**Project #3: ITSecurity Controls Baseline for Red Clay Renovations**

To ensure compatibility with existing policy and documentation, Red Clay Renovations’ IT Security policies, plans, and procedures will continue to use the following security control classes (management, operational, technical), as defined in NIST SP 800-53 rev 3 (p. 6).



**Security Controls Baseline**

Red Clay Renovations Security Controls Baseline shall include the security controls listed below. Security control definitions and implementation guidance shall be obtained from the most recent version of NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

1. **AC: Access Controls (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| AC-1  | Access Control Policy and Procedures  | AC-1  |
| AC-2  | Account Management  | AC-2 (1) (2) (3) (4)  |
| AC-3  | Access Enforcement  | AC-3  |
| AC-4  | Information Flow Enforcement  | AC-4  |
| AC-5  | Separation of Duties  | AC-5  |
| AC-6  | Least Privilege  | AC-6 (1) (2) (5) (9) (10)  |
| AC-7  | Unsuccessful Logon Attempts  | AC-7  |
| AC-8  | System Use Notification  | AC-8  |
| AC-11  | Session Lock  | AC-11 (1)  |
| AC-12  | Session Termination  | AC-12  |
| AC-14  | Permitted Actions without Identification or Authentication  | AC-14  |
| AC-17  | Remote Access  | AC-17 (1) (2) (3) (4)  |
| AC-18  | Wireless Access  | AC-18 (1)  |
| AC-19  | Access Control for Mobile Devices  | AC-19 (5)  |
| AC-20  | Use of External Information Systems  | AC-20 (1) (2)  |
| AC-21  | Information Sharing  | AC-21  |
| AC-22  | Publicly Accessible Content  | AC-22  |

1. **AT: Awareness and Training (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| AT-1  | Security Awareness and Training Policy and Procedures  | AT-1  |
| AT-2  | Security Awareness Training  | AT-2 (2)  |
| AT-3  | Role-Based Security Training  | AT-3  |
| AT-4  | Security Training Records  | AT-4  |

1. **AU: Audit and Accountability (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| AU-1  | Audit and Accountability Policy and Procedures  | AU-1  |
| AU-2  | Audit Events  | AU-2 (3)  |
| AU-3  | Content of Audit Records  | AU-3 (1)  |
| AU-4  | Audit Storage Capacity  | AU-4  |
| AU-5  | Response to Audit Processing Failures  | AU-5  |
| AU-6  | Audit Review, Analysis, and Reporting  | AU-6 (1) (3)  |
| AU-7  | Audit Reduction and Report Generation  | AU-7 (1)  |
| AU-8  | Time Stamps  | AU-8 (1)  |
| AU-9  | Protection of Audit Information  | AU-9 (4)  |
| AU-10  | Non-repudiation  | Not Selected  |
| AU-11  | Audit Record Retention  | AU-11  |
| AU-12  | Audit Generation  | AU-12  |

1. **CA: Security Assessment and Authorization (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| CA-1  | Security Assessment and Authorization Policies and Procedures  | CA-1  |
| CA-2  | Security Assessments  | CA-2 (1)  |
| CA-3  | System Interconnections  | CA-3 (5)  |
| CA-5  | Plan of Action and Milestones  | CA-5  |
| CA-6  | Security Authorization  | CA-6  |
| CA-7  | Continuous Monitoring  | CA-7 (1)  |
| CA-9  | Internal System Connections  | CA-9  |

1. **CM: Configuration Management (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| CM-1  | Configuration Management Policy and Procedures  | CM-1  |
| CM-2  | Baseline Configuration  | CM-2 (1) (3) (7)  |
| CM-3  | Configuration Change Control  | CM-3 (2)  |
| CM-4  | Security Impact Analysis  | CM-4  |
| CM-5  | Access Restrictions for Change  | CM-5  |
| CM-6  | Configuration Settings  | CM-6  |
| CM-7  | Least Functionality  | CM-7 (1) (2) (4)  |
| CM-8  | Information System Component Inventory  | CM-8 (1) (3) (5)  |
| CM-9  | Configuration Management Plan  | CM-9  |
| CM-10  | Software Usage Restrictions  | CM-10  |
| CM-11  | User-Installed Software  | CM-11  |

