

YOUR LOGO GOES HERE

SYSTEM SECURITY PLAN (SSP)

NIST 800-171 R2 / CMMC 2.0

ACME Consultants, LLP

SCOPING:

- **Name of System:** [name of contractor's internal, unclassified information system the SSP addresses]
- **DUNS #:** [contractor's DUNS #]
- **Contract #:** [contractor's contract # or other type of agreement description]
- **CAGE Code #:** [contractor's CAGE code #]

DISTRIBUTION: [list who this SSP is distributed to (e.g., contracting official, prime contractors, etc.)]

REVISION DATE: [list the date of the last revision]

SENSITIVE

Access Limited to Authorized Personnel

TABLE OF CONTENTS

| | |
|--|-----------|
| PREPARED BY & RECORD OF CHANGES | 8 |
| PREPARED BY | 8 |
| REVISION HISTORY | 8 |
| OWNERSHIP & CYBERSECURITY OVERVIEW | 9 |
| GENERAL DESCRIPTION / PURPOSE | 9 |
| CONTRACTS CONTAINING CUI | 9 |
| SYSTEM IDENTIFICATION - CUI OVERVIEW | 9 |
| KEY STAKEHOLDERS | 9 |
| DOCUMENTATION REPOSITORY | 10 |
| DATA PROTECTION CONSIDERATIONS | 10 |
| ADDITIONAL COMPLIANCE REQUIREMENTS | 10 |
| <i>STATUTORY REQUIREMENTS</i> | <i>10</i> |
| <i>REGULATORY REQUIREMENTS</i> | <i>10</i> |
| <i>CONTRACTUAL REQUIREMENTS</i> | <i>11</i> |
| SYSTEM ENVIRONMENT | 12 |
| OPERATING MODEL | 12 |
| INTERCONNECTIVITY OVERVIEW | 14 |
| IDENTIFICATION & AUTHENTICATION OVERVIEW | 14 |
| SYSTEM COMPONENTS & NETWORK BOUNDARIES | 14 |
| <i>HIGH-LEVEL NETWORK DIAGRAM</i> | <i>15</i> |
| <i>DATA FLOW DIAGRAM</i> | <i>16</i> |
| ROLES & PRIVILEGES | 17 |
| SUPPLY CHAIN OVERVIEW | 18 |
| ONGOING MAINTENANCE & SUPPORT PLAN | 18 |
| SYSTEM DEVELOPMENT LIFE CYCLE (SDLC) | 19 |
| OPERATIONAL PHASE | 19 |
| MILESTONES | 19 |
| IDENTIFIED DEFICIENCIES & REMEDIATION PLAN | 20 |
| SECURITY REQUIREMENTS | 20 |
| IDENTIFIED CONTROL / PRACTICE DEFICIENCIES | 20 |
| GLOSSARY: ACRONYMS & DEFINITIONS | 21 |
| ACRONYMS | 21 |
| DEFINITIONS | 22 |
| APPENDICES | 23 |
| APPENDIX A: DATA PROTECTION CONSIDERATIONS | 23 |
| <i>A-1: DATA SENSITIVITY</i> | <i>23</i> |
| <i>A-2: SAFETY & CRITICALITY</i> | <i>25</i> |
| <i>A-3: BASIC ASSURANCE REQUIREMENTS</i> | <i>27</i> |
| <i>A-4: ENHANCED ASSURANCE REQUIREMENTS</i> | <i>27</i> |
| APPENDIX B: HARDWARE AND SOFTWARE INVENTORY (HSI) | 28 |
| <i>B-1: HARDWARE ASSET</i> | <i>28</i> |
| <i>B-2: SOFTWARE ASSET</i> | <i>28</i> |
| APPENDIX C: INTERCONNECTIVITY DOCUMENTATION | 29 |
| <i>C-2: NECESSARY PORTS, PROTOCOLS & SERVICES</i> | <i>29</i> |
| APPENDIX D: EXTERNAL SYSTEM CONNECTIONS | 30 |
| APPENDIX E: ADDITIONAL SECURITY CONSIDERATIONS | 31 |
| <i>E-1: SPECIFIC RULES OF BEHAVIOR REQUIREMENTS</i> | <i>31</i> |
| <i>E-2: SPECIFIC SECURITY AWARENESS TRAINING REQUIREMENTS</i> | <i>31</i> |
| APPENDIX F: CYBERSECURITY ROLES & RESPONSIBILITIES | 32 |
| <i>F-1: INFORMATION SECURITY ROLE CATEGORIES</i> | <i>32</i> |
| <i>F-2: INFORMATION SECURITY SPECIALTY AREAS (ROLES)</i> | <i>33</i> |
| ANNEX 1 – SECURITY REQUIREMENTS (NIST SP 800-171 CUI & NFO CONTROLS / CMMC PRACTICES) | 39 |
| NIST SP 800-171 APPENDIX D: 3.1 ACCESS CONTROL | 39 |

