORT (MQTT) SECURITY</b>	<b>198</b>
<b>EMB-12: RESTRICT COMMUNICATIONS</b>	<b>198</b>
<b>EMB-13: AUTHORIZED COMMUNICATIONS</b>	<b>198</b>
<b>EMB-14: OPERATING ENVIRONMENT CERTIFICATION</b>	<b>198</b>
<b>EMB-15: SAFETY ASSESSMENT</b>	<b>199</b>
<b>EMB-16: CERTIFICATE-BASED AUTHENTICATION</b>	<b>199</b>
<b>EMB-17: CHIP-TO-CLOUD SECURITY</b>	<b>199</b>
<b>EMB-18: REAL-TIME OPERATING SYSTEM (RTOS) SECURITY</b>	<b>199</b>
<b>EMB-19: SAFE OPERATIONS</b>	<b>199</b>
<b>ENDPOINT SECURITY (END) POLICY &amp; STANDARDS</b>	<b>200</b>
<b>END-01: ENDPOINT SECURITY</b>	<b>200</b>
<b>END-02: ENDPOINT PROTECTION MEASURES</b>	<b>200</b>
<b>END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS</b>	<b>201</b>
END-03.1: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS   SOFTWARE INSTALLATION ALERTS	201
END-03.2: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS   GOVERNING ACCESS RESTRICTION FOR CHANGE	201
<b>END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE)</b>	<b>201</b>
END-04.1: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   AUTOMATIC ANTIMALWARE SIGNATURE UPDATES	202
END-04.2: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   DOCUMENTED PROTECTION MEASURES	202
END-04.3: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   CENTRALIZED MANAGEMENT OF ANTIMALWARE TECHNOLOGIES	203
END-04.4: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   NONSIGNATURE-BASED DETECTION	203
END-04.5: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   MALWARE PROTECTION MECHANISM TESTING	203

END-04.6: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   EVOLVING MALWARE THREATS	203
END-04.7: MALICIOUS CODE PROTECTION (ANTI-MALWARE)   ALWAYS ON PROTECTION	204
<b>END-05: SOFTWARE FIREWALL</b>	<b>204</b>
<b>END-06: ENDPOINT FILE INTEGRITY MONITORING (FIM)</b>	<b>205</b>
END-06.1: ENDPOINT FILE INTEGRITY MONITORING (FIM)   INTEGRITY CHECKS	205
END-06.2: ENDPOINT FILE INTEGRITY MONITORING (FIM)   INTEGRATION OF DETECTION & RESPONSE	205
END-06.3: ENDPOINT FILE INTEGRITY MONITORING (FIM)   AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS	206
END-06.4: ENDPOINT FILE INTEGRITY MONITORING (FIM)   AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	206
END-06.5: ENDPOINT FILE INTEGRITY MONITORING (FIM)   VERIFY BOOT PROCESS	206
END-06.6: ENDPOINT FILE INTEGRITY MONITORING (FIM)   PROTECTION OF BOOT FIRMWARE	206
END-06.7: ENDPOINT FILE INTEGRITY MONITORING (FIM)   BINARY OR MACHINE-EXECUTABLE CODE	207
<b>END-07: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS/HIPS)</b>	<b>207</b>
<b>END-08: PHISHING &amp; SPAM PROTECTION</b>	<b>207</b>
END-08.1: PHISHING & SPAM PROTECTION   CENTRAL MANAGEMENT	208
END-08.2: PHISHING & SPAM PROTECTION   AUTOMATIC SPAM AND PHISHING PROTECTION UPDATES	208
<b>END-09: TRUSTED PATH</b>	<b>208</b>
<b>END-10: MOBILE CODE</b>	<b>208</b>
<b>END-11: THIN NODES</b>	<b>209</b>
<b>END-12: PORT &amp; INPUT/OUTPUT (I/O) DEVICE ACCESS</b>	<b>210</b>
<b>END-13: SENSOR CAPABILITY</b>	<b>210</b>
END-13.1: SENSOR CAPABILITY   AUTHORIZED USE	210
END-13.2: SENSOR CAPABILITY   NOTICE OF COLLECTION	210
END-13.3: SENSOR CAPABILITY   COLLECTION MINIMIZATION	211
END-13.4: SENSOR CAPABILITY   SENSOR DELIVERY VERIFICATION	211
<b>END-14: COLLABORATIVE COMPUTING DEVICES</b>	<b>211</b>
END-14.1: COLLABORATIVE COMPUTING DEVICES   DISABLING/REMOVAL IN SECURE WORK AREAS	212
END-14.2: COLLABORATIVE COMPUTING DEVICES   EXPLICITLY INDICATE CURRENT PARTICIPANTS	212
<b>END-15: HYPERVISOR ACCESS</b>	<b>212</b>
<b>END-16: RESTRICT ACCESS TO SECURITY FUNCTIONS</b>	<b>212</b>
END-16.1: RESTRICT ACCESS TO SECURITY FUNCTIONS   HOST-BASED SECURITY FUNCTION ISOLATION	213
<b>HUMAN RESOURCES SECURITY (HRS) POLICY &amp; STANDARDS</b>	<b>214</b>
<b>HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT</b>	<b>214</b>
<b>HRS-02: POSITION CATEGORIZATION</b>	<b>214</b>
HRS-02.1: POSITION CATEGORIZATION   USERS WITH ELEVATED PRIVILEGES	215
HRS-02.2: POSITION CATEGORIZATION   PROBATIONARY PERIODS	215
<b>HRS-03: ROLES &amp; RESPONSIBILITIES</b>	<b>215</b>
HRS-03.1: ROLES & RESPONSIBILITIES   USER AWARENESS	216
HRS-03.2: ROLES & RESPONSIBILITIES   COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS	216
<b>HRS-04: PERSONNEL SCREENING</b>	<b>216</b>
HRS-04.1: PERSONNEL SCREENING   ROLES WITH SPECIAL PROTECTION MEASURES	217
HRS-04.2: PERSONNEL SCREENING   FORMAL INDOCTRINATION	217
HRS-04.3: PERSONNEL SCREENING   CITIZENSHIP REQUIREMENTS	217
HRS-04.4: PERSONNEL SCREENING   CITIZENSHIP IDENTIFICATION	217
<b>HRS-05: TERMS OF EMPLOYMENT</b>	<b>218</b>
HRS-05.1: TERMS OF EMPLOYMENT   RULES OF BEHAVIOR	218
HRS-05.2: TERMS OF EMPLOYMENT   SOCIAL MEDIA & SOCIAL NETWORKING RESTRICTIONS	219
HRS-05.3: TERMS OF EMPLOYMENT   USE OF COMMUNICATIONS TECHNOLOGY	219
HRS-05.4: TERMS OF EMPLOYMENT   USE OF CRITICAL TECHNOLOGIES	219
HRS-05.5: TERMS OF EMPLOYMENT   USE OF MOBILE DEVICES	220
HRS-05.6: TERMS OF EMPLOYMENT   SECURITY-MINDED DRESS CODE	220
HRS-05.7: TERMS OF EMPLOYMENT   POLICY FAMILIARIZATION & ACKNOWLEDGEMENT	220
<b>HRS-06: ACCESS AGREEMENTS</b>	<b>220</b>
HRS-06.1: ACCESS AGREEMENTS   CONFIDENTIALITY AGREEMENTS	221
HRS-06.2: ACCESS AGREEMENTS   POST-EMPLOYMENT OBLIGATIONS	221
<b>HRS-07: PERSONNEL SANCTIONS</b>	<b>221</b>
HRS-07.1: PERSONNEL SANCTIONS   WORKPLACE INVESTIGATIONS	222
<b>HRS-08: PERSONNEL TRANSFER</b>	<b>223</b>
<b>HRS-09: PERSONNEL TERMINATION</b>	<b>223</b>



HRS-09.1: PERSONNEL TERMINATION   ASSET COLLECTION	224
HRS-09.2: PERSONNEL TERMINATION   HIGH-RISK TERMINATIONS	224
HRS-09.3: PERSONNEL TERMINATION   POST-EMPLOYMENT REQUIREMENTS	225
HRS-09.4: PERSONNEL TERMINATION   AUTOMATED EMPLOYMENT STATUS NOTIFICATION	225
<b>HRS-10: THIRD-PARTY PERSONNEL SECURITY</b>	<b>225</b>
<b>HRS-11: SEPARATION OF DUTIES (SOD)</b>	<b>226</b>
<b>HRS-12: INCOMPATIBLE ROLES</b>	<b>226</b>
HRS-12.1: INCOMPATIBLE ROLES   TWO-PERSON RULE	227
<b>HRS-13: IDENTIFY CRITICAL SKILLS &amp; GAPS</b>	<b>227</b>
HRS-13.1: IDENTIFY CRITICAL SKILLS & GAPS   REMEDIATE IDENTIFIED SKILLS DEFICIENCIES	227
HRS-13.2: IDENTIFY CRITICAL SKILLS & GAPS   IDENTIFY VITAL CYBERSECURITY & DATA PRIVACY STAFF	227
HRS-13.3: IDENTIFY CRITICAL SKILLS & GAPS   ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & DATA PRIVACY STAFF	228
HRS-13.4: IDENTIFY CRITICAL SKILLS & GAPS   PERFORM SUCCESSION PLANNING	228
<b>IDENTIFICATION &amp; AUTHENTICATION (IAC) POLICY &amp; STANDARDS</b>	<b>229</b>
<b>IAC-01: IDENTITY &amp; ACCESS MANAGEMENT (IAM)</b>	<b>229</b>
IAC-01.1: IDENTITY & ACCESS MANAGEMENT (IAM)   RETAIN ACCESS RECORDS	229
IAC-01.2: IDENTITY & ACCESS MANAGEMENT (IAM)   AUTHENTICATE, AUTHORIZE AND AUDIT (AAA)	230
<b>IAC-02: IDENTIFICATION &amp; AUTHENTICATION FOR ORGANIZATIONAL USERS</b>	<b>230</b>
IAC-02.1: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS   GROUP AUTHENTICATION	231
IAC-02.2: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS   REPLAY-RESISTANT AUTHENTICATION	231
IAC-02.3: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS   ACCEPTANCE OF PIV CREDENTIALS	231
IAC-02.4: IDENTIFICATION & AUTHENTICATION FOR ORGANIZATIONAL USERS   OUT-OF-BAND AUTHENTICATION (OOBA)	232
<b>IAC-03: IDENTIFICATION &amp; AUTHENTICATION FOR NON-ORGANIZATIONAL USERS</b>	<b>232</b>
IAC-03.1: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   ACCEPTANCE OF PIV CREDENTIALS FROM OTHER ORGANIZATIONS	232
IAC-03.2: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   ACCEPTANCE OF THIRD-PARTY CREDENTIALS	232
IAC-03.3: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   USE OF FICAM-ISSUED PROFILES	233
IAC-03.4: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   DISASSOCIABILITY	233
IAC-03.5: IDENTIFICATION & AUTHENTICATION FOR NON-ORGANIZATIONAL USERS   ACCEPTANCE OF EXTERNAL AUTHENTICATORS	233
<b>IAC-04: IDENTIFICATION &amp; AUTHENTICATION FOR DEVICES</b>	<b>233</b>
IAC-04.1: IDENTIFICATION & AUTHENTICATION FOR DEVICES   DEVICE ATTESTATION	234
<b>IAC-05: IDENTIFICATION &amp; AUTHENTICATION FOR THIRD PARTY SYSTEMS &amp; SERVICES</b>	<b>234</b>
IAC-05.1: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES   INFORMATION EXCHANGE	234
IAC-05.2: IDENTIFICATION & AUTHENTICATION FOR THIRD PARTY SYSTEMS & SERVICES   PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	234
<b>IAC-06: MULTI-FACTOR AUTHENTICATION (MFA)</b>	<b>235</b>
IAC-06.1: MULTI-FACTOR AUTHENTICATION (MFA)   NETWORK ACCESS TO PRIVILEGED ACCOUNTS	235
IAC-06.2: MULTI-FACTOR AUTHENTICATION (MFA)   NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS	236
IAC-06.3: MULTI-FACTOR AUTHENTICATION (MFA)   LOCAL ACCESS TO PRIVILEGED ACCOUNTS	236
IAC-06.4: MULTI-FACTOR AUTHENTICATION (MFA)   OUT OF BAND (OOB) FACTOR	236
<b>IAC-07: USER PROVISIONING &amp; DE-PROVISIONING</b>	<b>236</b>
IAC-07.1: USER PROVISIONING & DE-PROVISIONING   CHANGE OF ROLES & DUTIES	237
IAC-07.2: USER PROVISIONING & DE-PROVISIONING   TERMINATION OF EMPLOYMENT	237
<b>IAC-08: ROLE-BASED ACCESS CONTROL (RBAC)</b>	<b>238</b>
<b>IAC-09: IDENTIFIER MANAGEMENT (USER NAMES)</b>	<b>238</b>
IAC-09.1: IDENTIFIER MANAGEMENT   USER IDENTITY (ID) MANAGEMENT	239
IAC-09.2: IDENTIFIER MANAGEMENT   IDENTITY USER STATUS	239
IAC-09.3: IDENTIFIER MANAGEMENT   DYNAMIC MANAGEMENT	239
IAC-09.4: IDENTIFIER MANAGEMENT   CROSS-ORGANIZATION MANAGEMENT	240
IAC-09.5: IDENTIFIER MANAGEMENT   PRIVILEGED ACCOUNT IDENTIFIERS	240
IAC-09.6: IDENTIFIER MANAGEMENT   PAIRWISE PSEUDONYMOUS IDENTIFIERS (PPID)	240
<b>IAC-10: AUTHENTICATOR MANAGEMENT</b>	<b>240</b>
IAC-10.1: AUTHENTICATOR MANAGEMENT   PASSWORD-BASED AUTHENTICATION	241
IAC-10.2: AUTHENTICATOR MANAGEMENT   PKI-BASED AUTHENTICATION	243
IAC-10.3: AUTHENTICATOR MANAGEMENT   IN-PERSON OR TRUSTED THIRD-PARTY REGISTRATION	243
IAC-10.4: AUTHENTICATOR MANAGEMENT   AUTOMATED SUPPORT FOR PASSWORD STRENGTH	244



