YOUR LOGO GOES HERE

CYBERSECURITY STANDARDIZED OPERATING PROCEDURES (CSOP)

Secure Controls Framework (SCF)
Security, Compliance & Resilience Program (SCRP)

ACME Business Consulting, Inc.

SENSITIVE

Access Limited to Authorized Personnel

Table of Contents

Overview, Instructions & Example 31
Key Terminology 31
Overview 31
Customization Guidance 31
Validating Needs for Procedures / Control Activities 31
Procedures Documentation 32
NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework 33
Example 33
Supporting Policies & Standards 36
Policies, Controls, Standards, Procedures & Guidelines Structure 36
Known Compliance Requirements 37
Statutory Requirements 37
Regulatory Requirements 37
Contractual Requirements 37
Cybersecurity & Data Protection Governance (GOV) Procedures 38
P-GOV-01: Cybersecurity & Data Protection Governance Program 38
P-GOV-01.1: Cybersecurity & Data Protection Governance Program | Steering Committee & Program Oversight 38
P-GOV-01.2: Cybersecurity & Data Protection Governance Program | Status Reporting To Governing Body 39
P-GOV-01.3: Cybersecurity & Data Protection Governance Program | Commitment To Continual Improvements 40
P-GOV-02: Publishing Cybersecurity & Data Protection Documentation 41
P-GOV-02.1: Publishing Cybersecurity & Data Protection Documentation | Exception Management 41
P-GOV-03: Periodic Review & Update of Cybersecurity & Data Protection Program 42
P-GOV-04: Assigned Cybersecurity & Data Protection Responsibilities 42
P-GOV-04.1: Assigned Cybersecurity & Data Protection Responsibilities | Accountability Structure 43
P-GOV-04.2: Assigned Cybersecurity & Data Protection Responsibilities | Authoritative Chain of Command 43
P-GOV-05: Measures of Performance 44
P-GOV-05.1: Measures of Performance | Key Performance Indicators (KPIs) 44
P-GOV-05.2: Measures of Performance | Key Risk Indicators (KRIs) 45
P-GOV-06: Contacts With Authorities 45
P-GOV-07: Contacts With Groups & Associations 45
P-GOV-08: Defined Business Context & Mission 46
P-GOV-09: Defined Control Objectives 46
P-GOV-10: Data Governance 47
P-GOV-11: Purpose Validation 47
P-GOV-12: Forced Technology Transfer (FTT) 48
P-GOV-13: State-Sponsored Espionage 48
P-GOV-14: Business As Usual (BAU) Secure Practices 49
P-GOV-15: Operationalizing Cybersecurity & Data Protection Practices 49
P-GOV-15.1: Operationalizing Cybersecurity & Data Protection Practices | Select Controls 50
P-GOV-15.2: Operationalizing Cybersecurity & Data Protection Practices | Implement Controls 50
P-GOV-15.3: Operationalizing Cybersecurity & Data Protection Practices | Assess Controls 51
P-GOV-15.4: Operationalizing Cybersecurity & Data Protection Practices | Authorize Technology Assets, Applications and/or Services (TAAS) 51
P-GOV-15.5: Operationalizing Cybersecurity & Data Protection Practices | Monitor Controls 52
P-GOV-16: Materiality Determination 52
P-GOV-16.1: Materiality Determination | Material Risks 53
P-GOV-16.2: Materiality Determination | Material Threats 53
P-GOV-17: Cybersecurity & Data Protection Status Reporting 54
P-GOV-18: Quality Management System (QMS) 54
P-GOV-19: Assurance 54
P-GOV-19.1: Assurance | Assurance Levels (AL) 55
P-GOV-19.2: Assurance | Assessment Objectives (AO) 55
P-GOV-20: Mergers, Acquisitions & Divestitures (MA&D) 56
P-GOV-20.1: Mergers, Acquisitions & Divestitures (MA&D) | Virtual Data Room (VDR) 56
Artificial Intelligence and Autonomous Technologies (AAT) Procedures 57

P-AAT-01: Artificial Intelligence (AI) & Autonomous Technologies Governance **57**
P-AAT-01.1: Artificial Intelligence (AI) & Autonomous Technologies Governance | AI & Autonomous Technologies-Related Legal Requirements Definition 58
P-AAT-01.2: Artificial Intelligence (AI) & Autonomous Technologies Governance | Trustworthy AI & Autonomous Technologies 58
P-AAT-01.3: Artificial Intelligence (AI) & Autonomous Technologies Governance | AI & Autonomous Technologies Value Sustainment 59
P-AAT-01.4: Artificial Intelligence (AI) & Autonomous Technologies Governance | AI Model & Agent Inventory & Lifecycle Management 60
P-AAT-02: Situational Awareness of AI & Autonomous Technologies **60**
P-AAT-02.1: Situational Awareness of AI & Autonomous Technologies | AI & Autonomous Technologies Risk Mapping 61
P-AAT-02.2: Situational Awareness of AI & Autonomous Technologies | AI & Autonomous Technologies Internal Controls 61
P-AAT-02.3: Situational Awareness of AI & Autonomous Technologies | Adequate Protections For AI & Autonomous Technologies 61
P-AAT-02.4: Situational Awareness of AI & Autonomous Technologies | AI Threat Modeling & Risk Assessment 62
P-AAT-03: AI & Autonomous Technologies Context Definition **62**
P-AAT-03.1: AI & Autonomous Technologies Context Definition | AI & Autonomous Technologies Mission and Goals Definition 63
P-AAT-03.2: AI & Autonomous Technologies Context Definition | Model & AI Agent Documentation 63
P-AAT-04: AI & Autonomous Technologies Business Case **64**
P-AAT-04.1: AI & Autonomous Technologies business Case | AI & Autonomous Technologies Potential Benefits Analysis 64
P-AAT-04.2: AI & Autonomous Technologies business Case | AI & Autonomous Technologies Potential Costs Analysis 65
P-AAT-04.3: AI & Autonomous Technologies business Case | AI & Autonomous Technologies Targeted Application Scope 65
P-AAT-04.4: AI & Autonomous Technologies business Case | AI & Autonomous Technologies Cost / Benefit Mapping 66
P-AAT-05: AI & Autonomous-Specific Training **66**
P-AAT-06: AI & Autonomous Technologies Fairness & Bias **67**
P-AAT-07: AI & Autonomous Technologies Risk Management Decisions **67**
P-AAT-07.1: AI & Autonomous Technologies Risk Management Decisions | AI & Autonomous Technologies Impact Assessment 68
P-AAT-07.2: AI & Autonomous Technologies Risk Management Decisions | AI & Autonomous Technologies Likelihood & Impact Risk Analysis 68
P-AAT-07.3: AI & Autonomous Technologies Risk Management Decisions | AI & Autonomous Technologies Continuous Improvements 68
P-AAT-08: Assigned Responsibilities for AI & Autonomous Technologies **69**
P-AAT-09: AI & Autonomous Technologies Risk Profiling **70**
P-AAT-09.1: AI & Autonomous Technologies Risk Profiling | AI & Autonomous Technologies High Risk Designations 70
P-AAT-10: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) **71**
P-AAT-10.1: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Trustworthiness Assessment 71
P-AAT-10.2: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Tools 72
P-AAT-10.3: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Trustworthiness Demonstration 72
P-AAT-10.4: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Safety Demonstration 73
P-AAT-10.5: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Resiliency Assessment 73
P-AAT-10.6: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Transparency & Accountability Assessment 74
P-AAT-10.7: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Privacy Assessment 74
P-AAT-10.8: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Fairness & Bias Assessment 74

P-AAT-10.9: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI & Autonomous Technologies Model Validation 75
P-AAT-10.10: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Results Evaluation 75
P-AAT-10.11: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Effectiveness 75
P-AAT-10.12: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Comparable Deployment Settings 76
P-AAT-10.13: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Post-Deployment Monitoring 76
P-AAT-10.14: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | Updating AI & Autonomous Technologies 77
P-AAT-10.15: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Reporting 77
P-AAT-10.16: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Empirically Validated Methods 78
P-AAT-10.17: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Benchmarking Content Provenance 78
P-AAT-10.18: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Model Collapse Mitigations 78
P-AAT-10.19: Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) | AI TEVV Third-Party Risk Management 79
P-AAT-11: Robust Stakeholder Engagement For AI & Autonomous Technologies **79**
P-AAT-11.1: Robust Stakeholder Engagement For AI & Autonomous Technologies | AI & Autonomous Technologies Stakeholder Feedback Integration 80
P-AAT-11.2: Robust Stakeholder Engagement For AI & Autonomous Technologies | AI & Autonomous Technologies Ongoing Assessments 80
P-AAT-11.3: Robust Stakeholder Engagement For AI & Autonomous Technologies | AI & Autonomous Technologies End User Feedback 81
P-AAT-11.4: Robust Stakeholder Engagement For AI & Autonomous Technologies | AI & Autonomous Technologies Incident & Error Reporting 81
P-AAT-12: AI & Autonomous Technologies Intellectual Property Infringement Protections **82**
P-AAT-12.1: AI & Autonomous Technologies Intellectual Property Infringement Protections | Data Source Identification 82
P-AAT-12.2: AI & Autonomous Technologies Intellectual Property Infringement Protections | Data Source Integrity 82
P-AAT-12.3: AI & Autonomous Technologies Intellectual Property Infringement Protections | Data Source Lineage & Origin Disclosure 83
P-AAT-12.4: AI & Autonomous Technologies Intellectual Property Infringement Protections | Digital Content Modification Logging 83
P-AAT-13: AI & Autonomous Technologies Stakeholder Diversity **84**
P-AAT-13.1: AI & Autonomous Technologies Stakeholder Diversity | AI & Autonomous Technologies Stakeholder Competencies 84
P-AAT-14: AI & Autonomous Technologies Requirements Definitions **85**
P-AAT-14.1: AI & Autonomous Technologies Requirements Definitions | AI & Autonomous Technologies Implementation Tasks Definition 85
P-AAT-14.2: AI & Autonomous Technologies Requirements Definitions | AI & Autonomous Technologies Knowledge Limits 86
P-AAT-15: AI & Autonomous Technologies Viability Decisions **86**
P-AAT-15.1: AI & Autonomous Technologies Viability Decisions | AI & Autonomous Technologies Negative Residual Risks 86
P-AAT-15.2: AI & Autonomous Technologies Viability Decisions | Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies 87
P-AAT-16: AI & Autonomous Technologies Production Monitoring **87**
P-AAT-16.1: AI & Autonomous Technologies Production Monitoring | AI & Autonomous Technologies Measurement Approaches 88
P-AAT-16.2: AI & Autonomous Technologies Production Monitoring | Measuring AI & Autonomous Technologies Effectiveness 88
P-AAT-16.3: AI & Autonomous Technologies Production Monitoring | Unmeasurable AI & Autonomous Technologies Risks 89

P-AAT-16.4: AI & Autonomous Technologies Production Monitoring | Efficacy of AI & Autonomous Technologies Measurement 89
P-AAT-16.5: AI & Autonomous Technologies Production Monitoring | AI & Autonomous Technologies Domain Expert Reviews 89
P-AAT-16.6: AI & Autonomous Technologies Production Monitoring | AI & Autonomous Technologies Performance Changes 90
P-AAT-16.7: AI & Autonomous Technologies Production Monitoring | Pre-Trained AI & Autonomous Technologies Models 90
P-AAT-16.8: AI & Autonomous Technologies Production Monitoring | AI & Autonomous Technologies Event Logging 91
P-AAT-16.9: AI & Autonomous Technologies Production Monitoring | Serious Incident Reporting For AI & Autonomous Technologies 91
P-AAT-16.10: AI & Autonomous Technologies Production Monitoring | Serious Incident Root Cause Analysis (RCA) For AI & Autonomous Technologies 92
P-AAT-16.11: AI & Autonomous Technologies Production Monitoring | Anomaly Detection & Human Oversight 92
P-AAT-16.12: AI & Autonomous Technologies Production Monitoring | Human-in-the-Loop & Escalation 93
P-AAT-16.13: AI & Autonomous Technologies Production Monitoring | Emergent Behavior & Collusion Protections 93
P-AAT-16.14: AI & Autonomous Technologies Production Monitoring | Multi-Agent Trust & Communication Validation 94
P-AAT-17: AI & Autonomous Technologies Harm Prevention **94**
P-AAT-17.1: AI & Autonomous Technologies Harm Prevention | AI & Autonomous Technologies Human Subject Protections 94
P-AAT-17.2: AI & Autonomous Technologies Harm Prevention | AI & Autonomous Technologies Environmental Impact & Sustainability 96
P-AAT-17.3: AI & Autonomous Technologies Harm Prevention | Previously Unknown AI & Autonomous Technologies Threats & Risks 96
P-AAT-17.4: AI & Autonomous Technologies Harm Prevention | Novel Risk Assessment Methods & Technologies 97
P-AAT-17.5: AI & Autonomous Technologies Harm Prevention | Fine Tuning Risk Mitigation 97
P-AAT-18: AI & Autonomous Technologies Risk Tracking Approaches **98**
P-AAT-18.1: AI & Autonomous Technologies Risk Tracking Approaches | AI & Autonomous Technologies Risk Response 98
P-AAT-19: AI & Autonomous Technologies Conformity **98**
P-AAT-19.1: AI & Autonomous Technologies Conformity | Manipulative or Deceptive Techniques 99
P-AAT-19.2: AI & Autonomous Technologies Conformity | Materially Distorting Behaviors 99
P-AAT-19.3: AI & Autonomous Technologies Conformity | Social Scoring 100
P-AAT-19.4: AI & Autonomous Technologies Conformity | Detrimental or Unfavorable Treatment 100
P-AAT-19.5: AI & Autonomous Technologies Conformity | Risk and Criminal Profiling 101
P-AAT-19.6: AI & Autonomous Technologies Conformity | Populating Facial Recognition Databases 101
P-AAT-19.7: AI & Autonomous Technologies Conformity | Emotion Inference 102
P-AAT-19.8: AI & Autonomous Technologies Conformity | Biometric Categorization 102
P-AAT-20: AI & Autonomous Technologies Development Practices **103**
P-AAT-20.1: AI & Autonomous Technologies Development Practices | AI & Autonomous Technologies Transparency 103
P-AAT-20.2: AI & Autonomous Technologies Development Practices | AI & Autonomous Technologies Implementation Documentation 104
P-AAT-20.3: AI & Autonomous Technologies Development Practices | AI & Autonomous Technologies Human Domain Knowledge Reliance 104
P-AAT-21: AI & Autonomous Technologies Registration **105**
P-AAT-22: AI & Autonomous Technologies Deployment **105**
P-AAT-22.1: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Human Oversight 106
P-AAT-22.2: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Oversight Measures 106
P-AAT-22.3: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Separate Verification 107
P-AAT-22.4: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Oversight Functions Competency 107
P-AAT-22.5: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Data Relevance 108
P-AAT-22.6: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Irregularity Reporting 108

