Restricted Distribution
Sensitive Information – For Official Use Only

Centers for Medicare & Medicaid Services

ACA System Security Plan Attachment 1
SSP Workbook

Version 1.0

August 1, 2012

(This Page Intentionally Blank)

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Version:
Document Date:

(This Page Intentionally Blank)

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Access Control (AC) – *Technical*

AC 1 Access Control Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 2 Account Management (Moderate)	
Control The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts using the frequency specified in Implementation Standard 1. For FTI: The agency must ensure that only authorized employees or contractors (as allowed by statute) of the agency receiving the information has access to FTI. (Pub 1075, Ref 9.2) **Implementation Standard(s)** 1. Review information system accounts within every one hundred eighty (180) days and require annual certification. 2. Remove or disable default user accounts. Rename active default accounts. 3. Implement centralized control of user access administrator functions. 4. Regulate the access provided to contractors and define security requirements for contractors.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 2(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to support the management of information system accounts.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 2(2) Enhancement (Moderate)	
Control The information system automatically terminates emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 2(3) Enhancement (Moderate)	
Control The information system automatically disables inactive accounts after one hundred eighty (180) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 2(4) Enhancement (Moderate)	
Control The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 2(7) Enhancement (Moderate)	
Control The organization:	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles;
(b) Tracks and monitors privileged role assignments; and
(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC 3 Access Enforcement (Moderate)

Control

The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Implementation Standard(s)
1. If encryption is used as an access control mechanism it must meet approved (FIPS 140-2 compliant and a NIST validated module) encryption standards (see SC-13).
2. If e-authentication is utilized in connection to access enforcement, refer to ARS Appendix D: E-authentication Standard.
3. Configure operating system controls to disable public "read" and "write" access to files, objects, and directories that may directly impact system functionality and/or performance, or that contain sensitive information.
4. Data stored in the information system must be protected with system access controls.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC 3(1) Enhancement (Moderate)

Control

[Withdrawn: Incorporated into AC-6].