<i>IAC-10.5: AUTHENTICATOR MANAGEMENT   PROTECTION OF AUTHENTICATORS</i>	244
<i>IAC-10.6: AUTHENTICATOR MANAGEMENT   NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS</i>	244
<i>IAC-10.7: AUTHENTICATOR MANAGEMENT   HARDWARE TOKEN-BASED AUTHENTICATION</i>	245
<i>IAC-10.8: AUTHENTICATOR MANAGEMENT   VENDOR-SUPPLIED DEFAULTS</i>	245
<i>IAC-10.9: AUTHENTICATOR MANAGEMENT   MULTIPLE INFORMATION SYSTEM ACCOUNTS</i>	245
<i>IAC-10.10: AUTHENTICATOR MANAGEMENT   EXPIRATION OF CACHED AUTHENTICATORS</i>	245
<i>IAC-10.11: AUTHENTICATOR MANAGEMENT   PASSWORD MANAGERS</i>	246
<i>IAC-10.12: AUTHENTICATOR MANAGEMENT   BIOMETRIC AUTHENTICATION</i>	246
<b>IAC-11: AUTHENTICATOR FEEDBACK</b>	<b>246</b>
<b>IAC-12: CRYPTOGRAPHIC MODULE AUTHENTICATION</b>	<b>247</b>
<i>IAC-12.1: CRYPTOGRAPHIC MODULE AUTHENTICATION   HARDWARE SECURITY MODULES (HSM)</i>	247
<b>IAC-13: ADAPTIVE IDENTIFICATION &amp; AUTHENTICATION</b>	<b>247</b>
<i>IAC-13.1: ADAPTIVE IDENTIFICATION &amp; AUTHENTICATION   SINGLE SIGN-ON (SSO)</i>	247
<i>IAC-13.2: ADAPTIVE IDENTIFICATION &amp; AUTHENTICATION   FEDERATED CREDENTIAL MANAGEMENT</i>	248
<b>IAC-14: RE-AUTHENTICATION</b>	<b>248</b>
<b>IAC-15: ACCOUNT MANAGEMENT</b>	<b>248</b>
<i>IAC-15.1: ACCOUNT MANAGEMENT   AUTOMATED SYSTEM ACCOUNT MANAGEMENT (DIRECTORY SERVICES)</i>	250
<i>IAC-15.2: ACCOUNT MANAGEMENT   REMOVAL OF TEMPORARY/EMERGENCY ACCOUNTS</i>	251
<i>IAC-15.3: ACCOUNT MANAGEMENT   DISABLE INACTIVE ACCOUNTS</i>	251
<i>IAC-15.4: ACCOUNT MANAGEMENT   AUTOMATED AUDIT ACTIONS</i>	251
<i>IAC-15.5: ACCOUNT MANAGEMENT   RESTRICTIONS ON SHARED GROUPS/ACCOUNTS</i>	251
<i>IAC-15.6: ACCOUNT MANAGEMENT   ACCOUNT DISABLING FOR HIGH RISK INDIVIDUALS</i>	252
<i>IAC-15.7: ACCOUNT MANAGEMENT   SYSTEM ACCOUNTS</i>	252
<i>IAC-15.8: ACCOUNT MANAGEMENT   USAGE CONDITIONS</i>	252
<i>IAC-15.9: ACCOUNT MANAGEMENT   EMERGENCY ACCOUNTS</i>	253
<b>IAC-16: PRIVILEGED ACCOUNT MANAGEMENT (PAM)</b>	<b>253</b>
<i>IAC-16.1: PRIVILEGED ACCOUNT MANAGEMENT (PAM)   PRIVILEGED ACCOUNT INVENTORIES</i>	254
<i>IAC-16.2: PRIVILEGED ACCOUNT MANAGEMENT (PAM)   PRIVILEGED ACCOUNT SEPARATION</i>	254
<b>IAC-17: PERIODIC REVIEW OF ACCOUNT PRIVILEGES</b>	<b>254</b>
<b>IAC-18: USER RESPONSIBILITIES FOR ACCOUNT MANAGEMENT</b>	<b>255</b>
<b>IAC-19: CREDENTIAL SHARING</b>	<b>255</b>
<b>IAC-20: ACCESS ENFORCEMENT</b>	<b>256</b>
<i>IAC-20.1: ACCESS ENFORCEMENT   ACCESS TO SENSITIVE DATA</i>	256
<i>IAC-20.2: ACCESS ENFORCEMENT   DATABASE ACCESS</i>	256
<i>IAC-20.3: ACCESS ENFORCEMENT   USE OF PRIVILEGED UTILITY PROGRAMS</i>	257
<i>IAC-20.4: ACCESS ENFORCEMENT   DEDICATED ADMINISTRATIVE MACHINES</i>	257
<i>IAC-20.5: ACCESS ENFORCEMENT   DUAL AUTHORIZATION FOR PRIVILEGED COMMANDS</i>	257
<i>IAC-20.6: ACCESS ENFORCEMENT   REVOCATION OF ACCESS AUTHORIZATIONS</i>	257
<i>IAC-20.7: ACCESS ENFORCEMENT   AUTHORIZED SYSTEM ACCOUNTS</i>	258
<b>IAC-21: LEAST PRIVILEGE</b>	<b>258</b>
<i>IAC-21.1: LEAST PRIVILEGE   AUTHORIZE ACCESS TO SECURITY FUNCTIONS</i>	258
<i>IAC-21.2: LEAST PRIVILEGE   NON-PRIVILEGED ACCESS FOR NON-SECURITY FUNCTIONS</i>	259
<i>IAC-21.3: LEAST PRIVILEGE   PRIVILEGED ACCOUNTS</i>	259
<i>IAC-21.4: LEAST PRIVILEGE   AUDITING USE OF PRIVILEGED FUNCTIONS</i>	259
<i>IAC-21.5: LEAST PRIVILEGE   PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS</i>	259
<i>IAC-21.6: LEAST PRIVILEGE   NETWORK ACCESS TO PRIVILEGED COMMANDS</i>	260
<i>IAC-21.7: LEAST PRIVILEGE   PRIVILEGE LEVELS FOR CODE EXECUTION</i>	260
<b>IAC-22: ACCOUNT LOCKOUT</b>	<b>260</b>
<b>IAC-23: CONCURRENT SESSION CONTROL</b>	<b>261</b>
<b>IAC-24: SESSION LOCK</b>	<b>261</b>
<i>IAC-24.1: SESSION LOCK   PATTERN-HIDING DISPLAYS</i>	261
<b>IAC-25: SESSION TERMINATION</b>	<b>261</b>
<i>IAC-25.1: SESSION TERMINATION   USER-INITIATED LOGOUTS/MESSAGE DISPLAYS</i>	262
<b>IAC-26: PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHORIZATION</b>	<b>262</b>
<b>IAC-27: REFERENCE MONITOR</b>	<b>262</b>
<b>IAC-28: IDENTITY PROOFING (IDENTITY VERIFICATION)</b>	<b>263</b>
<i>IAC-28.1: IDENTITY PROOFING (IDENTITY VERIFICATION)   MANAGEMENT APPROVAL FOR NEW OR CHANGED ACCOUNTS</i>	263
<i>IAC-28.2: IDENTITY PROOFING (IDENTITY VERIFICATION)   IDENTITY EVIDENCE</i>	263

IAC-28.3: IDENTITY PROOFING (IDENTITY VERIFICATION)   IDENTITY EVIDENCE VALIDATION & VERIFICATION	263
IAC-28.4: IDENTITY PROOFING (IDENTITY VERIFICATION)   IN-PERSON VALIDATION & VERIFICATION	264
IAC-28.5: IDENTITY PROOFING (IDENTITY VERIFICATION)   ADDRESS CONFIRMATION	264
<b>IAC-29: ATTRIBUTE-BASED ACCESS CONTROL (ABAC)</b>	<b>264</b>
<b>INCIDENT RESPONSE (IRO) POLICY &amp; STANDARDS</b>	<b>265</b>
<b>IRO-01: INCIDENTS RESPONSE OPERATIONS</b>	<b>265</b>
<b>IRO-02: INCIDENT HANDLING</b>	<b>265</b>
IRO-02.1: INCIDENT HANDLING   AUTOMATED INCIDENT HANDLING PROCESSES	266
IRO-02.2: INCIDENT HANDLING   INSIDER THREAT RESPONSE CAPABILITY	266
IRO-02.3: INCIDENT HANDLING   DYNAMIC RECONFIGURATION	267
IRO-02.4: INCIDENT HANDLING   INCIDENT CLASSIFICATION & PRIORITIZATION	267
IRO-02.5: INCIDENT HANDLING   CORRELATION WITH EXTERNAL ORGANIZATIONS	269
IRO-02.6: INCIDENT HANDLING   AUTOMATIC DISABLING OF SYSTEM	269
<b>IRO-03: INDICATORS OF COMPROMISE (IOC)</b>	<b>269</b>
<b>IRO-04: INCIDENT RESPONSE PLAN (IRP)</b>	<b>269</b>
IRO-04.1: INCIDENT RESPONSE PLAN (IRP)   DATA BREACH	270
IRO-04.2: INCIDENT RESPONSE PLAN (IRP)   IRP UPDATE	271
IRO-04.3: INCIDENT RESPONSE PLAN (IRP)   CONTINUOUS INCIDENT RESPONSE IMPROVEMENTS	271
<b>IRO-05: INCIDENT RESPONSE TRAINING</b>	<b>271</b>
IRO-05.1: INCIDENT RESPONSE TRAINING   SIMULATED INCIDENTS	272
IRO-05.2: INCIDENT RESPONSE TRAINING   AUTOMATED INCIDENT RESPONSE TRAINING ENVIRONMENTS	272
<b>IRO-06: INCIDENT RESPONSE TESTING</b>	<b>272</b>
IRO-06.1: INCIDENT RESPONSE TESTING   COORDINATION WITH RELATED PLANS	272
<b>IRO-07: INTEGRATED SECURITY INCIDENT RESPONSE TEAM (ISIRT)</b>	<b>273</b>
<b>IRO-08: CHAIN OF CUSTODY &amp; FORENSICS</b>	<b>273</b>
<b>IRO-09: SITUATIONAL AWARENESS FOR INCIDENTS</b>	<b>273</b>
IRO-09.1: SITUATIONAL AWARENESS FOR INCIDENTS   AUTOMATED TRACKING, DATA COLLECTION & ANALYSIS	274
<b>IRO-10: INCIDENT STAKEHOLDER REPORTING</b>	<b>274</b>
IRO-10.1: INCIDENT STAKEHOLDER REPORTING   AUTOMATED REPORTING	274
IRO-10.2: INCIDENT STAKEHOLDER REPORTING   CYBER INCIDENT REPORTING FOR COVERED DEFENSE INFORMATION (CDI)	275
IRO-10.3: INCIDENT STAKEHOLDER REPORTING   VULNERABILITIES RELATED TO INCIDENTS	275
IRO-10.4: INCIDENT STAKEHOLDER REPORTING   SUPPLY CHAIN COORDINATION	275
<b>IRO-11: INCIDENT REPORTING ASSISTANCE</b>	<b>276</b>
IRO-11.1: INCIDENT REPORTING ASSISTANCE   AUTOMATION SUPPORT OF AVAILABILITY OF INFORMATION/SUPPORT	276
IRO-11.2: INCIDENT REPORTING ASSISTANCE   COORDINATION WITH EXTERNAL PROVIDERS	276
<b>IRO-12: INFORMATION SPILLAGE RESPONSE</b>	<b>276</b>
IRO-12.1: INFORMATION SPILLAGE RESPONSE   RESPONSIBLE PERSONNEL	277
IRO-12.2: INFORMATION SPILLAGE RESPONSE   TRAINING	277
IRO-12.3: INFORMATION SPILLAGE RESPONSE   POST-SPILL OPERATIONS	277
IRO-12.4: INFORMATION SPILLAGE RESPONSE   EXPOSURE TO UNAUTHORIZED PERSONNEL	277
<b>IRO-13: ROOT CAUSE ANALYSIS (RCA) &amp; LESSONS LEARNED</b>	<b>277</b>
<b>IRO-14: REGULATORY &amp; LAW ENFORCEMENT CONTACTS</b>	<b>278</b>
<b>IRO-15: DETONATION CHAMBERS (SANDBOXES)</b>	<b>278</b>
<b>IRO-16: PUBLIC RELATIONS &amp; REPUTATION REPAIR</b>	<b>278</b>
<b>INFORMATION ASSURANCE (IAO) POLICY &amp; STANDARDS</b>	<b>279</b>
<b>IAO-01: INFORMATION ASSURANCE (IA) OPERATIONS</b>	<b>279</b>
IAO-01.1: INFORMATION ASSURANCE (IA) OPERATIONS   ASSESSMENT BOUNDARIES	279
<b>IAO-02: SECURITY ASSESSMENTS</b>	<b>279</b>
IAO-02.1: SECURITY ASSESSMENTS   INDEPENDENT ASSESSORS	280
IAO-02.2: SECURITY ASSESSMENTS   SPECIALIZED ASSESSMENTS	280
IAO-02.3: SECURITY ASSESSMENTS   THIRD-PARTY ASSESSMENTS	281
IAO-02.4: SECURITY ASSESSMENTS   SECURITY ASSESSMENT REPORT (SAR)	281
<b>IAO-03: SYSTEM SECURITY &amp; PRIVACY PLAN (SSPP)</b>	<b>281</b>
IAO-03.1: SYSTEM SECURITY & PRIVACY PLAN (SSPP)   PLAN/COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES	283
IAO-03.2: SYSTEM SECURITY & PRIVACY PLAN (SSPP)   ADEQUATE SECURITY FOR SENSITIVE / REGULATED DATA IN SUPPORT OF CONTRACTS	283
<b>IAO-04: THREAT ANALYSIS &amp; FLAW REMEDIATION DURING DEVELOPMENT</b>	<b>284</b>
<b>IAO-05: PLAN OF ACTION &amp; MILESTONES (POA&amp;M)</b>	<b>286</b>

