 **S System Security Plan**

**Project Name/Remedy#:**

**Checklist**

**Instructions –** This checklist should first be completed during ISDM Phase 3 (Requirements Analysis). The required controls should be designed and included in the system and will be validated during ISDM Phase 6 (Integration, Test, Acceptance).

**ISDM Phase 2** – Each security control may be answered by a business unit within DIS or by the Customer (administrative controls). The chart to the right translates the color in the table below to the unit typically charged with responding to the control. Deviations from this are expected based on the level of integration or complexity of the system being assessed. Checklist completion should be performed in a group setting to ensure improved accuracy of collective responses. The ISM, PM, and technical contacts should be included.

♠ - Security risk (use a ♠ to identify security risks, bring to System Owner’s attention for action)

♦ - Audit risk (use a ♦ to identify audit risks, bring to System Owner’s attention for action)

**ISDM Phase 6** – This column is to be completed when the selected controls can be validated through observation or testing of the system. The ISM validates the checklist.

|  |  |
| --- | --- |
| **Team** | **Color** |
| Addressed by existing controls |  |
| BEA |  |
| DBA |  |
| WEBDEV |  |
| Windows (WIN) |  |
| UNIX |  |
| NS (Network Services) |  |
| ISO (Information Security Office) |  |
| Mainframe (MF) |  |
| Business Unit Objective (BIZ) |  |