1. **Contingency Planning (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| CP-1  | Contingency Planning Policy and Procedures  | CP-1  |
| CP-2  | Contingency Plan  | CP-2 (1) (3) (8)  |
| CP-3  | Contingency Training  | CP-3  |
| CP-4  | Contingency Plan Testing  | CP-4 (1)  |
| CP-5  | **Withdrawn**  | ---  |
| CP-6  | Alternate Storage Site  | CP-6 (1) (3)  |
| CP-7  | Alternate Processing Site  | CP-7 (1) (2) (3)  |
| CP-8  | Telecommunications Services  | CP-8 (1) (2)  |
| CP-9  | Information System Backup  | CP-9 (1)  |
| CP-10  | Information System Recovery and Reconstitution  | CP-10 (2)  |

1. **IA: Identification and Authentication (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| IA-1  | Identification and Authentication Policy and Procedures  | IA-1  |
| IA-2  | Identification and Authentication (Organizational Users)  | IA-2 (1) (2) (3) (8) (11) (12)  |
| IA-3  | Device Identification and Authentication  | IA-3  |
| IA-4  | Identifier Management  | IA-4  |
| IA-5  | Authenticator Management  | IA-5 (1) (2) (3) (11)  |
| IA-6  | Authenticator Feedback  | IA-6  |
| IA-7  | Cryptographic Module Authentication  | IA-7  |
| IA-8  | Identification and Authentication (Non-Organizational Users)  | IA-8 (1) (2) (3) (4)  |

1. **IR: Incident Response (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| IR-1  | Incident Response Policy and Procedures  | IR-1  |
| IR-2  | Incident Response Training  | IR-2  |
| IR-3  | Incident Response Testing  | IR-3 (2)  |
| IR-4  | Incident Handling  | IR-4 (1)  |
| IR-5  | Incident Monitoring  | IR-5  |
| IR-6  | Incident Reporting  | IR-6 (1)  |
| IR-7  | Incident Response Assistance  | IR-7 (1)  |
| IR-8  | Incident Response Plan  | IR-8  |

1. **MA: Maintenance (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| MA-1  | System Maintenance Policy and Procedures  | MA-1  |
| MA-2  | Controlled Maintenance  | MA-2  |
| MA-3  | Maintenance Tools  | MA-3 (1) (2)  |
| MA-4  | Nonlocal Maintenance  | MA-4 (2)  |
| MA-5  | Maintenance Personnel  | MA-5  |

1. **MP: Media Protection (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| MP-1  | Media Protection Policy and Procedures  | MP-1  |
| MP-2  | Media Access  | MP-2  |
| MP-3  | Media Marking  | MP-3  |
| MP-4  | Media Storage  | MP-4  |
| MP-5  | Media Transport  | MP-5 (4)  |
| MP-6  | Media Sanitization  | MP-6  |
| MP-7  | Media Use  | MP-7 (1)  |

1. **PE: Physical and Environmental Protection (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| PE-1  | Physical and Environmental Protection Policy and Procedures  | PE-1  |
| PE-2  | Physical Access Authorizations  | PE-2  |
| PE-3  | Physical Access Control  | PE-3  |
| PE-4  | Access Control for Transmission Medium  | PE-4  |
| PE-5  | Access Control for Output Devices  | PE-5  |
| PE-6  | Monitoring Physical Access  | PE-6 (1)  |
| PE-8  | Visitor Access Records  | PE-8  |
| PE-9  | Power Equipment and Cabling  | PE-9  |
| PE-10  | Emergency Shutoff  | PE-10  |
| PE-11  | Emergency Power  | PE-11  |
| PE-12  | Emergency Lighting  | PE-12  |
| PE-13  | Fire Protection  | PE-13 (3)  |
| PE-14  | Temperature and Humidity Controls  | PE-14  |
| PE-15  | Water Damage Protection  | PE-15  |
| PE-16  | Delivery and Removal  | PE-16  |
| PE-17  | Alternate Work Site  | PE-17  |