IAO-05.1: PLAN OF ACTION & MILESTONES (POA&M)   POA&M AUTOMATION	286
IAO-06: TECHNICAL VERIFICATION	286
IAO-07: SECURITY AUTHORIZATION	286
<b>MAINTENANCE (MNT) POLICY &amp; STANDARDS</b>	<b>288</b>
<b>MNT-01: MAINTENANCE OPERATIONS</b>	<b>288</b>
<b>MNT-02: CONTROLLED MAINTENANCE</b>	<b>288</b>
MNT-02.1: CONTROLLED MAINTENANCE   AUTOMATED MAINTENANCE ACTIVITIES	289
<b>MNT-03: TIMELY MAINTENANCE</b>	<b>289</b>
MNT-03.1: TIMELY MAINTENANCE   PREVENTATIVE MAINTENANCE	289
MNT-03.2: TIMELY MAINTENANCE   PREDICTIVE MAINTENANCE	289
MNT-03.3: TIMELY MAINTENANCE   AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE	290
<b>MNT-04: MAINTENANCE TOOLS</b>	<b>290</b>
MNT-04.1: MAINTENANCE TOOLS   INSPECT TOOLS	290
MNT-04.2: MAINTENANCE TOOLS   INSPECT MEDIA	291
MNT-04.3: MAINTENANCE TOOLS   PREVENT UNAUTHORIZED REMOVAL	291
MNT-04.4: MAINTENANCE TOOLS   RESTRICT TOOL USE	291
<b>MNT-05: REMOTE MAINTENANCE</b>	<b>291</b>
MNT-05.1: REMOTE MAINTENANCE   AUDITING REMOTE MAINTENANCE	292
MNT-05.2: REMOTE MAINTENANCE   REMOTE MAINTENANCE NOTIFICATIONS	292
MNT-05.3: REMOTE MAINTENANCE   REMOTE MAINTENANCE CRYPTOGRAPHIC PROTECTION	292
MNT-05.4: REMOTE MAINTENANCE   REMOTE MAINTENANCE DISCONNECT VERIFICATION	292
MNT-05.5: REMOTE MAINTENANCE   REMOTE MAINTENANCE PRE-APPROVAL	293
MNT-05.6: REMOTE MAINTENANCE   REMOTE MAINTENANCE COMPARABLE SECURITY & SANITIZATION	293
MNT-05.7: REMOTE MAINTENANCE   SEPARATION OF MAINTENANCE SESSIONS	293
<b>MNT-06: MAINTENANCE PERSONNEL</b>	<b>293</b>
MNT-06.1: MAINTENANCE PERSONNEL   MAINTENANCE PERSONNEL WITHOUT APPROPRIATE ACCESS	294
MNT-06.2: MAINTENANCE PERSONNEL   NON-SYSTEM RELATED MAINTENANCE	294
<b>MNT-07: MAINTAIN CONFIGURATION CONTROL DURING MAINTENANCE</b>	<b>294</b>
<b>MNT-08: FIELD MAINTENANCE</b>	<b>295</b>
<b>MNT-09: OFF-SITE MAINTENANCE</b>	<b>295</b>
<b>MNT-10: MAINTENANCE VALIDATION</b>	<b>295</b>
<b>MNT-11: MAINTENANCE MONITORING</b>	<b>295</b>
<b>MOBILE DEVICE MANAGEMENT (MDM) POLICY &amp; STANDARDS</b>	<b>296</b>
<b>MDM-01: CENTRALIZED MANAGEMENT OF MOBILE DEVICES</b>	<b>296</b>
<b>MDM-02: ACCESS CONTROL FOR MOBILE DEVICES</b>	<b>296</b>
<b>MDM-03: FULL DEVICE &amp; CONTAINER-BASED ENCRYPTION</b>	<b>297</b>
<b>MDM-04: TAMPER PROTECTION &amp; DETECTION</b>	<b>297</b>
<b>MDM-05: REMOTE PURGING</b>	<b>298</b>
<b>MDM-06: PERSONALLY-OWNED MOBILE DEVICES</b>	<b>298</b>
<b>MDM-07: ORGANIZATION-OWNED MOBILE DEVICES</b>	<b>299</b>
<b>MDM-08: MOBILE DEVICE DATA RETENTION LIMITATIONS</b>	<b>299</b>
<b>MDM-09: MOBILE DEVICE GEOFENCING</b>	<b>299</b>
<b>MDM-10: SEPARATE MOBILE DEVICE PROFILES</b>	<b>299</b>
<b>MDM-11: RESTRICTING ACCESS TO AUTHORIZED DEVICES</b>	<b>299</b>
<b>NETWORK SECURITY (NET) POLICY &amp; STANDARDS</b>	<b>301</b>
<b>NET-01: NETWORK SECURITY CONTROLS (NSC)</b>	<b>301</b>
NET-01.1: NETWORK SECURITY CONTROLS (NSC)   ZERO TRUST ARCHITECTURE (ZTA)	301
<b>NET-02: LAYERED DEFENSES</b>	<b>301</b>
NET-02.1: LAYERED DEFENSES   DENIAL OF SERVICE (DOS) PROTECTION	302
NET-02.2: LAYERED DEFENSES   GUEST NETWORKS	302
NET-02.3: LAYERED DEFENSES   CROSS DOMAIN SOLUTIONS (CDS)	302
<b>NET-03: BOUNDARY PROTECTION</b>	<b>303</b>
NET-03.1: BOUNDARY PROTECTION   LIMIT NETWORK CONNECTIONS	304
NET-03.2: BOUNDARY PROTECTION   EXTERNAL TELECOMMUNICATIONS SERVICES	304
NET-03.3: BOUNDARY PROTECTION   PREVENT DISCOVERY OF INTERNAL INFORMATION	304
NET-03.4: BOUNDARY PROTECTION   PERSONAL DATA (PD)	305
NET-03.5: BOUNDARY PROTECTION   PREVENT UNAUTHORIZED EXFILTRATION	305

NET-03.6: BOUNDARY PROTECTION   DYNAMIC ISOLATION & SEGREGATION (SANDBOXING)	305
NET-03.7: BOUNDARY PROTECTION   ISOLATION OF INFORMATION SYSTEM COMPONENTS	306
NET-03.8: BOUNDARY PROTECTION   SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	306
<b>NET-04: DATA FLOW ENFORCEMENT – ACCESS CONTROL LISTS (ACLs)</b>	<b>306</b>
NET-04.1: DATA FLOW ENFORCEMENT   DENY TRAFFIC BY DEFAULT & ALLOW TRAFFIC BY EXCEPTION	307
NET-04.2: DATA FLOW ENFORCEMENT   OBJECT SECURITY ATTRIBUTES	307
NET-04.3: DATA FLOW ENFORCEMENT   CONTENT CHECK FOR ENCRYPTED DATA	308
NET-04.4: DATA FLOW ENFORCEMENT   EMBEDDED DATA TYPES	308
NET-04.5: DATA FLOW ENFORCEMENT   METADATA	308
NET-04.6: DATA FLOW ENFORCEMENT   HUMAN REVIEWS	308
NET-04.7: DATA FLOW ENFORCEMENT   SECURITY POLICY FILTERS	309
NET-04.8: DATA FLOW ENFORCEMENT   DATA TYPE IDENTIFIERS	309
NET-04.9: DATA FLOW ENFORCEMENT   DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS	309
NET-04.10: DATA FLOW ENFORCEMENT   DETECTION OF UNSANCTIONED INFORMATION	310
NET-04.11: DATA FLOW ENFORCEMENT   APPROVED SOLUTIONS	310
NET-04.12: DATA FLOW ENFORCEMENT   CROSS DOMAIN AUTHENTICATION	310
NET-04.13: DATA FLOW ENFORCEMENT   METADATA VALIDATION	311
<b>NET-05: SYSTEM INTERCONNECTIONS</b>	<b>311</b>
NET-05.1: SYSTEM INTERCONNECTIONS   EXTERNAL SYSTEM CONNECTIONS	312
NET-05.2: SYSTEM INTERCONNECTIONS   INTERNAL SYSTEM CONNECTIONS	312
<b>NET-06: NETWORK SEGMENTATION</b>	<b>313</b>
NET-06.1: NETWORK SEGMENTATION   SECURITY MANAGEMENT SUBNETS	313
NET-06.2: NETWORK SEGMENTATION   VIRTUAL LOCAL AREA NETWORK (VLAN) SEPARATION	314
NET-06.3: NETWORK SEGMENTATION   SENSITIVE / REGULATED DATA ENCLAVE (SECURE ZONE)	314
NET-06.4: NETWORK SEGMENTATION   SEGREGATION FROM ENTERPRISE SERVICES	314
NET-06.5: NETWORK SEGMENTATION   DIRECT INTERNET ACCESS RESTRICTIONS	314
<b>NET-07: REMOTE SESSION TERMINATION</b>	<b>315</b>
<b>NET-08: NETWORK INTRUSION DETECTION &amp; PREVENTION SYSTEMS (NIDS/NIPS)</b>	<b>315</b>
NET-08.1: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)   DMZ NETWORKS	315
NET-08.2: NETWORK INTRUSION DETECTION & PREVENTION SYSTEMS (NIDS/NIPS)   WIRELESS INTRUSION DETECTION/PREVENTION SYSTEMS (WIDS/WIPS)	316
<b>NET-09: SESSION INTEGRITY</b>	<b>316</b>
NET-09.1: SESSION INTEGRITY   INVALIDATE SESSION IDENTIFIERS AT LOGOUT	316
NET-09.2: SESSION INTEGRITY   UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	316
<b>NET-10 DOMAIN NAME SERVICE (DNS) RESOLUTION</b>	<b>316</b>
NET-10.1: DOMAIN NAME SERVICE (DNS) RESOLUTION   ARCHITECTURE & PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	317
NET-10.2: DOMAIN NAME SERVICE (DNS) RESOLUTION   SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	317
NET-10.3: DOMAIN NAME SERVICE (DNS) RESOLUTION   SENDER POLICY FRAMEWORK (SPF)	318
NET-10.4: DOMAIN NAME SERVICE (DNS) RESOLUTION   DOMAIN REGISTRAR SECURITY	318
<b>NET-11: OUT-OF-BAND CHANNELS</b>	<b>318</b>
<b>NET-12: SAFEGUARDING DATA OVER OPEN NETWORKS</b>	<b>318</b>
NET-12.1: SAFEGUARDING DATA OVER OPEN NETWORKS   WIRELESS LINK PROTECTION	319
NET-12.2: SAFEGUARDING DATA OVER OPEN NETWORKS   END-USER MESSAGING TECHNOLOGIES	319
<b>NET-13: ELECTRONIC MESSAGING</b>	<b>320</b>
<b>NET-14: REMOTE ACCESS</b>	<b>320</b>
NET-14.1: REMOTE ACCESS   AUTOMATED MONITORING & CONTROL	321
NET-14.2: REMOTE ACCESS   PROTECTION OF CONFIDENTIALITY/INTEGRITY USING ENCRYPTION	321
NET-14.3: REMOTE ACCESS   MANAGED ACCESS CONTROL POINTS	321
NET-14.4: REMOTE ACCESS   PRIVILEGED COMMANDS & ACCESS	321
NET-14.5: REMOTE ACCESS   WORK FROM ANYWHERE (WFA) – TELECOMMUTING SECURITY	321
NET-14.6: REMOTE ACCESS   THIRD-PARTY REMOTE ACCESS GOVERNANCE	322
NET-14.7: REMOTE ACCESS   ENDPOINT SECURITY VALIDATION	322
NET-14.8: REMOTE ACCESS   EXPEDITIOUS DISCONNECT/DISABLE CAPABILITY	322
<b>NET-15: WIRELESS NETWORKING</b>	<b>323</b>
NET-15.1: WIRELESS ACCESS   AUTHENTICATION & ENCRYPTION	323
NET-15.2: WIRELESS ACCESS   DISABLE WIRELESS NETWORKING	324