| | |
|---|-----------|
| 3.1.1 (AC.L1-3.1.1) LIMIT SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, OR DEVICES (INCLUDING OTHER SYSTEMS). | 39 |
| 3.1.2 (AC.L1-3.1.2) LIMIT SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE. | 40 |
| 3.1.3 (AC.L2-3.1.3) CONTROL THE FLOW OF CUI IN ACCORDANCE WITH APPROVED AUTHORIZATIONS. | 40 |
| 3.1.4 (AC.L2-3.1.4) SEPARATE THE DUTIES OF INDIVIDUALS TO REDUCE THE RISK OF MALEVOLENT ACTIVITY WITHOUT COLLUSION. | 41 |
| 3.1.5 (AC.L2-3.1.5) EMPLOY THE PRINCIPLE OF LEAST PRIVILEGE, INCLUDING FOR SPECIFIC SECURITY FUNCTIONS AND PRIVILEGED ACCOUNTS. | 42 |
| 3.1.6 (AC.L2-3.1.6) USE NON-PRIVILEGED ACCOUNTS OR ROLES WHEN ACCESSING NON-SECURITY FUNCTIONS. | 43 |
| 3.1.7 (AC.L2-3.1.7) PREVENT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS AND AUDIT THE EXECUTION OF SUCH FUNCTIONS. | 44 |
| 3.1.8 (AC.L2-3.1.8) LIMIT UNSUCCESSFUL LOGON ATTEMPTS. | 44 |
| 3.1.9 (AC.L2-3.1.9) PROVIDE PRIVACY AND SECURITY NOTICES CONSISTENT WITH APPLICABLE CUI RULES. | 45 |
| 3.1.10 (AC.L2-3.1.10) USE SESSION LOCK WITH PATTERN-HIDING DISPLAYS TO PREVENT ACCESS AND VIEWING OF DATA AFTER PERIOD OF INACTIVITY. | 46 |
| 3.1.11 (AC.L2-3.1.11) TERMINATE (AUTOMATICALLY) A USER SESSION AFTER A DEFINED CONDITION. | 47 |
| 3.1.12 (AC.L2-3.1.12) MONITOR AND CONTROL REMOTE ACCESS SESSIONS. | 47 |
| 3.1.13 (AC.L2-3.1.13) EMPLOY CRYPTOGRAPHIC MECHANISMS TO PROTECT THE CONFIDENTIALITY OF REMOTE ACCESS SESSIONS. | 48 |
| 3.1.14 (AC.L2-3.1.14) ROUTE REMOTE ACCESS VIA MANAGED ACCESS CONTROL POINTS. | 49 |
| 3.1.15 (AC.L2-3.1.15) AUTHORIZE REMOTE EXECUTION OF PRIVILEGED COMMANDS AND REMOTE ACCESS TO SECURITY-RELEVANT INFORMATION. | 50 |
| 3.1.16 (AC.L2-3.1.16) AUTHORIZE WIRELESS ACCESS PRIOR TO ALLOWING SUCH CONNECTIONS. | 51 |
| 3.1.17 (AC.L2-3.1.17) PROTECT WIRELESS ACCESS USING AUTHENTICATION AND ENCRYPTION. | 51 |
| 3.1.18 (AC.L2-3.1.18) CONTROL CONNECTION OF MOBILE DEVICES. | 52 |
| 3.1.19 (AC.L2-3.1.19) ENCRYPT CUI ON MOBILE DEVICES AND MOBILE COMPUTING PLATFORMS. | 53 |
| 3.1.20 (AC.L1-3.1.20) VERIFY AND CONTROL/LIMIT CONNECTIONS TO AND USE OF EXTERNAL SYSTEMS. | 53 |
| 3.1.21 (AC.L2-3.1.21) LIMIT USE OF ORGANIZATIONAL PORTABLE STORAGE DEVICES ON EXTERNAL SYSTEMS. | 54 |
| 3.1.22 (AC.L1-3.1.22) CONTROL CUI POSTED OR PROCESSED ON PUBLICLY ACCESSIBLE SYSTEMS. | 55 |
| NIST SP 800-171 APPENDIX D: 3.2 AWARENESS & TRAINING | 57 |
| 3.2.1 (AT.L2-3.2.1) ENSURE THAT MANAGERS, SYSTEMS ADMINISTRATORS, AND USERS OF ORGANIZATIONAL SYSTEMS ARE MADE AWARE OF THE SECURITY RISKS ASSOCIATED WITH THEIR ACTIVITIES AND OF THE APPLICABLE POLICIES, STANDARDS, AND PROCEDURES RELATED TO THE SECURITY OF THOSE SYSTEMS. | 57 |
| 3.2.2 (AT.L2-3.2.2) ENSURE THAT ORGANIZATIONAL PERSONNEL ARE ADEQUATELY TRAINED TO CARRY OUT THEIR ASSIGNED INFORMATION SECURITY-RELATED DUTIES AND RESPONSIBILITIES. | 58 |
| 3.2.3 (AT.L2-3.2.3) PROVIDE SECURITY AWARENESS TRAINING ON RECOGNIZING AND REPORTING POTENTIAL INDICATORS OF INSIDER THREAT. | 58 |
| NIST SP 800-171 APPENDIX D: 3.3 AUDIT & ACCOUNTABILITY | 60 |
| 3.3.1 (AU.L2-3.3.1) CREATE, PROTECT, AND RETAIN SYSTEM AUDIT RECORDS TO THE EXTENT NEEDED TO ENABLE THE MONITORING, ANALYSIS, INVESTIGATION, AND REPORTING OF UNLAWFUL, UNAUTHORIZED, OR INAPPROPRIATE SYSTEM ACTIVITY. | 60 |
| 3.3.2 (AU.L2-3.3.2) ENSURE THAT THE ACTIONS OF INDIVIDUAL SYSTEM USERS CAN BE UNIQUELY TRACED TO THOSE USERS SO THEY CAN BE HELD ACCOUNTABLE FOR THEIR ACTIONS. | 61 |
| 3.3.3 (AU.L2-3.3.3) REVIEW AND UPDATE AUDITED EVENTS. | 61 |
| 3.3.4 (AU.L2-3.3.4) ALERT IN THE EVENT OF AN AUDIT PROCESS FAILURE. | 62 |
| 3.3.5 (AU.L2-3.3.5) CORRELATE AUDIT REVIEW, ANALYSIS, AND REPORTING PROCESSES FOR INVESTIGATION AND RESPONSE TO INDICATIONS OF INAPPROPRIATE, SUSPICIOUS, OR UNUSUAL ACTIVITY. | 63 |
| 3.3.6 (AU.L2-3.3.6) PROVIDE AUDIT REDUCTION AND REPORT GENERATION TO SUPPORT ON-DEMAND ANALYSIS AND REPORTING. | 64 |
| 3.3.7 (AU.L2-3.3.7) PROVIDE A SYSTEM CAPABILITY THAT COMPARES AND SYNCHRONIZES INTERNAL SYSTEM CLOCKS WITH AN AUTHORITATIVE SOURCE TO GENERATE TIME STAMPS FOR AUDIT RECORDS. | 64 |
| 3.3.8 (AU.L2-3.3.8) PROTECT AUDIT INFORMATION AND AUDIT TOOLS FROM UNAUTHORIZED ACCESS, MODIFICATION, AND DELETION. | 65 |
| 3.3.9 (AU.L2-3.3.9) LIMIT MANAGEMENT OF AUDIT FUNCTIONALITY TO A SUBSET OF PRIVILEGED USERS. | 66 |
| NIST SP 800-171 APPENDIX D: 3.4 CONFIGURATION MANAGEMENT | 68 |
| 3.4.1 (CM.L2-3.4.1) ESTABLISH AND MAINTAIN BASELINE CONFIGURATIONS AND INVENTORIES OF ORGANIZATIONAL SYSTEMS (INCLUDING HARDWARE, SOFTWARE, FIRMWARE, AND DOCUMENTATION) THROUGHOUT THE RESPECTIVE SYSTEM DEVELOPMENT LIFE CYCLES. | 68 |
| 3.4.2 (CM.L2-3.4.2) ESTABLISH AND ENFORCE SECURITY CONFIGURATION SETTINGS FOR INFORMATION TECHNOLOGY PRODUCTS EMPLOYED IN ORGANIZATIONAL SYSTEMS. | 69 |
| 3.4.3 (CM.L2-3.4.3) TRACK, REVIEW, APPROVE/DISAPPROVE, AND AUDIT CHANGES TO ORGANIZATIONAL SYSTEMS. | 69 |