P-AAT-22.7: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Use Notification To Employees 109
P-AAT-22.8: AI & Autonomous Technologies Deployment | AI & Autonomous Technologies Use Notification To Users 109
P-AAT-23: AI & Autonomous Technologies Output Marking **109**
P-AAT-24: Real World Testing of AI & Autonomous Technologies **110**
P-AAT-25: AI & Autonomous Technologies System Value Chain **110**
P-AAT-25.1: AI & Autonomous Technologies System Value Chain | AI & Autonomous Technologies System Value Chain Fallbacks 111
P-AAT-26: AI & Autonomous Technologies Testing Techniques **111**
P-AAT-26.1: AI & Autonomous Technologies Testing Techniques | Generative Artificial Intelligence (GAI) Identification 111
P-AAT-26.2: AI & Autonomous Technologies Testing Techniques | AI & Autonomous Technologies Capabilities Testing 112
P-AAT-26.3: AI & Autonomous Technologies Testing Techniques | Real-World Testing 112
P-AAT-26.4: AI & Autonomous Technologies Testing Techniques | Documenting Testing Guidance 112
P-AAT-27: AI & Autonomous Technologies Output Filtering **113**
P-AAT-27.1: AI & Autonomous Technologies Output Filtering | Human Moderation 113
P-AAT-28: AI Model Resilience **114**
P-AAT-28.1: AI Model Resilience | Model Pollution 114
P-AAT-28.2: AI Model Resilience | Cascading Hallucination Defense 114
P-AAT-28.3: AI Model Resilience | Resource Exhaustion & DoS Resilience 115
P-AAT-29: AI Agent Governance **115**
P-AAT-29.1: AI Agent Governance | Infrastructure Hardening & Isolation 115
P-AAT-29.2: AI Agent Governance | AI Agent Limitations 116
P-AAT-29.3: AI Agent Governance | Tool & API Invocation Controls 116
P-AAT-29.4: AI Agent Governance | Orchestration Protocol Safeguards 117
P-AAT-29.5: AI Agent Governance | Data Pipeline & Input Integrity 117
P-AAT-29.6: AI Agent Governance | Privileged Role & Delegation Boundaries 118
P-AAT-29.7: AI Agent Governance | AI Agent Data Access Restrictions 118
P-AAT-29.8: AI Agent Governance | Data Extraction 118
P-AAT-29.9: AI Agent Governance | AI Agent Identity & Impersonation Defense 119
P-AAT-29.10: AI Agent Governance | AI Agent Logic Integrity 119
P-AAT-29.11: AI Agent Governance | Sandboxing AI Agents 119
P-AAT-29.12: AI Agent Governance | Prompt Injection Defense 120
P-AAT-29.13: AI Agent Governance | Agent Kill Switch / User Control 120
P-AAT-29.14: AI Agent Governance | Adversarial & Red Team Testing 120
P-AAT-29.15: AI Agent Governance | Self-Modification Controls 121
P-AAT-29.16: AI Agent Governance | Purging AI Agent Data 121
P-AAT-29.17: AI Agent Governance | Delegation and Chaining Control 121
P-AAT-29.18: AI Agent Governance | Behavioral Drift Detection 122
P-AAT-29.19: AI Agent Governance | AI Agent Action Authentication & Authorization 122
P-AAT-29.20: AI Agent Governance | Transparency & Audit 123
P-AAT-29.21: AI Agent Governance | Explainability 123
P-AAT-29.22: AI Agent Governance | Ethics, Fairness & Bias Detection 123
P-AAT-29.23: AI Agent Governance | Agent Output Integrity & Verification 124
P-AAT-30: Agentic Output Traceability & Repudiation **124**
P-AAT-30.1: Agentic Output Traceability & Repudiation | AI Agent Logging 124
P-AAT-30.2: Agentic Output Traceability & Repudiation | Session Management 125
P-AAT-31: Human-in-the-Loop Workload & Manipulation **125**
P-AAT-32: Robotic Process Automation (RPA) **126**
P-AAT-32.1: Robotic Process Automation (RPA) | Business Process Task Enumeration 126
Asset Management (AST) Procedures **127**
P-AST-01: Asset Governance **127**
P-AST-01.1: Asset Governance | Asset-Service Dependencies 127
P-AST-01.2: Asset Governance | Stakeholder Identification & Involvement 128
P-AST-01.3: Asset Governance | Standardized Naming Convention 128

P-AST-01.4: Asset Governance | Approved Technologies 129
P-AST-02: Asset Inventories **129**
P-AST-02.1: Asset Inventories | Updates During Installations/Removals 130
P-AST-02.2: Asset Inventories | Automated Unauthorized Component Detection 130
P-AST-02.3: Asset Inventories | Component Duplication Avoidance 131
P-AST-02.4: Asset Inventories | Approved Baseline Deviations 131
P-AST-02.5: Asset Inventories | Network Access Control (NAC) 131
P-AST-02.6: Asset Inventories | Dynamic Host Configuration Protocol (DHCP) Server Logging 132
P-AST-02.7: Asset Inventories | Software Licensing Restrictions 132
P-AST-02.8: Asset Inventories | Data Action Mapping 132
P-AST-02.9: Asset Inventories | Configuration Management Database (CMDB) 133
P-AST-02.10: Asset Inventories | Automated Location Tracking 134
P-AST-02.11: Asset Inventories | Component Assignment 134
P-AST-03: Asset Ownership Assignment **134**
P-AST-03.1: Asset Ownership Assignment | Accountability Information 135
P-AST-03.2: Asset Ownership Assignment | Provenance 135
P-AST-04: Network Diagrams & Data Flow Diagrams (DFDs) **136**
P-AST-04.1: Network Diagrams & Data Flow Diagrams (DFDs) | Asset Scope Classification 136
P-AST-04.2: Network Diagrams & Data Flow Diagrams (DFDs) | Control Applicability Boundary Graphical Representation 137
P-AST-04.3: Network Diagrams & Data Flow Diagrams (DFDs) | Compliance-Specific Asset Identification 138
P-AST-05: Security of Assets & Media **139**
P-AST-05.1: Security of Assets & Media | Management Approval For External Media Transfer 139
P-AST-06: Unattended End-User Equipment **139**
P-AST-06.1: Unattended End-User Equipment | Asset Storage In Automobiles 140
P-AST-07: Kiosks & Point of Interaction (PoI) Devices **140**
P-AST-08: Physical Tamper Detection **141**
P-AST-09: Secure Disposal, Destruction or Re-Use of Equipment **141**
P-AST-10: Return of Assets **142**
P-AST-11: Removal of Assets **142**
P-AST-12: Use of Personal Devices **143**
P-AST-13: Use of Third-Party Devices **143**
P-AST-14: Usage Parameters **144**
P-AST-14.1: Usage Parameters | Bluetooth & Wireless Devices 144
P-AST-14.2: Usage Parameters | Infrared Communications 144
P-AST-15: Logical Tamper Protection **145**
P-AST-15.1: Logical Tamper Protection | Technology Asset Inspections 145
P-AST-16: Bring Your Own Device (BYOD) Usage **146**
P-AST-17: Prohibited Equipment & Services **146**
P-AST-18: Roots of Trust Protection **147**
P-AST-19: Telecommunications Equipment **147**
P-AST-20: Video Teleconference (VTC) Security **148**
P-AST-21: Voice over Internet Protocol (VoIP) Security **148**
P-AST-22: Microphones & Web Cameras **149**
P-AST-23: Multi-Function Devices (MFD) **149**
P-AST-24: Travel-Only Devices **150**
P-AST-25: Re-Imaging Devices After Travel **151**
P-AST-26: System Administrative Processes **151**
P-AST-27: Jump Server **152**
P-AST-28: Database Administrative Processes **152**
P-AST-28.1: Database Administrative Processes | Database Management System (DBMS) 153
P-AST-29: Radio Frequency Identification (RFID) Security **153**
P-AST-29.1: Radio Frequency Identification (RFID) Security | Contactless Access Control Systems 154
P-AST-30: Decommissioning **154**
P-AST-31: Asset Categorization **155**
P-AST-31.1: Asset Categorization | Categorize Artificial Intelligence (AI)-Related Technologies 156
P-AST-31.2: Asset Categorization | High-Risk Asset Categorization 157
P-AST-31.3: Asset Categorization | Asset Attributes 157

P-AST-32: Automated Network Asset Discovery 158

Business Continuity & Disaster Recovery (BCD) Procedures 159

P-BCD-01: Business Continuity Management System (BCMS) 159

P-BCD-01.1: Business Continuity Management System (BCMS) | Coordinate with Related Plans 159

P-BCD-01.2: Business Continuity Management System (BCMS) | Coordinate With External Service Providers 160

P-BCD-01.3: Business Continuity Management System (BCMS) | Transfer To Alternate Processing/Storage Site 160

P-BCD-01.4: Business Continuity Management System (BCMS) | Recovery Time/Point Objectives (RTO/RPO) 160

P-BCD-01.5: Business Continuity Management System (BCMS) | Recovery Operations Criteria 161

P-BCD-01.6: Business Continuity Management System (BCMS) | Recovery Operations Communications 161

P-BCD-02: Identify Critical Assets 162

P-BCD-02.1: Identify Critical Assets | Resume All Missions & Business Functions 162

P-BCD-02.2: Identify Critical Assets | Continue Essential Mission & Business Functions 163

P-BCD-02.3: Identify Critical Assets | Resume Essential Mission & Business Functions 163

P-BCD-02.4: Identify Critical Assets | Data Storage Location Reviews 163

P-BCD-03: Contingency Training 164

P-BCD-03.1: Contingency Training | Simulated Events 164

P-BCD-03.2: Contingency Training | Automated Training Environments 165

P-BCD-04: Contingency Plan Testing & Exercises 165

P-BCD-04.1: Contingency Plan Testing & Exercises | Coordinated Testing with Related Plans 165

P-BCD-04.2: Contingency Plan Testing & Exercises | Alternate Storage & Processing Sites 166

P-BCD-05: Contingency Plan Root Cause Analysis (RCA) & Lessons Learned 166

P-BCD-06: Ongoing Contingency Planning 166

P-BCD-06.1: Ongoing Contingency Planning | Contingency Planning Components 167

P-BCD-06.2: Ongoing Contingency Planning | Contingency Plan Update Notifications 167

P-BCD-07: Alternative Security Measures 168

P-BCD-08: Alternate Storage Site 168

P-BCD-08.1: Alternate Storage Site | Separation from Primary Site 169

P-BCD-08.2: Alternate Storage Site | Accessibility 169

P-BCD-09: Alternate Processing Site 169

P-BCD-09.1: Alternate Processing Site | Separation from Primary Site 170

P-BCD-09.2: Alternate Processing Site | Accessibility 170

P-BCD-09.3: Alternate Processing Site | Alternate Site Priority of Service 171

P-BCD-09.4: Alternate Processing Site | Preparation for Use 171

P-BCD-09.5: Alternate Processing Site | Inability to Return to Primary Site 172

P-BCD-10: Telecommunications Services Availability 172

P-BCD-10.1: Telecommunications Services Availability | Telecommunications Priority of Service Provisions 172

P-BCD-10.2: Telecommunications Services Availability | Separation of Primary/Alternate Providers 173

P-BCD-10.3: Telecommunications Services Availability | Provider Contingency Plan 173

P-BCD-10.4: Telecommunications Services Availability | Alternate Communications Channels 174

P-BCD-11: Data Backups 174

P-BCD-11.1: Data Backups | Testing for Reliability & Integrity 175

P-BCD-11.2: Data Backups | Separate Storage for Critical Information 175

P-BCD-11.3: Data Backups | Recovery Images 176

P-BCD-11.4: Data Backups | Cryptographic Protection 176

P-BCD-11.5: Data Backups | Test Restoration Using Sampling 176

P-BCD-11.6: Data Backups | Transfer to Alternate Storage Site 177

P-BCD-11.7: Data Backups | Redundant Secondary System 177

P-BCD-11.8: Data Backups | Dual Authorization For Backup Media Destruction 178

P-BCD-11.9: Data Backups | Backup Access 178

P-BCD-11.10: Data Backups | Backup Modification and/or Destruction 179

P-BCD-12: Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution 179

P-BCD-12.1: Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | Transaction Recovery 179

P-BCD-12.2: Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | Failover Capability 180

P-BCD-12.3: Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | Electronic Discovery (eDiscovery) 180

P-BCD-12.4: Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | Restore Within Time Period 180
P-BCD-13: Backup & Restoration Hardware Protection 181
P-BCD-13.1: Backup & Restoration Hardware Protection | Restoration Integrity Verification 181
P-BCD-14: Isolated Recovery Environment 182
P-BCD-15: Reserve Hardware 182
P-BCD-16: AI & Autonomous Technologies Incidents 183
Capacity & Performance Planning (CAP) Procedures 184
P-CAP-01: Capacity & Performance Management 184
P-CAP-02: Resource Priority 184
P-CAP-03: Capacity Planning 184
P-CAP-04: Performance Monitoring 185
P-CAP-05: Elastic Expansion 185
P-CAP-06: Regional Delivery 186
Change Management (CHG) Procedures 187
P-CHG-01: Change Management Program 187
P-CHG-02: Configuration Change Control 187
P-CHG-02.1: Configuration Change Control | Prohibition Of Changes 188
P-CHG-02.2: Configuration Change Control | Test, Validate & Document Changes 189
P-CHG-02.3: Configuration Change Control | Cybersecurity & Data Protection Representative for Asset Lifecycle Changes 189
P-CHG-02.4: Configuration Change Control | Automated Security Response 190
P-CHG-02.5: Configuration Change Control | Cryptographic Management 190
P-CHG-03: Security Impact Analysis for Changes 190
P-CHG-04: Access Restriction For Change 191
P-CHG-04.1: Access Restrictions For Change | Automated Access Enforcement/Auditing 192
P-CHG-04.2: Access Restrictions For Change | Signed Components 192
P-CHG-04.3: Access Restrictions For Change | Dual Authorization for Change 192
P-CHG-04.4: Access Restrictions For Change | Permissions To Implement Changes 193
P-CHG-04.5: Access Restrictions For Change | Library Privileges 193
P-CHG-05: Stakeholder Notification of Changes 193
P-CHG-06: Cybersecurity Functionality Verification 194
P-CHG-06.1: Cybersecurity Functionality Verification | Report Verification Results 194
P-CHG-07: Emergency Changes 195
P-CHG-07.1: Emergency Changes | Documenting Emergency Changes 195
Cloud Security (CLD) Procedures 196
P-CLD-01: Cloud Services 196
P-CLD-01.1: Cloud Services | Cloud Infrastructure Onboarding 196
P-CLD-01.2: Cloud Services | Cloud Infrastructure Offboarding 197
P-CLD-02: Cloud Security Architecture 197
P-CLD-03: Cloud Infrastructure Security Subnet 198
P-CLD-04: Application Programming Interface (API) Security 198
P-CLD-04.1: Application Programming Interface (API) Security | API Gateway 199
P-CLD-05: Virtual Machine Images 199
P-CLD-06: Multi-Tenant Environments 199
P-CLD-06.1: Multi-Tenant Environments | Customer Responsibility Matrix (CRM) 200
P-CLD-06.2: Multi-Tenant Environments | Multi-Tenant Event Logging Capabilities 200
P-CLD-06.3: Multi-Tenant Environments | Multi-Tenant Forensics Capabilities 201
P-CLD-06.4: Multi-Tenant Environments | Multi-Tenant Incident Response Capabilities 201
P-CLD-07: Data Handling & Portability 201
P-CLD-08: Standardized Virtualization Formats 202
P-CLD-09 Geolocation Requirements for Processing, Storage and Service Locations 202
P-CLD-10: Sensitive Data In Public Cloud Providers 203
P-CLD-11: Cloud Access Security Broker (CASB) 203
P-CLD-12: Side Channel Attack Prevention 204
P-CLD-13: Hosted Assets, Applications & Services 204