NET-15.3: WIRELESS ACCESS   RESTRICT CONFIGURATION BY USERS	324
NET-15.4: WIRELESS ACCESS   WIRELESS BOUNDARIES	324
NET-15.5: WIRELESS ACCESS   ROGUE WIRELESS DETECTION	324
<b>NET-16: INTRANETS</b>	<b>325</b>
<b>NET-17: DATA LOSS PREVENTION (DLP)</b>	<b>325</b>
<b>NET-18: DNS &amp; CONTENT FILTERING</b>	<b>325</b>
NET-18.1: DNS & CONTENT FILTERING   ROUTE TRAFFIC TO PROXY SERVERS	326
NET-18.2: DNS & CONTENT FILTERING   VISIBILITY OF ENCRYPTED COMMUNICATIONS	326
NET-18.3: DNS & CONTENT FILTERING   ROUTE PRIVILEGED NETWORK ACCESS	326
<b>PHYSICAL &amp; ENVIRONMENTAL SECURITY (PES) POLICY &amp; STANDARDS</b>	<b>327</b>
<b>PES-01: PHYSICAL &amp; ENVIRONMENTAL PROTECTIONS</b>	<b>327</b>
PES-01.1: PHYSICAL & ENVIRONMENTAL PROTECTIONS   SITE SECURITY PLAN (SITEPLAN)	327
<b>PES-02: PHYSICAL ACCESS AUTHORIZATIONS</b>	<b>327</b>
PES-02.1: PHYSICAL ACCESS AUTHORIZATIONS   ROLE-BASED PHYSICAL ACCESS	328
PES-02.2: PHYSICAL ACCESS AUTHORIZATIONS   DUAL AUTHORIZATION FOR PHYSICAL ACCESS	328
<b>PES-03: PHYSICAL ACCESS CONTROL</b>	<b>329</b>
PES-03.1: PHYSICAL ACCESS CONTROL   CONTROLLED INGRESS & EGRESS POINTS	330
PES-03.2: PHYSICAL ACCESS CONTROL   LOCKABLE PHYSICAL CASINGS	330
PES-03.3: PHYSICAL ACCESS CONTROL   PHYSICAL ACCESS LOGS	330
PES-03.4: PHYSICAL ACCESS CONTROL   ACCESS TO INFORMATION SYSTEMS	331
<b>PES-04: PHYSICAL SECURITY OF OFFICES, ROOMS &amp; FACILITIES</b>	<b>331</b>
PES-04.1: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES   WORKING IN SECURE AREAS	332
PES-04.2: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES   SEARCHES	332
PES-04.3: PHYSICAL SECURITY OF OFFICES, ROOMS & FACILITIES   TEMPORARY STORAGE	332
<b>PES-05: MONITORING PHYSICAL ACCESS</b>	<b>333</b>
PES-05.1: MONITORING PHYSICAL ACCESS   INTRUSION ALARMS/SURVEILLANCE EQUIPMENT	333
PES-05.2: MONITORING PHYSICAL ACCESS   MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS	333
<b>PES-06: VISITOR CONTROL</b>	<b>334</b>
PES-06.1: VISITOR CONTROL   DISTINGUISH VISITORS FROM ON-SITE PERSONNEL	334
PES-06.2: VISITOR CONTROL   IDENTIFICATION REQUIREMENT	334
PES-06.3: VISITOR CONTROL   RESTRICT UNESCORTED ACCESS	335
PES-06.4: VISITOR CONTROL   AUTOMATED RECORDS MANAGEMENT & REVIEW	335
PES-06.5: VISITOR CONTROL   MINIMIZE VISITOR PERSONAL DATA (PD)	335
PES-06.6: VISITOR CONTROL   VISITOR ACCESS REVOCATION	335
<b>PES-07: SUPPORTING UTILITIES</b>	<b>336</b>
PES-07.1: SUPPORTING UTILITIES   AUTOMATIC VOLTAGE CONTROLS	336
PES-07.2: SUPPORTING UTILITIES   EMERGENCY SHUTOFF	336
PES-07.3: SUPPORTING UTILITIES   EMERGENCY POWER	336
PES-07.4: SUPPORTING UTILITIES   EMERGENCY LIGHTING	337
PES-07.5: SUPPORTING UTILITIES   WATER DAMAGE PROTECTION	337
PES-07.6: SUPPORTING UTILITIES   AUTOMATION SUPPORT FOR WATER DAMAGE PROTECTION	337
PES-07.7: SUPPORTING UTILITIES   REDUNDANT CABLING	337
<b>PES-08: FIRE PROTECTION</b>	<b>337</b>
PES-08.1: FIRE PROTECTION   FIRE DETECTION DEVICES	338
PES-08.2: FIRE PROTECTION   FIRE SUPPRESSION DEVICES	338
PES-08.3: FIRE PROTECTION   AUTOMATIC FIRE SUPPRESSION	338
<b>PES-09: TEMPERATURE &amp; HUMIDITY CONTROLS</b>	<b>338</b>
PES-09.1: TEMPERATURE & HUMIDITY CONTROLS   MONITORING WITH ALARMS/NOTIFICATIONS	338
<b>PES-10: DELIVERY &amp; REMOVAL</b>	<b>339</b>
<b>PES-11: ALTERNATE WORK SITE</b>	<b>339</b>
<b>PES-12: EQUIPMENT SITING &amp; PROTECTION</b>	<b>340</b>
PES-12.1: EQUIPMENT SITING & PROTECTION   TRANSMISSION MEDIUM SECURITY	340
PES-12.2: EQUIPMENT SITING & PROTECTION   ACCESS CONTROL FOR OUTPUT DEVICES	340
<b>PES-13: INFORMATION LEAKAGE DUE TO ELECTROMAGNETIC SIGNALS EMANATIONS</b>	<b>341</b>
<b>PES-14: ASSET MONITORING AND TRACKING</b>	<b>341</b>
<b>PES-15: ELECTROMAGNETIC PULSE (EMP) PROTECTION</b>	<b>341</b>
<b>PES-16: COMPONENT MARKING</b>	<b>342</b>
<b>PES-17: PROXIMITY SENSOR</b>	<b>342</b>



**DATA PRIVACY (PRI) POLICY & STANDARDS**

<b>PRI-01: DATA PRIVACY PROGRAM</b>	<b>343</b>
<i>PRI-01.1: DATA PRIVACY PROGRAM   CHIEF PRIVACY OFFICER (CPO)</i>	343
<i>PRI-01.2: DATA PRIVACY PROGRAM   PRIVACY ACT STATEMENTS</i>	343
<i>PRI-01.3: DATA PRIVACY PROGRAM   DISSEMINATION OF PRIVACY PROGRAM INFORMATION</i>	344
<i>PRI-01.4: DATA PRIVACY PROGRAM   DATA PROTECTION OFFICER (DPO)</i>	344
<i>PRI-01.5: DATA PRIVACY PROGRAM   BINDING CORPORATE RULES (BCR)</i>	344
<i>PRI-01.6: DATA PRIVACY PROGRAM   SECURITY OF PERSONAL DATA</i>	344
<i>PRI-01.7: DATA PRIVACY PROGRAM   LIMITING PERSONAL DATA DISCLOSURES</i>	344
<b>PRI-02: DATA PRIVACY NOTICE</b>	<b>345</b>
<i>PRI-02.1: DATA PRIVACY NOTICE   PURPOSE SPECIFICATION</i>	345
<i>PRI-02.2: DATA PRIVACY NOTICE   AUTOMATED DATA MANAGEMENT PROCESSES</i>	345
<i>PRI-02.3: DATA PRIVACY NOTICE   COMPUTER MATCHING AGREEMENTS (CMA)</i>	346
<i>PRI-02.4: DATA PRIVACY NOTICE   SYSTEM OF RECORDS NOTICE (SORN)</i>	346
<i>PRI-02.5: DATA PRIVACY NOTICE   SYSTEM OF RECORDS NOTICE (SORN) REVIEW PROCESS</i>	346
<i>PRI-02.6: DATA PRIVACY NOTICE   PRIVACY ACT EXEMPTIONS</i>	346
<i>PRI-02.7: DATA PRIVACY NOTICE   REAL-TIME OR LAYERED NOTICE</i>	347
<b>PRI-03: CHOICE &amp; CONSENT</b>	<b>347</b>
<i>PRI-03.1: CHOICE &amp; CONSENT   TAILORED CONSENT</i>	347
<i>PRI-03.2: CHOICE &amp; CONSENT   JUST-IN-TIME NOTICE &amp; UPDATED CONSENT</i>	347
<i>PRI-03.3: CHOICE &amp; CONSENT   PROHIBITION OF SELLING OR SHARING PERSONAL DATA (PD)</i>	348
<i>PRI-03.4: CHOICE &amp; CONSENT   REVOKE CONSENT</i>	348
<i>PRI-03.5: CHOICE &amp; CONSENT   PRODUCT OR SERVICE DELIVERY RESTRICTIONS</i>	348
<i>PRI-03.6: CHOICE &amp; CONSENT   AUTHORIZED AGENT</i>	348
<i>PRI-03.7: CHOICE &amp; CONSENT   ACTIVE PARTICIPATION BY DATA SUBJECTS</i>	348
<i>PRI-03.8: CHOICE &amp; CONSENT   GLOBAL PRIVACY CONTROL (GPC)</i>	349
<b>PRI-04: RESTRICT COLLECTION TO IDENTIFIED PURPOSE</b>	<b>349</b>
<i>PRI-04.1: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   AUTHORITY TO COLLECT, USE, MAINTAIN &amp; SHARE PERSONAL DATA (PD)</i>	349
<i>PRI-04.2: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   PRIMARY SOURCES</i>	349
<i>PRI-04.3: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   IDENTIFIABLE IMAGE COLLECTION</i>	349
<i>PRI-04.4: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   ACQUIRED PERSONAL DATA</i>	350
<i>PRI-04.5: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   VALIDATE COLLECTED PERSONAL DATA</i>	350
<i>PRI-04.6: RESTRICT COLLECTION TO IDENTIFIED PURPOSE   RE-VALIDATE COLLECTED PERSONAL DATA</i>	350
<b>PRI-05: PERSONAL DATA RETENTION &amp; DISPOSAL</b>	<b>350</b>
<i>PRI-05.1: PERSONAL DATA RETENTION &amp; DISPOSAL   INTERNAL USE OF PERSONAL DATA FOR TESTING, TRAINING AND RESEARCH</i>	350
<i>PRI-05.2: PERSONAL DATA RETENTION &amp; DISPOSAL   PERSONAL DATA ACCURACY &amp; INTEGRITY</i>	351
<i>PRI-05.3: PERSONAL DATA RETENTION &amp; DISPOSAL   DATA MASKING</i>	351
<i>PRI-05.4: PERSONAL DATA RETENTION &amp; DISPOSAL   USAGE RESTRICTIONS OF SENSITIVE PERSONAL DATA</i>	351
<i>PRI-05.5: PERSONAL DATA RETENTION &amp; DISPOSAL   INVENTORY OF PERSONAL DATA</i>	351
<i>PRI-05.6: PERSONAL DATA RETENTION &amp; DISPOSAL   PERSONAL DATA INVENTORY AUTOMATION SUPPORT</i>	352
<i>PRI-05.7: PERSONAL DATA RETENTION &amp; DISPOSAL   PERSONAL DATA CATEGORIES</i>	352
<b>PRI-06: DATA SUBJECT ACCESS</b>	<b>352</b>
<i>PRI-06.1: DATA SUBJECT ACCESS   CORRECTING INACCURATE PERSONAL DATA</i>	352
<i>PRI-06.2: DATA SUBJECT ACCESS   NOTICE OF CORRECTION OR PROCESSING CHANGE</i>	353
<i>PRI-06.3: DATA SUBJECT ACCESS   APPEAL ADVERSE DECISION</i>	353
<i>PRI-06.4: DATA SUBJECT ACCESS   USER FEEDBACK MANAGEMENT</i>	353
<i>PRI-06.5: DATA SUBJECT ACCESS   RIGHT TO ERASURE</i>	353
<i>PRI-06.6: DATA SUBJECT ACCESS   DATA PORTABILITY</i>	354
<i>PRI-06.7: DATA SUBJECT ACCESS   PERSONAL DATA EXPORTABILITY</i>	354
<b>PRI-07: INFORMATION SHARING WITH THIRD PARTIES</b>	<b>354</b>
<i>PRI-07.1: INFORMATION SHARING WITH THIRD PARTIES   PRIVACY REQUIREMENTS FOR CONTRACTORS &amp; SERVICE PROVIDERS</i>	354
<i>PRI-07.2: INFORMATION SHARING WITH THIRD PARTIES   JOINT PROCESSING OF PERSONAL DATA</i>	355
<i>PRI-07.3: INFORMATION SHARING WITH THIRD PARTIES   OBLIGATION TO INFORM THIRD PARTIES</i>	355
<i>PRI-07.4: INFORMATION SHARING WITH THIRD PARTIES   REJECT UNAUTHORIZED DISCLOSURE REQUESTS</i>	355
<b>PRI-08: TESTING, TRAINING &amp; MONITORING</b>	<b>355</b>

<b>PRI-09: PERSONAL DATA LINEAGE</b>	<b>356</b>
<b>PRI-10: DATA QUALITY MANAGEMENT</b>	<b>356</b>
<i>PRI-10.1: DATA QUALITY MANAGEMENT   AUTOMATION</i>	356
<i>PRI-10.2: DATA QUALITY MANAGEMENT   DATA ANALYTICS BIAS</i>	357
<b>PRI-11: DATA TAGGING</b>	<b>357</b>
<b>PRI-12: UPDATING PERSONAL DATA</b>	<b>357</b>
<b>PRI-13: DATA MANAGEMENT BOARD</b>	<b>357</b>
<b>PRI-14: DATA PRIVACY RECORDS &amp; REPORTING</b>	<b>358</b>
<i>PRI-14.1: DATA PRIVACY RECORDS &amp; REPORTING   ACCOUNTING OF DISCLOSURES</i>	358
<i>PRI-14.2: DATA PRIVACY RECORDS &amp; REPORTING   NOTIFICATION OF DISCLOSURE REQUEST TO DATA SUBJECT</i>	358
<b>PRI-15: REGISTER AS A DATA CONTROLLER AND/OR DATA PROCESSOR</b>	<b>359</b>
<b>PRI-16: POTENTIAL HUMAN RIGHTS ABUSES</b>	<b>359</b>
<b>PRI-17: DATA SUBJECT COMMUNICATIONS</b>	<b>359</b>
<i>PRI-17.1: DATA SUBJECT COMMUNICATIONS   CONSPICUOUS LINK TO PRIVACY NOTICE</i>	360
<i>PRI-17.2: DATA SUBJECT COMMUNICATIONS   NOTICE OF FINANCIAL INCENTIVE</i>	360
<b>PROJECT &amp; RESOURCE MANAGEMENT (PRM) POLICY &amp; STANDARDS</b>	<b>361</b>
<b>PRM-01: CYBERSECURITY &amp; DATA PRIVACY PORTFOLIO MANAGEMENT</b>	<b>361</b>
<i>PRM-01.1: CYBERSECURITY &amp; DATA PRIVACY PORTFOLIO MANAGEMENT   STRATEGIC PLAN &amp; OBJECTIVES</i>	361
<i>PRM-01.2: CYBERSECURITY &amp; DATA PRIVACY PORTFOLIO MANAGEMENT   TARGETED CAPABILITY MATURITY LEVELS</i>	361
<b>PRM-02: CYBERSECURITY &amp; DATA PRIVACY RESOURCE MANAGEMENT</b>	<b>362</b>
<b>PRM-03: ALLOCATION OF RESOURCES</b>	<b>362</b>
<b>PRM-04: CYBERSECURITY &amp; DATA PRIVACY IN PROJECT MANAGEMENT</b>	<b>362</b>
<b>PRM-05: CYBERSECURITY &amp; DATA PRIVACY REQUIREMENTS DEFINITION</b>	<b>362</b>
<b>PRM-06: BUSINESS PROCESS DEFINITION</b>	<b>363</b>
<b>PRM-07: SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) MANAGEMENT</b>	<b>363</b>
<b>PRM-08: MANAGE ORGANIZATIONAL KNOWLEDGE</b>	<b>363</b>
<b>RISK MANAGEMENT (RSK) POLICY &amp; STANDARDS</b>	<b>365</b>
<b>RSK-01: RISK MANAGEMENT PROGRAM (RMP)</b>	<b>365</b>
<i>RSK-01.1: RISK MANAGEMENT PROGRAM (RMP)   RISK FRAMING</i>	365
<i>RSK-01.2: RISK MANAGEMENT PROGRAM (RMP)   RISK MANAGEMENT RESOURCING</i>	366
<i>RSK-01.3: RISK MANAGEMENT PROGRAM (RMP)   RISK TOLERANCE</i>	366
<i>RSK-01.4: RISK MANAGEMENT PROGRAM (RMP)   RISK THRESHOLD</i>	367
<i>RSK-01.5: RISK MANAGEMENT PROGRAM (RMP)   RISK APPETITE</i>	367
<b>RSK-02: RISK-BASED SECURITY CATEGORIZATION</b>	<b>368</b>
<i>RSK-02.1: RISK-BASED SECURITY CATEGORIZATION   IMPACT-LEVEL PRIORITIZATION</i>	368
<b>RSK-03: RISK IDENTIFICATION</b>	<b>368</b>
<i>RSK-03.1: RISK IDENTIFICATION   RISK CATALOG</i>	369
<b>RSK-04: RISK ASSESSMENT</b>	<b>369</b>
<i>RSK-04.1: RISK ASSESSMENT   RISK REGISTER</i>	370
<b>RSK-05: RISK RANKING</b>	<b>370</b>
<b>RSK-06: RISK REMEDIATION</b>	<b>370</b>
<i>RSK-06.1: RISK REMEDIATION   RISK RESPONSE</i>	371
<i>RSK-06.2: RISK REMEDIATION   COMPENSATING COUNTERMEASURES</i>	371
<b>RSK-07: RISK ASSESSMENT UPDATE</b>	<b>372</b>
<b>RSK-08: BUSINESS IMPACT ANALYSIS (BIA)</b>	<b>372</b>
<b>RSK-09: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM</b>	<b>372</b>
<i>RSK-09.1: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM   SUPPLY CHAIN RISK ASSESSMENT</i>	373
<i>RSK-09.2: SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROGRAM   AI &amp; AUTONOMOUS TECHNOLOGIES SUPPLY CHAIN IMPACTS</i>	374
<b>RSK-10: DATA PROTECTION IMPACT ASSESSMENT (DPIA)</b>	<b>374</b>
<b>RSK-11: RISK MONITORING</b>	<b>375</b>
<b>RSK-12: RISK CULTURE</b>	<b>375</b>
<b>SECURE ENGINEERING &amp; ARCHITECTURE (SEA) POLICY &amp; STANDARDS</b>	<b>376</b>
<b>SEA-01: SECURE ENGINEERING PRINCIPLES</b>	<b>376</b>
<i>SEA-01.1: SECURE ENGINEERING PRINCIPLES   CENTRALIZED MANAGEMENT OF CYBERSECURITY &amp; DATA PRIVACY CONTROLS</i>	377
<i>SEA-01.2: SECURE ENGINEERING PRINCIPLES   ACHIEVING RESILIENCE REQUIREMENTS</i>	377
<b>SEA-02: ALIGNMENT WITH ENTERPRISE ARCHITECTURE</b>	<b>377</b>