| | |
|--|-----------|
| 3.4.4 (CM.L2-3.4.4) ANALYZE THE SECURITY IMPACT OF CHANGES PRIOR TO IMPLEMENTATION. | 70 |
| 3.4.5 (CM.L2-3.4.5) DEFINE, DOCUMENT, APPROVE, AND ENFORCE PHYSICAL AND LOGICAL ACCESS RESTRICTIONS ASSOCIATED WITH CHANGES TO ORGANIZATIONAL SYSTEMS. | 71 |
| 3.4.6 (CM.L2-3.4.6) EMPLOY THE PRINCIPLE OF LEAST FUNCTIONALITY BY CONFIGURING ORGANIZATIONAL SYSTEMS TO PROVIDE ONLY ESSENTIAL CAPABILITIES. | 72 |
| 3.4.7 (CM.L2-3.4.7) RESTRICT, DISABLE, AND PREVENT THE USE OF NONESSENTIAL FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES. | 73 |
| 3.4.8 (CM.L2-3.4.8) APPLY DENY-BY-EXCEPTION (BLACKLIST) POLICY TO PREVENT THE USE OF UNAUTHORIZED SOFTWARE OR DENY-ALL, PERMIT-BY-EXCEPTION (WHITELISTING) POLICY TO ALLOW THE EXECUTION OF AUTHORIZED SOFTWARE. | 74 |
| 3.4.9 (CM.L2-3.4.9) CONTROL AND MONITOR USER-INSTALLED SOFTWARE. | 75 |
| NIST SP 800-171 APPENDIX D: 3.5 IDENTIFICATION & AUTHENTICATION | 77 |
| 3.5.1 (IA.L1-3.5.1) IDENTIFY SYSTEM USERS, PROCESSES ACTING ON BEHALF OF USERS, OR DEVICES. | 77 |
| 3.5.2 (IA.L1-3.5.2) AUTHENTICATE (OR VERIFY) THE IDENTITIES OF THOSE USERS, PROCESSES, OR DEVICES, AS A PREREQUISITE TO ALLOWING ACCESS TO ORGANIZATIONAL SYSTEMS. | 77 |
| 3.5.3 (IA.L2-3.5.3) USE MULTIFACTOR AUTHENTICATION FOR LOCAL AND NETWORK ACCESS TO PRIVILEGED ACCOUNTS AND FOR NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS. | 78 |
| 3.5.4 (IA.L2-3.5.4) EMPLOY REPLAY-RESISTANT AUTHENTICATION MECHANISMS FOR NETWORK ACCESS TO PRIVILEGED AND NON-PRIVILEGED ACCOUNTS. | 79 |
| 3.5.5 (IA.L2-3.5.5) PREVENT REUSE OF IDENTIFIERS FOR A DEFINED PERIOD. | 80 |
| 3.5.6 (IA.L2-3.5.6) DISABLE IDENTIFIERS AFTER A DEFINED PERIOD OF INACTIVITY. | 80 |
| 3.5.7 (IA.L2-3.5.7) ENFORCE A MINIMUM PASSWORD COMPLEXITY AND CHANGE OF CHARACTERS WHEN NEW PASSWORDS ARE CREATED. | 81 |
| 3.5.8 (IA.L2-3.5.8) PROHIBIT PASSWORD REUSE FOR A SPECIFIED NUMBER OF GENERATIONS. | 82 |
| 3.5.9 (IA.L2-3.5.9) ALLOW TEMPORARY PASSWORD USE FOR SYSTEM LOGONS WITH AN IMMEDIATE CHANGE TO A PERMANENT PASSWORD. | 83 |
| 3.5.10 (IA.L2-3.5.10) STORE AND TRANSMIT ONLY CRYPTOGRAPHICALLY-PROTECTED PASSWORDS. | 83 |
| 3.5.11 (IA.L2-3.5.11) OBSCURE FEEDBACK OF AUTHENTICATION INFORMATION. | 84 |
| NIST SP 800-171 APPENDIX D: 3.6 INCIDENT RESPONSE | 86 |
| 3.6.1 (IR.L2-3.6.1) ESTABLISH AN OPERATIONAL INCIDENT-HANDLING CAPABILITY FOR ORGANIZATIONAL SYSTEMS THAT INCLUDES ADEQUATE PREPARATION, DETECTION, ANALYSIS, CONTAINMENT, RECOVERY, AND USER RESPONSE ACTIVITIES. | 86 |
| 3.6.2 (IR.L2-3.6.2) TRACK, DOCUMENT, AND REPORT INCIDENTS TO APPROPRIATE ORGANIZATIONAL OFFICIALS AND/OR AUTHORITIES. | 87 |
| 3.6.3 (IR.L2-3.6.3) TEST THE ORGANIZATIONAL INCIDENT RESPONSE CAPABILITY. | 88 |
| NIST SP 800-171 APPENDIX D: 3.7 MAINTENANCE | 89 |
| 3.7.1 (MA.L2-3.7.1) PERFORM MAINTENANCE ON ORGANIZATIONAL SYSTEMS. | 89 |
| 3.7.2 (MA.L2-3.7.2) PROVIDE EFFECTIVE CONTROLS ON THE TOOLS, TECHNIQUES, MECHANISMS, AND PERSONNEL USED TO CONDUCT SYSTEM MAINTENANCE. | 89 |
| 3.7.3 (MA.L2-3.7.3) ENSURE EQUIPMENT REMOVED FOR OFF-SITE MAINTENANCE IS SANITIZED OF ANY CUI. | 90 |
| 3.7.4 (MA.L2-3.7.4) CHECK MEDIA CONTAINING DIAGNOSTIC AND TEST PROGRAMS FOR MALICIOUS CODE BEFORE THE MEDIA ARE USED IN ORGANIZATIONAL SYSTEMS. | 91 |
| 3.7.5 (MA.L2-3.7.5) REQUIRE MULTIFACTOR AUTHENTICATION TO ESTABLISH NONLOCAL MAINTENANCE SESSIONS VIA EXTERNAL NETWORK CONNECTIONS AND TERMINATE SUCH CONNECTIONS WHEN NONLOCAL MAINTENANCE IS COMPLETE. | 91 |
| 3.7.6 (MA.L2-3.7.6) SUPERVISE THE MAINTENANCE ACTIVITIES OF MAINTENANCE PERSONNEL WITHOUT REQUIRED ACCESS AUTHORIZATION. | 92 |
| NIST SP 800-171 APPENDIX D: 3.8 MEDIA PROTECTION | 94 |
| 3.8.1 (MP.L2-3.8.1) PROTECT (E.G., PHYSICALLY CONTROL AND SECURELY STORE) SYSTEM MEDIA CONTAINING CUI, BOTH PAPER AND DIGITAL. | 94 |
| 3.8.2 (MP.L2-3.8.2) LIMIT ACCESS TO CUI ON SYSTEM MEDIA TO AUTHORIZED USERS. | 94 |
| 3.8.3 (MP.L1-3.8.3) SANITIZE OR DESTROY SYSTEM MEDIA CONTAINING CUI BEFORE DISPOSAL OR RELEASE FOR REUSE. | 95 |
| 3.8.4 (MP.L2-3.8.4) MARK MEDIA WITH NECESSARY CUI MARKINGS AND DISTRIBUTION LIMITATIONS. | 96 |
| 3.8.5 (MP.L2-3.8.5) CONTROL ACCESS TO MEDIA CONTAINING CUI AND MAINTAIN ACCOUNTABILITY FOR MEDIA DURING TRANSPORT OUTSIDE OF CONTROLLED AREAS. | 97 |
| 3.8.6 (MP.L2-3.8.6) IMPLEMENT CRYPTOGRAPHIC MECHANISMS TO PROTECT THE CONFIDENTIALITY OF INFORMATION STORED ON DIGITAL MEDIA DURING TRANSPORT OUTSIDE OF CONTROLLED AREAS UNLESS OTHERWISE PROTECTED BY ALTERNATIVE PHYSICAL SAFEGUARDS. | 97 |
| 3.8.7 (MP.L2-3.8.7) CONTROL THE USE OF REMOVABLE MEDIA ON SYSTEM COMPONENTS. | 98 |
| 3.8.8 (MP.L2-3.8.8) PROHIBIT THE USE OF PORTABLE STORAGE DEVICES WHEN SUCH DEVICES HAVE NO IDENTIFIABLE OWNER. | 99 |
| 3.8.9 (MP.L2-3.8.9) PROTECT THE CONFIDENTIALITY OF BACKUP CUI AT STORAGE LOCATIONS. | 99 |