P-CLD-13.1: Hosted Assets, Applications & Services | Authorized Individuals For Hosted Assets, Applications & Services 204
P-CLD-13.2: Hosted Assets, Applications & Services | Sensitive/Regulated Data On Hosted Assets, Applications & Services 205
P-CLD-14: Prohibition On Unverified Hosted Assets, Applications & Services **205**
P-CLD-15: Software Defined Storage (SDS) **206**
Compliance (CPL) Procedures **207**
P-CPL-01: Statutory, Regulatory & Contractual Compliance **207**
P-CPL-01.1: Statutory, Regulatory & Contractual Compliance | Non-Compliance Oversight 207
P-CPL-01.2: Statutory, Regulatory & Contractual Compliance | Compliance Scope 208
P-CPL-01.3: Statutory, Regulatory & Contractual Compliance | Ability To Demonstrate Conformity 208
P-CPL-01.4: Statutory, Regulatory & Contractual Compliance | Conformity Assessment 209
P-CPL-01.5: Statutory, Regulatory & Contractual Compliance | Declaration of Conformity 209
P-CPL-01.6: Statutory, Regulatory & Contractual Compliance | Assessment Team Subject Matter Expertise 210
P-CPL-02: Cybersecurity & Data Protection Controls Oversight **211**
P-CPL-02.1: Cybersecurity & Data Protection Controls Oversight | Internal Audit Function 212
P-CPL-02.2: Cybersecurity & Data Protection Controls Oversight | Periodic Audits 213
P-CPL-02.3: Cybersecurity & Data Protection Controls Oversight | Corrective Action 213
P-CPL-03: Cybersecurity & Data Protection Assessments **214**
P-CPL-03.1: Cybersecurity & Data Protection Assessments| Independent Assessors 215
P-CPL-03.2: Cybersecurity & Data Protection Assessments | Functional Review Of Cybersecurity & Data Protection Controls 215
P-CPL-03.3: Cybersecurity & Data Protection Assessments | Assessor Access 216
P-CPL-03.4: Cybersecurity & Data Protection Assessments | Assessment Methods 216
P-CPL-03.5: Cybersecurity & Data Protection Assessments | Assessment Rigor 217
P-CPL-03.6: Cybersecurity & Data Protection Assessments | Evidence Request List (ERL) 217
P-CPL-03.7: Cybersecurity & Data Protection Assessments | Evidence Sampling 217
P-CPL-04: Audit Activities **218**
P-CPL-05: Legal Assessment of Investigative Inquires **218**
P-CPL-05.1: Legal Assessment of Investigative Inquires | Investigation Request Notifications 219
P-CPL-05.2: Legal Assessment of Investigative Inquires | Investigation Access Restrictions 219
P-CPL-06: Government Surveillance **220**
P-CPL-07: Grievances **220**
P-CPL-07.1: Grievances | Grievance Response 221
P-CPL-08: Localized Representation **221**
P-CPL-08.1: Localized Representation | Representative Powers 221
P-CPL-09: Control Reciprocity **222**
P-CPL-10: Control Inheritance **222**
P-CPL-11: Dual Use Technology **222**
P-CPL-11.1: Dual Use Technology | USML or CCL Identification 223
P-CPL-11.2: Dual Use Technology | Export-Controlled Access Restrictions 223
P-CPL-11.3: Dual Use Technology | Export Activities Documentation 224
P-CPL-12: Statement of Applicability (SOA) **224**
Configuration Management (CFG) Procedures **226**
P-CFG-01: Configuration Management Program **226**
P-CFG-01.1: Configuration Management Program | Assignment of Responsibility 226
P-CFG-02: Secure Baseline Configurations **227**
P-CFG-02.1: System Hardening Through Baseline Configurations | Reviews & Updates 229
P-CFG-02.2: Secure Baseline Configurations | Automated Central Management & Verification 229
P-CFG-02.3: Secure Baseline Configurations | Retention Of Previous Configurations 230
P-CFG-02.4: Secure Baseline Configurations | Development & Test Environments 230
P-CFG-02.5: Secure Baseline Configurations | Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas 231
P-CFG-02.6: Secure Baseline Configurations | Network Device Configuration File Synchronization 232
P-CFG-02.7: Secure Baseline Configurations | Approved Configuration Deviations 232
P-CFG-02.8: Secure Baseline Configurations | Respond To Unauthorized Changes 232
P-CFG-02.9: Secure Baseline Configurations | Baseline Tailoring 233

P-CFG-03: Least Functionality 233
P-CFG-03.1: Least Functionality | Periodic Review 234
P-CFG-03.2: Least Functionality | Prevent Unauthorized Software Execution 235
P-CFG-03.3: Least Functionality | Explicitly Allow / Deny Applications 235
P-CFG-03.4: Least Functionality | Split Tunneling 236
P-CFG-04: Software Usage Restrictions 236
P-CFG-04.1: Software Usage Restrictions | Open Source Software 237
P-CFG-04.2: Software Usage Restrictions | Unsupported Internet Browsers & Email Clients 237
P-CFG-05: User-Installed Software 237
P-CFG-05.1: User-Installed Software | Unauthorized Installation Alerts 238
P-CFG-05.2: User-Installed Software | Prohibit Installation Without Privileged Status 238
P-CFG-06: Configuration Enforcement 239
P-CFG-06.1: Configuration Enforcement | Integrity Assurance & Enforcement (IAE) 239
P-CFG-07: Zero-Touch Provisioning (ZTP) 239
P-CFG-08: Sensitive / Regulated Data Access Enforcement 240
P-CFG-08.1: Sensitive / Regulated Data Access Enforcement | Sensitive / Regulated Data Actions 240

Continuous Monitoring (MON) Procedures 242
P-MON-01: Continuous Monitoring 242
P-MON-01.1: Continuous Monitoring | Intrusion Detection & Prevention Systems (IDS & IPS) 243
P-MON-01.2: Continuous Monitoring | Automated Tools for Real-Time Analysis 244
P-MON-01.3: Continuous Monitoring | Inbound & Outbound Communications Traffic 244
P-MON-01.4: Continuous Monitoring | System Generated Alerts 245
P-MON-01.5: Continuous Monitoring | Wireless Intrusion Detection System (WIDS) 246
P-MON-01.6: Continuous Monitoring | Host-Based Devices 246
P-MON-01.7: Continuous Monitoring | File Integrity Monitoring (FIM) 247
P-MON-01.8: Continuous Monitoring | Security Event Monitoring 247
P-MON-01.9: Continuous Monitoring | Proxy Logging 248
P-MON-01.10: Continuous Monitoring | Deactivated Account Activity 249
P-MON-01.11: Continuous Monitoring | Automated Response To Suspicious Events 249
P-MON-01.12: Continuous Monitoring | Automated Alerts 249
P-MON-01.13: Continuous Monitoring | Alert Threshold Tuning 250
P-MON-01.14: Continuous Monitoring | Individuals Posing Greater Risk 250
P-MON-01.15: Continuous Monitoring | Privileged User Oversight 250
P-MON-01.16: Continuous Monitoring | Analyze & Prioritize Monitoring Requirements 251
P-MON-01.17: Continuous Monitoring | Real-Time Session Monitoring 251
P-MON-02: Centralized Event Log Collection 252
P-MON-02.1: Centralized Security Event Log Collection | Correlate Monitoring Information 254
P-MON-02.2: Centralized Security Event Log Collection | Central Review & Analysis 254
P-MON-02.3: Centralized Security Event Log Collection | Integration of Scanning & Other Monitoring Information 255
P-MON-02.4: Centralized Security Event Log Collection | Correlation with Physical Monitoring 255
P-MON-02.5: Centralized Security Event Log Collection | Permitted Actions 256
P-MON-02.6: Centralized Security Event Log Collection | Audit Level Adjustment 256
P-MON-02.7: Centralized Security Event Log Collection | System-Wide/Time-Correlated Audit Trail 257
P-MON-02.8: Centralized Security Event Log Collection | Changes by Authorized Individuals 257
P-MON-02.9: Centralized Security Event Log Collection | Inventory of Technology Asset Event Logging 257
P-MON-03: Content of Event Logs 258
P-MON-03.1: Content Of Event Logs | Sensitive Audit Information 259
P-MON-03.2: Content Of Event Logs | Audit Trails 259
P-MON-03.3: Content Of Event Logs | Privileged Functions Logging 260
P-MON-03.4: Content Of Event Logs | Verbosity Logging for Boundary Devices 261
P-MON-03.5: Content Of Event Logs | Limit Personal Data (PD) In Audit Records 261
P-MON-03.6: Content Of Event Logs | Centralized Management of Planned Audit Record Content 261
P-MON-03.7: Content Of Event Logs | Database Logging 262
P-MON-04: Event Log Storage Capacity 262
P-MON-05: Response To Event Log Processing Failures 263
P-MON-05.1: Response To Audit Processing Failures | Real-Time Alerts of Event Logging Failure 263

P-MON-05.2: Response To Audit Processing Failures | Event Log Storage Capacity Alerting 264
P-MON-06: Monitoring Reporting 264
P-MON-06.1: Monitoring Reporting | Query Parameter Audits of Personal Data 265
P-MON-06.2: Monitoring Reporting | Trend Analysis Reporting 265
P-MON-07: Time Stamps 266
P-MON-07.1: Time Stamps | Synchronization With Authoritative Time Source 266
P-MON-08: Protection of Event Logs 267
P-MON-08.1: Protection of Event Logs | Event Log Backup on Separate Physical Systems / Components 267
P-MON-08.2: Protection of Event Logs | Access by Subset of Privileged Users 268
P-MON-08.3: Protection of Event Logs | Cryptographic Protection of Event Log Information 268
P-MON-08.4: Protection of Event Logs | Dual Authorization for Event Log Movement 268
P-MON-09: Non-Repudiation 269
P-MON-09.1: Non-Repudiation | Identity Binding 269
P-MON-10: Event Log Retention 270
P-MON-11: Monitoring For Information Disclosure 270
P-MON-11.1: Monitoring For Information Disclosure | Analyze Traffic for Covert Exfiltration 271
P-MON-11.2: Monitoring For Information Disclosure | Unauthorized Network Services 271
P-MON-11.3: Monitoring For Information Disclosure | Monitoring for Indicators of Compromise (IOC) 271
P-MON-12: Session Audit 272
P-MON-13: Alternate Event Logging Capability 272
P-MON-14: Cross-Organizational Monitoring 273
P-MON-14.1: Cross-Organizational Monitoring | Sharing of Event Logs 273
P-MON-15: Covert Channel Analysis 273
P-MON-16: Anomalous Behavior 274
P-MON-16.1: Anomalous Behavior | Insider Threats 274
P-MON-16.2: Anomalous Behavior | Third-Party Threats 275
P-MON-16.3: Anomalous Behavior | Unauthorized Activities 275
P-MON-16.4: Anomalous Behavior | Account Creation and Modification Logging 275
P-MON-17: Event Log Analysis & Triage 276
P-MON-17.1: Event Log Analysis & Triage | Event Log Review Escalation Matrix 276
P-MON-18: File Activity Monitoring (FAM) 276
Cryptographic Protections (CRY) Procedures 278
P-CRY-01: Use of Cryptographic Controls 278
P-CRY-01.1: Use of Cryptographic Controls | Alternate Physical Protection 279
P-CRY-01.2: Use of Cryptographic Controls | Export-Controlled Cryptography 279
P-CRY-01.3: Use of Cryptographic Controls | Pre/Post Transmission Handling 280
P-CRY-01.4: Use of Cryptographic Controls | Conceal/Randomize Communications 280
P-CRY-01.5: Use of Cryptographic Controls | Cryptographic Cipher Suites and Protocols Inventory 280
P-CRY-02: Cryptographic Module Authentication 281
P-CRY-03: Transmission Confidentiality 281
P-CRY-04: Transmission Integrity 282
P-CRY-05: Encrypting Data At Rest 282
P-CRY-05.1: Encrypting Data At Rest | Storage Media 283
P-CRY-05.2: Encrypting Data at Rest | Offline Storage 283
P-CRY-05.3: Encrypting Data at Rest | Database Encryption 284
P-CRY-06: Non-Console Administrative Access 284
P-CRY-07: Wireless Access Authentication & Encryption 284
P-CRY-08: Public Key Infrastructure (PKI) 285
P-CRY-08.1: Public Key Infrastructure (PKI) | Availability 285
P-CRY-09: Cryptographic Key Management 286
P-CRY-09.1: Cryptographic Key Management | Symmetric Keys 287
P-CRY-09.2: Cryptographic Key Management | Asymmetric Keys 287
P-CRY-09.3: Cryptographic Key Management | Cryptographic Key Loss or Change 288
P-CRY-09.4: Cryptographic Key Management | Control & Distribution of Cryptographic Keys 288
P-CRY-09.5: Cryptographic Key Management | Assigned Owners 289
P-CRY-09.6: Cryptographic Key Management | Third-Party Cryptographic Keys 289
P-CRY-09.7: Cryptographic Key Management | External System Cryptographic Key Control 289

P-CRY-10: Transmission of Cybersecurity & Data Protection Attributes 290
P-CRY-11: Certificate Authorities 290
P-CRY-12: Certificate Monitoring 290
P-CRY-13: Cryptographic Hash 291
Data Classification & Handling (DCH) Procedures 292
P-DCH-01: Data Protection 292
P-DCH-01.1: Data Protection | Data Stewardship 292
P-DCH-01.2: Data Protection | Sensitive/Regulated Data Protection 292
P-DCH-01.3: Data Protection | Sensitive / Regulated Media Records 293
P-DCH-01.4: Data Protection | Defining Access Authorizations for Sensitive / Regulated Data 293
P-DCH-02: Data & Asset Classification 294
P-DCH-02.1: Data & Asset Classification | Highest Classification Level 294
P-DCH-03: Media Access 295
P-DCH-03.1: Media Access | Disclosure of Information 296
P-DCH-03.2: Media Access | Masking Displayed Data 296
P-DCH-03.3: Media Access | Controlled Release 297
P-DCH-04: Media Marking 297
P-DCH-04.1: Media Marking | Automated Marking 297
P-DCH-05: Cybersecurity & Data Protection Attributes 298
P-DCH-05.1: Cybersecurity & Data Protection Attributes | Dynamic Attribute Association 298
P-DCH-05.2: Cybersecurity & Data Protection Attributes | Attribute Value Changes By Authorized Individuals 299
P-DCH-05.3: Cybersecurity & Data Protection Attributes | Maintenance of Attribute Associations By System 299
P-DCH-05.4: Cybersecurity & Data Protection Attributes | Association of Attributes By Authorized Individuals 299
P-DCH-05.5: Cybersecurity & Data Privacy Protection | Attribute Displays for Output Devices 300
P-DCH-05.6: Cybersecurity & Data Protection Attributes | Data Subject Attribute Associations 300
P-DCH-05.7: Cybersecurity & Data Protection Attributes | Consistent Attribute Interpretation 301
P-DCH-05.8: Cybersecurity & Data Protection Attributes | Identity Association Techniques & Technologies 301
P-DCH-05.9: Cybersecurity & Data Protection Attributes | Attribute Reassignment 301
P-DCH-05.10: Cybersecurity & Data Protection Attributes | Attribute Configuration By Authorized Individuals 302
P-DCH-05.11: Cybersecurity & Data Protection Attributes | Audit Changes 302
P-DCH-06: Media Storage 303
P-DCH-06.1: Media Storage | Physically Secure All Media 303
P-DCH-06.2: Media Storage | Sensitive Data Inventories 304
P-DCH-06.3: Media Storage | Periodic Scans for Sensitive / Regulated Data 304
P-DCH-06.4: Media Storage | Making Sensitive Data Unreadable In Storage 304
P-DCH-06.5: Media Storage | Storing Authentication Data 305
P-DCH-07: Media Transportation 306
P-DCH-07.1: Media Transportation | Custodians 306
P-DCH-07.2: Media Transportation | Encrypting Data In Storage Media 307
P-DCH-08: Physical Medial Disposal 307
P-DCH-09: System Media Sanitization 308
P-DCH-09.1: System Media Sanitization | System Media Sanitization Documentation 309
P-DCH-09.2: System Media Sanitization | Equipment Testing 309
P-DCH-09.3: System Media Sanitization | Sanitization of Personal Data (PD) 309
P-DCH-09.4: System Media Sanitization | First Time Use Sanitization 310
P-DCH-09.5: System Media Sanitization | Dual Authorization for Sensitive Data Destruction 310
P-DCH-10: Media Use 310
P-DCH-10.1: Media Use | Limitations on Use 311
P-DCH-10.2: Media Use | Prohibit Use Without Owner 312
P-DCH-11: Data Reclassification 312
P-DCH-12: Removable Media Security 312
P-DCH-13: Use of External Technology Assets, Applications and/or Services (TAAS) 313
P-DCH-13.1: Use of External Technology Assets, Applications and/or Services (TAAS) | Limits of Authorized Use 313
P-DCH-13.2: Use of External Technology Assets, Applications and/or Services (TAAS) | Portable Storage Devices 314
P-DCH-13.3: Use of External Technology Assets, Applications and/or Services (TAAS) | Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS) 315