SEA-02.1: ALIGNMENT WITH ENTERPRISE ARCHITECTURE   STANDARDIZED TERMINOLOGY	378
SEA-02.2: ALIGNMENT WITH ENTERPRISE ARCHITECTURE   OUTSOURCING NON-ESSENTIAL FUNCTIONS OR SERVICES	378
SEA-02.3: ALIGNMENT WITH ENTERPRISE ARCHITECTURE   TECHNICAL DEBT REVIEWS	379
<b>SEA-03: DEFENSE-IN-DEPTH (DiD) ARCHITECTURE</b>	<b>379</b>
SEA-03.1: DEFENSE-IN-DEPTH (DiD) ARCHITECTURE   SYSTEM PARTITIONING	379
SEA-03.2: DEFENSE-IN-DEPTH (DiD) ARCHITECTURE   APPLICATION PARTITIONING	380
<b>SEA-04: PROCESS ISOLATION</b>	<b>380</b>
SEA-04.1: PROCESS ISOLATION   SECURITY FUNCTION ISOLATION	380
SEA-04.2: PROCESS ISOLATION   HARDWARE SEPARATION	381
SEA-04.3: PROCESS ISOLATION   THREAD SEPARATION	381
<b>SEA-05: INFORMATION IN SHARED RESOURCES</b>	<b>382</b>
<b>SEA-06: PREVENT PROGRAM EXECUTION</b>	<b>382</b>
<b>SEA-07: PREDICTABLE FAILURE ANALYSIS</b>	<b>382</b>
SEA-07.1: PREDICTABLE FAILURE ANALYSIS   TECHNOLOGY LIFECYCLE MANAGEMENT	382
SEA-07.2: PREDICTABLE FAILURE ANALYSIS   FAIL SECURE	383
SEA-07.3: PREDICTABLE FAILURE ANALYSIS   FAIL SAFE	383
<b>SEA-08: NON-PERSISTENCE</b>	<b>384</b>
SEA-08.1: NON-PERSISTENCE   REFRESH FROM TRUSTED SOURCES	384
<b>SEA-09: INFORMATION OUTPUT FILTERING</b>	<b>384</b>
SEA-09.1: INFORMATION OUTPUT FILTERING   LIMIT PERSONAL DATA (PD) DISSEMINATION	384
<b>SEA-10: MEMORY PROTECTION</b>	<b>385</b>
<b>SEA-11: HONEYPOTS</b>	<b>385</b>
<b>SEA-12: HONEYCLIENTS</b>	<b>385</b>
<b>SEA-13: HETEROGENEITY</b>	<b>386</b>
SEA-13.1: HETEROGENEITY   VIRTUALIZATION TECHNIQUES	386
<b>SEA-14: CONCEALMENT &amp; MISDIRECTION</b>	<b>386</b>
SEA-14.1: CONCEALMENT & MISDIRECTION   RANDOMNESS	386
SEA-14.2: CONCEALMENT & MISDIRECTION   CHANGE PROCESSING & STORAGE LOCATIONS	387
<b>SEA-15: DISTRIBUTED PROCESSING &amp; STORAGE</b>	<b>387</b>
<b>SEA-16: NON-MODIFIABLE EXECUTABLE PROGRAMS</b>	<b>387</b>
<b>SEA-17: SECURE LOG-ON PROCEDURES</b>	<b>388</b>
<b>SEA-18: SYSTEM USE NOTIFICATION (LOGON BANNER)</b>	<b>388</b>
SEA-18.1: SYSTEM USE NOTIFICATION   STANDARDIZED MICROSOFT WINDOWS BANNER	388
SEA-18.2: SYSTEM USE NOTIFICATION   TRUNCATED BANNER	388
<b>SEA-19: PREVIOUS LOGON NOTIFICATION</b>	<b>389</b>
<b>SEA-20: CLOCK SYNCHRONIZATION</b>	<b>389</b>
<b>SECURITY OPERATIONS (OPS) POLICY &amp; STANDARDS</b>	<b>390</b>
<b>OPS-01: OPERATIONS SECURITY</b>	<b>390</b>
OPS-01.1: OPERATIONS SECURITY   STANDARDIZED OPERATING PROCEDURES (SOP)	390
<b>OPS-02: SECURITY CONCEPT OF OPERATIONS (CONOPS)</b>	<b>391</b>
<b>OPS-03: SERVICE DELIVERY (BUSINESS PROCESS SUPPORT)</b>	<b>391</b>
<b>OPS-04: SECURITY OPERATIONS CENTER (SOC)</b>	<b>391</b>
<b>OPS-05: SECURE PRACTICES GUIDELINES</b>	<b>392</b>
<b>SECURITY AWARENESS &amp; TRAINING (SAT) POLICY &amp; STANDARDS</b>	<b>393</b>
<b>SAT-01: CYBERSECURITY &amp; DATA PRIVACY-MINDED WORKFORCE</b>	<b>393</b>
<b>SAT-02: CYBERSECURITY &amp; DATA PRIVACY AWARENESS TRAINING</b>	<b>394</b>
SAT-02.1: CYBERSECURITY & DATA PRIVACY AWARENESS TRAINING   SIMULATED CYBER ATTACK SCENARIO TRAINING	394
SAT-02.2: CYBERSECURITY & DATA PRIVACY AWARENESS TRAINING   SOCIAL ENGINEERING & MINING	395
<b>SAT-03: CYBERSECURITY &amp; DATA PRIVACY ROLE-BASED TRAINING</b>	<b>395</b>
SAT-03.1: CYBERSECURITY & DATA PRIVACY TRAINING   PRACTICAL EXERCISES	396
SAT-03.2: CYBERSECURITY & DATA PRIVACY TRAINING   SUSPICIOUS COMMUNICATIONS & ANOMALOUS SYSTEM BEHAVIOR	397
SAT-03.3: CYBERSECURITY & DATA PRIVACY TRAINING   SENSITIVE INFORMATION STORAGE, HANDLING & PROCESSING	397
SAT-03.4: CYBERSECURITY & DATA PRIVACY TRAINING   VENDOR SECURITY TRAINING	397
SAT-03.5: CYBERSECURITY & DATA PRIVACY TRAINING   PRIVILEGED USERS	397
SAT-03.6: CYBERSECURITY & DATA PRIVACY TRAINING   CYBER THREAT ENVIRONMENT	398
SAT-03.7: CYBERSECURITY & DATA PRIVACY TRAINING   CONTINUING PROFESSIONAL EDUCATION (CPE) - CYBERSECURITY & DATA PRIVACY PERSONNEL	398

SAT-03.8: CYBERSECURITY & DATA PRIVACY TRAINING   CONTINUING PROFESSIONAL EDUCATION (CPE) - DEVOPS PERSONNEL	398
<b>SAT-04: CYBERSECURITY &amp; DATA PRIVACY TRAINING RECORDS</b>	<b>398</b>
<b>TECHNOLOGY DEVELOPMENT &amp; ACQUISITION (TDA) POLICY &amp; STANDARDS</b>	<b>400</b>
<b>TDA-01: TECHNOLOGY DEVELOPMENT &amp; ACQUISITION</b>	<b>400</b>
TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION   PRODUCT MANAGEMENT	400
TDA-01.2: TECHNOLOGY DEVELOPMENT & ACQUISITION   INTEGRITY MECHANISMS FOR SOFTWARE/FIRMWARE UPDATES	401
TDA-01.3: TECHNOLOGY DEVELOPMENT & ACQUISITION   MALWARE TESTING PRIOR TO RELEASE	401
<b>TDA-02: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS</b>	<b>401</b>
TDA-02.1: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   PORTS, PROTOCOLS & SERVICES IN USE	402
TDA-02.2: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   INFORMATION ASSURANCE ENABLED PRODUCTS	402
TDA-02.3: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   DEVELOPMENT METHODS, TECHNIQUES & PROCESSES	402
TDA-02.4: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   PRE-ESTABLISHED SECURITY CONFIGURATIONS	403
TDA-02.5: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   IDENTIFICATION & JUSTIFICATION OF PORTS, PROTOCOLS & SERVICES	403
TDA-02.6: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   USE OF INSECURE PORTS, PROTOCOLS & SERVICES	403
TDA-02.7: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS   CYBERSECURITY & DATA PRIVACY REPRESENTATIVES FOR PRODUCT CHANGES	404
<b>TDA-03: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS</b>	<b>404</b>
TDA-03.1: COMMERCIAL OFF-THE-SHELF (COTS) SECURITY SOLUTIONS   SUPPLIER DIVERSITY	404
<b>TDA-04: DOCUMENTATION REQUIREMENTS</b>	<b>405</b>
TDA-04.1: DOCUMENTATION REQUIREMENTS   FUNCTIONAL PROPERTIES	405
TDA-04.2: DOCUMENTATION REQUIREMENTS   SOFTWARE BILL OF MATERIALS (SBOM)	406
<b>TDA-05: DEVELOPER ARCHITECTURE &amp; DESIGN</b>	<b>406</b>
TDA-05.1: DEVELOPER ARCHITECTURE & DESIGN   PHYSICAL DIAGNOSTIC & TEST INTERFACES	406
TDA-05.2: DEVELOPER ARCHITECTURE & DESIGN   DIAGNOSTIC & TEST INTERFACE MONITORING	407
<b>TDA-06: SECURE CODING</b>	<b>407</b>
TDA-06.1: SECURE CODING   CRITICALITY ANALYSIS	409
TDA-06.2: SECURE CODING   THREAT MODELING	409
TDA-06.3: SECURE CODING   SOFTWARE ASSURANCE MATURITY MODEL (SAMM)	409
TDA-06.4: SECURE CODING   SUPPORTING TOOLCHAIN	409
TDA-06.5: SECURE CODING   SOFTWARE DESIGN REVIEW	409
<b>TDA-07: SECURE DEVELOPMENT ENVIRONMENTS</b>	<b>410</b>
<b>TDA-08: SEPARATION OF DEVELOPMENT, TESTING &amp; OPERATIONAL ENVIRONMENTS</b>	<b>410</b>
TDA-08.1: SEPARATION OF DEVELOPMENT, TESTING & OPERATIONAL ENVIRONMENTS   SECURE MIGRATION PRACTICES	410
<b>TDA-09: CYBERSECURITY &amp; DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT</b>	<b>411</b>
TDA-09.1: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   CONTINUOUS MONITORING PLAN	411
TDA-09.2: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   STATIC CODE ANALYSIS	411
TDA-09.3: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   DYNAMIC CODE ANALYSIS	412
TDA-09.4: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   MALFORMED INPUT TESTING	412
TDA-09.5: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   APPLICATION PENETRATION TESTING	412
TDA-09.6: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   SECURE SETTINGS BY DEFAULT	413
TDA-09.7: CYBERSECURITY & DATA PRIVACY TESTING THROUGHOUT DEVELOPMENT   MANUAL CODE REVIEW	413
<b>TDA-10: USE OF LIVE DATA</b>	<b>413</b>
TDA-10.1: USE OF LIVE DATA   TEST DATA INTEGRITY	413
<b>TDA-11: PRODUCT TAMPERING AND COUNTERFEITING (PTC)</b>	<b>414</b>
TDA-11.1: PRODUCT TAMPERING AND COUNTERFEITING (PTC)   ANTI-COUNTERFEIT TRAINING	414
TDA-11.2: PRODUCT TAMPERING AND COUNTERFEITING (PTC)   COMPONENT DISPOSAL	414
<b>TDA-12: CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS</b>	<b>414</b>
<b>TDA-13: DEVELOPER SCREENING</b>	<b>414</b>
<b>TDA-14: DEVELOPER CONFIGURATION MANAGEMENT</b>	<b>415</b>
TDA-14.1: DEVELOPER CONFIGURATION MANAGEMENT   SOFTWARE/FIRMWARE INTEGRITY VERIFICATION	415
TDA-14.2: DEVELOPER CONFIGURATION MANAGEMENT   HARDWARE INTEGRITY VERIFICATION	415
<b>TDA-15: DEVELOPER THREAT ANALYSIS &amp; FLAW REMEDIATION</b>	<b>416</b>
<b>TDA-16: DEVELOPER-PROVIDED TRAINING</b>	<b>416</b>
<b>TDA-17: UNSUPPORTED SYSTEMS</b>	<b>416</b>