| | |
|--|------------|
| NIST SP 800-171 APPENDIX D: 3.9 PERSONNEL SECURITY | 101 |
| 3.9.1 (PS.L2-3.9.1) SCREEN INDIVIDUALS PRIOR TO AUTHORIZING ACCESS TO ORGANIZATIONAL SYSTEMS CONTAINING CUI. | 101 |
| 3.9.2 (PS.L2-3.9.2) ENSURE THAT CUI AND ORGANIZATIONAL SYSTEMS CONTAINING CUI ARE PROTECTED DURING AND AFTER PERSONNEL ACTIONS SUCH AS TERMINATIONS AND TRANSFERS. | 101 |
| NIST SP 800-171 APPENDIX D: 3.10 PHYSICAL PROTECTION | 103 |
| 3.10.1 (PE.L1-3.10.1) LIMIT PHYSICAL ACCESS TO ORGANIZATIONAL SYSTEMS, EQUIPMENT, AND THE RESPECTIVE OPERATING ENVIRONMENTS TO AUTHORIZED INDIVIDUALS. | 103 |
| 3.10.2 (PE.L2-3.10.2) PROTECT AND MONITOR THE PHYSICAL FACILITY AND SUPPORT INFRASTRUCTURE FOR ORGANIZATIONAL SYSTEMS. | 103 |
| 3.10.3 (PE.L1-3.10.3) ESCORT VISITORS AND MONITOR VISITOR ACTIVITY. | 104 |
| 3.10.4 (PE.L1-3.10.4) MAINTAIN AUDIT LOGS OF PHYSICAL ACCESS. | 105 |
| 3.10.5 (PE.L1-3.10.5) CONTROL AND MANAGE PHYSICAL ACCESS DEVICES. | 106 |
| 3.10.6 (PE.L2-3.10.6) ENFORCE SAFEGUARDING MEASURES FOR CUI AT ALTERNATE WORK SITES (E.G., TELEWORK SITES). | 106 |
| NIST SP 800-171 APPENDIX D: 3.11 RISK ASSESSMENT | 108 |
| 3.11.1 (RM.L2-3.11.1) PERIODICALLY ASSESS THE RISK TO ORGANIZATIONAL OPERATIONS (INCLUDING MISSION, FUNCTIONS, IMAGE, OR REPUTATION), ORGANIZATIONAL ASSETS, AND INDIVIDUALS, RESULTING FROM THE OPERATION OF ORGANIZATIONAL SYSTEMS AND THE ASSOCIATED PROCESSING, STORAGE, OR TRANSMISSION OF CUI. | 108 |
| 3.11.2 (RM.L2-3.11.2) SCAN FOR VULNERABILITIES IN ORGANIZATIONAL SYSTEMS AND APPLICATIONS PERIODICALLY AND WHEN NEW VULNERABILITIES AFFECTING THOSE SYSTEMS AND APPLICATIONS ARE IDENTIFIED. | 108 |
| 3.11.3 (RM.L2-3.11.3) REMEDIATE VULNERABILITIES IN ACCORDANCE WITH ASSESSMENTS OF RISK. | 109 |
| NIST SP 800-171 APPENDIX D: 3.12 SECURITY ASSESSMENT | 111 |
| 3.12.1 (CA.L2-3.12.1) PERIODICALLY ASSESS THE SECURITY CONTROLS IN ORGANIZATIONAL SYSTEMS TO DETERMINE IF THE CONTROLS ARE EFFECTIVE IN THEIR APPLICATION. | 111 |
| 3.12.2 (CA.L2-3.12.2) DEVELOP AND IMPLEMENT PLANS OF ACTION DESIGNED TO CORRECT DEFICIENCIES AND REDUCE OR ELIMINATE VULNERABILITIES IN ORGANIZATIONAL SYSTEMS. | 111 |
| 3.12.3 (CA.L2-3.12.3) MONITOR SECURITY CONTROLS ON AN ONGOING BASIS TO ENSURE THE CONTINUED EFFECTIVENESS OF THE CONTROLS. | 112 |
| 3.12.4 (CA.L2-3.12.4) DEVELOP, DOCUMENT, AND PERIODICALLY UPDATE SYSTEM SECURITY PLANS THAT DESCRIBE SYSTEM BOUNDARIES, SYSTEM ENVIRONMENTS OF OPERATION, HOW SECURITY REQUIREMENTS ARE IMPLEMENTED, AND THE RELATIONSHIPS WITH OR CONNECTIONS TO OTHER SYSTEMS. | 113 |
| NIST SP 800-171 APPENDIX D: 3.13 SYSTEM & COMMUNICATIONS PROTECTION | 115 |
| 3.13.1 (SC.L1-3.13.1) MONITOR, CONTROL, AND PROTECT COMMUNICATIONS (E.G., INFORMATION TRANSMITTED OR RECEIVED BY ORGANIZATIONAL SYSTEMS) AT THE EXTERNAL BOUNDARIES AND KEY INTERNAL BOUNDARIES OF ORGANIZATIONAL SYSTEMS. | 115 |
| 3.13.2 (SC.L2-3.13.2) EMPLOY ARCHITECTURAL DESIGNS, SOFTWARE DEVELOPMENT TECHNIQUES, AND SYSTEMS ENGINEERING PRINCIPLES THAT PROMOTE EFFECTIVE INFORMATION SECURITY WITHIN ORGANIZATIONAL SYSTEMS. | 116 |
| 3.13.3 (SC.L2-3.13.3) SEPARATE USER FUNCTIONALITY FROM SYSTEM MANAGEMENT FUNCTIONALITY. | 117 |
| 3.13.4 (SC.L2-3.13.4) PREVENT UNAUTHORIZED AND UNINTENDED INFORMATION TRANSFER VIA SHARED SYSTEM RESOURCES. | 117 |
| 3.13.5 (SC.L1-3.13.5) IMPLEMENT SUBNETWORKS FOR PUBLICLY ACCESSIBLE SYSTEM COMPONENTS THAT ARE PHYSICALLY OR LOGICALLY SEPARATED FROM INTERNAL NETWORKS. | 118 |
| 3.13.6 (SC.L2-3.13.6) DENY NETWORK COMMUNICATIONS TRAFFIC BY DEFAULT AND ALLOW NETWORK COMMUNICATIONS TRAFFIC BY EXCEPTION (E.G., DENY ALL, PERMIT BY EXCEPTION). | 119 |
| 3.13.7 (SC.L2-3.13.7) PREVENT REMOTE DEVICES FROM SIMULTANEOUSLY ESTABLISHING NON-REMOTE CONNECTIONS WITH ORGANIZATIONAL SYSTEMS AND COMMUNICATING VIA SOME OTHER CONNECTION TO RESOURCES IN EXTERNAL NETWORKS (E.G. SPLIT TUNNELING). | 120 |
| 3.13.8 (SC.L2-3.13.8) IMPLEMENT CRYPTOGRAPHIC MECHANISMS TO PREVENT UNAUTHORIZED DISCLOSURE OF CUI DURING TRANSMISSION UNLESS OTHERWISE PROTECTED BY ALTERNATIVE PHYSICAL SAFEGUARDS. | 120 |
| 3.13.9 (SC.L2-3.13.9) TERMINATE NETWORK CONNECTIONS ASSOCIATED WITH COMMUNICATIONS SESSIONS AT THE END OF THE SESSIONS OR AFTER A DEFINED PERIOD OF INACTIVITY. | 121 |
| 3.13.10 (SC.L2-3.13.10) ESTABLISH AND MANAGE CRYPTOGRAPHIC KEYS FOR CRYPTOGRAPHY EMPLOYED IN ORGANIZATIONAL SYSTEMS. | 122 |
| 3.13.11 (SC.L2-3.13.11) EMPLOY FIPS-VALIDATED CRYPTOGRAPHY WHEN USED TO PROTECT THE CONFIDENTIALITY OF CUI. | 123 |
| 3.13.12 (SC.L2-3.13.12) PROHIBIT REMOTE ACTIVATION OF COLLABORATIVE COMPUTING DEVICES AND PROVIDE INDICATION OF DEVICES IN USE TO USERS PRESENT AT THE DEVICE. | 123 |
| 3.13.13 (SC.L2-3.13.13) CONTROL AND MONITOR THE USE OF MOBILE CODE. | 124 |
| 3.13.14 (SC.L2-3.13.14) CONTROL AND MONITOR THE USE OF VOICE OVER INTERNET PROTOCOL (VOIP) TECHNOLOGIES. | 125 |
| 3.13.15 (SC.L2-3.13.15) PROTECT THE AUTHENTICITY OF COMMUNICATIONS SESSIONS. | 125 |
| 3.13.16 (SC.L2-3.13.16) PROTECT THE CONFIDENTIALITY OF CUI AT REST. | 126 |
| NIST SP 800-171 APPENDIX D: 3.14 SYSTEM & INFORMATION INTEGRITY | 128 |

| | |
|---|-----|
| 3.14.1 (SI.L1-3.14.1) IDENTIFY, REPORT, AND CORRECT INFORMATION AND SYSTEM FLAWS IN A TIMELY MANNER. | 128 |
| 3.14.2 (SI.L1-3.14.2) PROVIDE PROTECTION FROM MALICIOUS CODE AT APPROPRIATE LOCATIONS WITHIN ORGANIZATIONAL SYSTEMS. | 129 |
| 3.14.3 (SI.L2-3.14.3) MONITOR SYSTEM SECURITY ALERTS AND ADVISORIES AND TAKE APPROPRIATE ACTIONS IN RESPONSE. | 129 |
| 3.14.4 (SI.L1-3.14.4) UPDATE MALICIOUS CODE PROTECTION MECHANISMS WHEN NEW RELEASES ARE AVAILABLE. | 130 |
| 3.14.5 (SI.L1-3.14.5) PERFORM PERIODIC SCANS OF ORGANIZATIONAL SYSTEMS AND REAL-TIME SCANS OF FILES FROM EXTERNAL SOURCES AS FILES ARE DOWNLOADED, OPENED, OR EXECUTED. | 131 |
| 3.14.6 (SI.L2-3.14.6) MONITOR ORGANIZATIONAL SYSTEMS, INCLUDING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC, TO DETECT ATTACKS AND INDICATORS OF POTENTIAL ATTACKS. | 132 |
| 3.14.7 (SI.L2-3.14.7) IDENTIFY UNAUTHORIZED USE OF ORGANIZATIONAL SYSTEMS. | 132 |