P-DCH-13.4: Use of External Technology Assets, Applications and/or Services (TAAS) | Non-Organizationally Owned Technology Assets, Applications and/or Services (TAAS) 315
P-DCH-14: Information Sharing 316
P-DCH-14.1: Information Sharing | Information Search & Retrieval 317
P-DCH-14.2: Information Sharing | Transfer Authorizations 317
P-DCH-14.3: Information Sharing | Data Access Mapping 317
P-DCH-15: Publicly Accessible Content 318
P-DCH-16: Data Mining Protection 318
P-DCH-17: Ad-Hoc Transfers 319
P-DCH-18: Media & Data Retention 319
P-DCH-18.1: Media & Data Retention | Minimize Sensitive / Regulated Data 320
P-DCH-18.2: Media & Data Retention | Limit Sensitive / Regulated Data In Testing, Training & Research) 321
P-DCH-18.3: Media & Data Retention | Temporary Files Containing Personal Data 321
P-DCH-19: Geographic Location of Data 322
P-DCH-20: Archived Data Sets 322
P-DCH-21: Information Disposal 323
P-DCH-22: Data Quality Operations 323
P-DCH-22.1: Data Quality Operations | Updating & Correcting Personal Data (PD) 324
P-DCH-22.2: Data Quality Operations | Data Tags 324
P-DCH-22.3: Data Quality Operations | Primary Source Personal Data (PD) Collection 324
P-DCH-23: De-Identification (Anonymization) 325
P-DCH-23.1: De-Identification (Anonymization) | De-Identify Dataset Upon Collection 325
P-DCH-23.2: De-Identification (Anonymization) | Archiving 325
P-DCH-23.3: De-Identification (Anonymization) | Release 326
P-DCH-23.4: De-Identification (Anonymization) | Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers 326
P-DCH-23.5: De-Identification (Anonymization) | Statistical Disclosure Control 327
P-DCH-23.6: De-Identification (Anonymization) | Differential Data Privacy 327
P-DCH-23.7: De-Identification (Anonymization) | Automated De-Identification of Sensitive Data 327
P-DCH-23.8: De-Identification (Anonymization) | Motivated Intruder 328
P-DCH-23.9: De-Identification (Anonymization) | Code Names 328
P-DCH-24: Information Location 329
P-DCH-24.1: Information Location | Automated Tools to Support Information Location 329
P-DCH-25: Transfer of Sensitive and/or Regulated Data 330
P-DCH-25.1: Transfer of Sensitive and/or Regulated Data | Transfer Activity Limits 330
P-DCH-26: Data Localization 330
P-DCH-27: Data Rights Management (DRM) 331
Embedded Technology (EMB) Procedures 332
P-EMB-01: Embedded Technology Security Program 332
P-EMB-02: Internet of Things (IoT) 332
P-EMB-03: Operational Technology (OT) 333
P-EMB-04: Interface Security 333
P-EMB-05: Embedded Technology Configuration Monitoring 334
P-EMB-06: Prevent Alterations 335
P-EMB-07: Embedded Technology Maintenance 335
P-EMB-08: Resilience To Outages 335
P-EMB-09: Power Level Monitoring 336
P-EMB-10: Embedded Technology Reviews 336
P-EMB-11: Message Queuing Telemetry Transport (MQTT) Security 337
P-EMB-12: Restrict Communications 337
P-EMB-13: Authorized Communications 337
P-EMB-14: Operating Environment Certification 338
P-EMB-15: Safety Assessment 338
P-EMB-16: Certificate-Based Authentication 338
P-EMB-17: Chip-To-Cloud Security 339
P-EMB-18: Real-Time Operating System (RTOS) Security 339
P-EMB-19: Safe Operations 339

ENDPOINT SECURITY (END) PROCEDURES 341
P-END-01: ENDPOINT DEVICE MANAGEMENT (EDM) 341
P-END-01.1: ENDPOINT DEVICE MANAGEMENT (EDM) | UNIFIED ENDPOINT DEVICE MANAGEMENT (UEDM) 341
P-END-02: UNIFIED ENDPOINT DEVICE MANAGEMENT (UEDM) 342
P-END-03: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS 343
P-END-03.1: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS | SOFTWARE INSTALLATION ALERTS 343
P-END-03.2: PROHIBIT INSTALLATION WITHOUT PRIVILEGED STATUS | GOVERNING ACCESS RESTRICTION FOR CHANGE 343
P-END-04: MALICIOUS CODE PROTECTION (ANTI-MALWARE) 344
P-END-04.1: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | AUTOMATIC ANTIMALWARE SIGNATURE UPDATES 345
P-END-04.2: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | DOCUMENTED PROTECTION MEASURES 345
P-END-04.3: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | CENTRALIZED MANAGEMENT OF ANTIMALWARE TECHNOLOGIES 346
P-END-04.4: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | NONSIGNATURE-BASED DETECTION 346
P-END-04.5: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | MALWARE PROTECTION MECHANISM TESTING 346
P-END-04.6: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | EVOLVING MALWARE THREATS 347
P-END-04.7: MALICIOUS CODE PROTECTION (ANTI-MALWARE) | ALWAYS ON PROTECTION 347
P-END-05: SOFTWARE FIREWALL 348
P-END-06: ENDPOINT FILE INTEGRITY MONITORING (FIM) 348
P-END-06.1: ENDPOINT FILE INTEGRITY MONITORING (FIM) | INTEGRITY CHECKS 349
P-END-06.2: ENDPOINT FILE INTEGRITY MONITORING (FIM) | ENDPOINT DETECTION & RESPONSE (EDR) 349
P-END-06.3: ENDPOINT FILE INTEGRITY MONITORING (FIM) | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS 349
P-END-06.4: ENDPOINT FILE INTEGRITY MONITORING (FIM) | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS 350
P-END-06.5: ENDPOINT FILE INTEGRITY MONITORING (FIM) | VERIFY BOOT PROCESS 350
P-END-06.6: ENDPOINT FILE INTEGRITY MONITORING (FIM) | PROTECTION OF BOOT FIRMWARE 351
P-END-06.7: ENDPOINT FILE INTEGRITY MONITORING (FIM) | BINARY OR MACHINE-EXECUTABLE CODE 351
P-END-06.8: ENDPOINT FILE INTEGRITY MONITORING (FIM) | EXTENDED DETECTION & RESPONSE (XDR) 351
P-END-07: HOST INTRUSION DETECTION AND PREVENTION SYSTEMS (HIDS/HIPS) 352
P-END-08: PHISHING & SPAM PROTECTION 352
P-END-08.1: PHISHING & SPAM PROTECTION | CENTRAL MANAGEMENT 353
P-END-08.2: PHISHING & SPAM PROTECTION | AUTOMATIC SPAM AND PHISHING PROTECTION UPDATES 353
P-END-09: TRUSTED PATH 353
P-END-10: MOBILE CODE 354
P-END-11: THIN NODES 355
P-END-12: PORT & INPUT/OUTPUT (I/O) DEVICE ACCESS 355
P-END-13: SENSOR CAPABILITY 355
P-END-13.1: SENSOR CAPABILITY | AUTHORIZED USE 356
P-END-13.2: SENSOR CAPABILITY | NOTICE OF COLLECTION 356
P-END-13.3: SENSOR CAPABILITY | COLLECTION MINIMIZATION 357
P-END-13.4: SENSOR CAPABILITY | SENSOR DELIVERY VERIFICATION 357
P-END-14: COLLABORATIVE COMPUTING DEVICES 357
P-END-14.1: COLLABORATIVE COMPUTING DEVICES | DISABLING/REMOVAL IN SECURE WORK AREAS 358
P-END-14.2: COLLABORATIVE COMPUTING DEVICES | EXPLICITLY INDICATE CURRENT PARTICIPANTS 358
P-END-14.3: COLLABORATIVE COMPUTING DEVICES | PARTICIPANT IDENTITY VERIFICATION 359
P-END-14.4: COLLABORATIVE COMPUTING DEVICES | PARTICIPANT CONNECTION MANAGEMENT 360
P-END-14.5: COLLABORATIVE COMPUTING DEVICES | MALICIOUS LINK & FILE PROTECTIONS 360
P-END-14.6: COLLABORATIVE COMPUTING DEVICES | EXPLICIT INDICATION OF USE 361
P-END-15: HYPERVISOR ACCESS 361
P-END-16: RESTRICT ACCESS TO SECURITY FUNCTIONS 362
P-END-16.1: RESTRICT ACCESS TO SECURITY FUNCTIONS| HOST-BASED SECURITY FUNCTION ISOLATION 362
HUMAN RESOURCES SECURITY (HRS) PROCEDURES 364
P-HRS-01: HUMAN RESOURCES SECURITY MANAGEMENT 364
P-HRS-01.1: HUMAN RESOURCES SECURITY MANAGEMENT | ONBOARDING, TRANSFERRING & OFFBOARDING PERSONNEL 365
P-HRS-02: POSITION CATEGORIZATION 366
P-HRS-02.1: POSITION CATEGORIZATION | USERS WITH ELEVATED PRIVILEGES 367
P-HRS-02.2: POSITION CATEGORIZATION | PROBATIONARY PERIODS 367
P-HRS-03: DEFINED ROLES & RESPONSIBILITIES 368
P-HRS-03.1: DEFINED ROLES & RESPONSIBILITIES | USER AWARENESS 368
P-HRS-03.2: DEFINED ROLES & RESPONSIBILITIES | COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS 369

P-HRS-04: Personnel Screening 369
P-HRS-04.1: Personnel Screening | Roles With Special Protection Measures 370
P-HRS-04.2: Personnel Screening | Formal Indoctrination 370
P-HRS-04.3: Personnel Screening | Citizenship Requirements 371
P-HRS-04.4: Personnel Screening | Citizenship Identification 371
P-HRS-05: Terms of Employment 371
P-HRS-05.1: Terms of Employment | Rules of Behavior 372
P-HRS-05.2: Terms of Employment | Social Media & Social Networking Restrictions 373
P-HRS-05.3: Terms of Employment | Technology Use Restrictions 373
P-HRS-05.4: Terms of Employment | Use of Critical Technologies 374
P-HRS-05.5: Terms of Employment | Use of Mobile Devices 374
P-HRS-05.6: Terms of Employment | Security-Minded Dress Code 375
P-HRS-05.7: Terms of Employment | Policy Familiarization & Acknowledgement 375
P-HRS-06: Access Agreements 375
P-HRS-06.1: Access Agreements | Confidentiality Agreements 376
P-HRS-06.2: Access Agreements | Post-Employment Requirements Awareness 376
P-HRS-07: Personnel Sanctions 377
P-HRS-07.1: Personnel Sanctions | Workplace Investigations 377
P-HRS-07.2: Personnel Sanctions | Updating Disciplinary Processes 378
P-HRS-07.3: Personnel Sanctions | Preventative Access Restriction 378
P-HRS-08: Personnel Transfer 379
P-HRS-09: Personnel Termination 379
P-HRS-09.1: Personnel Termination | Asset Collection 380
P-HRS-09.2: Personnel Termination | High-Risk Terminations 381
P-HRS-09.3: Personnel Termination | Post-Employment Requirements Notification 381
P-HRS-09.4: Personnel Termination | Automated Employment Status Notification 382
P-HRS-10: Third-Party Personnel Security 382
P-HRS-11: Separation of Duties (SoD) 383
P-HRS-12: Incompatible Roles 383
P-HRS-12.1: Incompatible Roles | Two-Person Rule 384
P-HRS-13: Identify Critical Skills & Gaps 384
P-HRS-13.1: Identify Critical Skills & Gaps | Remediate Identified Skills Deficiencies 385
P-HRS-13.2: Identify Critical Skills & Gaps | Identify Vital Cybersecurity & Data Privacy Staff 385
P-HRS-13.3: Identify Critical Skills & Gaps | Establish Redundancy for Vital Cybersecurity & Data Privacy Staff 385
P-HRS-13.4: Identify Critical Skills & Gaps | Perform Succession Planning 386
P-HRS-14: Identifying Authorized Work Locations 386
P-HRS-14.1: Identifying Authorized Work Locations | Communicating Authorized Work Locations 387
P-HRS-15: Reporting Suspicious Activities 387
Identification & Authentication (IAC) Procedures 388
P-IAC-01: Identity & Access Management (IAM) 388
P-IAC-01.1: Identity & Access Management (IAM) | Retain Access Records 388
P-IAC-01.2: Identity & Access Management (IAM) | Authenticate, Authorize and Audit (AAA) 389
P-IAC-01.3: Identity & Access Management (IAM) | User & Service Account Inventories 389
P-IAC-02: Identification & Authentication for Organizational Users 390
P-IAC-02.1: Identification & Authentication for Organizational Users | Group Authentication 390
P-IAC-02.2: Identification & Authentication for Organizational Users | Replay-Resistant Authentication 391
P-IAC-02.3: Identification & Authentication for Organizational Users | Acceptance of PIV Credentials 391
P-IAC-02.4: Identification & Authentication for Organizational Users | Out-of-Band Authentication (OOBA) 391
P-IAC-03: Identification & Authentication for Non-Organizational Users 392
P-IAC-03.1: Identification & Authentication for Non-Organizational Users | Acceptance of PIV Credentials from Other Organizations 392
P-IAC-03.2: Identification & Authentication for Non-Organizational Users | Acceptance of Third-Party Credentials 393
P-IAC-03.3: Identification & Authentication for Non-Organizational Users | Use of FICAM-Issued Profiles 393
P-IAC-03.4: Identification & Authentication for Non-Organizational Users | Disassociability 393
P-IAC-03.5: Identification & Authentication for Non-Organizational Users | Acceptance of External Authenticators 394

P-IAC-04: Identification & Authentication for Devices **394**
P-IAC-04.1: Identification & Authentication for Devices | Device Attestation *395*
P-IAC-04.2: Identification & Authentication for Devices | Device Authorization Enforcement *395*
P-IAC-05: Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS) **396**
P-IAC-05.1: Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS) | Information Exchange *396*
P-IAC-05.2: Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS) | Privileged Access by Non-Organizational Users *396*
P-IAC-06: Multi-Factor Authentication (MFA) **397**
P-IAC-06.1: Multi-Factor Authentication (MFA) | Network Access to Privileged Accounts *397*
P-IAC-06.2: Multi-Factor Authentication (MFA) | Network Access to Non-Privileged Accounts *398*
P-IAC-06.3: Multi-Factor Authentication (MFA) | Local Access to Privileged Accounts *398*
P-IAC-06.4: Multi-Factor Authentication (MFA) | Out of Band (OOB) Factor *399*
P-IAC-06.5: Multi-Factor Authentication (MFA) | Alternative Multi-Factor Authentication *399*
P-IAC-07: User Provisioning & De-Provisioning **399**
P-IAC-07.1: User Provisioning & De-Provisioning | Change of Roles & Duties *400*
P-IAC-07.2: User Provisioning & De-Provisioning | Termination of Employment *401*
P-IAC-08: Role-Based Access Control (RBAC) **401**
P-IAC-09: Identifier Management (User Names) **402**
P-IAC-09.1: Identifier Management | User Identity (ID) Management *404*
P-IAC-09.2: Identifier Management | Identity User Status *404*
P-IAC-09.3: Identifier Management | Dynamic Management *405*
P-IAC-09.4: Identifier Management | Cross-Organization Management *405*
P-IAC-09.5: Identifier Management | Privileged Account Identifiers *405*
P-IAC-09.6: Identifier Management | Pairwise Pseudonymous Identifiers (PPID) *407*
P-IAC-10: Authenticator Management **407**
P-IAC-10.1: Authenticator Management | Password-Based Authentication *408*
P-IAC-10.2: Authenticator Management | PKI-Based Authentication *410*
P-IAC-10.3: Authenticator Management | In-Person or Trusted Third-Party Registration *410*
P-IAC-10.4: Authenticator Management | Automated Support For Password Strength *411*
P-IAC-10.5: Authenticator Management | Protection of Authenticators *411*
P-IAC-10.6: Authenticator Management | No Embedded Unencrypted Static Authenticators *412*
P-IAC-10.7: Authenticator Management | Hardware Token-Based Authentication *412*
P-IAC-10.8: Authenticator Management | Vendor-Supplied Defaults *412*
P-IAC-10.9: Authenticator Management | Multiple System Accounts *413*
P-IAC-10.10: Authenticator Management | Expiration of Cached Authenticators *413*
P-IAC-10.11: Authenticator Management | Password Managers *413*
P-IAC-10.12: Authenticator Management | Biometric Authentication *414*
P-IAC-10.13: Authenticator Management | Events Requiring Authenticator Change *414*
P-IAC-10.14: Authenticator Management | Passkeys *415*
P-IAC-11: Authenticator Feedback **415**
P-IAC-12: Cryptographic Module Authentication **416**
P-IAC-12.1: Cryptographic Module Authentication | Hardware Security Modules (HSM) *416*
P-IAC-13: Adaptive Identification & Authentication **416**
P-IAC-13.1: Adaptive Identification & Authentication | Single Sign-On (SSO) Transparent Authentication *417*
P-IAC-13.2: Adaptive Identification & Authentication | Federated Credential Management *417*
P-IAC-13.3: Adaptive Identification & Authentication | Continuous Authentication *417*
P-IAC-14: Re-Authentication **418**
P-IAC-15: Account Management **418**
P-IAC-15.1: Account Management | Automated System Account Management (Directory Services) *420*
P-IAC-15.2: Account Management | Removal of Temporary/Emergency Accounts *421*
P-IAC-15.3: Account Management | Disable Inactive Accounts *421*
P-IAC-15.4: Account Management | Automated Audit Actions *422*
P-IAC-15.5: Account Management | Restrictions on Shared Groups/Accounts *422*
P-IAC-15.6: Account Management | Account Disabling for High Risk Individuals *422*
P-IAC-15.7: Account Management | System Account Reviews *423*
P-IAC-15.8: Account Management | Usage Conditions *423*