**O =** Organization-wide function – supporting all baselines, **S =** System, **P =** Personnel

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Control No.** | **Control Name** | **Type of Control/**  **Primary Team** | **Control Consideration**  **(ISDM Phase 2: Requirements Analysis)** | **Validated**  **(ISDM Phase 6: Integration, Test Acceptance)** |
| **Access Control** | | | |  |
| AC-1 | Access Control Policy and Procedures | Technical | O – AP&P 4-05 |  |
| AC-2 | Account Management |
| AC-3 | Access Enforcement | Technical/BEA |  |  |
| AC-4 | Information Flow Enforcement | Technical/BEA |  |  |
| AC-5 | Separation of Duties | Technical/BEA |  |  |
| AC-6 | Least Privilege | Technical/BEA |  |  |
| AC-7 | Unsuccessful Login Attempts | Technical/BEA |  |  |
| AC-8 | System Use Notification | Technical/BEA |  |  |
| AC-9 | Previous Logon (Access) Notification | Technical | N/A |  |
| AC-10 | Concurrent Session Control | Technical | N/A |  |
| AC-11 | Session Lock | Technical/BEA |  |  |
| AC-12 | Session Termination |  | (Withdrawn)\* |  |
| AC-13 | Supervision and Review—Access Control |  | (Withdrawn) |  |
| AC-14 | Permitted Actions without Identification or Authentication | Technical/BEA |  |  |
| AC-15 | Automated Marking |  | (Withdrawn) |  |
| AC-16 | Security Attributes | Technical | N/A |  |
| AC-17 | Remote Access | Technical/BEA |  |  |
| AC-18 | Wireless Access | Technical/BEA |  |  |
| AC-19 | Access Control for Mobile Devices | Technical/BEA |  |  |
| AC-20 | Use of External Information Systems | Technical/BEA |  |  |
| AC-21 | User-Based Collaboration and Information Sharing | Technical/BEA |  |  |
| AC-22 | Publicly Accessible Content | Technical/BEA |  |  |
| **Awareness & Training** | | | |  |
| AT-1 | Security Awareness and Training Policy and Procedures | Operational | O – Security Awareness Training Program |  |
| AT-2 | Security Awareness |
| AT-3 | Security Training |
| AT-4 | Security Training Records |
| AT-5 | Contacts with Security Groups and Associations |
| **Audit & Accountability** | | | |  |
| AU-1 | Audit and Accountability Policy and Procedures | Technical | O – AP&P 4-05. |  |
| AU-2 | Auditable Events | Technical/BIZ |  |  |
| AU-3 | Content of Audit Records | Technical/BIZ |  |  |
| AU-4 | Audit Storage Capacity | Technical/DBA |  |  |
| AU-5 | Response to Audit Processing Failures | Technical/DBA |  |  |
| AU-6 | Audit Review, Analysis, and Reporting |  | (Withdrawn)\* |  |
| AU-7 | Audit Reduction and Report Generation | Technical/WIN |  |  |
| AU-8 | Time Stamps | Technical/BEA |  |  |
| AU-9 | Protection of Audit Information | Technical/BEA |  |  |
| AU-10 | Non-repudiation | Technical | N/A |  |
| AU-11 | Audit Record Retention | Technical/BEA | *Refer to GS1-SL to properly configure, direct questions to the ISO* |  |
| AU-12 | Audit Generation | Technical/BEA |  |  |
| AU-13 | Monitoring for Information Disclosure | Technical | N/A |  |
| AU-14 | Session Audit | Technical | N/A |  |
| **Security Assessment & Authorization** | | | |  |
| CA-1 | Security Assessment and Authorization Policies and Procedures | Management | O – ISDM Toolkit |  |
| CA-2 | Security Assessments | Management | Not currently in place |  |
| CA-3 | Information System Connections | Management/BEA |  |  |
| CA-4 | Security Certification |  | (Withdrawn)\* |  |
| CA-5 | Plan of Action and Milestones | Management | O – ISDM Toolkit |  |
| CA-6 | Security Authorization | Management |
| CA-7 | Continuous Monitoring | Management |
| **Configuration Management** | | | |  |
| CM-1 | Configuration Management Policy and Procedures | Operational | O – ISDM Toolkit |  |
| CM-2 | Baseline Configuration |
| CM-3 | Configuration Change Control |
| CM-4 | Security Impact Analysis |
| CM-5 | Access Restrictions for Change |
| CM-6 | Configuration Settings |
| CM-7 | Least Functionality | O – AP&P 4-03 (X.N. 8) |  |
| CM-8 | Information System Component Inventory | O – AP&P 4-05. |  |
| CM-9 | Configuration Management Plan |
| **Contingency Planning** | | | |  |
| CP-1 | Contingency Planning Policy and Procedures | Operational | O – DR/COOP Function |  |