TDA-17.1: UNSUPPORTED SYSTEMS   ALTERNATE SOURCES FOR CONTINUED SUPPORT	417
<b>TDA-18: INPUT DATA VALIDATION</b>	<b>417</b>
<b>TDA-19: ERROR HANDLING</b>	<b>417</b>
<b>TDA-20: ACCESS TO PROGRAM SOURCE CODE</b>	<b>418</b>
TDA-20.1: ACCESS TO PROGRAM SOURCE CODE   SOFTWARE RELEASE INTEGRITY VERIFICATION	418
TDA-20.2: ACCESS TO PROGRAM SOURCE CODE   ARCHIVING SOFTWARE RELEASES	418
TDA-20.3: ACCESS TO PROGRAM SOURCE CODE   SOFTWARE ESCROW	418
<b>THIRD-PARTY MANAGEMENT (TPM) POLICY &amp; STANDARDS</b>	<b>419</b>
<b>TPM-01: THIRD-PARTY MANAGEMENT</b>	<b>419</b>
TPM-01.1: THIRD-PARTY MANAGEMENT   THIRD-PARTY INVENTORIES	419
<b>TPM-02: THIRD-PARTY CRITICALITY ASSESSMENTS</b>	<b>420</b>
<b>TPM-03: SUPPLY CHAIN PROTECTION</b>	<b>420</b>
TPM-03.1: SUPPLY CHAIN PROTECTION   ACQUISITION STRATEGIES, TOOLS & METHODS	420
TPM-03.2: SUPPLY CHAIN PROTECTION   LIMIT POTENTIAL HARM	421
TPM-03.3: SUPPLY CHAIN PROTECTION   PROCESSES TO ADDRESS WEAKNESSES OR DEFICIENCIES	421
TPM-03.4: SUPPLY CHAIN PROTECTION   ADEQUATE SUPPLY	421
<b>TPM-04: THIRD-PARTY SERVICES</b>	<b>421</b>
TPM-04.1: THIRD-PARTY SERVICES   THIRD-PARTY RISK ASSESSMENTS & APPROVALS	422
TPM-04.2: THIRD-PARTY SERVICES   EXTERNAL CONNECTIVITY REQUIREMENTS - IDENTIFICATION OF PORTS, PROTOCOLS & SERVICES	423
TPM-04.3: THIRD-PARTY SERVICES   CONFLICT OF INTERESTS	423
TPM-04.4: THIRD-PARTY SERVICES   THIRD-PARTY PROCESSING, STORAGE AND SERVICE LOCATIONS	423
<b>TPM-05: THIRD-PARTY CONTRACT REQUIREMENTS</b>	<b>424</b>
TPM-05.1: THIRD-PARTY CONTRACT REQUIREMENTS   SECURITY COMPROMISE NOTIFICATION AGREEMENTS	424
TPM-05.2: THIRD-PARTY CONTRACT REQUIREMENTS   CONTRACT FLOW-DOWN REQUIREMENTS	424
TPM-05.3: THIRD-PARTY CONTRACT REQUIREMENTS   THIRD-PARTY AUTHENTICATION PRACTICES	425
TPM-05.4: THIRD-PARTY CONTRACT REQUIREMENTS   RESPONSIBLE, ACCOUNTABLE, SUPPORTIVE, CONSULTED & INFORMED (RASCI) MATRIX	425
TPM-05.5: THIRD-PARTY CONTRACT REQUIREMENTS   THIRD-PARTY SCOPE REVIEW	425
TPM-05.6: THIRD-PARTY CONTRACT REQUIREMENTS   FIRST-PARTY DECLARATION (1PD)	426
TPM-05.7: THIRD-PARTY CONTRACT REQUIREMENTS   BREAK CLAUSES	426
<b>TPM-06: THIRD-PARTY PERSONNEL SECURITY</b>	<b>427</b>
<b>TPM-07: MONITORING FOR THIRD-PARTY INFORMATION DISCLOSURE</b>	<b>427</b>
<b>TPM-08: REVIEW OF THIRD-PARTY SERVICES</b>	<b>427</b>
<b>TPM-09: THIRD-PARTY DEFICIENCY REMEDIATION</b>	<b>428</b>
<b>TPM-10: MANAGING CHANGES TO THIRD-PARTY SERVICES</b>	<b>428</b>
<b>TPM-11: THIRD-PARTY INCIDENT RESPONSE &amp; RECOVERY CAPABILITIES</b>	<b>428</b>
<b>THREAT MANAGEMENT (THR) POLICY &amp; STANDARDS</b>	<b>429</b>
<b>THR-01: THREAT AWARENESS PROGRAM</b>	<b>429</b>
<b>THR-02: INDICATORS OF EXPOSURE (IOE)</b>	<b>429</b>
<b>THR-03: THREAT INTELLIGENCE FEEDS</b>	<b>429</b>
<b>THR-04: INSIDER THREAT PROGRAM</b>	<b>430</b>
<b>THR-05: INSIDER THREAT AWARENESS</b>	<b>430</b>
<b>THR-06: VULNERABILITY DISCLOSURE PROGRAM (VDP)</b>	<b>431</b>
<b>THR-07: THREAT HUNTING</b>	<b>431</b>
<b>THR-08: TAINTING</b>	<b>431</b>
<b>THR-09: THREAT CATALOG</b>	<b>432</b>
<b>THR-10: THREAT ANALYSIS</b>	<b>432</b>
<b>VULNERABILITY &amp; PATCH MANAGEMENT (VPM) POLICY &amp; STANDARDS</b>	<b>433</b>
<b>VPM-01: VULNERABILITY &amp; PATCH MANAGEMENT PROGRAM</b>	<b>433</b>
VPM-01.1: VULNERABILITY & PATCH MANAGEMENT PROGRAM   ATTACK SURFACE SCOPE	433
<b>VPM-02: VULNERABILITY REMEDIATION PROCESS</b>	<b>434</b>
<b>VPM-03: VULNERABILITY RANKING</b>	<b>434</b>
VPM-03.1: VULNERABILITY RANKING   VULNERABILITY EXPLOITATION ANALYSIS	434
<b>VPM-04: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES</b>	<b>435</b>
VPM-04.1: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES   STABLE VERSIONS	435
VPM-04.2: CONTINUOUS VULNERABILITY REMEDIATION ACTIVITIES   FLAW REMEDIATION WITH PERSONAL DATA (PD)	435



<b>VPM-05: SOFTWARE &amp; FIRMWARE PATCHING</b>	<b>436</b>
<i>VPM-05.1: SOFTWARE &amp; FIRMWARE PATCHING   CENTRALIZED MANAGEMENT OF FLAW REMEDIATION PROCESSES</i>	438
<i>VPM-05.2: SOFTWARE &amp; FIRMWARE PATCHING   AUTOMATED REMEDIATION STATUS</i>	439
<i>VPM-05.3: SOFTWARE &amp; FIRMWARE PATCHING   TIME TO REMEDIATE/BENCHMARKS FOR CORRECTIVE ACTION</i>	439
<i>VPM-05.4: SOFTWARE &amp; FIRMWARE PATCHING   AUTOMATED SOFTWARE &amp; FIRMWARE UPDATES</i>	439
<i>VPM-05.5: SOFTWARE &amp; FIRMWARE PATCHING   REMOVAL OF PREVIOUS VERSIONS</i>	439
<b>VPM-06: VULNERABILITY SCANNING</b>	<b>440</b>
<i>VPM-06.1: VULNERABILITY SCANNING   UPDATE TOOL CAPABILITY</i>	441
<i>VPM-06.2: VULNERABILITY SCANNING   BREADTH/DEPTH OF COVERAGE</i>	441
<i>VPM-06.3: VULNERABILITY SCANNING   PRIVILEGED ACCESS</i>	441
<i>VPM-06.4: VULNERABILITY SCANNING   TREND ANALYSIS</i>	441
<i>VPM-06.5: VULNERABILITY SCANNING   REVIEW HISTORICAL EVENT LOGS</i>	442
<i>VPM-06.6: VULNERABILITY SCANNING   EXTERNAL VULNERABILITY ASSESSMENT SCANS</i>	442
<i>VPM-06.7: VULNERABILITY SCANNING   INTERNAL VULNERABILITY ASSESSMENT SCANS</i>	442
<i>VPM-06.8: VULNERABILITY SCANNING   ACCEPTABLE DISCOVERABLE INFORMATION</i>	442
<i>VPM-06.9: VULNERABILITY SCANNING   CORRELATE SCANNING INFORMATION</i>	443
<b>VPM-07: PENETRATION TESTING</b>	<b>443</b>
<i>VPM-07.1: PENETRATION TESTING   INDEPENDENT PENETRATION AGENT OR TEAM</i>	444
<b>VPM-08: TECHNICAL SURVEILLANCE COUNTERMEASURES SECURITY</b>	<b>444</b>
<b>VPM-09: REVIEWING VULNERABILITY SCANNER USAGE</b>	<b>444</b>
<b>VPM-10: RED TEAM EXERCISES</b>	<b>445</b>
<b>WEB SECURITY (WEB) POLICY &amp; STANDARDS</b>	<b>446</b>
<b>WEB-01: WEB SECURITY</b>	<b>446</b>
<i>WEB-01.1: WEB SECURITY   UNAUTHORIZED CODE</i>	446
<b>WEB-02: USE OF DEMILITARIZED ZONES (DMZs)</b>	<b>447</b>
<b>WEB-03: WEB APPLICATION FIREWALL (WAF)</b>	<b>447</b>
<b>WEB-04: CLIENT-FACING WEB SERVICES</b>	<b>448</b>
<b>WEB-05: COOKIE MANAGEMENT</b>	<b>448</b>
<b>WEB-06: STRONG CUSTOMER AUTHENTICATION (SCA)</b>	<b>448</b>
<b>WEB-07: WEB SECURITY STANDARD</b>	<b>449</b>
<b>WEB-08: WEB APPLICATION FRAMEWORK</b>	<b>449</b>
<b>WEB-09: VALIDATION &amp; SANITIZATION</b>	<b>449</b>
<b>WEB-10: SECURE WEB TRAFFIC</b>	<b>449</b>
<b>WEB-11: OUTPUT ENCODING</b>	<b>449</b>
<b>WEB-12: WEB BROWSER SECURITY</b>	<b>450</b>
<b>WEB-13: WEBSITE CHANGE DETECTION</b>	<b>450</b>
<b>WEB-14: PUBLICLY ACCESSIBLE CONTENT REVIEWS</b>	<b>451</b>
<b>GLOSSARY: ACRONYMS &amp; DEFINITIONS</b>	<b>452</b>
<b>ACRONYMS</b>	<b>452</b>
<b>DEFINITIONS</b>	<b>452</b>
<b>KEY WORD INDEX</b>	<b>453</b>
<b>RECORD OF CHANGES</b>	<b>454</b>

---

## NOTICE – REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

---

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

- The National Institute of Standards and Technology (NIST):<sup>1</sup>
  - NIST AI 100-1: *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-63B, *Digital Identity Guidelines*
  - NIST SP 800-64: *Security Considerations in Secure Development Life Cycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personal Data (PD)*
  - NIST SP 800-160: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST Framework for Improving Critical Cybersecurity (Cybersecurity Framework)
- The International Organization for Standardization (ISO):<sup>2</sup>
  - ISO/IEC 15288: *Systems and Software Engineering -- System Life Cycle Processes*
  - ISO/IEC 22301: *Societal Security – Business Continuity Management Systems – Requirements*
  - ISO/IEC 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
  - ISO/IEC 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personal Data (PD) in Public Clouds Acting as PD Processors*
  - ISO/IEC 27701: *Information Technology - Security Techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management – Requirements and Guidelines*
- Other influencing frameworks (alphabetical order):
  - Center for Internet Security (CIS) Critical Security Controls (CSC)<sup>3</sup>
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)<sup>4</sup>
  - Computer Security Incident Handling Guide<sup>5</sup>
  - Control Objectives for Information and Related Technologies (COBIT)<sup>6</sup>
  - Defense Information Systems Agency (DISA) Secure Technology Implementation Guides (STIGs)<sup>7</sup>
  - Department of Defense Cybersecurity Maturity Model Certification (CMMC)<sup>8</sup>
  - Guide to Integrating Forensic Techniques into Incident Response<sup>9</sup>
  - Open Web Application Security Project (OWASP)<sup>10</sup>
  - Payment Card Industry Data Security Standard (PCI DSS)<sup>11</sup>
  - Privacy by Design (PbD)<sup>12</sup>

---

<sup>1</sup> National Institute of Standards and Technology - <https://csrc.nist.gov/publications/sp>

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

<sup>3</sup> Center for Internet Security - <https://www.cisecurity.org/>

<sup>4</sup> Cloud Security Alliance - <https://cloudsecurityalliance.org/>

<sup>5</sup> Computer Security Incident Handling Guide - <https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final>

<sup>6</sup> COBIT - <https://www.isaca.org/resources/cobit>

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

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

<sup>9</sup> Guide to Integrating Forensic Techniques into Incident Response - <https://csrc.nist.gov/publications/detail/sp/800-86/final>

<sup>10</sup> OWASP - <https://owasp.org/>

<sup>11</sup> Payment Card Industry Security Standards Council - <https://www.pcisecuritystandards.org/>

<sup>12</sup> Term and principles coined by Dr. Ann Cavoukian - <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>

---

## DIGITAL SECURITY PROGRAM (DSP) OVERVIEW

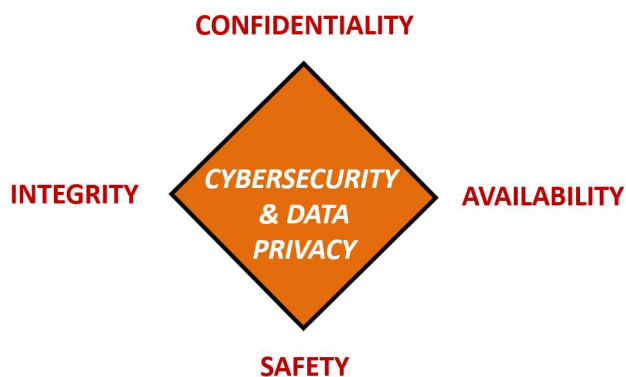
---

### INTRODUCTION

The **Digital Security Program (DSP)** provides definitive information on the prescribed measures used to establish and enforce the cybersecurity and data protection program at ACME Business Consulting, Inc. ([Company Name]).