NIST SP 800-171 APPENDIX E: NON-FEDERAL ORGANIZATION (NFO) CONTROLS **134**

| | |
|---|-----|
| AC-1 ACCESS CONTROL POLICY & PROCEDURES | 134 |
| AT-1 SECURITY AWARENESS & TRAINING POLICY & PROCEDURES | 134 |
| AT-4 SECURITY TRAINING RECORDS | 135 |
| AU-1 AUDIT & ACCOUNTABILITY POLICY & PROCEDURES | 135 |
| CA-1 SECURITY ASSESSMENT & AUTHORIZATION POLICY & PROCEDURES | 136 |
| CA-2(1) SECURITY ASSESSMENTS INDEPENDENT ASSESSORS | 136 |
| CA-3 SYSTEM INTERCONNECTIONS | 137 |
| CA-3(5) SYSTEM INTERCONNECTIONS RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS | 138 |
| CA-7(1) CONTINUOUS MONITORING INDEPENDENT ASSESSMENT | 138 |
| CA-9 INTERNAL SYSTEM CONNECTIONS | 139 |
| CM-1 CONFIGURATION MANAGEMENT POLICY & PROCEDURES | 139 |
| CM-2(1) BASELINE CONFIGURATION REVIEWS & UPDATES | 140 |
| CM-2(7) BASELINE CONFIGURATION CONFIGURE SYSTEMS, COMPONENTS OR DEVICES FOR HIGH-RISK AREAS | 140 |
| CM-3(2) CONFIGURATION CHANGE CONTROL TEST / VALIDATE / DOCUMENT CHANGES | 141 |
| CM-8(5) SYSTEM COMPONENT INVENTORY NO DUPLICATE ACCOUNTING OF COMPONENTS | 141 |
| CM-9 CONFIGURATION MANAGEMENT PLAN | 142 |
| IA-1 IDENTIFICATION & AUTHENTICATION POLICY & PROCEDURES | 143 |
| IR-1 INCIDENT RESPONSE POLICY & PROCEDURES | 143 |
| IR-8 INCIDENT RESPONSE PLAN | 144 |
| MA-1 SYSTEM MAINTENANCE POLICY & PROCEDURES | 144 |
| MA-4(2) NON-LOCAL MAINTENANCE DOCUMENT NON-LOCAL MAINTENANCE | 145 |
| MP-1 MEDIA PROTECTION POLICY & PROCEDURES | 145 |
| PE-1 PHYSICAL & ENVIRONMENTAL PROTECTION POLICY & PROCEDURES | 146 |
| PE-6(1) MONITORING PHYSICAL ACCESS INTRUSION ALARMS / SURVEILLANCE EQUIPMENT | 147 |
| PE-8 VISITOR ACCESS RECORDS | 147 |
| PE-16 DELIVERY & REMOVAL | 148 |
| PL-1 SECURITY PLANNING POLICY & PROCEDURES | 148 |
| PL-2(3) SYSTEM SECURITY PLAN PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES | 149 |
| PL-4 RULES OF BEHAVIOR | 149 |
| PL-4(1) RULES OF BEHAVIOR SOCIAL MEDIA & NETWORKING RESTRICTIONS | 150 |
| PL-8 INFORMATION SECURITY ARCHITECTURE | 150 |
| PS-1 PERSONNEL SECURITY POLICY & PROCEDURES | 151 |
| PS-6 ACCESS AGREEMENTS | 152 |
| PS-7 THIRD-PARTY PERSONNEL SECURITY | 152 |
| PS-8 PERSONNEL SANCTIONS | 153 |
| RA-1 RISK ASSESSMENT POLICY & PROCEDURES | 153 |
| RA-5(1) VULNERABILITY SCANNING UPDATE TOOL CAPABILITY | 154 |
| RA-5(2) VULNERABILITY SCANNING UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED | 154 |
| SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES | 155 |
| SA-2 ALLOCATION OF RESOURCES | 156 |
| SA-3 SYSTEM DEVELOPMENT LIFE CYCLE | 156 |
| SA-4 ACQUISITION PROCESS | 157 |
| SA-4(1) ACQUISITION PROCESS FUNCTIONAL PROPERTIES OF SECURITY CONTROLS | 157 |
| SA-4(2) ACQUISITION PROCESS DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS | 158 |
| SA-4(9) ACQUISITION PROCESS FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE | 158 |
| SA-4(10) ACQUISITION PROCESS USE OF APPROVED PIV PRODUCTS | 159 |
| SA-5 SYSTEM DOCUMENTATION | 159 |

| | |
|---|-----|
| SA-9 EXTERNAL SYSTEM SERVICES | 160 |
| SA-9(2) EXTERNAL SYSTEM SERVICES IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES | 161 |
| SA-10 DEVELOPER CONFIGURATION MANAGEMENT | 161 |
| SA-11 DEVELOPER SECURITY TESTING AND EVALUATION | 162 |
| SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES | 162 |
| SC-7(3) BOUNDARY PROTECTION ACCESS POINTS | 163 |
| SC-7(4) BOUNDARY PROTECTION EXTERNAL TELECOMMUNICATIONS SERVICES | 163 |
| SC-20 SECURE NAME /ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) | 164 |
| SC-21 SECURE NAME /ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | 165 |
| SC-22 ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE | 165 |
| SC-39 PROCESS ISOLATION | 166 |
| SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES | 166 |
| SI-4(5) SYSTEM MONITORING SYSTEM-GENERATED ALERTS | 167 |
| SI-16 MEMORY PROTECTION | 167 |

EXAMPLE

OWNERSHIP & CYBERSECURITY OVERVIEW

The objective of the System Security Plan (SSP) document is to have a simple, easy-to-reference document that covers pertinent information about the Controlled Unclassified Information (CUI) environment. This is a “living document” that is meant to be updated as conditions change.

The goal of this document is simple - anyone not familiar with the CUI environment should be able to read it and gain a fundamental understanding of the systems involved, the risks, and the security controls required to maintain an acceptable level of security.

Essentially, this document provides a centralized repository for knowledge that is specific to the CUI environment and its applicable security controls. The SSP reflects input from those responsible for the systems that make up the CUI environment, including information owners, system operators, and other stakeholders.

GENERAL DESCRIPTION / PURPOSE

[provide a high-level description of the purpose of the system/application/service that is in scope]

CONTRACTS CONTAINING CUI

[list the applicable contracts that contain CUI protection requirements]

SYSTEM IDENTIFICATION - CUI OVERVIEW

[provide a descriptive narrative of how CUI is defined by the applicable contract(s). Include a description of the function/purpose of the internal unclassified information system(s)/network(s) that is(are) addressed in the plan.]

Example:

Contract XXXXXX defines CUI as schematic diagrams that are pertinent to the XYZ project.

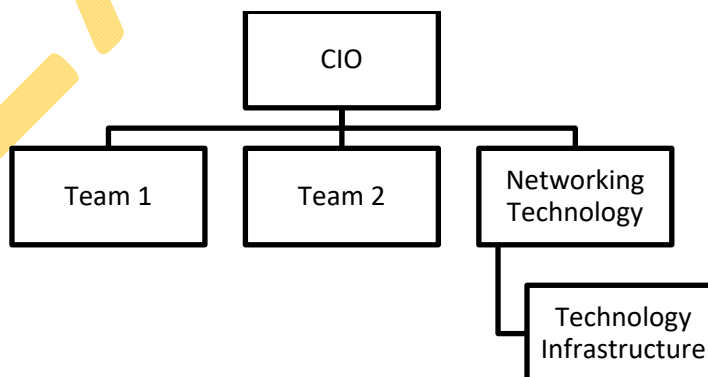
KEY STAKEHOLDERS

CUI protection is a combined effort from the following stakeholders:

- Stakeholder 1, Position
- Stakeholder 2, Position
- Stakeholder 3, Position

Example:

It is sometimes worthwhile to include an organization chart, since this can assist with problem escalations.



DOCUMENTATION REPOSITORY

Information security-related project and system documentation can be found at:

[add URL for network share, etc.]

DATA PROTECTION CONSIDERATIONS

The assets within the CUI environment are assessed, based on data sensitivity and mission criticality, in order to ensure the appropriate level of protection is applied.

[Appendix A \(Data Protection Considerations\)](#) provides the methodology for how data is classified in terms of data sensitivity and criticality to the CUI environment.

ADDITIONAL COMPLIANCE REQUIREMENTS

In addition to CUI protection requirements from the Defense Federal Acquisition Regulation Supplement (DFARS 252.204-7012), the following compliance requirements are also applicable, due to overlapping requirements for cybersecurity and privacy controls:

STATUTORY REQUIREMENTS

[fill-in applicable statutory requirements]

Example statutory requirements include:

- *Cable Communications Policy Act (CCPA)*
- *Children's Internet Protection Act (CIPA)*
- *Children's Online Privacy Protection Act (COPPA)*
- *Computer Fraud and Abuse Act (CFAA)*
- *Consumer Credit Reporting Reform Act (CCRRA)*
- *Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)*
- *Electronic Communications Privacy Act (ECPA)*
- *Electronic Freedom of Information Act (E-FOIA)*
- *Electronic Funds Transfer Act (EFTA)*
- *Fair & Accurate Credit Transactions Act (FACTA)*
- *Fair Credit Reporting Act (FCRA)*
- *Family Education Rights and Privacy Act (FERPA)*
- *Federal Information Security Management Act (FISMA)*
- *Federal Trade Commission Act (FTCA)*
- *Gramm Leach Bliley Act (GLBA)*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *Privacy Act*
- *Right to Financial Privacy Act (RFPA)*
- *Sarbanes Oxley Act (SOX)*
- *Telecommunications Act*
- *Telephone Consumer Protection Act (TCPA)*
- *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)*
- *Video Privacy Protection Act (VPPA)*
- *US State - Massachusetts 201 CMR 17.00*
- *US State - Oregon Identity Theft Protection Act (ORS 646A)*
- *International - United Kingdom Data Protection Act (UK DPA)*

REGULATORY REQUIREMENTS

[fill-in applicable regulatory requirements]

Example regulatory requirements include:

- *Federal Acquisition Regulation (FAR 52.204-21)*
- *European Union General Data Protection Regulation (EU GDPR)*

- *Financial Industry Regulatory Authority (FINRA)*
- *National Industrial Security Program Operating Manual (NISPOM)*
- *Department of Defense Information Assurance Risk Management Framework (DIARMF) (DoDI 8510.01)*
- *Federal Risk and Authorization Management Program (FedRAMP)*
- *New York Department of Financial Services (NY DFS) 23 NYCCRR 500*
- *North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)*

CONTRACTUAL REQUIREMENTS

[fill-in applicable contractual requirements]

Example contractual requirements include:

- *Payment Card Industry Data Security Standard (PCI DSS)*
- *Generally Accepted Privacy Principles (GAPP)*
- *American Institute of CPAs Service Organization Control (AICPA SOC2)*
- *Center for Internet Security Critical Security Controls (CIS CSC)*
- *Cloud Security Alliance Cloud Controls Matrix (CSA CCM)*

EXAMPLE

SYSTEM ENVIRONMENT

This section contains a detailed topology narrative and graphic shall that clearly depicts the system environment, including system boundaries, system interconnections, and key components.