P-IAC-15.9: Account Management | Emergency Accounts 424
P-IAC-16: Privileged Account Management (PAM) 424
P-IAC-16.1: Privileged Account Management (PAM) | Privileged Account Inventories 425
P-IAC-16.2: Privileged Account Management (PAM) | Privileged Account Separation 425
P-IAC-16.3: Privileged Account Management (PAM) | Privileged Command Execution 426
P-IAC-16.4: Privileged Account Management (PAM) | Dedicated Privileged Account 426
P-IAC-17: Periodic Review of Account Privileges 427
P-IAC-18: User Responsibilities for Account Management 427
P-IAC-19: Credential Sharing 428
P-IAC-20: Access Enforcement 428
P-IAC-20.1: Access Enforcement | Access To Sensitive Data 430
P-IAC-20.2: Access Enforcement | Database Access 431
P-IAC-20.3: Access Enforcement | Use of Privileged Utility Programs 431
P-IAC-20.4: Access Enforcement | Dedicated Administrative Machines 431
P-IAC-20.5: Access Enforcement | Dual Authorization for Privileged Commands 432
P-IAC-20.6: Access Enforcement | Revocation of Access Authorizations 432
P-IAC-20.7: Access Enforcement | Authorized System Accounts 433
P-IAC-21: Least Privilege 433
P-IAC-21.1: Least Privilege | Authorize Access to Security Functions 434
P-IAC-21.2: Least Privilege | Non-Privileged Access for Non-Security Functions 434
P-IAC-21.3: Least Privilege | Management Approval For Privileged Accounts 435
P-IAC-21.4: Least Privilege | Auditing Use of Privileged Functions 435
P-IAC-21.5: Least Privilege | Prohibit Non-Privileged Users from Executing Privileged Functions 436
P-IAC-21.6: Least Privilege | Network Access to Privileged Commands 436
P-IAC-21.7: Least Privilege | Privilege Levels for Code Execution 437
P-IAC-22: Account Lockout 437
P-IAC-23: Concurrent Session Control 438
P-IAC-24: Session Lock 438
P-IAC-24.1: Session Lock | Pattern-Hiding Displays 439
P-IAC-25: Session Termination 439
P-IAC-25.1: Session Termination | User-Initiated Logouts/Message Displays 440
P-IAC-26: Permitted Actions Without Identification or Authorization 440
P-IAC-27: Reference Monitor 440
P-IAC-28: Identity Proofing (Identity Verification) 441
P-IAC-28.1: Identity Proofing (Identity Verification) | Management Approval For New or Changed Accounts 441
P-IAC-28.2: Identity Proofing (Identity Verification) | Identity Evidence 442
P-IAC-28.3: Identity Proofing (Identity Verification) | Identity Evidence Validation & Verification 442
P-IAC-28.4: Identity Proofing (Identity Verification) | In-Person Validation & Verification 442
P-IAC-28.5: Identity Proofing (Identity Verification) | Address Confirmation 443
P-IAC-29: Attribute-Based Access Control (ABAC) 443
P-IAC-29.1: Attribute-Based Access Control (ABAC) | Real-Time Access Decisions 444
P-IAC-29.2: Attribute-Based Access Control (ABAC) | Access Profile Rules 444
Incident Response (IRO) Procedures 445
P-IRO-01: Incidents Response Operations 445
P-IRO-02: Incident Handling 445
P-IRO-02.1: Incident Handling | Automated Incident Handling Processes 446
P-IRO-02.2: Incident Handling | Insider Threat Response Capability 446
P-IRO-02.3: Incident Handling | Dynamic Reconfiguration 447
P-IRO-02.4: Incident Handling | Incident Classification & Prioritization 447
P-IRO-02.5: Incident Handling | Correlation with External Organizations 449
P-IRO-02.6: Incident Handling | Automatic Disabling of Technology Assets, Applications and/or Services (TAAS) 450
P-IRO-03: Indicators of Compromise (IOC) 450
P-IRO-04: Incident Response Plan (IRP) 450
P-IRO-04.1: Incident Response Plan (IRP) | Data Breach 451
P-IRO-04.2: Incident Response Plan (IRP) | IRP Update 452
P-IRO-04.3: Incident Response Plan (IRP) | Continuous Incident Response Improvements 452
P-IRO-05: Incident Response Training 452

P-IRO-05.1: Incident Response Training | Simulated Incidents 453
P-IRO-05.2: Incident Response Training | Automated Incident Response Training Environments 453
P-IRO-06: Incident Response Testing 454
P-IRO-06.1: Incident Response Testing | Coordination with Related Plans 454
P-IRO-07: Integrated Security Incident Response Team (ISIRT) 455
P-IRO-08: Chain of Custody & Forensics 455
P-IRO-09: Situational Awareness For Incidents 456
P-IRO-09.1: Situational Awareness For Incidents | Automated Tracking, Data Collection & Analysis 456
P-IRO-09.2: Situational Awareness For Incidents | Recurring Incident Analysis 456
P-IRO-10: Incident Stakeholder Reporting 457
P-IRO-10.1: Incident Stakeholder Reporting | Automated Reporting 458
P-IRO-10.2: Incident Stakeholder Reporting | Cyber Incident Reporting for Sensitive / Regulated Data 458
P-IRO-10.3: Incident Stakeholder Reporting | Vulnerabilities Related To Incidents 459
P-IRO-10.4: Incident Stakeholder Reporting | Supply Chain Coordination 459
P-IRO-10.5: Incident Stakeholder Reporting | Serious Incident Reporting 460
P-IRO-11: Incident Reporting Assistance 461
P-IRO-11.1: Incident Reporting Assistance | Automation Support of Availability of Information/Support 461
P-IRO-11.2: Incident Reporting Assistance | Coordination With External Providers 462
P-IRO-12: Sensitive / Regulated Data Spill Response 462
P-IRO-12.1: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Responsible Personnel 463
P-IRO-12.2: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Spill Training 463
P-IRO-12.3: Sensitive / Regulated Data Spill Response | Post-Sensitive / Regulated Data Spill Operations 463
P-IRO-12.4: Sensitive / Regulated Data Spill Response | Sensitive / Regulated Data Exposure to Unauthorized Personnel 464
P-IRO-13: Root Cause Analysis (RCA) & Lessons Learned 464
P-IRO-14: Regulatory & Law Enforcement Contacts 464
P-IRO-15: Detonation Chambers (Sandboxes) 465
P-IRO-16: Public Relations & Reputation Repair 465
Information Assurance (IAO) Procedures 467
P-IAO-01: Information Assurance (IA) Operations 467
P-IAO-01.1: Information Assurance (IA) Operations | Assessment Boundaries 467
P-IAO-02: Assessments 468
P-IAO-02.1: Assessments | Independent Assessors 469
P-IAO-02.2: Assessments | Specialized Assessments 469
P-IAO-02.3: Assessments | Third-Party Assessments 470
P-IAO-02.4: Assessments | Security Assessment Report (SAR) 470
P-IAO-03: System Security & Privacy Plan (SSPP) 471
P-IAO-03.1: System Security & Privacy Plan (SSPP) | Plan/Coordinate with Other Organizational Entities 473
P-IAO-03.2: System Security & Privacy Plan (SSPP)| Adequate Security for Sensitive / Regulated Data In Support of Contracts 473
P-IAO-04: Threat Analysis & Flaw Remediation During Development 474
P-IAO-05: Plan of Action & Milestones (POA&M) 475
P-IAO-05.1: Plan of Action & Milestones (POA&M) | POA&M Automation 476
P-IAO-06: Technical Verification 476
P-IAO-07: Security Authorization 477
Maintenance (MNT) Procedures 478
P-MNT-01: Maintenance Operations 478
P-MNT-02: Controlled Maintenance 478
P-MNT-02.1: Controlled Maintenance | Automated Maintenance Activities 479
P-MNT-03: Timely Maintenance 479
P-MNT-03.1: Timely Maintenance | Preventative Maintenance 479
P-MNT-03.2: Timely Maintenance | Predictive Maintenance 480
P-MNT-03.3: Timely Maintenance | Automated Support for Predictive Maintenance 480
P-MNT-04: Maintenance Tools 481
P-MNT-04.1: Maintenance Tools | Inspect Tools 481
P-MNT-04.2: Maintenance Tools | Inspect Media 482
P-MNT-04.3: Maintenance Tools | Prevent Unauthorized Removal 482

P-MNT-04.4: Maintenance Tools | Restrict Tool Use 482
P-MNT-05: Remote Maintenance 483
P-MNT-05.1: Remote Maintenance | Auditing Remote Maintenance 483
P-MNT-05.2: Remote Maintenance | Remote Maintenance Notifications 484
P-MNT-05.3: Remote Maintenance | Remote Maintenance Cryptographic Protection 484
P-MNT-05.4: Remote Maintenance | Remote Maintenance Disconnect Verification 484
P-MNT-05.5: Remote Maintenance | Remote Maintenance Pre-Approval 485
P-MNT-05.6: Remote Maintenance | Remote Maintenance Comparable Security & Sanitization 485
P-MNT-05.7: Remote Maintenance | Separation of Maintenance Sessions 486
P-MNT-06: Maintenance Personnel 486
P-MNT-06.1: Maintenance Personnel | Maintenance Personnel Without Appropriate Access 486
P-MNT-06.2: Maintenance Personnel | Non-System Related Maintenance 487
P-MNT-07: Maintain Configuration Control During Maintenance 487
P-MNT-08: Field Maintenance 488
P-MNT-09: Off-Site Maintenance 488
P-MNT-10: Maintenance Validation 488
P-MNT-11: Maintenance Monitoring 489
Mobile Device Management (MDM) Procedures 490
P-MDM-01: Centralized Management Of Mobile Devices 490
P-MDM-02: Access Control For Mobile Devices 490
P-MDM-03: Full Device & Container-Based Encryption 491
P-MDM-04: Tamper Protection & Detection 492
P-MDM-05: Remote Purging 492
P-MDM-06: Personally-Owned Mobile Devices 492
P-MDM-07: Organization-Owned Mobile Devices 493
P-MDM-08: Mobile Device Data Retention Limitations 494
P-MDM-09: Mobile Device Geofencing 494
P-MDM-10: Separate Mobile Device Profiles 495
P-MDM-11: Restricting Access To Authorized Assets, Applications & Services 495
Network Security (NET) Procedures 496
P-NET-01: Network Security Controls (NSC) 496
P-NET-01.1: Network Security Controls (NSC) | Zero Trust Architecture (ZTA) 496
P-NET-02: Layered Defenses 497
P-NET-02.1: Layered Defenses | Denial of Service (DoS) Protection 497
P-NET-02.2: Layered Defenses | Guest Networks 498
P-NET-02.3: Layered Defenses | Cross Domain Solutions (CDS) 498
P-NET-03: Boundary Protection 499
P-NET-03.1: Boundary Protection | Limit Network Connections 500
P-NET-03.2: Boundary Protection | External Telecommunications Services 500
P-NET-03.3: Boundary Protection | Prevent Discovery of Internal Information 501
P-NET-03.4: Boundary Protection | Personal Data (PD) 501
P-NET-03.5: Boundary Protection | Prevent Unauthorized Exfiltration 502
P-NET-03.6: Boundary Protection | Dynamic Isolation & Segregation (Sandboxing) 502
P-NET-03.7: Boundary Protection | Isolation of System Components 503
P-NET-03.8: Boundary Protection | Separate Subnets for Connecting To Different Security Domains 503
P-NET-04: Data Flow Enforcement – Access Control Lists (ACLs) 503
P-NET-04.1: Data Flow Enforcement | Deny Traffic by Default & Allow Traffic by Exception 504
P-NET-04.2: Data Flow Enforcement | Object Security Attributes 505
P-NET-04.3: Data Flow Enforcement | Content Check For Encrypted Data 505
P-NET-04.4: Data Flow Enforcement | Embedded Data Types 505
P-NET-04.5: Data Flow Enforcement | Metadata 506
P-NET-04.6: Data Flow Enforcement | Human Reviews 506
P-NET-04.7: Data Flow Enforcement | Policy Decision Point (PDP) 507
P-NET-04.8: Data Flow Enforcement | Data Type Identifiers 507
P-NET-04.9: Data Flow Enforcement | Decomposition Into Policy-Relevant Subcomponents 508
P-NET-04.10: Data Flow Enforcement | Detection of Unsanctioned Information 508
P-NET-04.11: Data Flow Enforcement | Approved Solutions 509

P-NET-04.12: Data Flow Enforcement | Cross Domain Authentication 509
P-NET-04.13: Data Flow Enforcement | Metadata Validation 509
P-NET-04.14: Data Flow Enforcement | Application Proxy 510
P-NET-05: Interconnection Security Agreements (ISAs) **510**
P-NET-05.1: Interconnection Security Agreements (ISAs) | External System Connections 511
P-NET-05.2: Interconnection Security Agreements (ISAs) | Internal System Connections 512
P-NET-06: Network Segmentation (macrosegmentation) **512**
P-NET-06.1: Network Segmentation | Security Management Subnets 513
P-NET-06.2: Network Segmentation | Virtual Local Area Network (VLAN) Separation 514
P-NET-06.3: Network Segmentation | Sensitive / Regulated Data Enclave (Secure Zone) 514
P-NET-06.4: Network Segmentation | Segregation From Enterprise Services 515
P-NET-06.5: Network Segmentation | Direct Internet Access Restrictions 515
P-NET-06.6: Network Segmentation | Microsegmentation 516
P-NET-06.7: Network Segmentation | Software Defined Networking (SDN) 516
P-NET-07: Network Connection Termination **517**
P-NET-08: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) **517**
P-NET-08.1: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) | DMZ Networks 518
P-NET-08.2: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) | Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) 518
P-NET-08.3: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) | Host Containment 519
P-NET-08.4: Network Intrusion Detection & Prevention Systems (NIDS/NIPS) | Resource Containment 519
P-NET-09: Session Integrity **519**
P-NET-09.1: Session Integrity | Invalidate Session Identifiers at Logout 520
P-NET-09.2: Session Integrity | Unique System-Generated Session Identifiers 520
P-NET-10: Domain Name Service (DNS) Resolution **520**
P-NET-10.1: Domain Name Service (DNS) Resolution | Architecture & Provisioning For Name/Address Resolution Service 521
P-NET-10.2: Domain Name Service (DNS) Resolution | Secure Name/Address Resolution Service (Recursive or Caching Resolver) 522
P-NET-10.3: Domain Name Service (DNS) Resolution | Sender Policy Framework (SPF) 522
P-NET-10.4: Domain Name Service (DNS) Resolution | Domain Registrar Security 522
P-NET-11: Out-of-Band Channels **523**
P-NET-12: Safeguarding Data Over Open Networks **523**
P-NET-12.1: Safeguarding Date Over Open Networks | Wireless Link Protection 524
P-NET-12.2: Safeguarding Date Over Open Networks | End-User Messaging Technologies 524
P-NET-13: Electronic Messaging **525**
P-NET-14: Remote Access **525**
P-NET-14.1: Remote Access | Automated Monitoring & Control 526
P-NET-14.2: Remote Access | Protection of Confidentiality/Integrity Using Encryption 526
P-NET-14.3: Remote Access | Managed Access Control Points 527
P-NET-14.4: Remote Access | Privileged Commands & Access 527
P-NET-14.5: Remote Access | Work From Anywhere (WFA) – Telecommuting Security 528
P-NET-14.6: Remote Access | Third-Party Remote Access Governance 528
P-NET-14.7: Remote Access | Endpoint Security Validation 529
P-NET-14.8: Remote Access | Expeditious Disconnect/Disable Capability 529
P-NET-15: Wireless Networking **530**
P-NET-15.1: Wireless Access | Authentication & Encryption 530
P-NET-15.2: Wireless Access | Disable Wireless Networking 531
P-NET-15.3: Wireless Access | Restrict Configuration By Users 531
P-NET-15.4: Wireless Access | Wireless Boundaries 531
P-NET-15.5: Wireless Access | Rogue Wireless Detection 532
P-NET-16: Intranets **532**
P-NET-17: Data Loss Prevention (DLP) **533**
P-NET-18: DNS & Content Filtering **533**
P-NET-18.1: DNS & Content Filtering | Route Internal Traffic To Proxy Servers 534
P-NET-18.2: DNS & Content Filtering | Visibility of Encrypted Communications 534
P-NET-18.3: DNS & Content Filtering | Route Privileged Network Access 535
P-NET-18.4: DNS & Content Filtering | Protocol Compliance Enforcement 535