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 4 Information Flow Enforcement (Moderate)	
Control The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 5 Separation of Duties (Moderate)	
Control The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion; b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations. **Implementation Standard(s)** 1. Ensure that audit functions are not performed by security personnel responsible for administering access control. 2. Maintain a limited group of administrators with access based upon the users' roles and responsibilities. 3. Ensure that critical mission functions and information system support functions are divided among separate individuals. 4. Ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups. 5. Ensure that an independent entity, not the Business Owner, System Developer(s)/Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 6 Least Privilege (Moderate)	
Control The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with missions and business functions. For FTI: Access to FTI must be strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body or commission. No person should be given more FTI than is needed for performance of his/her duties. **Implementation Standard(s)** 1. Disable all file system access not explicitly required for system, application, and administrator functionality. 2. Contractors must be provided with minimal system and physical access, and must agree to and support the security requirements. The contractor selection process must assess the contractor's ability to adhere to and support security policy. 3. Restrict the use of database management utilities to only authorized database administrators. Prevent users from accessing database data files at the logical data view, field, or field-value level. Implement table-level access control. 4. Ensure that only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of job duties. 5. Disable all system and removable media boot access unless it is explicitly authorized by the CIO for compelling operational needs. If authorized, boot access is password protected.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 6(1) Enhancement (Moderate)	
Control The organization explicitly authorizes access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware; and security relevant information is restricted to explicitly authorized individuals.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 6(2) Enhancement (Moderate)	
Control The organization requires that users of information system accounts, or roles, with access to administrator accounts or security functions, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 7 Unsuccessful Login Attempts (Moderate)	
Control The information system: a. Enforces the limit of consecutive invalid login attempts by a user specified in Implementation Standard 1 during the time period specified in Implementation Standard 1; and b. Automatically disables or locks the account/node until released after the time period specified in Implementation Standard 1 when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection. **Implementation Standard(s)** 1. Configure the information system to lock out the user account automatically after three (3) failed log-on attempts by a user. For FTI: Automatically lock the account/node until an authorized system administrator reinstates the account (Pub 1075 Ref. Exhibit 8)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 8 System Use Notification (Moderate)	
Control The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The approved banner for information systems is: - You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only. - Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. - By using this information system, you understand and consent to the following: * You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. * Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system. For FTI: The warning banner must contain reference to the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431. (Pub 1075, Sec 9.2; Exhibit 13)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC 10 Concurrent Session Control (Moderate)	
Control The information system limits the number of concurrent sessions for each system account to one (1) session. The number of concurrent application/process sessions is limited and enforced to the number of sessions expressly required for the performance of job duties and any requirement for more than one (1) concurrent application/process session is documented in the security plan.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 11 Session Lock (Moderate)	
Control The information system: a. Prevents further access to the system by initiating a session lock after fifteen (15) minutes of inactivity; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 12 Session Termination (Moderate)	
Control [Withdrawn: Incorporated into SC-10].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 13 Supervision and Review Access Control (Moderate)	
Control [Withdrawn: Incorporated into AC-2 and AU-6].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 14 Permitted Actions without Identification or Authentication (Moderate)	
Control The organization: a. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication; and b. Configures Information systems to permit public access only to the extent necessary to accomplish mission objectives, without first requiring individual identification and authentication. **Implementation Standard(s)** 1. Identify and document specific user actions that can be performed on the information system without identification or authentication.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 14(1) Enhancement (Moderate)	
Control The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 15 Automated Marking (Moderate)	
Control [Withdrawn: Incorporated into MP-3].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 17 Remote Access (Moderate)	
Control Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. **Implementation Standard(s)** 1. Require callback capability with re-authentication to verify connections from authorized locations when the Medicare Data Communications Network (MDCN) or Multi-Protocol Label Switching (MPLS) service network cannot be used. 2. If e-authentication is implemented as a remote access solution or associated with remote access, refer to ARS Appendix D: E-authentication Standard. For FTI, complete Safeguard Procedures Report (SPR) section 9.20.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(2) Enhancement (Moderate)	
Control The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(3) Enhancement (Moderate)	
Control The information system routes all remote accesses through a limited number of managed access control points.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(4) Enhancement (Moderate)	
Control The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(5) Enhancement (Moderate)	
Control The organization monitors for unauthorized remote connections to the information system at least quarterly, and takes appropriate action if an unauthorized connection is discovered.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 17(7) Enhancement (Moderate)	
Control The organization ensures that remote sessions used for remote administration employ additional security measures (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled) and the approved encryption standard (see SC-13), and the sessions are audited.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 17(8) Enhancement (Moderate)	
Control The organization disables Bluetooth and peer-to-peer networking protocols within the information system except for explicitly identified components in support of specific operational requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 18 Wireless Access (Moderate)	
Control The organization prohibits the installation of wireless access points (WAP) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Monitors for unauthorized wireless access to the information system; and b. Enforces requirements for wireless connections to the information system. **Implementation Standard(s)** 1. If wireless access is explicitly approved, wireless device service set identifier broadcasting is disabled and the following wireless access controls are implemented: (a) Encryption protection is enabled; (b) Access points are placed in secure areas; (c) Access points are shut down when not in use (i.e., nights, weekends); (d) A firewall is implemented between the wireless network and the wired infrastructure; (e) MAC address authentication is utilized; (f) Static IP addresses, not DHCP, is utilized; (g) Personal firewalls are utilized on all wireless clients; (h) File sharing is disabled on all wireless clients; (i) Intrusion detection agents are deployed on the wireless side of the firewall; and (j) Wireless activity is monitored and recorded, and the records are reviewed on a regular basis.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 18(1) Enhancement (Moderate)	
Control If wireless access is explicitly approved, the information system protects wireless access to the system using authentication and encryption. For FTI: The agency shall authorize, document, and monitor all wireless access to the information system in accordance with NIST 800-48 Revision 1 (Pub 1075 Ref. 9.2) For FTI, complete SPR section 9.20.3.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC 18(2) Enhancement (Moderate)

Control

The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points quarterly, and takes appropriate action if an unauthorized connection is discovered.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

AC 19 Access Control for Mobile Devices (Moderate)