1. **PL: Planning (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| PL-1  | Security Planning Policy and Procedures  | PL-1  |
| PL-2  | System Security Plan  | PL-2 (3)  |
| PL-4  | Rules of Behavior  | PL-4 (1)  |
| PL-8  | Information Security Architecture  | PL-8  |

1. **PS: Personnel Security (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| PS-1  | Personnel Security Policy and Procedures  | PS-1  |
| PS-2  | Position Risk Designation  | PS-2  |
| PS-3  | Personnel Screening  | PS-3  |
| PS-4  | Personnel Termination  | PS-4  |
| PS-5  | Personnel Transfer  | PS-5  |
| PS-6  | Access Agreements  | PS-6  |
| PS-7  | Third-Party Personnel Security  | PS-7  |
| PS-8  | Personnel Sanctions  | PS-8  |

1. **RA: Risk Assessment (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| RA-1  | Risk Assessment Policy and Procedures  | RA-1  |
| RA-2  | Security Categorization  | RA-2  |
| RA-3  | Risk Assessment  | RA-3  |
| RA-5  | Vulnerability Scanning  | RA-5 (1) (2) (5)  |

1. **SA: System and Services Acquisition (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| SA-1  | System and Services Acquisition Policy and Procedures  | SA-1  |
| SA-2  | Allocation of Resources  | SA-2  |
| SA-3  | System Development Life Cycle  | SA-3  |
| SA-4  | Acquisition Process  | SA-4 (1) (2) (9) (10)  |
| SA-5  | Information System Documentation  | SA-5  |
| SA-8  | Security Engineering Principles  | SA-8  |
| SA-9  | External Information System Services  | SA-9 (2)  |
| SA-10  | Developer Configuration Management  | SA-10  |
| SA-11  | Developer Security Testing and Evaluation  | SA-11  |

1. **SC: System and Communications Protection (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| SC-1  | System and Communications Protection Policy and Procedures  | SC-1  |
| SC-5 | Denial of Service Protection | SC-5 |
| SC-7 | Boundary Protection | SC-7  |
| SC-8 | Transmission Confidentiality | SC-8 |
| SC-18 | Mobile Code | SC-18 |
| SC-19 | Voice Over Internet Protocol | SC-19 |
| SC-28  | Protection of Information at Rest  | SC-28  |
| SC-39  | Process Isolation  | SC-39  |

1. **SI: System and Information Integrity (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| SI-1  | System and Information Integrity Policy and Procedures  | SI-1  |
| SI-2  | Flaw Remediation  | SI-2 (2)  |
| SI-3  | Malicious Code Protection  | SI-3 (1) (2)  |
| SI-4  | Information System Monitoring  | SI-4 (2) (4) (5)  |
| SI-5  | Security Alerts, Advisories, and Directives  | SI-5  |
| SI-7  | Software, Firmware, and Information Integrity  | SI-7 (1) (7)  |
| SI-8  | Spam Protection  | SI-8 (1) (2)  |
| SI-10  | Information Input Validation  | SI-10  |
| SI-11  | Error Handling  | SI-11  |
| SI-12  | Information Handling and Retention  | SI-12  |
| SI-16  | Memory Protection  | SI-16  |

1. **PM: Program Management (Management Controls Family)**

|  |  |  |
| --- | --- | --- |
| PM-1  | Information Security Program Plan  | all |
| PM-2  | Senior Information Security Officer  | all |
| PM-3  | Information Security Resources  | all |
| PM-4  | Plan of Action and Milestones Process  | all |
| PM-5  | Information System Inventory  | all |
| PM-6  | Information Security Measures of Performance  | all |
| PM-7  | Enterprise Architecture  | all |
| PM-8  | Critical Infrastructure Plan  | all |
| PM-9  | Risk Management Strategy  | all |
| PM-10  | Security Authorization Process  | all |
| PM-11  | Mission/Business Process Definition  | all |
| PM-12  | Insider Threat Program  | all |
| PM-13  | Information Security Workforce  | all |
| PM-14  | Testing, Training, and Monitoring  | all |
| PM-15  | Contacts with Security Groups and Associations  | all |
| PM-16  | Threat Awareness Program  | all |