P-NET-18.5: DNS & Content Filtering | Domain Name Verification 535
P-NET-18.6: DNS & Content Filtering | Internet Address Denylisting 536
P-NET-18.7: DNS & Content Filtering | Bandwidth Control 536
P-NET-18.8: DNS & Content Filtering | Authenticated Proxy 537
P-NET-18.9: DNS & Content Filtering | Certificate Denylisting 537
P-NET-19: Content Disarm and Reconstruction (CDR) 537
P-NET-20: Email Content Protections 538
P-NET-20.1: Email Content Protections | Email Domain Reputation Protections 538
P-NET-20.2: Email Content Protections | Email Domain Reputation Protections 539
P-NET-20.3: Email Content Protections | Authenticated Received Chain 539
P-NET-20.4: Email Content Protections | Domain-Based Message Authentication Reporting and Conformance (DMARC) 539
P-NET-20.5: Email Content Protections | User Digital Signatures for Outgoing Email 540
P-NET-20.6: Email Content Protections | Encryption for Outgoing Email 540
P-NET-20.7: Email Content Protections | Adaptive Email Protections 540
P-NET-20.8: Email Content Protections | Email Labeling 541
P-NET-20.9: Email Content Protections | User Threat Reporting 541
Physical & Environmental Security (PES) Procedure 543
P-PES-01: Physical & Environmental Protections 543
P-PES-01.1: Physical & Environmental Protections | Physical Security Plan (PSP) 543
P-PES-01.2: Physical & Environmental Protections | Zone-Based Physical Security 544
P-PES-02: Physical Access Authorizations 545
P-PES-02.1: Physical Access Authorizations | Role-Based Physical Access 545
P-PES-02.2: Physical Access Authorizations | Dual Authorization for Physical Access 546
P-PES-03: Physical Access Control 546
P-PES-03.1: Physical Access Control | Controlled Ingress & Egress Points 548
P-PES-03.2: Physical Access Control | Lockable Physical Casings 548
P-PES-03.3: Physical Access Control | Physical Access Logs 549
P-PES-03.4: Physical Access Control | Access To Critical Systems 549
P-PES-04: Physical Security of Offices, Rooms & Facilities 550
P-PES-04.1: Physical Security of Offices, Rooms & Facilities | Working in Secure Areas 550
P-PES-04.2: Physical Security of Offices, Rooms & Facilities | Searches 551
P-PES-04.3: Physical Security of Offices, Rooms & Facilities | Temporary Storage 551
P-PES-05: Monitoring Physical Access 552
P-PES-05.1: Monitoring Physical Access | Intrusion Alarms/Surveillance Equipment 552
P-PES-05.2: Monitoring Physical Access | Monitoring Physical Access To Critical Systems 553
P-PES-06: Visitor Control 553
P-PES-06.1: Visitor Control | Distinguish Visitors from On-Site Personnel 554
P-PES-06.2: Visitor Control | Identification Requirement 554
P-PES-06.3: Visitor Control | Restrict Unescorted Access 555
P-PES-06.4: Visitor Control | Automated Records Management & Review 555
P-PES-06.5: Visitor Control | Minimize Visitor Personal Data (PD) 556
P-PES-06.6: Visitor Control | Visitor Access Revocation 556
P-PES-07: Supporting Utilities 556
P-PES-07.1: Supporting Utilities | Automatic Voltage Controls 557
P-PES-07.2: Supporting Utilities | Emergency Shutoff 557
P-PES-07.3: Supporting Utilities | Emergency Power 558
P-PES-07.4: Supporting Utilities | Emergency Lighting 558
P-PES-07.5: Supporting Utilities | Water Damage Protection 558
P-PES-07.6: Supporting Utilities | Automation Support for Water Damage Protection 559
P-PES-07.7: Supporting Utilities | Redundant Cabling 559
P-PES-08: Fire Protection 559
P-PES-08.1: Fire Protection | Fire Detection Devices 560
P-PES-08.2: Fire Protection | Fire Suppression Devices 560
P-PES-08.3: Fire Protection | Automatic Fire Suppression 561
P-PES-09: Temperature & Humidity Controls 561
P-PES-09.1: Temperature & Humidity Controls | Monitoring with Alarms/Notifications 561

P-PES-10: Delivery & Removal 562
P-PES-11: Alternate Work Site 562
P-PES-12: Equipment Siting & Protection 563
P-PES-12.1: Equipment Siting & Protection | Transmission Medium Security 563
P-PES-12.2: Equipment Siting & Protection | Access Control For Output Devices 564
P-PES-13: Information Leakage Due To Electromagnetic Signals Emanations 564
P-PES-14: Asset Monitoring and Tracking 565
P-PES-15: Electromagnetic Pulse (EMP) Protection 565
P-PES-16: Component Marking 566
P-PES-17: Proximity Sensor 566
P-PES-18: On-Site Client Segregation 567
P-PES-19: Physical Access Device Inventories 567
Data Privacy (PRI) Procedures 569
P-PRI-01: Data Privacy Program 569
P-PRI-01.1: Data Privacy Program | Chief Privacy Officer (CPO) 569
P-PRI-01.2: Data Privacy Program | Privacy Act Statements 570
P-PRI-01.3: Data Privacy Program | Dissemination of Privacy Program Information 570
P-PRI-01.4: Data Privacy Program | Data Protection Officer (DPO) 571
P-PRI-01.5: Data Privacy Program | Binding Corporate Rules (BCR) 571
P-PRI-01.6: Data Privacy Program | Security of Personal Data 571
P-PRI-01.7: Data Privacy Program | Limiting Personal Data (PD) Disclosures 572
P-PRI-01.8: Data Privacy Program | Data Fiduciary 572
P-PRI-01.9: Data Privacy Program | Personal Data (PD) Process Manager 573
P-PRI-01.10: Data Privacy Program | Financial Incentives For Personal Data (PD) 573
P-PRI-01.11: Data Privacy Program | Reasonable Data Privacy Practices 573
P-PRI-02: Data Privacy Notice 574
P-PRI-02.1: Data Privacy Notice | Purpose Specification 575
P-PRI-02.2: Data Privacy Notice | Automated Data Management Processes 575
P-PRI-02.3: Data Privacy Notice | Computer Matching Agreements (CMA) 576
P-PRI-02.4: Data Privacy Notice | System of Records Notice (SORN) 576
P-PRI-02.5: Data Privacy Notice | System of Records Notice (SORN) Review Process 576
P-PRI-02.6: Data Privacy Notice | Privacy Act Exemptions 577
P-PRI-02.7: Data Privacy Notice | Real-Time or Layered Notice 577
P-PRI-02.8: Data Privacy Notice | Purpose Compatibility 578
P-PRI-02.9: Data Privacy Notice | Privacy Notice Formatting 578
P-PRI-02.10: Data Privacy Notice | Symmetry In Choice 579
P-PRI-02.11: Data Privacy Notice | Choice Architecture 579
P-PRI-02.12: Data Privacy Notice | Choice Architecture Testing 579
P-PRI-02.13: Data Privacy Notice | Notice of Right To Limit 580
P-PRI-02.14: Data Privacy Notice | Alternative Means To Deliver Privacy Notice 580
P-PRI-03: Choice & Consent 580
P-PRI-03.1: Choice & Consent | Tailored Consent 581
P-PRI-03.2: Choice & Consent | Just-In-Time Notice & Updated Consent 581
P-PRI-03.3: Choice & Consent | Prohibition of Selling, Processing and/or Sharing Personal Data (PD) 582
P-PRI-03.4: Choice & Consent | Revoke Consent 582
P-PRI-03.5: Choice & Consent | Product or Service Delivery Restrictions 583
P-PRI-03.6: Choice & Consent | Authorized Agent 583
P-PRI-03.7: Choice & Consent | Active Participation By Data Subjects 583
P-PRI-03.8: Choice & Consent | Global Privacy Control (GPC) 584
P-PRI-03.9: Choice & Consent | Continued Use of Personal Data (PD) 584
P-PRI-03.10: Choice & Consent | Cease Processing, Storing and/or Sharing Personal Data (PD) 585
P-PRI-03.11: Choice & Consent | Communicating Processing Changes 585
P-PRI-03.12: Choice & Consent | Data Subject Opt-In Consent 585
P-PRI-03.13: Choice & Consent | Data Subject Opt-In Consent 586
P-PRI-04: Restrict Collection To Identified Purpose 586
P-PRI-04.1: Restrict Collection To Identified Purpose | Authority To Collect, Process, Store & Share Personal Data (PD) 587

P-PRI-04.2: Restrict Collection To Identified Purpose | Primary Sources 587
P-PRI-04.3: Restrict Collection To Identified Purpose | Identifiable Image Collection 588
P-PRI-04.4: Restrict Collection To Identified Purpose | Acquired Personal Data (PD) 588
P-PRI-04.5: Restrict Collection To Identified Purpose | Validate Collected Personal Data (PD) 588
P-PRI-04.6: Restrict Collection To Identified Purpose | Re-Validate Collected Personal Data (PD) 589
P-PRI-04.7: Restrict Collection To Identified Purpose | Personal Data (PD) Collection Methods 589
P-PRI-05: Personal Data (PD) Retention & Disposal **589**
P-PRI-05.1: Personal Data (PD) Retention & Disposal | Internal Use of Personal Data For Testing, Training and Research 590
P-PRI-05.2: Personal Data (PD) Retention & Disposal | Personal Data Accuracy & Integrity 590
P-PRI-05.3: Personal Data (PD) Retention & Disposal | Data Masking 591
P-PRI-05.4: Personal Data (PD) Retention & Disposal | Usage Restrictions of Sensitive Personal Data (PD) 591
P-PRI-05.5: Personal Data (PD) Retention & Disposal | Inventory Of Personal Data (PD) 592
P-PRI-05.6: Personal Data (PD) Retention & Disposal | Personal Data (PD) Inventory Automation Support 592
P-PRI-05.7: Personal Data (PD) Retention & Disposal | Personal Data (PD) Categories 593
P-PRI-05.8: Personal Data (PD) Retention & Disposal | Personal Data (PD) Formats 593
P-PRI-06: Data Subject Empowerment **593**
P-PRI-06.1: Data Subject Empowerment | Correcting Inaccurate Personal Data 594
P-PRI-06.2: Data Subject Empowerment | Notice of Correction or Processing Change 595
P-PRI-06.3: Data Subject Empowerment | Appeal Adverse Decision 595
P-PRI-06.4: Data Subject Empowerment | User Feedback Management 595
P-PRI-06.5: Data Subject Empowerment | Right to Erasure 596
P-PRI-06.6: Data Subject Empowerment | Data Portability 596
P-PRI-06.7: Data Subject Empowerment | Personal Data (PD) Exportability 597
P-PRI-06.8: Data Subject Empowerment | Data Subject Authentication 597
P-PRI-07: Information Sharing With Third Parties **597**
P-PRI-07.1: Information Sharing With Third Parties | Privacy Requirements For Contractors & Service Providers 598
P-PRI-07.2: Information Sharing With Third Parties | Joint Processing of Personal Data (PD) 599
P-PRI-07.3: Information Sharing With Third Parties | Obligation To Inform Third Parties 599
P-PRI-07.4: Information Sharing With Third Parties | Reject Unauthenticated or Untrustworthy Disclosure Requests 599
P-PRI-07.5: Information Sharing With Third Parties | Justification To Reject Disclosure Requests 600
P-PRI-08: Testing, Training & Monitoring **600**
P-PRI-09: Personal Data Lineage **601**
P-PRI-10: Data Quality Management **601**
P-PRI-10.1: Data Quality Management | Data Quality Automation 602
P-PRI-10.2: Data Quality Management | Data Analytics Bias 602
P-PRI-11: Data Tagging **602**
P-PRI-12: Updating Personal Data (PD) Process **603**
P-PRI-12.1: Updating Personal Data (PD) Process | Enabling Data Subjects To Update Personal Data (PD) 603
P-PRI-13: Data Management Board **604**
P-PRI-14: Documenting Data Processing Activities **604**
P-PRI-14.1: Documenting Data Processing Activities | Accounting of Disclosures 605
P-PRI-14.2: Documenting Data Processing Activities | Notification of Disclosure Request To Data Subject 605
P-PRI-15: Register As A Data Controller and/or Data Processor **606**
P-PRI-16: Potential Human Rights Abuses **606**
P-PRI-17: Data Subject Communications **607**
P-PRI-17.1: Data Subject Communications | Conspicuous Link To Privacy Notice 607
P-PRI-17.2: Data Subject Communications | Notice of Financial Incentive 607
P-PRI-17.3: Data Subject Communications | Data Subject Communications Documentation 608
P-PRI-17.4: Data Subject Communications | Data Subject Communications Metrics 608
P-PRI-17.5: Data Subject Communications | Data Subject Communications Disclosure 609
P-PRI-18: Data Controller Communications **609**
P-PRI-19: Automated Decision-Making Technology (ADMT) For Data Subject Actions **609**
P-PRI-19.1: Automated Decision-Making Technology (ADMT) For Data Subject Actions | Automated Decision-Making Technology (ADMT) Use Notification 610
P-PRI-19.2: Automated Decision-Making Technology (ADMT) For Data Subject Actions | Automated Decision-Making Technology (ADMT) Opt-Out Consent 610

P-PRI-19.3: Automated Decision-Making Technology (ADMT) For Data Subject Actions | Automated Decision-Making Technology (ADMT) Transparency 611
P-PRI-20: Data Brokers 611
P-PRI-21: Notice of Right To Opt-Out 611
P-PRI-21.1: Notice of Right To Opt-Out | Opt-Out Links 612
P-PRI-21.2: Notice of Right To Opt-Out | Alternative Out-Out Link 612
Project & Resource Management (PRM) Procedures 614
P-PRM-01: Cybersecurity & Data Protection Portfolio Management 614
P-PRM-01.1: Cybersecurity & Data Protection Portfolio Management | Strategic Plan & Objectives 614
P-PRM-01.2: Cybersecurity & Data Protection Portfolio Management | Targeted Capability Maturity Levels 615
P-PRM-02: Cybersecurity & Data Protection Resource Management 615
P-PRM-02.1: Cybersecurity & Data Protection Resource Management | Prioritization To Address Evolving Risks & Threats 616
P-PRM-03: Allocation of Resources 616
P-PRM-04: Cybersecurity & Data Protection In Project Management 617
P-PRM-05: Cybersecurity & Data Protection Requirements Definition 617
P-PRM-06: Business Process Definition 617
P-PRM-07: System Development Life Cycle (SDLC) Management 618
P-PRM-08: Manage Organizational Knowledge 618
Risk Management (RSK) Procedures 620
P-RSK-01: Risk Management Program (RMP) 620
P-RSK-01.1: Risk Management Program (RMP) | Risk Framing 620
P-RSK-01.2: Risk Management Program (RMP) | Risk Management Resourcing 621
P-RSK-01.3: Risk Management Program (RMP) | Risk Tolerance 621
P-RSK-01.4: Risk Management Program (RMP) | Risk Threshold 622
P-RSK-01.5: Risk Management Program (RMP) | Risk Appetite 622
P-RSK-02: Risk-Based Security Categorization 623
P-RSK-02.1: Risk-Based Security Categorization | Impact-Level Prioritization 623
P-RSK-03: Risk Identification 624
P-RSK-03.1: Risk Identification | Risk Catalog 624
P-RSK-04: Risk Assessment 624
P-RSK-04.1: Risk Assessment | Risk Register 626
P-RSK-04.2: Risk Assessment | Risk Assessment Methodology 626
P-RSK-04.3: Risk Assessment | Instances Requiring A Risk Assessment 626
P-RSK-04.4: Risk Assessment | Risk Assessment Stakeholder Involvement 627
P-RSK-05: Risk Ranking 627
P-RSK-06: Risk Remediation 628
P-RSK-06.1: Risk Remediation | Risk Response 628
P-RSK-06.2: Risk Remediation | Compensating Countermeasures 629
P-RSK-06.3: Risk Remediation | Risk Treatment Options 629
P-RSK-06.4: Risk Remediation | Risk Treatment Plan 630
P-RSK-07: Risk Assessment Update 630
P-RSK-08: Business Impact Analysis (BIA) 631
P-RSK-09: Supply Chain Risk Management (SCRM) Program 631
P-RSK-09.1: Supply Chain Risk Management (SCRM) Program | Supply Chain Risk Assessment 633
P-RSK-09.2: Supply Chain Risk Management (SCRM) Program | AI & Autonomous Technologies Supply Chain Impacts 633
P-RSK-10: Data Protection Impact Assessment (DPIA) 634
P-RSK-11: Risk Monitoring 635
P-RSK-12: Risk Culture 635
P-RSK-13: Executive Leadership Approval For Managing Material Risk 636
P-RSK-13.1: Executive Leadership Approval For Managing Material Risk | Documented Alternatives 636
P-RSK-13.2: Executive Leadership Approval For Managing Material Risk | Documented Alternatives 637
Secure Engineering & Architecture (SEA) Procedure 639
P-SEA-01: Secure Engineering Principles 639
P-SEA-01.1: Secure Engineering Principles | Centralized Management of Cybersecurity & Data Protection Controls 640