[Company Name] is committed to protecting its employees, partners, clients and [Company Name] from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with [Company Name] data and systems, applications and services. Therefore, it is the responsibility of both [Company Name] personnel and third-parties to be aware of and adhere to [Company Name]'s cybersecurity and data protection requirements.

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



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

### PURPOSE

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

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

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

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

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

## SCOPE & APPLICABILITY

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

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

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

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

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

## POLICY OVERVIEW

To ensure an acceptable level of cybersecurity risk, [Company Name] must design, implement and maintain a coherent set of policies, standards, procedures and guidelines to manage risks to its data and systems.

The DSP addresses the policies, standards and guidelines. Data/process owners, in conjunction with asset custodians, are responsible for creating, implementing and updated operational procedures to comply with DSP requirements.

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

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

## VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES

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

## EXCEPTION TO STANDARDS

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

## UPDATES TO POLICIES & STANDARDS

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



## KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms*, is the primary reference document that [Company Name] uses to define common cybersecurity terms.

<sup>13</sup> Key terminology to be aware of includes:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<sup>13</sup> NIST IR 7298 - <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf>

### MANAGEMENT DIRECTION FOR CYBERSECURITY & DATA PROTECTION

The objective is to provide management direction and support for cybersecurity and data protection in accordance with business requirements and relevant laws and regulations.<sup>17</sup>

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

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

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

### POLICIES, CONTROLS, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

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

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

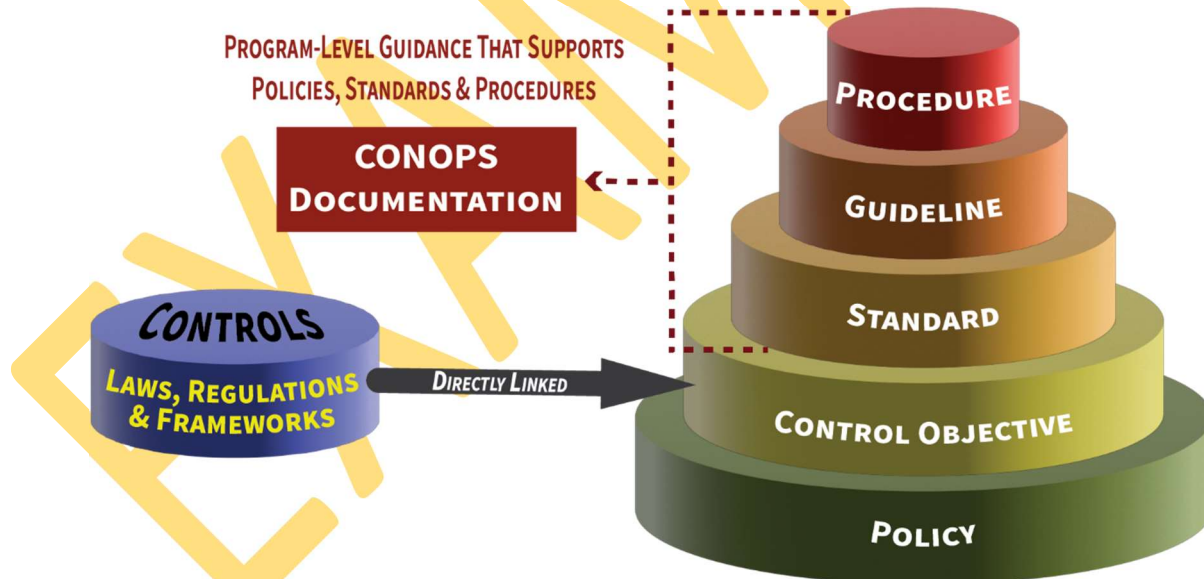


Figure 1. Cybersecurity Documentation Hierarchy

As referenced in this graphic, a Concept of Operations (CONOPS) is a cybersecurity-focused description that addresses life cycle concepts. This can include concepts for sustainment, logistics, maintenance and training. CONOPS augment and support an organization's policies, standards and procedures. Examples of CONOPS documentation includes, but is not limited to:

- Risk management (e.g., Risk Management Program (RMP))
- Vulnerability management (e.g., Vulnerability & Patch Management Program (VPMP))
- Incident response (e.g., Integrated Incident Response Program (IIRP))
- Business Continuity / Disaster Recovery (e.g., Continuity of Operations Plan (COOP))

<sup>17</sup> ISO 27002:2013 5.1

---

## CYBERSECURITY & DATA PROTECTION (GOV) POLICY & STANDARDS

---

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

**Policy:** [Company Name] shall implement and maintain a maturity-based capability to strengthen the security and resilience of its technology infrastructure and data protection mechanisms against both physical and cyber threats. Security control decisions shall take applicable statutory, regulatory and contractual obligations into account, but [Company Name] acknowledges that being compliant does not equate to being secure, so all stakeholders shall protect the confidentiality, integrity, availability and safety of [Company Name]'s technology resources and data, regardless of the geographic location of the data or technology in use. Cybersecurity and data protection controls shall be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and technology in use.

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

### GOV-01: CYBERSECURITY & DATA PROTECTION GOVERNANCE PROGRAM

**Control Objective:** The organization facilitates the implementation of cybersecurity & data protection governance controls.<sup>18</sup>

**Standard:** [Company Name]'s cybersecurity & data protection policies and standards must be represented in a single document, the Digital Security Program (DSP) that:

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

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

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

**Control Objective:** The organization coordinates cybersecurity, data privacy and business alignment through a steering committee or advisory board, comprising of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.<sup>19</sup>

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

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

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

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

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

**Control Objective:** The organization provides governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.

---

<sup>18</sup> ISO 27001-2013: 4.3, 4.4, 5.1, 6.1.1 | ISO 27002-2022: 5.1, 5.4, 5.37 | NIST SP 800-53 R5: PM-1

<sup>19</sup> ISO 27001-2013: 4.3, 6.2, 7.4, 9.3, 10.2

Standard: [Company Name]’s Chief Information Security Officer (CISO) must:

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

Guidelines: None

## **GOV-02: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION**

Control Objective: The organization establishes, maintains and disseminates cybersecurity & data protection policies, standards and procedures.<sup>20</sup>

Standard: The Digital Security Program (DSP) document represents the consolidation of [Company Name]’s cybersecurity & data protection policies and standards.<sup>21</sup> The DSP is endorsed by [Company Name]’s executive management and shall be:

- (a) Disseminated to the appropriate parties to ensure all affected personnel are made aware of and understand their applicable requirements to protect cardholder data;<sup>22</sup>
- (b) Reviewed and updated on no less than an annual basis, or as business/technology changes require modifications to the DSP, to ensure proper coverage for applicable statutory, regulatory and contractual requirements;<sup>23</sup>
- (c) Enforced by [Company Name] personnel through “business as usual” secure practices in the form of Standardized Operating Procedures (SOP) that shall be developed, enforced and maintained at the control operator level; and
- (d) Enforced through [Company Name]’s supply chain in the form of contractual requirements with those third-parties that have the ability to directly or indirectly influence the confidentiality, integrity and/or availability of [Company Name]’s technology assets and/or sensitive/regulated data.

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

It is important to update policies and procedures as needed to address changes in processes, technologies, and business objectives. Without cybersecurity & data privacy policies, individuals will make their own value decisions on the controls that are required within the organization which may result in the organization neither meeting its statutory, regulatory and/or contractual obligations, nor being able to adequately protect its technology and data in a consistent manner.

### **GOV-02.1: PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION | EXCEPTION MANAGEMENT**

Control Objective: The organization prohibits exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.

Standard: For exception management purposes, [Company Name]:

- (a) Prohibits any exception to a policy;
- (b) Permits limited exceptions to a standard, when the following is met:
  1. Requests for exception to a standard are formally submitted to [Company Name]’s cybersecurity function;
  2. A legitimate business justification for deviation from the standard is provided;
  3. One (1), or more, compensating control(s) is/are implemented to reduce the risk associated with the deficient standard;
  4. A timeline for remediation is documented in a Plan of Action & Milestones (POA&M), or similar document, to track the deficiency through remediation.

Guidelines: For exception management purposes:

- A policy is defined as a high-level statement of management intent that exists to influence and guide both present and future decision making to be in line with the philosophy, objectives and strategic plans established by [Company Name]’s executive leadership team.
- A standard is a mandatory requirement regarding processes, actions and configurations that is designed to satisfy a requirement (e.g., control, law, regulation, etc.).

<sup>20</sup> ISO 27001-2013: 4.3, 5.2, 7.5.1, 7.5.2, 7.5.3 | ISO 27002-2022: 5.1, 5.37 | NIST SP 800-53 R5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1 | NIST CSF: ID.GV-1 | NIST SP 800-171A: 3.4.9[a], 3.9.2[a]

<sup>21</sup> NIST SP 800-171A R3 IPD: A.03.15.01.a[01]

<sup>22</sup> NIST SP 800-171A R3 IPD: A.03.15.01.a[02]

<sup>23</sup> NIST SP 800-171A R3 IPD: A.03.15.01.b[01], A.03.15.01.b[02]



---

## CHANGE MANAGEMENT (CHG) POLICY & STANDARDS

---

Management Intent: The purpose of the Change Management (CHG) policy is for both technology and business leadership to proactively manage change. Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur or malicious code could be introduced. This includes the assessment, authorization and monitoring of technical changes across the enterprise.

Policy: [Company Name] shall implement and maintain appropriate change management practices to reduce the risk associated with unauthorized or improper change. [Company Name] requires active stakeholder involvement to ensure changes are appropriately tested, validated and documented before implementing any change on a production network.

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

### CHG-01: CHANGE MANAGEMENT PROGRAM

Control Objective: The organization facilitates the implementation of change management controls.<sup>119</sup>

Standard: [Company Name]'s Change Management Program requires data/process owners and asset custodians to test, validate and document changes to systems before implementing the changes on the production network. Changes for any production system, application and/or service must:

- (a) Be:
  1. Reviewed by an individual with the appropriate authority and knowledge to understand the impact of the change;<sup>120</sup>
  2. Approved by a [Company Name] employee with the appropriate authority and knowledge to understand the impact of the change;<sup>121</sup> and
  3. Approved by [Company Name]'s Change Control Board (CCB);
- (b) Sufficiently document the following criteria to enable independent review:
  1. Reason for, and description of, the change;
  2. Documentation of security impact;
  3. Documented change approval by authorized parties;
  4. Functionality testing to verify the change:
    - i. Did not adversely impact the security of the network; and
    - ii. Performs as expected;
  5. For bespoke and custom software changes, all updates are tested for compliance with applicable statutory, regulatory and contractual obligations; and
  6. Procedures to address failures and return to a secure state;
- (c) Ensure all applicable statutory, regulatory and contractual requirements are confirmed to be in place on all new or changed systems and networks; and
- (d) As applicable, update affected documentation to include the changes to prevent inconsistencies between network documentation and the actual configuration.

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

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

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

---

<sup>119</sup> ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3 | NIST SP 800-171 R2: 3.4.3 | NIST CSF: PR.IP-3

<sup>120</sup> NIST SP 800-171A R3 IPD: A.03.04.03.b[01]

<sup>121</sup> NIST SP 800-171A R3 IPD: A.03.04.03.b[02]

## CHG-02: CONFIGURATION CHANGE CONTROL

Control Objective: The organization governs the technical configuration change control processes.<sup>122</sup>

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

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

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

### CHG-02.1: CONFIGURATION CHANGE CONTROL | PROHIBITION OF CHANGES

Control Objective: The organization prohibits unauthorized changes, unless organization-approved change requests are received.<sup>123</sup>

Standard: To prohibit unauthorized changes, [Company Name] requires:

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

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

### CHG-02.2: CONFIGURATION CHANGE CONTROL | TEST, VALIDATE & DOCUMENT CHANGES

Control Objective: The organization tests and documents proposed changes in a non-production environment before changes are implemented in a production environment.<sup>124</sup>

Standard: Data/process owners and asset custodians must:

- (a) Where technically feasible, test and validate configuration changes in a test environment, prior to deploying the change in the production environment,<sup>125</sup> and

<sup>122</sup> ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3, SA-8(31) | NIST CSF: PR.IP-3 | NIST SP 800-171 R2: 3.4.3 | NIST SP 800-171A: 3.4.3[a], 3.4.3[b], 3.4.3[c], 3.4.3[d]

<sup>123</sup> NIST SP 800-53 R5: CM-3(1)

<sup>124</sup> ISO 27002-2022: 8.19, 8.32 | NIST SP 800-53 R5: CM-3(2), CM-3(7), SA-8(31) | NIST SP 800-171 R2: NFO - CM-3(2)

<sup>125</sup> NIST SP 800-171A R3 IPD: A.03.04.03.c[02]

---

## DATA CLASSIFICATION & HANDLING (DCH) POLICY & STANDARDS

---

**Management Intent:** The purpose of the Data Classification & Handling (DCH) policy is to ensure that technology assets are properly classified and measures are implemented to protect [Company Name]'s data from unauthorized disclosure, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance obligations dictate the safeguards that must be in place to protect the confidentiality, integrity and availability of data.