Control

The organization prohibits the connection of portable and mobile devices (e.g., notebook computers, personal digital assistants [PDA], cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) to information systems unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization:
a. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops;
b. Monitors for unauthorized connections of mobile devices to information systems;
c. Enforces requirements for the connection of mobile devices to information systems;
d. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;
e. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and
f. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 19(1) Enhancement (Moderate)	
Control The organization restricts the use of writable, removable media in information systems.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 19(2) Enhancement (Moderate)	
Control The organization prohibits the use of personally owned, removable media in information systems.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 19(3) Enhancement (Moderate)	
Control The organization prohibits the use of removable media in information systems when the media has no identifiable owner.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 20 Use of External Information Systems (Moderate)	
Control The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum: a. The types of applications that can be accessed from external information systems; b. The maximum FIPS 199 security category of information that can be processed, stored, and transmitted; c. How other users of the external information system will be prevented from accessing federal information; d. The use of virtual private networking (VPN) and firewall technologies; e. The use of and protection against the vulnerabilities of wireless technologies; f. The maintenance of adequate physical security controls; g. The use of virus and spyware protection software; and h. How often the security capabilities of installed software are to be updated. **Implementation Standard(s)** 1. Instruct all personnel working from home to implement fundamental security controls and practices, including passwords, virus protection, and personal firewalls. Limit remote access only to information resources required by home users to complete job duties. Require that any government-owned equipment be used only for business purposes by authorized employees. 2. (For PII only) Only organization owned computers and software can be used to process, access, and store PII. For FTI: 3. If the agency allows alternative work sites, such as employee's home or other non-traditional work sites, the FTI remains subject to the same safeguard requirements as the agency's offices. (Pub. 1075, Ref 4.7) 4. Only agency-owned computers, media and software will be used to receive, process, access and store FTI. The agency must retain ownership and control for the security configuration of all hardware, software and end-point equipment connecting to public communication networks including encryption keys. (Pub. 1075, Ref 4.7.1)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AC 20(1) Enhancement (Moderate)	
Control The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 20(2) Enhancement (Moderate)	
Control The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AC 22 Publicly Accessible Content (Moderate)	
Control The organization: a. Designates individuals authorized to post information onto an information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the information system; d. Reviews the content on the publicly accessible information system for nonpublic information monthly; and e. Removes nonpublic information from the publicly accessible information system, if discovered.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Access Control Family (AC) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Awareness and Training (AT) – *Operational*

AT 1 Security Awareness and Training Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AT 2 Security Awareness (Moderate)	
Control The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users prior to accessing any system's information, when required by system changes, and within every three hundred sixty-five (365) days thereafter. For FTI: Awareness training specific to protecting FTI and the sanctions for misuse of FTI must be provided initially prior to granting access to FTI and annually thereafter. (Pub. 1075 Ref. 6.2, 9.4)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AT 3 Security Training (Moderate)	
Control The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) refresher training within every three hundred sixty-five (365) days thereafter. For FTI: The disclosure awareness requirements apply to all agency employees with access to FTI, including program and information technology personnel and contractors, such as case workers, managers, system administrators, database administrators and application developers. (Pub. 1075, Ref 6.2 and 9.4) **Implementation Standard(s)** 1. Require personnel with significant information security roles and responsibilities to undergo appropriate information system security training prior to authorizing access to networks, systems, and/or applications; when required by system changes; and refresher training within every three hundred sixty-five (365) days thereafter.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AT 4 Security Training Records (Moderate)	
Control The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for three (3) years. For FTI: Granting employees or contractors access to FTI must be preceded by each employee or contractor certifying his/her understanding of the agency's security policy and procedures for safeguarding FTI. The certification must be maintained for 5 years. (Pub 1075, section 6.2)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Awareness and Training Family (AT) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Audit and Accountability (AU) – *Technical*

AU 1 Audit and Accountability Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 2 Auditable Events (Moderate)
Control
The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the list of auditable events specified in the Implementation Standards; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; and c. Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations. For FTI: Audit logs must enable tracking activities taking place on the system. Pub 1075, Exhibit 9, System Audit Management Guidelines, contains requirements for creating audit-related processes at both the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application that contain FTI. (Pub 1075 9.3, Ref. Exhibit 9) **Implementation Standard(s)** 1. Generate audit records for the following events: **(a) User account management activities,** **(b) System shutdown,** **(c) System reboot,** **(d) System errors,** **(e) Application shutdown,** **(f) Application restart,** **(g) Application errors,** **(h) File creation,** **(i) File deletion,** **(j) File modification,** **(k) Failed and successful log-ons,** **(l) Security policy modifications, and** **(m) Use of administrator privileges.** 2. Enable logging for perimeter devices, including firewalls and routers. (a) Log packet screening denials originating from un-trusted networks, (b) Packet screening denials originating from trusted networks, **(c) User account management,**

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

(d) Modification of packet filters,
(e) Application errors,
(f) System shutdown and reboot,
(g) System errors, and
(h) Modification of proxy services.
3. Verify that proper logging is enabled in order to audit administrator activities.