P-SEA-01.2: Secure Engineering Principles | Achieving Resilience Requirements 640
P-SEA-01.3: Secure Engineering Principles | Resilience Capabilities 641
P-SEA-02: Alignment With Enterprise Architecture 642
P-SEA-02.1: Alignment With Enterprise Architecture | Standardized Terminology 642
P-SEA-02.2: Alignment With Enterprise Architecture | Outsourcing Non-Essential Functions or Services 643
P-SEA-02.3: Alignment With Enterprise Architecture | Technical Debt Reviews 643
P-SEA-03: Defense-In-Depth (DiD) Architecture 643
P-SEA-03.1: Defense-In-Depth (DiD) Architecture | System Partitioning 644
P-SEA-03.2: Defense-In-Depth (DiD) Architecture | Application Partitioning 644
P-SEA-04: Process Isolation 645
P-SEA-04.1: Process Isolation | Security Function Isolation 645
P-SEA-04.2: Process Isolation | Hardware Separation 646
P-SEA-04.3: Process Isolation | Thread Separation 646
P-SEA-04.4: Process Isolation | System Privileges Isolation 646
P-SEA-05: Information In Shared Resources 647
P-SEA-06: Prevent Program Execution 647
P-SEA-07: Predictable Failure Analysis 648
P-SEA-07.1: Predictable Failure Analysis | Technology Lifecycle Management 648
P-SEA-07.2: Predictable Failure Analysis | Fail Secure 649
P-SEA-07.3: Predictable Failure Analysis | Fail Safe 649
P-SEA-08: Non-Persistence 649
P-SEA-08.1: Non-Persistence | Refresh from Trusted Sources 650
P-SEA-09: Information Output Filtering 650
P-SEA-09.1: Information Output Filtering | Limit Personal Data (PD) Dissemination 651
P-SEA-10: Memory Protection 651
P-SEA-11: Honeypots 651
P-SEA-12: Honeyclients 652
P-SEA-13: Heterogeneity 652
P-SEA-13.1: Heterogeneity | Virtualization Techniques 653
P-SEA-14: Concealment & Misdirection 653
P-SEA-14.1: Concealment & Misdirection | Randomness 653
P-SEA-14.2: Concealment & Misdirection | Change Processing & Storage Locations 654
P-SEA-15: Distributed Processing & Storage 654
P-SEA-16: Non-Modifiable Executable Programs 655
P-SEA-17: Secure Log-On Procedures 655
P-SEA-18: System Use Notification (Logon Banner) 655
P-SEA-18.1: System Use Notification | Standardized Microsoft Windows Banner 656
P-SEA-18.2: System Use Notification | Truncated Banner 656
P-SEA-19: Previous Logon Notification 657
P-SEA-20: Clock Synchronization 657
P-SEA-21: Application Container 658
P-SEA-22: Privileged Environments 658
Security Operations (OPS) Procedures 660
P-OPS-01: Operations Security 660
P-OPS-01.1: Operations Security | Standardized Operating Procedures (SOP) 660
P-OPS-02: Security Concept Of Operations (CONOPS) 661
P-OPS-03: Service Delivery (Business Process Support) 662
P-OPS-04: Security Operations Center (SOC) 662
P-OPS-05: Secure Practices Guidelines 663
P-OPS-06: Security Orchestration, Automation, and Response (SOAR) 663
P-OPS-07: Shadow Information Technology Detection 664
Security Awareness & Training (SAT) Procedures 665
P-SAT-01: Cybersecurity & Data Protection-Minded Workforce 665
P-SAT-01.1: Cybersecurity & Data Protection-Minded Workforce | Maintaining Workforce Development Relevancy 665
P-SAT-02: Cybersecurity & Data Protection Awareness Training 666
P-SAT-02.1: Cybersecurity & Data Protection Awareness Training | Simulated Cyber Attack Scenario Training 667

P-SAT-02.2: Cybersecurity & Data Protection Awareness Training | Social Engineering & Mining 668
P-SAT-03: Cybersecurity & Data Protection Role-Based Training 668
P-SAT-03.1: Cybersecurity & Data Protection Training | Practical Exercises 669
P-SAT-03.2: Cybersecurity & Data Protection Training | Suspicious Communications & Anomalous System Behavior 670
P-SAT-03.3: Cybersecurity & Data Protection Training | Sensitive / Regulated Data Storage, Handling & Processing 670
P-SAT-03.4: Cybersecurity & Data Protection Training | Vendor Security Training 671
P-SAT-03.5: Cybersecurity & Data Protection Training | Privileged Users 671
P-SAT-03.6: Cybersecurity & Data Protection Training | Cyber Threat Environment 671
P-SAT-03.7: Cybersecurity & Data Protection Training | Continuing Professional Education (CPE) - Cybersecurity & Data Privacy Personnel 672
P-SAT-03.8: Cybersecurity & Data Protection Training | Continuing Professional Education (CPE) - DevOps Personnel 672
P-SAT-03.9: Cybersecurity & Data Protection Training | Counterintelligence Training 673
P-SAT-04: Cybersecurity & Data Protection Training Records 673
P-SAT-05: Cybersecurity Knowledge Sharing 673
Technology Development & Acquisition (TDA) Procedures 675
P-TDA-01: Technology Development & Acquisition 675
P-TDA-01.1: Technology Development & Acquisition | Product Management 675
P-TDA-01.2: Technology Development & Acquisition | Integrity Mechanisms for Software/Firmware Updates 676
P-TDA-01.3: Technology Development & Acquisition | Malware Testing Prior To Release 677
P-TDA-01.4: Technology Development & Acquisition | DevSecOps 677
P-TDA-02: Minimum Viable Product (MVP) Security Requirements 677
P-TDA-02.1: Minimum Viable Product (MVP) Security Requirements | Ports, Protocols & Services In Use 678
P-TDA-02.2: Minimum Viable Product (MVP) Security Requirements | Information Assurance Enabled Products 678
P-TDA-02.3: Minimum Viable Product (MVP) Security Requirements | Development Methods, Techniques & Processes 678
P-TDA-02.4: Minimum Viable Product (MVP) Security Requirements | Pre-Established Security Configurations 679
P-TDA-02.5: Minimum Viable Product (MVP) Security Requirements | Identification & Justification of Ports, Protocols & Services 679
P-TDA-02.6: Minimum Viable Product (MVP) Security Requirements | Use of Insecure Ports, Protocols & Services 680
P-TDA-02.7: Minimum Viable Product (MVP) Security Requirements | Cybersecurity & Data Privacy Representatives For Product Changes 680
P-TDA-02.8: Minimum Viable Product (MVP) Security Requirements | Minimizing Attack Surfaces 680
P-TDA-02.9: Minimum Viable Product (MVP) Security Requirements | Ongoing Product Security Support 681
P-TDA-02.10: Minimum Viable Product (MVP) Security Requirements | Product Testing & Reviews 681
P-TDA-02.11: Minimum Viable Product (MVP) Security Requirements | Disclosure of Vulnerabilities 682
P-TDA-02.12: Minimum Viable Product (MVP) Security Requirements | Products With Digital Elements 682
P-TDA-02.13: Minimum Viable Product (MVP) Security Requirements | Reporting Exploitable Vulnerabilities 683
P-TDA-02.14: Minimum Viable Product (MVP) Security Requirements | Logging Syntax 683
P-TDA-03: Commercial Off-The-Shelf (COTS) Security Solutions 683
P-TDA-03.1: Commercial Off-The-Shelf (COTS) Security Solutions | Supplier Diversity 684
P-TDA-04: Documentation Requirements 684
P-TDA-04.1: Documentation Requirements | Functional Properties 685
P-TDA-04.2: Documentation Requirements | Software Bill of Materials (SBOM) 685
P-TDA-05: Developer Architecture & Design 686
P-TDA-05.1: Developer Architecture & Design | Physical Diagnostic & Test Interfaces 687
P-TDA-05.2: Developer Architecture & Design | Diagnostic & Test Interface Monitoring 687
P-TDA-06: Secure Software Development Practices (SSDP) 688
P-TDA-06.1: Secure Coding | Criticality Analysis 689
P-TDA-06.2: Secure Coding | Threat Modeling 690
P-TDA-06.3: Secure Coding | Software Assurance Maturity Model (SAMM) 690
P-TDA-06.4: Secure Coding | Supporting Toolchain 691
P-TDA-06.5: Secure Coding | Software Design Review 691
P-TDA-06.6: Secure Coding | Software Design Root Cause Analysis 691
P-TDA-07: Secure Development Environments 692

P-TDA-08: Separation of Development, Testing & Operational Environments 692
P-TDA-08.1: Separation of Development, Testing & Operational Environments | Secure Migration Practices 693
P-TDA-09: Cybersecurity & Data Protection Testing Throughout Development 693
P-TDA-09.1: Cybersecurity & Data Protection Testing Throughout Development | Continuous Monitoring Plan 694
P-TDA-09.2: Cybersecurity & Data Protection Testing Throughout Development | Static Code Analysis 694
P-TDA-09.3: Cybersecurity & Data Privacy Testing Throughout Development | Dynamic Code Analysis 695
P-TDA-09.4: Cybersecurity & Data Privacy Testing Throughout Development | Malformed Input Testing 695
P-TDA-09.5: Cybersecurity & Data Privacy Testing Throughout Development | Application Penetration Testing 696
P-TDA-09.6: Cybersecurity & Data Privacy Testing Throughout Development | Secure Settings By Default 696
P-TDA-09.7: Cybersecurity & Data Privacy Testing Throughout Development | Manual Code Review 697
P-TDA-10: Use of Live Data 697
P-TDA-10.1: Use of Live Data | Test Data Integrity 697
P-TDA-11: Product Tampering and Counterfeiting (PTC) 698
P-TDA-11.1: Product Tampering and Counterfeiting (PTC) | Anti-Counterfeit Training 698
~~*P-TDA-11.2: Product Tampering and Counterfeiting (PTC) | Component Disposal*~~ 699
P-TDA-12: Customized Development of Critical Components 699
P-TDA-13: Developer Screening 700
P-TDA-14: Developer Configuration Management 700
P-TDA-14.1: Developer Configuration Management | Software/Firmware Integrity Verification 700
P-TDA-14.2: Developer Configuration Management | Hardware Integrity Verification 701
P-TDA-15: Developer Threat Analysis & Flaw Remediation 701
P-TDA-16: Developer-Provided Training 702
P-TDA-17: Unsupported Systems 702
P-TDA-17.1: Unsupported Systems | Alternate Sources For Continued Support 703
P-TDA-18: Input Data Validation 703
P-TDA-19: Error Handling 704
P-TDA-20: Access to Program Source Code 704
P-TDA-20.1: Access to Program Source Code | Software Release Integrity Verification 705
P-TDA-20.2: Access to Program Source Code | Archiving Software Releases 705
P-TDA-20.3: Access to Program Source Code | Software Escrow 705
P-TDA-20.4: Access to Program Source Code | Approved Code 706
P-TDA-21: Access to Program Source Code 706
P-TDA-22: Technical Documentation Artifacts 707
P-TDA-22.1: Technical Documentation Artifacts | Product-Specific Risk Assessment Artifacts 707
Third-Party Management (TPM) Procedures 708
P-TPM-01: Third-Party Management 708
P-TPM-01.1: Third-Party Management | Third-Party Inventories 708
P-TPM-02: Third-Party Criticality Assessments 709
P-TPM-03: Supply Chain Risk Management (SCRM) 709
P-TPM-03.1: Supply Chain Protection | Acquisition Strategies, Tools & Methods 710
P-TPM-03.2: Supply Chain Protection | Limit Potential Harm 710
P-TPM-03.3: Supply Chain Protection | Processes To Address Weaknesses or Deficiencies 711
P-TPM-03.4: Supply Chain Protection | Adequate Supply 711
P-TPM-04: Third-Party Services 711
P-TPM-04.1: Third-Party Services | Third-Party Risk Assessments & Approvals 712
P-TPM-04.2: Third-Party Services | External Connectivity Requirements - Identification of Ports, Protocols & Services 713
P-TPM-04.3: Third-Party Services | Conflict of Interests 713
P-TPM-04.4: Third-Party Services | Third-Party Processing, Storage and Service Locations 713
P-TPM-05: Third-Party Contract Requirements 714
P-TPM-05.1: Third-Party Contract Requirements | Security Compromise Notification Agreements 715
P-TPM-05.2: Third-Party Contract Requirements | Contract Flow-Down Requirements 715
P-TPM-05.3: Third-Party Contract Requirements | Third-Party Authentication Practices 716
P-TPM-05.4: Third-Party Contract Requirements | Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix 716
P-TPM-05.5: Third-Party Contract Requirements | Third-Party Scope Review 717
P-TPM-05.6: Third-Party Contract Requirements | First-Party Declaration (1PD) 717

P-TPM-05.7: Third-Party Contract Requirements | Break Clauses 718
P-TPM-05.8: Third-Party Contract Requirements | Third-Party Attestation (3PA) 718
P-TPM-06: Third-Party Personnel Security 718
P-TPM-07: Monitoring for Third-Party Information Disclosure 719
P-TPM-08: Review of Third-Party Services 719
P-TPM-09: Third-Party Deficiency Remediation 720
P-TPM-10: Managing Changes to Third-Party Services 720
P-TPM-11: Third-Party Incident Response & Recovery Capabilities 721
Threat Management (THR) Procedures 722
P-THR-01: Threat Awareness Program 722
P-THR-02: Indicators of Exposure (IOE) 722
P-THR-03: Threat Intelligence Feeds 723
P-THR-03.1: Threat Intelligence Feeds | Threat Intelligence Reporting 723
P-THR-04: Insider Threat Program 724
P-THR-05: Insider Threat Awareness 724
P-THR-06: Vulnerability Disclosure Program (VDP) 725
P-THR-06.1: Vulnerability Disclosure Program (VDP) | Security Disclosure Contact Information 725
P-THR-07: Threat Hunting 726
P-THR-08: Tainting 726
P-THR-09: Threat Catalog 727
P-THR-10: Threat Analysis 727
P-THR-11: Behavioral Baselining 728
Vulnerability & Patch Management (VPM) Procedures 729
P-VPM-01: Vulnerability & Patch Management Program 729
P-VPM-01.1: Vulnerability & Patch Management Program | Attack Surface Scope 729
P-VPM-02: Vulnerability Remediation Process 730
P-VPM-03: Vulnerability Ranking 730
P-VPM-03.1: Vulnerability Ranking | Vulnerability Exploitation Analysis 731
P-VPM-04: Continuous Vulnerability Remediation Activities 731
P-VPM-04.1: Continuous Vulnerability Remediation Activities | Stable Versions 732
P-VPM-04.2: Continuous Vulnerability Remediation Activities | Flaw Remediation with Personal Data (PD) 732
P-VPM-04.3: Continuous Vulnerability Remediation Activities | Deferred Patching Decisions 733
P-VPM-05: Software & Firmware Patching 733
P-VPM-05.1: Software & Firmware Patching | Centralized Management of Flaw Remediation Processes 735
P-VPM-05.2: Software & Firmware Patching | Automated Remediation Status 736
P-VPM-05.3: Software & Firmware Patching | Time To Remediate/Benchmarks For Corrective Action 736
P-VPM-05.4: Software & Firmware Patching | Automated Software & Firmware Updates 736
P-VPM-05.5: Software & Firmware Patching | Removal of Previous Versions 737
P-VPM-05.6: Software & Firmware Patching | Pre-Deployment Patch Testing 737
P-VPM-05.7: Software & Firmware Patching | Out-of-Cycle Patching 738
P-VPM-05.8: Software & Firmware Patching | Software Patch Integrity 738
P-VPM-06: Vulnerability Scanning 739
P-VPM-06.1: Vulnerability Scanning | Update Tool Capability 740
P-VPM-06.2: Vulnerability Scanning | Breadth/Depth of Coverage 740
P-VPM-06.3: Vulnerability Scanning | Privileged Access 740
P-VPM-06.4: Vulnerability Scanning | Trend Analysis 741
P-VPM-06.5: Vulnerability Scanning | Review Historical Event Logs 741
P-VPM-06.6: Vulnerability Scanning | External Vulnerability Assessment Scans 742
P-VPM-06.7: Vulnerability Scanning | Internal Vulnerability Assessment Scans 742
P-VPM-06.8: Vulnerability Scanning | Acceptable Discoverable Information 742
P-VPM-06.9: Vulnerability Scanning | Correlate Scanning Information 743
P-VPM-07: Penetration Testing 743
P-VPM-07.1: Penetration Testing | Independent Penetration Agent or Team 744
P-VPM-08: Technical Surveillance Countermeasures Security 744
P-VPM-09: Reviewing Vulnerability Scanner Usage 745
P-VPM-10: Red Team Exercises 745
Web Security (WEB) Procedures 746