Instruction: This does not require depicting every device, but would include an instance of operating systems in use, virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations, firewalls, routers, switches, copiers, printers, lab equipment, etc. If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. Include or reference (e.g., to an inventory database or spreadsheet) a complete hardware and software inventory, including make/model/version and maintenance responsibility.

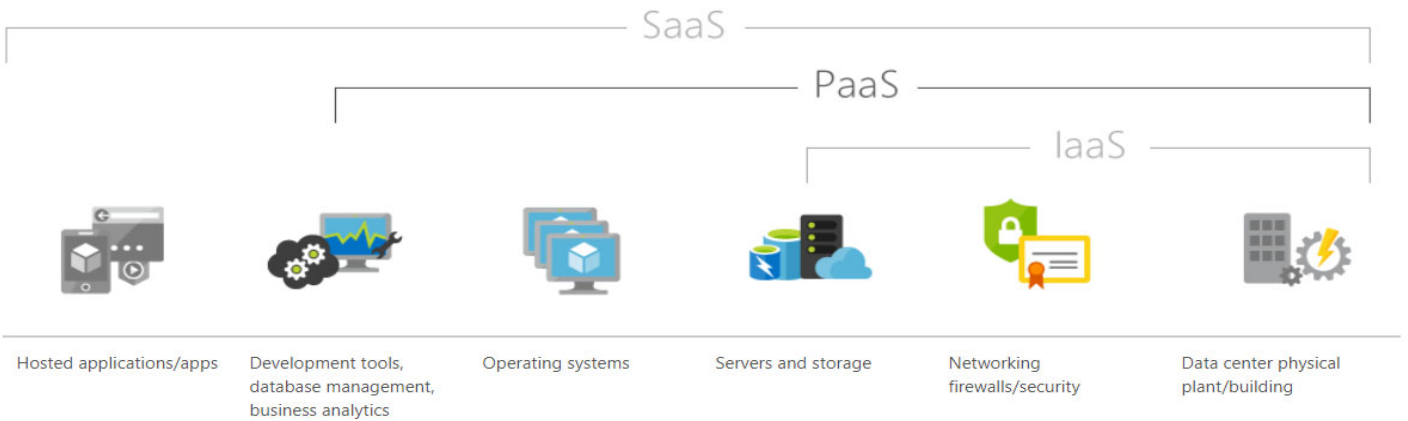
Delete this and all other instructions from your final version of this document.

OPERATING MODEL

| Operating Environment Where CUI Exists (check all that apply) | | |
|---|---------------------|--|
| <input type="checkbox"/> | Public Cloud | Cloud services and infrastructure supporting multiple organizations and clients |
| <input type="checkbox"/> | Private Cloud | Cloud services and infrastructure dedicated to a specific organization and no other clients |
| <input type="checkbox"/> | Data Center | Company-owned & operated datacenter. |
| <input type="checkbox"/> | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) |
| <input type="checkbox"/> | Dispersed Endpoints | CUI can be found on workstations and other endpoints. |
| <input type="checkbox"/> | Other | Explain: |

| High-Level Overview of Where CUI Is Stored, Transmitted or Processed (check all that apply) | | |
|---|------------------------------------|--|
| <input type="checkbox"/> | End User Workstations | End user workstations (e.g., desktops & laptops) |
| <input type="checkbox"/> | Mobile Devices | Mobile devices (e.g., tablets or smartphones) |
| <input type="checkbox"/> | Industrial Control System (ICS) | Devices that control manufacturing processes |
| <input type="checkbox"/> | Internal application/service | Internal application (e.g., ERM, SAP, ticket system, change control, etc.) |
| <input type="checkbox"/> | Software as a Service (SaaS) | Web-based applications (e.g., Google Apps, Salesforce, GoToMeeting, WebEx) |
| <input type="checkbox"/> | Platform as a Service (PaaS) | Web-based major applications (e.g., Azure Cloud Services) |
| <input type="checkbox"/> | Infrastructure as a Service (IaaS) | Cloud environments (e.g., Azure, AWS, Rackspace) |
| <input type="checkbox"/> | Other | Explain: |

Example:



EXAMPLE

INTERCONNECTIVITY OVERVIEW

[provide a descriptive narrative how systems within the CUI environment communicate – is it internal only? Does it communicate outside of the company’s network?]

[Appendix B \(Hardware and Software Inventory\)](#), provides a breakdown of assets that comprise the CUI environment in both the production and development instances.

[Appendix C \(Interconnectivity Documentation\)](#), provides a detailed description of ports, protocols and services, in use within the CUI environment.

IDENTIFICATION & AUTHENTICATION OVERVIEW

[provide a descriptive narrative of how the system handles identification & authentication]
[describe how many users are involved. Also describe how many administrators are involved]

Example:

Vendor accounts will be created in the ACME instance and pushed to the XXXXX instance. Only one account per vendor will be allowed. The vendor account will be inactivated when the vendor submits their documentation.

The two instances of XXXXX will use different methods for user identification and authentication, since the XXXXX-hosted instance will be externally accessible to vendors.

ACME Instance

- User Names: AD integration
- Passwords: AD integration
- Account Reviews: Tied into AD
- Account Deactivation: Tied into AD

XXXXX Instance

- User Names:
 - ACME Users: Ping Federate (AD integration)
 - Non-ACME Users: Local XXXXX account (hosted instance only)
- Passwords:
 - ACME Users: Ping Federate (AD integration)
 - Non-ACME Users: TBD
- Account Reviews:
 - ACME Users: Ping Federate (AD integration)
 - Non-ACME Users: TBD
- Account Deactivation: Tied into AD
 - ACME Users: Ping Federate (AD integration)
 - Non-ACME Users: TBD

SYSTEM COMPONENTS & NETWORK BOUNDARIES

[provide a descriptive narrative of what makes up the CUI operating environment, including defining the assets involved and the system boundaries]

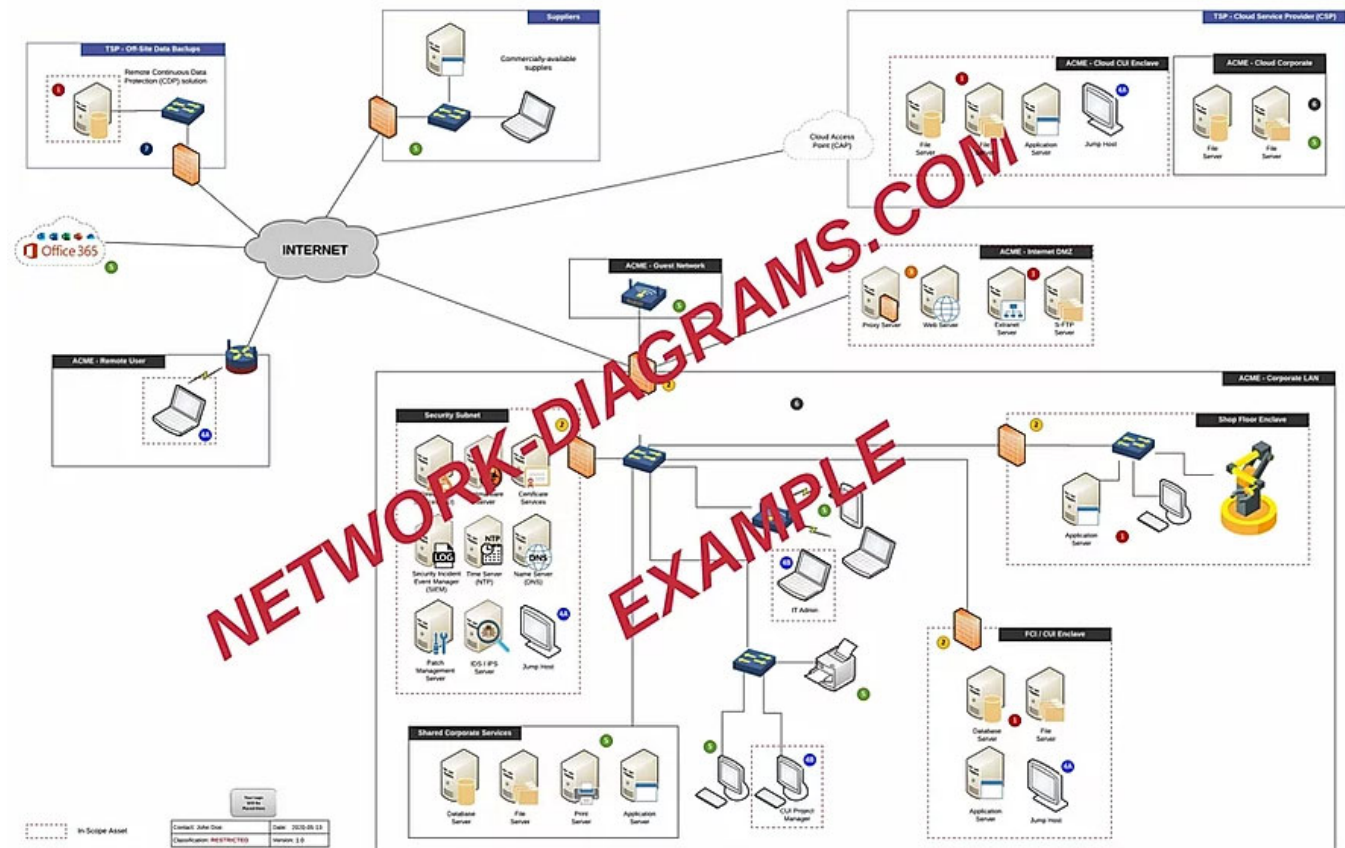
Example:

XYZ is designed with two distinct instances, running in two different environments:

- *Internal XXXXX instance that is housed in ACME’s datacenter (Datacenter 1); and*
- *Hosted XXXXX instance in Microsoft’s Azure private cloud.*

HIGH-LEVEL NETWORK DIAGRAM

[add network diagram here - if you do not have a network diagram, you can work with <https://www.network-diagrams.com> to obtain a quality network diagram and data flow diagram for your CUI environment (see below for an example)]



Instruction: Useful tools to create a high-level network diagram include:

- Microsoft Visio (network diagram templates) or
- Department of Homeland Security's free tool, the Cyber Security Evaluation Tool (CSET) - <https://www.cisa.gov/downloading-and-installing-cset>

Provide a diagram that portrays the system boundaries and all applicable connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system.

Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

Formal names of components as they are known by the project team in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

DATA FLOW DIAGRAM

[add data flow diagram here]

Instruction: Useful tools to create a data flow diagram include:

- Microsoft Visio (network diagram templates) or
- Department of Homeland Security's free tool, the Cyber Security Evaluation Tool (CSET) - https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

EXAMPLE

ROLES & PRIVILEGES

Cybersecurity roles and responsibilities are based on the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, as described in NIST Special Publication 800-181. [Appendix F \(Cybersecurity Roles and Responsibilities\)](#) lists the types of roles and responsibilities that are applicable to the CUI environment.

[specific to handling CUI, identify the roles and associated privileges of those roles]

| Role | Internal or External | Privileged (P) Non-Privileged (NP) or No Logical Access (NLA) | Authorized Privileges | Functions Performed |
|------|----------------------|---|-----------------------|---------------------|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Example:

| Role | Internal or External | Privileged (P) Non-Privileged (NP) or No Logical Access (NLA) | Authorized Privileges | Functions Performed |
|----------------------|----------------------|---|-----------------------|--|
| UNIX sysadmin | Internal | P | Full Access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client administrator | Internal | NP | Portal administration | Add/remote client users. Create, modify and delete client applications |
| Program director | Internal | NLA | None | Reviews, approves and enforces policy |

Instruction: This table must include all roles including systems administrators and database administrators as a role types. This includes web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact CUI.

This table must also include whether these roles are fulfilled by foreign nationals or roles that exist outside the United States, since that may impact compliance obligations.

Delete this and all other instructions from your final version of this document.

SUPPLY CHAIN OVERVIEW

[provide a descriptive narrative of how vendors are involved in supporting how CUI is stored, processed or transmitted, if applicable]

Example:

There is currently only one (1) vendor involved in the supply chain for the CUI environment:

- *Vendor: VENDOR1*
- *Contract #: (123) 456-7890*
- *Support Contact: Jim Somebody*
- *Services Purchased: Platinum Support (contract #123456789) 24x7x365 support*

ONGOING MAINTENANCE & SUPPORT PLAN

[provide a descriptive narrative of how maintenance operations are conducted. This includes patch management and vulnerability remediation from ongoing vulnerability management scans]

Example:

VENDOR1 is currently providing Professional Services (PS) support for the initial configuration and integration of the tool. Once Technology Infrastructure has its XYZ administrator fully integrated, the amount of external support from XYZ, will decrease. Professional Services (PS) engagements will be on a case-by-case basis to augment CS Governance's organic capabilities.

XYZ System

Asset Owner: John Doe, SOC Director & contact #

Asset Custodian(s):

- *Primary XXXXX, Role & contact #*
- *Secondary XXXXX, Role & contact #*

Patching is conducted in accordance with the Vulnerability & Patch Management Program (VPMP).

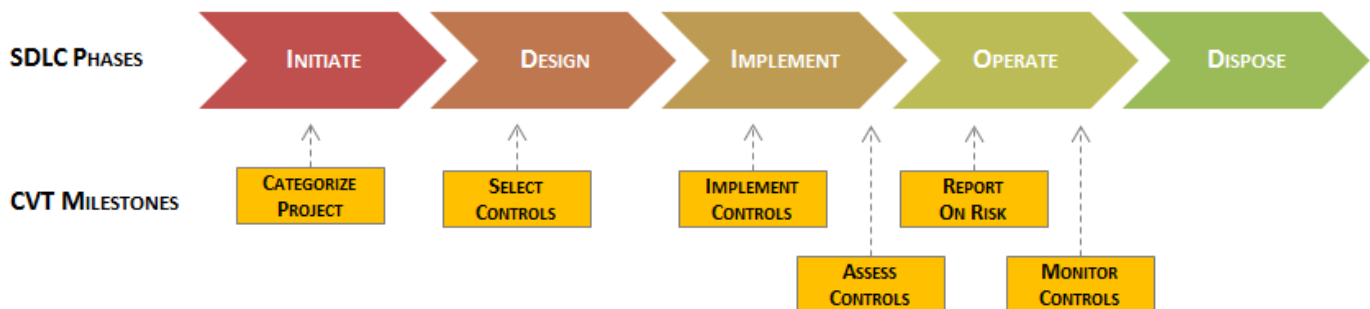
SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

OPERATIONAL PHASE

The CUI environment is currently:

| Operational Status | | |
|--------------------------|--------------------|--|
| <input type="checkbox"/> | Operational | CUI is being used by systems in a production environment. |
| <input type="checkbox"/> | Under Development | CUI is being used by systems in a developmental / testing environment. |
| <input type="checkbox"/> | Major Modification | CUI systems are undergoing a major change, development, or transition. |
| <input type="checkbox"/> | Other | Explain: |

The dates planned and dates reached for each phase of the System Development Lifecycle (SDLC) and Control Validation Testing (CVT) milestones:



| Traditional SDLC Phase | Date Planned | Date Reached |
|----------------------------|--------------|--------------|
| Initiate | ? | ? |
| Develop / Design / Acquire | ? | ? |
| Implement | ? | ? |
| Operate & Maintain | ? | ? |
| Dispose | ? | ? |

MILESTONES

[Enter a narrative about the planned milestones planned for the life of the systems that make up the CUI environment]

Example:

XYZ is currently in the operate phase. Updates and changes to XYZ is expected throughout the fiscal year. There are currently no envisioned alterations to XYZ that would severely affect its operational status during updates and changes to the system environment. XYZ will be undergoing major modification during the course of FY2018, including network engineering, security engineering, and systems engineering

INSTRUCTIONS: All milestones about operational status should be stated. If the system is about to go through a major revision, all milestones along the way should be listed as well.

Delete this and all other instructions from your final version of this document.

ANNEX 1 – SECURITY REQUIREMENTS (NIST SP 800-171 CUI & NFO CONTROLS / CMMC PRACTICES)

The SSP consists of the applicable NIST SP 800-53 rev4 controls, as mapped in NIST SP 800-171 Appendix D (CUI controls) and Appendix E (NFO controls).