| CP-2 | Contingency Plan |
| CP-3 | Contingency Training |
| CP-4 | Contingency Plan Testing and Exercises |
| CP-5 | Contingency Plan Update |  | (Withdrawn) |  |
| CP-6 | Alternate Storage Site | Operational | O – DR/COOP Function |  |
| CP-7 | Alternate Processing Site |
| CP-8 | Telecommunications Services |
| CP-9 | Information System Backup | Operational/WIN |  |  |
| CP-10 | Information System Recovery and Reconstitution | Operational/DBA |  |  |
| **I & A** | | | |  |
| IA-1 | Identification and Authentication Policy and Procedures | Technical | O – AP&P’s 4-03, 4-04, and 4-05 |  |
| IA-2 | Identification and Authentication  (Organizational Users) | Technical/BEA |  |  |
| IA-3 | Device Identification and Authentication | Technical/BEA |  |  |
| IA-4 | Identifier Management | Technical | O – AP&P’s 4-03, 4-04, and 4-05 (User Account management). |  |
| IA-5 | Authenticator Management | Technical/BEA |  |  |
| IA-6 | Authenticator Feedback | Technical | Specified in AP&P’s 4-03 |  |
| IA-7 | Cryptographic Module Authentication | Technical/WIN |  |  |
| IA-8 | Identification and Authentication (Non-Organizational Users) | Technical/BEA |  |  |
| **Incident Response** | | | |  |
| IR-1 | Incident Response Policy and Procedures | Operational | O – CSIRT Function |  |
| IR-2 | Incident Response Training |
| IR-3 | Incident Response Testing and Exercises |
| IR-4 | Incident Handling |
| IR-5 | Incident Monitoring |
| IR-6 | Incident Reporting |
| IR-7 | Incident Response Assistance |
| IR-8 | Incident Response Plan |
| **Maintenance** | | | |  |  |  |  |
| MA-1 | System Maintenance Policy and Procedures | Operational | O – Change Management Function |  |
| MA-2 | Controlled Maintenance |
| MA-3 | Maintenance Tools |
| MA-4 | Non-Local Maintenance |
| MA-5 | Maintenance Personnel |
| MA-6 | Timely Maintenance |
| **Media Protection** | | | |  |
| MP-1 | Media Protection Policy and Procedures | Operational | O – Data Center Controls |  |
| MP-2 | Media Access |
| MP-3 | Media Marking |
| MP-4 | Media Storage |
| MP-5 | Media Transport |
| MP-6 | Media Sanitization | Operational | O – Operating Procedure DIS-006 |  |
| **Physical & Environmental Protection** | | | |  |
| PE-1 | Physical and Environmental Protection Policy and Procedures | Operational | O – Data Center Controls |  |
| PE-2 | Physical Access Authorizations |
| PE-3 | Physical Access Control |
| PE-4 | Access Control for Transmission Medium |
| PE-5 | Access Control for Output Devices |
| PE-6 | Monitoring Physical Access |
| PE-7 | Visitor Control |
| PE-8 | Access Records |
| PE-9 | Power Equipment and Power Cabling |
| PE-10 | Emergency Shutoff |
| PE-11 | Emergency Power |
| PE-12 | Emergency Lighting |
| PE-13 | Fire Protection |
| PE-14 | Temperature and Humidity Controls |
| PE-15 | Water Damage Protection |
| PE-16 | Delivery and Removal |
| PE-17 | Alternate Work Site |
| PE-18 | Location of Information System Components |
| PE-19 | Information Leakage |
| **Planning** | | | |  |
| PL-1 | Security Planning Policy and Procedures | Management | O – AP&P 4-03 |  |
| PL-2 | System Security Plan | Management | O – ISDM Toolkit |  |
| PL-3 | System Security Plan Update |  | (Withdrawn)\* |  |
| PL-4 | Rules of Behavior | Management/BEA |  |  |
| PL-5 | Privacy Impact Assessment | Management/BEA |  |  |
| PL-6 | Security-Related Activity Planning | Management | O – ISDM Toolkit, DR & CSIRT functions |  |
| **Personnel Security** | | | |  |
| PS-1 | Personnel Security Policy and Procedures | Operational | O – Multiple DFS AP&P’s |  |
| PS-2 | Position Categorization |
| PS-3 | Personnel Screening |
| PS-4 | Personnel Termination |
| PS-5 | Personnel Transfer |
| PS-6 | Access Agreements |
| PS-7 | Third-Party Personnel Security |
| PS-8 | Personnel Sanctions |
| **Risk Assessment** | | | |  |
| RA-1 | Risk Assessment Policy and Procedures | Management | O – AP&P 4-03 |  |
| RA-2 | Security Categorization | O – SSP |  |
| RA-3 | Risk Assessment | O – SSP Checklist |  |
| RA-4 | Risk Assessment Update |  | (Withdrawn) |  |