P-WEB-01: Web Security 746
P-WEB-01.1: Web Security | Unauthorized Code 746
P-WEB-02: Use of Demilitarized Zones (DMZs) 746
P-WEB-03: Web Application Firewall (WAF) 747
P-WEB-04: Client-Facing Web Services 747
P-WEB-05: Cookie Management 748
P-WEB-06: Strong Customer Authentication (SCA) 748
P-WEB-07: Web Security Standard 749
P-WEB-08: Web Application Framework 749
P-WEB-09: Validation & Sanitization 749
P-WEB-10: Secure Web Traffic 750
P-WEB-11: Output Encoding 750
P-WEB-12: Web Browser Security 750
P-WEB-13: Website Change Detection 751
P-WEB-14: Publicly Accessible Content Reviews 751
Glossary: Acronyms & Definitions 752
Acronyms 752
Definitions 753
Record of Changes 754

(1) Researches, establishes and maintains formal contact with select groups and/or associations within the cybersecurity and data protection communities. Security groups and associations include, but are not limited to:
    a. Special Interest Groups (SIGs);
    b. Professional associations; and
    c. Peer groups of cybersecurity and data protection professionals in similar organizations.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

P-GOV-08: Defined Business Context & Mission

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

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007], in conjunction with Systems Security Management [OG-WRL-014]:

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

P-GOV-09: Defined Control Objectives

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

Procedure / Control Activity: Executive Cybersecurity Leadership [OG-WRL-007], in conjunction with Systems Security Management [OG-WRL-014]:

P-MON-07: TIME STAMPS

Control: Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.

Procedure / Control Activity: Systems Administration [IO-WRL-005], in conjunction with Systems Security Analysis [IO-WRL-006]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing and storing time. [142]
    a. Time stamps for audit records: [143]
        i. Use Coordinated Universal Time (UTC);
        ii. Have a fixed local time offset from UTC, or
        iii. Include the local time offset as part of the time stamp are recorded;
    b. Technology assets have the correct and consistent time with one (1) second granularity of time measurement; [144]and
    c. Time data is protected from unauthorized modification.
(2) Enables NTP for client computers to maintain system time synchronization to with NIST Internet Time Servers (ITS); [145]
    a. Utilizes the official ITS for primary and alternate time sources.
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-MON-07.1: TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE

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

Procedure / Control Activity: Systems Administration [IO-WRL-005], in conjunction with Systems Security Analysis [IO-WRL-006]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to configure systems and applications to use authoritative Network Time Protocol (NTP) sources for its time-synchronization, to synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing and storing time. [146]
(2) Enables NTP for client computers to maintain system time synchronization with NIST Internet Time Servers (ITS) [147]that:[148]
    a. Use Coordinated Universal Time (UTC);
    b. Have a fixed local time offset from UTC; or
    c. Include the local time offset as part of the time stamp.
(3) Synchronizes the internal system clocks to the authoritative time source with a granularity of one (1) second or smaller.
(4) Utilizes the official ITS for primary and alternate time sources.
(5) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

---

[142] *NIST SP 800-171A / CMMC 2.0: 3.3.7[a] & 3.3.7[c] / AU.L2-3.3.7[a] & AU.L2-3.3.7[c]*
[143] *NIST SP 800-171A R3: A.03.03.07.a*
[144] *NIST SP 800-171A R3: A.03.03.07.b[01], A.03.03.07.ODP[01]*
[145] *NIST ITS - https://tf.nist.gov/tf-cgi/servers.cgi*
[146] *NIST SP 800-171A / CMMC 2.0: 3.3.7[a] & 3.3.7[c] / AU.L2-3.3.7[a] & AU.L2-3.3.7[c]*
[147] *NIST ITS - https://tf.nist.gov/tf-cgi/servers.cgi*
[148] *NIST SP 800-171A R3: A.03.03.07.b[02]*

a. Distributes copies of the change to key personnel; and
b. Communicates the changes and updates to key personnel.

(6) If necessary, requests corrective action to address identified deficiencies.
(7) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(8) If necessary, documents the results of corrective action and notes findings.
(9) If necessary, requests additional corrective action to address unremediated deficiencies.

P-MON-08: Protection of Event Logs

Control: Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.

Procedure / Control Activity: Defensive Cybersecurity [PD-WRL-001], in conjunction with Systems Security Management [OG-WRL-014] and Cybersecurity Architecture [DD-WRL-001]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to protect the confidentiality and integrity of audit information by: [149]
    a. Securing audit trails so they cannot be altered; [150]
    b. Limiting viewing of audit trails to those with a job-related need; [151]
    c. Protection event logging tools from unauthorized access and/or modification to protect event logs from unauthorized modification and/destruction; [152]
    d. Promptly backing up audit trail files to a centralized log server or media that is difficult to alter;
    e. Writing logs for external-facing technologies onto a log server on the internal LAN;
    f. Using File Integrity Monitoring (FIM) or change detection software on logs to ensure that existing log data cannot be changed without generating alerts, although new data being added should not cause an alert;
    g. Identifying all approved users with the ability to alter or destroy data; and
    h. Ensuring approved users are properly trained to handle sensitive/regulated data.
(2) Retain event logs for the time period consistent with ACME's records retention schedule. [153]
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-MON-08.1: Protection of Event Logs | Event Log Backup on Separate Physical Systems / Components

Control: Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.

Procedure / Control Activity: Secure Systems Development [DD-WRL-004], in conjunction with Systems Administration [IO-WRL-005], Cybersecurity Architecture [DD-WRL-001] and Asset Owner [OG-ORG-007]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to enable the implementation of appropriate physical, administrative and technical mechanisms to ensure event logs are backed up onto a physically different system or system component than the system or component being monitored:
    a. Security Incident Event Manager (SIEM); or
    b. Log collector.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:

---

[149] *NIST SP 800-171A / CMMC 2.0: 3.3.8[a], 3.3.8[b], 3.3.8[c], 3.3.8[d], 3.3.8[e] & 3.3.8[f] / AU.L2-3.3.8[a], AU.L2-3.3.8[b], AU.L2-3.3.8[c], AU.L2-3.3.8[d], AU.L2-3.3.8[e] & AU.L2-3.3.8[f]*
[150] *NIST SP 800-171A R3: A.03.03.06.b[01], A.03.03.06.b[02]*
[151] *NIST SP 800-171A R3: A.03.03.08.b*
[152] *NIST SP 800-171A R3: A.03.03.08.a[01]*
[153] *NIST SP 800-171A R3: A.03.03.03.b*

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

P-HRS-12.1: INCOMPATIBLE ROLES | TWO-PERSON RULE

Control: Mechanisms exist to enforce a two-person rule for implementing changes to sensitive Technology Assets, Applications and/or Services (TAAS).

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Management [OG-WRL-014], Cybersecurity Workforce Management [OG-WRL-003] and Cybersecurity Legal Advice [OG-WRL-006]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to enable the implementation of appropriate physical, administrative and technical mechanisms to develop and implement a two-person rule for implementing changes to sensitive system components and system-level information to ensure that any changes to selected system components and information cannot occur unless two qualified individuals implement such changes.
    a. The two individuals possess sufficient skills / expertise to determine if the proposed changes are correct implementations of approved changes.
(2) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(3) If necessary, requests corrective action to address identified deficiencies.
(4) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(5) If necessary, documents the results of corrective action and notes findings.
(6) If necessary, requests additional corrective action to address unremediated deficiencies.

P-HRS-13: IDENTIFY CRITICAL SKILLS & GAPS

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

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Management [OG-WRL-014], Cybersecurity Workforce Management [OG-WRL-003] and Cybersecurity Legal Advice [OG-WRL-006]:

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

P-HRS-13.1: IDENTIFY CRITICAL SKILLS & GAPS | REMEDIATE IDENTIFIED SKILLS DEFICIENCIES
Control: Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Management [OG-WRL-014], Cybersecurity Workforce Management [OG-WRL-003] and Cybersecurity Legal Advice [OG-WRL-006]:

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

P-HRS-13.2: IDENTIFY CRITICAL SKILLS & GAPS | IDENTIFY VITAL CYBERSECURITY & DATA PRIVACY STAFF
Control: Mechanisms exist to identify vital cybersecurity and data privacy staff.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Management [OG-WRL-014], Cybersecurity Workforce Management [OG-WRL-003] and Cybersecurity Legal Advice [OG-WRL-006]:

(1) Identifies the objectives and activities necessary to support ACME's corporate mission:
    a. Current maturity capability levels associated with cybersecurity and data privacy-related People, Processes, Technologies, Data & Facilities (PPTDF).
    b. Target maturity capability levels associated with cybersecurity and data privacy-related PPTDF.
    c. Resource requirements.
    d. Cybersecurity and data privacy specific:
        i. Vision.
        ii. Mission.
        iii. Strategy.
    e. Prioritized objectives to accomplish the business plan.
(2) Identifies critical staff by:
    a. Identifying vital cybersecurity and data privacy staff;
    b. Documenting the role, function, responsibility and reasons that supports their designation as vital;
    c. Where possible, identifying staff that can backfill vital roles.
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-HRS-13.3: IDENTIFY CRITICAL SKILLS & GAPS | ESTABLISH REDUNDANCY FOR VITAL CYBERSECURITY & DATA PRIVACY STAFF
Control: Mechanisms exist to establish redundancy for vital cybersecurity and data privacy staff.

Procedure / Control Activity: The Human Resources (HR) department, in conjunction with Systems Security Management [OG-WRL-014], Cybersecurity Workforce Management [OG-WRL-003] and Cybersecurity Legal Advice [OG-WRL-006]:

(1) Conducts a critical skills inventory that:

e. Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

(3) Detects Red Flags that have been incorporated into the ITPP;
(4) Responds appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
(5) Ensures the ITPP is updated periodically to reflect changes in risks from identity theft.
(6) Develops processes to identify Red Flags that are relevant to detecting a possible risk of identity theft to customers through the following means:
    a. Verify the identity of persons opening accounts;
    b. Detect the Red Flags that the financial institution or creditor identifies as relevant in connection with the opening of an account or any existing account;
    c. Assess whether the Red Flags detected evidence a risk of identity theft;
    d. Mitigate the risk of identity theft, commensurate with the degree of risk posed;
    e. Train staff to implement the ITPP; and
    f. Oversee service provider arrangements.
(7) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(8) If necessary, requests corrective action to address identified deficiencies.
(9) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(10) If necessary, documents the results of corrective action and notes findings.
(11) If necessary, requests additional corrective action to address unremediated deficiencies.

P-IRO-02.3: INCIDENT HANDLING | DYNAMIC RECONFIGURATION

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

Procedure / Control Activity: Systems Administration [IO-WRL-005], in conjunction with Asset Owner [OG-ORG-007], Crisis Management Specialist [PD-ORG-002], Disaster Recovery Team Leader [IN-ORG-003] and Business Continuity Team Leader [IN-ORG-001]:

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

P-IRO-02.4: INCIDENT HANDLING | INCIDENT CLASSIFICATION & PRIORITIZATION

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

Procedure / Control Activity: Systems Security Management [OG-WRL-014], in conjunction with Systems Security Analysis [IO-WRL-006], Integrated Security Incident Response Team (ISIRT) Leader [PD-ORG-004] and Incident Response [PD-WRL-003]:

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

#	Threat	Category	Category Description
0	**Training**	**Simulated Incident** (Training & Exercises)	This category is used during exercises and approved testing of internal/external network defenses or responses.
1	**Illegal Content or Activities**	**Illegal Content**	This category is used for any data that is illegal to have in possession. This includes illegal content such as child pornography or classified information on unclassified systems.
2		**Criminal Conduct**	This category is used for any incident that would be considered criminal conduct. This includes embezzlement, corporate espionage, terrorism/national security threats, fraud, violence or other conduct that would constitute a criminal felony or misdemeanor charge.
3	**Safety**	**Technology Compromise**	This category is used for any incident that has safety implications from the compromise of the technology to be used in a manner it was not designed for. This includes categories of technologies that includes Operational Technology (OT) and Internet of Things (IoT).
4	**Confidentiality**	**Breach of Sensitive Data**	This category is used for any incident that has involves the unauthorized disclosure or compromise of sensitive/regulated data. This includes sensitive Personal Data (PD) and Intellectual Property (IP).
5	**Nefarious Activity**	**Malware**	This category is used for malware-related incidents. Any software code intentionally created or introduced into multiple systems for the distinct purpose of causing hard or loss to the computer system, its data or other resources (e.g., spyware, adware, viruses, Trojans, worms, etc.).

P-PES-03.3: Physical Access Control | Physical Access Logs

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

Procedure / Control Activity: Physical Security Specialist [IO-ORG-004]:

(1) Uses vendor-recommended settings and industry-recognized secure practices to configure access control systems to log the following information:
    a. Physical location of the access;
    b. Direction of access, if possible (e.g., ingress or egress);
    c. Identity of the person accessing the location; and
    d. Indication of success or failure.
(2) Uses a visitor log to maintain a physical audit trail of visitor activity: [527]
    a. At a minimum, document the visitor's name, the company represented and the onsite personnel authorizing physical access;
    b. Retain this log for a minimum of one (1) year, unless otherwise restricted by law;
    c. Review visitor access records at least monthly; and
    d. Report anomalies in visitor access records to in accordance with ACME's Incident Response Plan (IRP).
(3) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and
    b. Communicates the changes and updates to key personnel.
(4) If necessary, requests corrective action to address identified deficiencies.
(5) If necessary, validates corrective action occurred to appropriately remediate deficiencies.
(6) If necessary, documents the results of corrective action and notes findings.
(7) If necessary, requests additional corrective action to address unremediated deficiencies.

P-PES-03.4: Physical Access Control | Access To Critical Systems

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

Procedure / Control Activity: Asset Owner [OG-ORG-007], in conjunction with Physical Security Specialist [IO-ORG-004] and Physical Security Manager [IO-ORG-003]:

(1) Restricts physical access to sensitive/regulated data or mission-critical (SC1) and business-critical (SC2) Technology Assets, Applications and/or Services (TAAS).
(2) Develops unique physical security zones to determine specific areas that are more vulnerable to unauthorized use, theft or viewing of data where enhanced physical safeguards should be implemented:
    a. Facilities management implements physical access authorization mechanisms to secure workspaces, such as:
        i. Proximity badges; or
        ii. Personalized PIN pad
    b. Line supervisors and manage facilitate "clean desk" requirements for all work areas to ensure media containing sensitive/regulated data is properly secured when the workspace is not occupied, including:
        i. Filing cabinets, lockable drawers / overhead cabinets, storage rooms and any other storage unit containing sensitive/regulated data will be locked when not in use; and
        ii. Whiteboards, dry-erase boards, cork boards, writing tablets and similar common shared work areas will be sanitized (e.g., erased, removed or shredded) when not in use.
(3) Issues visitors a physical token (e.g., a badge or access device) that:
    a. Identifies the visitors as not onsite personnel;
    b. Is surrendered before leaving the facility or at the date of expiration; and
    c. Expires through automated or visual means (e.g., different color for each day).
(4) On at least an annual basis, during the [1st, 2nd, 3rd, 4th] quarter of the calendar year, reviews the process for non-conforming instances. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
    a. Distributes copies of the change to key personnel; and

[527] *NIST SP 800-171A / CMMC 2.0: 3.10.3[b] / PE.L1-3.10.3[b] | NIST SP 800-171A R3: A.03.10.07.b*