NIST SP 800-171 APPENDIX D: 3.1 ACCESS CONTROL

These controls are associated with access control:

3.1.1 (AC.L1-3.1.1) LIMIT SYSTEM ACCESS TO AUTHORIZED USERS, PROCESSES ACTING ON BEHALF OF AUTHORIZED USERS, OR DEVICES (INCLUDING OTHER SYSTEMS).

| Summary of NIST SP 800-171 & CMMC Controls Implementation |
|---|
| Implementation Status (check all that apply): <input type="checkbox"/> Implemented (control execution internal to ACME) <input type="checkbox"/> Implemented (control execution external to ACME via contract and/or shared responsibility) <input type="checkbox"/> Partially Implemented (<i>Identified in POA&M</i>) <input type="checkbox"/> Planned (<i>Identified in POA&M</i>) <input type="checkbox"/> Alternative Implementation (<i>Compensating Controls</i>) <input type="checkbox"/> Not applicable |
| Process Owner: [name of the individual or team accountable for the procedure being performed] |
| Process Operator: [name of the individual or team responsible to perform the procedure's tasks] |
| Occurrence: [how often the procedure need is performed] |
| Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence] |
| Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure] |
| Description of Control Implementation: Supporting policy(es): Identification & Authentication (IAC) & Third-Party Management (TPM) Supporting standard(s): IAC-15, IAC-20, TPM-05 & TPM-05.2 Supporting procedure(s): P-IAC-25, P-IAC-20, P-TPM-05 & P-TPM-05.2 [briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement] |
| Assessment Objectives (AOs) - Determine if: 3.1.3[a] - information flow control policies are defined. [briefly describe how this AO is implemented] 3.1.3[b] - methods and enforcement mechanisms for controlling the flow of CUI are defined. [briefly describe how this AO is implemented] 3.1.3[c] - designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. [briefly describe how this AO is implemented] 3.1.3[d] - authorizations for controlling the flow of CUI are defined. [briefly describe how this AO is implemented] 3.1.3[e] - approved authorizations for controlling the flow of CUI are enforced. [briefly describe how this AO is implemented] |

Summary of NIST SP 800-171 & CMMC Controls Implementation

3.1.2 (AC.L1-3.1.2) LIMIT SYSTEM ACCESS TO THE TYPES OF TRANSACTIONS AND FUNCTIONS THAT AUTHORIZED USERS ARE PERMITTED TO EXECUTE.

Summary of NIST SP 800-171 & CMMC Controls Implementation

Implementation Status (check all that apply):

- Implemented (control execution internal to ACME)
- Implemented (control execution external to ACME via contract and/or shared responsibility)
- Partially Implemented (*Identified in POA&M*)
- Planned (*Identified in POA&M*)
- Alternative Implementation (*Compensating Controls*)
- Not applicable

Process Owner: [name of the individual or team accountable for the procedure being performed]

Process Operator: [name of the individual or team responsible to perform the procedure's tasks]

Occurrence: [how often the procedure need is performed]

Location of Additional Documentation:

[location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]

Technology in Use:

[if applicable, the name of the application/system/service used to perform the procedure]

Description of Control Implementation:

Supporting policy(es): Identification & Authentication (IAC)
Supporting standard(s): IAC-15
Supporting procedure(s): P-IAC-15

[briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement]

Assessment Objectives (AOs) - Determine if:

3.1.2[a] - the types of transactions and functions that authorized users are permitted to execute are defined.

[briefly describe how this AO is implemented]

3.1.2[b] - system access is limited to the defined types of transactions and functions for authorized users.

[briefly describe how this AO is implemented]

3.1.3 (AC.L2-3.1.3) CONTROL THE FLOW OF CUI IN ACCORDANCE WITH APPROVED AUTHORIZATIONS.

Summary of NIST SP 800-171 & CMMC Controls Implementation

Implementation Status (check all that apply):

- Implemented (control execution internal to ACME)
- Implemented (control execution external to ACME via contract and/or shared responsibility)
- Partially Implemented (*Identified in POA&M*)
- Planned (*Identified in POA&M*)
- Alternative Implementation (*Compensating Controls*)
- Not applicable

| Summary of NIST SP 800-171 & CMMC Controls Implementation |
|--|
| Process Owner: [name of the individual or team accountable for the procedure being performed] |
| Process Operator: [name of the individual or team responsible to perform the procedure's tasks] |
| Occurrence: [how often the procedure need is performed] |
| Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence] |
| Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure] |
| <p>Description of Control Implementation: Supporting policy(es): Data Classification & Handling (DCH), Identification & Authentication (IAC) & Network Security (NET) Supporting standard(s): DCH-03, IAC-08, NET-04 & NET-18 Supporting procedure(s): P-DCH-03, P-IAC-08, P-NET-04 & P-NET-18</p> <p>[briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement]</p> <p>Assessment Objectives (AOs) - Determine if:</p> <p>3.1.3[a] - information flow control policies are defined. [briefly describe how this AO is implemented]</p> <p>3.1.3[b] - methods and enforcement mechanisms for controlling the flow of CUI are defined. [briefly describe how this AO is implemented]</p> <p>3.1.3[c] - designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. [briefly describe how this AO is implemented]</p> <p>3.1.3[d] - authorizations for controlling the flow of CUI are defined. [briefly describe how this AO is implemented]</p> <p>3.1.3[e] - approved authorizations for controlling the flow of CUI are enforced. [briefly describe how this AO is implemented]</p> |

3.1.4 (AC.L2-3.1.4) SEPARATE THE DUTIES OF INDIVIDUALS TO REDUCE THE RISK OF MALEVOLENT ACTIVITY WITHOUT COLLUSION.

| Summary of NIST SP 800-171 & CMMC Controls Implementation |
|--|
| Implementation Status (check all that apply): <input type="checkbox"/> Implemented (control execution internal to ACME) <input type="checkbox"/> Implemented (control execution external to ACME via contract and/or shared responsibility) <input type="checkbox"/> Partially Implemented (<i>Identified in POA&M</i>) <input type="checkbox"/> Planned (<i>Identified in POA&M</i>) <input type="checkbox"/> Alternative Implementation (<i>Compensating Controls</i>) <input type="checkbox"/> Not applicable |
| Process Owner: [name of the individual or team accountable for the procedure being performed] |
| Process Operator: [name of the individual or team responsible to perform the procedure's tasks] |

Summary of NIST SP 800-171 & CMMC Controls Implementation

Occurrence: [how often the procedure need is performed]

Location of Additional Documentation:
[location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]

Technology in Use:
[if applicable, the name of the application/system/service used to perform the procedure]

Description of Control Implementation:
Supporting policy(es): Human Resources Security (HRS)
Supporting standard(s): HRS-11
Supporting procedure(s): P-HRS-11

[briefly describe the solution and how it is implemented or simply reference the policy/standard/procedure where more detailed information can address this requirement]

Assessment Objectives (AOs) - Determine if:

3.1.4[a] - the duties of individuals requiring separation are defined.
[briefly describe how this AO is implemented]

3.1.4[b] - responsibilities for duties that require separation are assigned to separate individuals.
[briefly describe how this AO is implemented]

3.1.4[c] - access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.
[briefly describe how this AO is implemented]

3.1.5 (AC.L2-3.1.5) EMPLOY THE PRINCIPLE OF LEAST PRIVILEGE, INCLUDING FOR SPECIFIC SECURITY FUNCTIONS AND PRIVILEGED ACCOUNTS.

Summary of NIST SP 800-171 & CMMC Controls Implementation

Implementation Status (check all that apply):

- Implemented (control execution internal to ACME)
- Implemented (control execution external to ACME via contract and/or shared responsibility)
- Partially Implemented (*Identified in POA&M*)
- Planned (*Identified in POA&M*)
- Alternative Implementation (*Compensating Controls*)
- Not applicable

Process Owner: [name of the individual or team accountable for the procedure being performed]

Process Operator: [name of the individual or team responsible to perform the procedure's tasks]

Occurrence: [how often the procedure need is performed]

Location of Additional Documentation:
[location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]

Technology in Use:
[if applicable, the name of the application/system/service used to perform the procedure]

Description of Control Implementation:
Supporting policy(es): Identification & Authentication (IAC)
Supporting standard(s): IAC-16, IAC-16.1, IAC-21, IAC-21.1 & IAC-21.3
Supporting procedure(s): P-IAC-16, P-IAC-16.1, P-IAC-21, P-IAC-21.1 & P-IAC-21.3