| RA-5 | Vulnerability Scanning | Management | To be implemented… |  |
| **System & Services Acquisition** | | | |  |
| SA-1 | System and Services Acquisition Policy and Procedures | Management | O – AP&P 4-06 |  |
| SA-2 | Allocation of Resources | Management | ISDM Toolkit |  |
| SA-3 | Life Cycle Support |
| SA-4 | Acquisitions |
| SA-5 | Information System Documentation |
| SA-6 | Software Usage Restrictions | Management | N/A |  |
| SA-7 | User-Installed Software | Management | N/A |  |
| SA-8 | Security Engineering Principles | Management | ISDM Toolkit |  |
| SA-9 | External Information System Services | Management/BEA | *IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, SERVICES* |  |
| SA-10 | Developer Configuration Management | Management | ISDM Toolkit |  |
| SA-11 | Developer Security Testing | Management | ISDM Toolkit |  |
| SA-12 | Supply Chain Protection | Management | N/A |  |
| SA-13 | Trustworthiness | Management | N/A (pending RMF) |  |
| SA-14 | Critical Information System Components | Management/WINWIN |  |  |
| **System & Communications Protection** | | | |  |
| SC-1 | System and Communications Protection Policy and Procedures | Technical | AP&P 4-03, AP&P 4-04 |  |
| SC-2 | Application Partitioning | Technical/BEA |  |  |
| SC-3 | Security Function Isolation | Technical | N/A |  |
| SC-4 | Information in Shared Resources | Technical/WIN |  |  |
| SC-5 | Denial of Service Protection | Technical/WIN |  |  |
| SC-6 | Resource Priority | Technical | N/A |  |
| SC-7 | Boundary Protection | Technical/WIN |  |  |
| SC-8 | Transmission Integrity | Technical/WIN |  |  |
| SC-9 | Transmission Confidentiality | Technical/WIN |  |  |
| SC-10 | Network Disconnect | Technical/WIN |  |  |
| SC-11 | Trusted Path | Technical | N/A |  |
| SC-12 | Cryptographic Key Establishment and Management | Technical/WIN |  |  |
| SC-13 | Use of Cryptography | Technical/WIN |  |  |
| SC-14 | Public Access Protections | Technical/WIN |  |  |
| SC-15 | Collaborative Computing Devices | Technical | N/A |  |
| SC-16 | Transmission of Security Attributes | Technical | N/A |  |
| SC-17 | Public Key Infrastructure Certificates | Technical | N/A |  |
| SC-18 | Mobile Code | Technical/BEA |  |  |
| SC-19 | Voice Over Internet Protocol | Technical | N/A |  |
| SC-20 | Secure Name /Address Resolution Service (Authoritative Source) | Technical/BEA |  |  |
| SC-21 | Secure Name /Address Resolution Service  (Recursive or Caching Resolver) | Technical/WebDev |  |  |
| SC-22 | Architecture and Provisioning for  Name/Address Resolution Service | Technical/WIN |  |  |
| SC-23 | Session Authenticity | Technical/BEA |  |  |
| SC-24 | Fail in Known State | Technical | N/A |  |
| SC-25 | Thin Nodes | Technical | N/A |  |
| SC-26 | Honey pots | Technical | N/A |  |
| SC-27 | Operating System-Independent Applications | Technical | N/A |  |
| SC-28 | Protection of Information at Rest | Technical/BEA |  |  |
| SC-29 | Heterogeneity | Technical | N/A |  |
| SC-30 | Virtualization Techniques | Technical | N/A |  |
| SC-31 | Covert Channel Analysis | Technical | N/A |  |
| SC-32 | Information System Partitioning | Technical/DBA |  |  |
| SC-33 | Transmission Preparation Integrity | Technical | SC-8 |  |
| SC-34 | Non-Modifiable Executable Programs | Technical | N/A |  |
| **System & Information Integrity** | | | |  |
| SI-1 | System and Information Integrity Policy and Procedures | Operational | O – AP&P 4-03, DIS-015, AP&P 4-03 X. H.,  AP&P 4-03 XI, AP&P 4-03 XI |  |
| SI-2 | Flaw Remediation |
| SI-3 | Malicious Code Protection |
| SI-4 | Information System Monitoring |
| SI-5 | Security Alerts, Advisories, and Directives |
| SI-6 | Security Functionality Verification |  | N/A |  |
| SI-7 | Software and Information Integrity |  | O – AP&P 4-03 X. W.11.e |  |
| SI-8 | Spam Protection |  | O – AP&P 4-04, SPAM Reporting procedures |  |
| SI-9 | Information Input Restrictions | Operational/BEA |  |  |
| SI-10 | Information Input Validation | Operational/BEA |  |  |
| SI-11 | Error Handling | Operational/BEA |  |  |
| SI-12 | Information Output Handling and Retention | Operational | CSIRT Function |  |