**Policy:** In accordance with all applicable statutory, regulatory and contractual obligations for cybersecurity and data protection, [Company Name] shall implement and maintain appropriate administrative, technical and physical security measures to protect the confidentiality, integrity and availability of its data, regardless if the data is in hardcopy or digital form. [Company Name] shall utilize methods of sanitizing or destroying digital and physical media so that data recovery is technically infeasible.

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

### DCH-01: DATA PROTECTION

**Control Objective:** The organization facilitates the implementation of data protection controls. <sup>344</sup>

**Standard:** [Company Name]'s Chief Information Security Officer (CISO), or the CISO's designated representative(s), must develop and implement:

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

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

#### DCH-01.1: DATA PROTECTION | DATA STEWARDSHIP

**Control Objective:** The organization ensures data stewardship is assigned, documented and communicated. <sup>345</sup>

**Standard:** [Company Name]'s Chief Information Security Officer (CISO), Chief Privacy Officer (CPO), Data Protection Officer (DPO), or their designated representative(s), must:

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

---

<sup>344</sup> ISO 27002-2022: 5.9, 5.10, 5.12, 5.33, 7.1, 8.12 | NIST SP 800-53 R5: MP-1 | NIST CSF: PR.DS-5 | NIST SP 800-171 R2: 3.8.1, NFO - MP-1 | NIST SP 800-171A: 3.8.1[a], 3.8.1[b], 3.8.1[c], 3.8.1[d]

<sup>345</sup> NIST SP 800-53 R5: SA-4(12)

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

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

Control Objective: The organization protects sensitive/regulated data wherever it is stored.

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

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

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

Sources for information about index tokens include:

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

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

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

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

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

Guidelines: None

### **DCH-01.4: DATA PROTECTION | DEFINING ACCESS AUTHORIZATIONS FOR SENSITIVE / REGULATED DATA**

Control Objective: The organization explicitly defines authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.

Standard: Data/process owners must:

- (a) Define specific roles for individuals and/or groups, as it pertains to business practices for interacting with sensitive/regulated data;



---

## TECHNOLOGY DEVELOPMENT & ACQUISITION (TDA) POLICY & STANDARDS

---

**Management Intent:** The purpose of the Technology Development & Acquisition (TDA) policy is to ensure technologies are developed and/or acquired according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.

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

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

### TDA-01: TECHNOLOGY DEVELOPMENT & ACQUISITION

**Control Objective:** The organization facilitates the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.<sup>1163</sup>

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

- (a) Ensures acquisition strategies, contract tools and procurement methods:
  - 1. Identify supply chain risks;<sup>1164</sup>
  - 2. Protect against supply chain risks;<sup>1165</sup> and
  - 3. Mitigate supply chain risks;<sup>1166</sup>
- (b) Incorporates cybersecurity & data privacy principles into the asset's lifecycle; and
- (c) Tailors acquisitions, contract tools and procurement methods to ensure compliance with applicable statutory, regulatory and contractual obligations.

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

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

#### TDA-01.1: TECHNOLOGY DEVELOPMENT & ACQUISITION | PRODUCT MANAGEMENT

**Control Objective:** The organization designs and implements product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.<sup>1167</sup>

**Standard:** [Company Name] requires that products and/or services are proactively managed to:

- (a) Maintain appropriate documentation on how [Company Name] provides validated software updates/patches throughout the product life cycle to assure its continued security;
- (b) Allow for the application of security updates to the products software and firmware:
  - 1. Processes must support reverting to a previously-installed version if the update fails; and

---

<sup>1163</sup> ISO 27002-2022: 8.25, 8.30 | NIST SP 800-53 R5: PL-1, SA-1, SA-4, SA-23 | NIST CSF: PR.DS-7 | NIST SP 800-171 R2: NFO - SA-4

<sup>1164</sup> NIST SP 800-171A R3 IPD: A.03.17.02[01]

<sup>1165</sup> NIST SP 800-171A R3 IPD: A.03.17.02[02]

<sup>1166</sup> NIST SP 800-171A R3 IPD: A.03.17.02[03]

<sup>1167</sup> NIST SP 800-53 R5: SA-23

2. The roll-back would revert to the most recent installed version.
- (c) Verify the authenticity and integrity of any software update through cryptographic means, prior to the installation of the update:
1. Product updates must be possible in an offline environment; and
  2. Offline updates must also support the same authenticity and integrity validation process.
- (d) Maintain an event log that, at a minimum, contains the following events:
1. Successful and unsuccessful login attempts;
  2. Change of user authentication credentials;
  3. Changes in the list of valid user accounts (e.g., addition, modification or deletion of accounts); and
  4. Successful and unsuccessful software updates.
- (e) Prevent tampering of security-related event logs through transmitting logs to an external data storage location or security store the logs in non-volatile memory that prevents non-privileged users from deleting, moving or altering log file contents; and
- (f) Enable secure decommissioning of the product by allowing users to securely purge or erase (e.g., zeroization) all user-defined data that includes:
1. Configuration data; and
  2. Sensitive data.

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

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

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

Standard: [Company Name] requires that products incorporate integrity mechanisms for software/firmware updates that include:

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

Guidelines: None

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

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

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

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

Guidelines: None

#### **TDA-02: MINIMUM VIABLE PRODUCT (MVP) SECURITY REQUIREMENTS**

Control Objective: The organization ensures risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).<sup>1168</sup>

Standard: Data/process owners and asset custodians must:

- (a) Take cybersecurity & data privacy requirements into account when purchasing systems or outsourcing solutions; and

<sup>1168</sup> ISO 27002-2022: 8.25, 8.29, 8.30 | NIST SP 800-53 R5: SA-4 | NIST SP 800-171 R2: NFO - SA-4

**- SUPPLEMENTAL DOCUMENTATION -**

# **DIGITAL SECURITY PROGRAM (DSP)**

---

**ANNEXES, TEMPLATES & REFERENCES**

---

Version 2022.3



**INTERNAL USE**

Access Limited to Internal Use Only

## TABLE OF CONTENTS

<b>ANNEXES</b>	<b>3</b>
ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES	3
ANNEX 2: DATA CLASSIFICATION EXAMPLES	10
ANNEX 3: DATA RETENTION PERIODS	12
ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES	14
ANNEX 5: RULES OF BEHAVIOR (ACCEPTABLE & UNACCEPTABLE USE)	16
ANNEX 6: GUIDELINES FOR PERSONAL USE OF ORGANIZATIONAL IT RESOURCES	18
ANNEX 7: RISK MANAGEMENT FRAMEWORK (RMF)	19
ANNEX 8: SYSTEM HARDENING	22
ANNEX 9: SAFETY CONSIDERATIONS WITH EMBEDDED TECHNOLOGY	24
ANNEX 10: INDICATORS OF COMPROMISE (IOC)	25
<b>TEMPLATES</b>	<b>28</b>
TEMPLATE 1: MANAGEMENT DIRECTIVE (POLICY AUTHORIZATION)	28
TEMPLATE 2: USER ACKNOWLEDGEMENT FORM	29
TEMPLATE 3: USER EQUIPMENT RECEIPT OF ISSUE	30
TEMPLATE 4: SERVICE PROVIDER NON-DISCLOSURE AGREEMENT (NDA)	31
TEMPLATE 5: INCIDENT RESPONSE PLAN (IRP)	32
TEMPLATE 6: INCIDENT RESPONSE FORM	43
TEMPLATE 7: APPOINTMENT ORDERS (INFORMATION SECURITY OFFICER)	44
TEMPLATE 8: PRIVILEGED USER ACCOUNT REQUEST FORM	45
TEMPLATE 9: CHANGE MANAGEMENT REQUEST FORM	46
TEMPLATE 10: CHANGE CONTROL BOARD (CCB) MEETING MINUTES	48
TEMPLATE 11: PLAN OF ACTION & MILESTONES (POA&M) / RISK REGISTER	49
TEMPLATE 12: PORTS, PROTOCOLS & SERVICES (PPS)	50
TEMPLATE 13: BUSINESS IMPACT ANALYSIS (BIA)	51
TEMPLATE 14: DISASTER RECOVERY PLAN (DRP) & BUSINESS CONTINUITY PLAN (BCP)	53
TEMPLATE 15: PRIVACY IMPACT ASSESSMENT (PIA)	57
<b>REFERENCES</b>	<b>59</b>
REFERENCE 1: DSP EXCEPTION REQUEST PROCESS	59
REFERENCE 2: ELECTRONIC DISCOVERY (EDISCOVERY) GUIDELINES	60
REFERENCE 3: TYPES OF SECURITY CONTROLS	61
REFERENCE 4: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)	62



**ANNEX 1: DATA CLASSIFICATION & HANDLING GUIDELINES**

**DATA CLASSIFICATION**

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

**CUI-Restricted**

**Sensitive Personal Data (sPD)-Restricted**

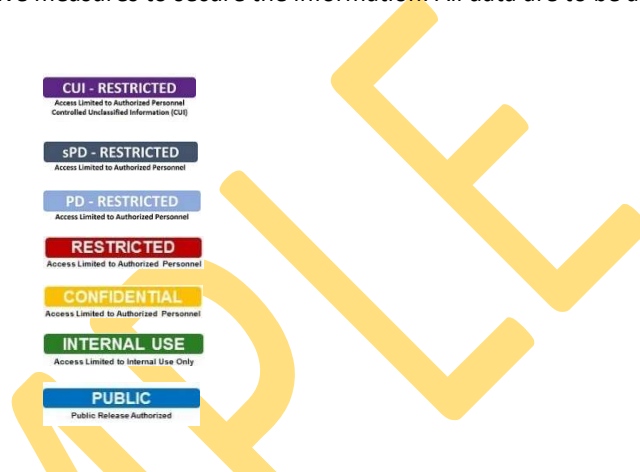
**Personal Data (PD)-Restricted**

**Restricted**

**Confidential**

**Internal Use**

**Public**



Classification		Data Sensitivity Description
Controlled Unclassified Information (CUI) - Restricted	Definition	CUI-Restricted information is U.S. Government regulated data that is highly-sensitive business information and the level of protection is dictated externally by both NIST SP 800-171 and Cybersecurity Maturity Model Certification (CMMC) requirements. CUI-Restricted information must be limited to only authorized employees, contractors and business partners with a specific business need.
	Potential Impact of Loss	<ul style="list-style-type: none"> <li>· <b>SIGNIFICANT DAMAGE</b> would occur if CUI-Restricted information were to become available to unauthorized parties either internal or external to ACME.</li> <li>· Impact could include negatively affecting ACME’s competitive position, violating statutory, regulatory and/or contractual requirements and damaging the company’s reputation.</li> </ul>
Sensitive Personal Data (sPD) Restricted	Definition	Sensitive Personal Data (sPD) is a subset of Personal Data (PD) that is highly-sensitive information about individuals (e.g., consumers, clients and/or employees) and the level of protection is dictated externally by statutory, regulatory and/or contractual requirements. sPD Restricted information must be limited to what is authorized in the Privacy Notice for how and where the sPD is authorized to be stored, processed and/or transmitted.
	Potential Impact of Loss	<ul style="list-style-type: none"> <li>· <b>SIGNIFICANT DAMAGE</b> would occur if sPD Restricted information were to become available to unauthorized parties either internal or external to ACME.</li> <li>· Impact could include negatively affecting ACME’s competitive position, violating statutory, regulatory and/or contractual requirements, damaging the company’s reputation and posing a risk to identified individuals (e.g., identity theft, stalking, harassment, etc.).</li> </ul>

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

## LABELING

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

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

## GENERAL ASSUMPTIONS

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

## PERSONAL DATA (PD)

PD is any information about an individual maintained by ACME including any information that:

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

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

- Name
  - Full name;
  - Maiden name;
  - Mother's maiden name; and
  - Alias(es);
- Personal Identification Numbers
  - Social Security Number (SSN);
  - Passport number;
  - Driver's license number;
  - Taxpayer Identification Number (TIN), and
  - Financial account or credit card number;
- Address Information
  - Home address; and
  - Personal email address;
- Personal Characteristics
  - Photographic image (especially of the face or other identifying characteristics, such as scars or tattoos);
  - Fingerprints;
  - Handwriting, and
  - Other biometric data:
    - Retina scan;
    - Voice signature; and
    - Facial geometry; and
- Linkable Information
  - Date of birth;

**DATA HANDLING GUIDELINES**

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

- For **Federal Contract Information (FCI)**, the following sources are authoritative for FCI data handling:
  - 48 CFR § 52.204-21 (basic safeguarding for Covered Contractor Information Systems (CCIS))
- For **Controlled Unclassified Information (CUI)**, the following sources are authoritative for CUI data handling:
  - 32 CFR § 2002
  - DoD Instruction 5200.48
  - NIST SP 800-171 rev2

Handling Controls	CUI - RESTRICTED	Restricted	Confidential	Internal Use	Public
<b>Non-Disclosure Agreement (NDA)</b>	▪ <b>NDA is required prior to access by non-employees.</b>	▪ <b>NDA is required prior to access by non-employees.</b>	▪ NDA is recommended prior to access by non-employees.	<i>No NDA requirements</i>	<i>No NDA requirements</i>
<b>Internal Network Transmission (wired &amp; wireless)</b>	▪ <b>Encryption is required</b> ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication	▪ <b>Encryption is required</b> ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	<i>No special requirements</i>	<i>No special requirements</i>
<b>External Network Transmission (wired &amp; wireless)</b>	▪ <b>Encryption is required</b> ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Logical access must use multi-factor authentication ▪ Remote access must use multi-factor authentication	▪ <b>Encryption is required</b> ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and multi-factor authentication	▪ <b>Encryption is required</b> ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended	<i>No special requirements</i>
<b>Data At Rest (file servers, databases, archives, etc.)</b>	▪ <b>Encryption is required</b> ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ <b>Encryption is required</b> ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups



## ANNEX 2: DATA CLASSIFICATION EXAMPLES

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

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

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

---

## ANNEX 4: BASELINE SECURITY CATEGORIZATION GUIDELINES

---

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

### SAFETY & CRITICALITY

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

There are four (4) SC levels:

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

#### **MISSION CRITICAL (SC1)**

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

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

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

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

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

#### **BUSINESS CRITICAL (SC2)**

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

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

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

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

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

#### **NON-CRITICAL (SC3)**

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

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

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