For FTI: Generate audit records for the following events in addition to those specified in other controls, plus those bolded above:
(a) All successful and unsuccessful authorization attempts.
(b) All changes to logical access control authorities (e.g., rights, permissions).
(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.
(d) The audit trail shall capture the enabling or disabling of audit report generation services.
(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 2(1) Enhancement (Moderate)	
Control [Withdrawn: Incorporated into AU-12].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 2(2) Enhancement (Moderate)	
Control [Withdrawn: Incorporated into AU-12].	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 2(3) Enhancement (Moderate)	
Control The organization reviews and updates the list of auditable events within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 2(4) Enhancement (Moderate)	
Control The organization includes execution of privileged functions in the list of events to be audited by the information system, including administrator and user account activities, failed and successful log-on, security policy modifications, use of administrator privileges, system shutdowns, reboots, errors and access authorizations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 3 Content of Audit Records (Moderate)	
Control The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. **Implementation Standard(s)** 1. (For PHI only) Record disclosures of sensitive information, including protected health and financial information. Log information type, date, time, receiving party, and releasing party. Verify within every ninety (90) days for each extract that the data is erased or its use is still required.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
AU 3(1) Enhancement (Moderate)	
Control The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 4 Audit Storage Capacity (Moderate)	
Control The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 5 Response to Audit Processing Failures (Moderate)	
Control The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions in response to an audit failure or audit storage capacity issue: - Shutdown the information system, - Stop generating audit records, or - Overwrite the oldest records, in the case that storage media is unavailable. For FTI: Shutting down the system, stopping the generation of audit reports or overwriting the oldest records is not an appropriate action. (Pub 1075 section 3.0)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 6 Audit Review, Analysis, and Reporting (Moderate)	
Control The organization: a. Reviews and analyzes information system audit records regularly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to operations, assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. For FTI: All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. (see IRS Pub. 1075, section 3.0) **Implementation Standard(s)** 1. Review system records for initialization sequences, log-ons and errors; system processes and performance; and system resources utilization to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alert notification for technical personnel review and assessment. 2. Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment. 3. Investigate suspicious activity or suspected violations on the information system, report findings to appropriate officials and take appropriate action. 4. Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior. 5. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created. 6. Perform manual reviews of system audit records randomly on demand but at least once every thirty (30) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 6(1) Enhancement (Moderate)	
Control The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 6(2) Enhancement (Moderate)	
Control [Withdrawn: Incorporated into SI-4].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 7 Audit Reduction and Report Generation (Moderate)	
Control The information system provides an audit reduction and report generation capability.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 7(1) Enhancement (Moderate)	
Control The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 8 Time Stamps (Moderate)	
Control The information system uses internal system clocks to generate time stamps for audit records.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 8(1) Enhancement (Moderate)	
Control The information system synchronizes internal information system clocks daily and at system boot.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 9 Protection of Audit Information (Moderate)	
Control The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 10 Non Repudiation (Moderate)	
Control The information system protects against an individual falsely denying having performed a particular action.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 11 Audit Record Retention (Moderate)	
Control The organization retains audit records for ninety (90) days and archive old records for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and information retention requirements. For FTI: 1. Employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer. (Pub 1075 Ref. 3.1) 2. To support the audit of FTI activities, all organizations must ensure that audit information is archived for six (6) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored. (Pub 1075 Ref. 9.3) **Implementation Standard(s)** 1. (For PII only) Audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

AU 12 Audit Generation (Moderate)	
Control The information system: a. Provides audit record generation capability for the following events in addition to those specified in other controls: - All successful and unsuccessful authorization attempts. - All changes to logical access control authorities (e.g., rights, permissions). - All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. - The audit trail shall capture the enabling or disabling of audit report generation services. - The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database). b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
AU 12(1) Enhancement (Moderate)	
Control The information system compiles audit records from multiple components throughout the system into a system-wide (logical or physical) time-correlated audit trail.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Audit and Accountability Family (AU) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Security Assessment and Authorization (CA) – *Management*

CA 1 Security Assessment and Authorization Policies and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CA 2 Security Assessments (Moderate)	
Control The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system within every three hundred sixty-five (365) days in accordance with the Information Security (IS) Acceptable Risk Safeguards (ARS) Including Minimum Security Requirements (CMSR) Standard, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment within every three hundred sixty-five (365) days, in writing, to the Business Owner who is responsible for reviewing the assessment documentation and updating system security documentation where necessary to reflect any changes to the system. For FTI: The agency shall conduct, periodically, but at least annually, an assessment of the security controls in the systems that receive, store, process or transmit FTI. (Pub 1075, Ref. 9.4) **Implementation Standard(s)** 1. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems. 2. The annual security assessment requirement mandated by OMB requires all CMSRs attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period. 3. The Business Owner notifies the CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 2(1) Enhancement (Moderate)	
Control The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 3 Information System Connections (Moderate)	
Control The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements. **Implementation Standard(s)** 1. Record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 4 Security Certification (Moderate)	
Control [Withdrawn: Incorporated into CA-2].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CA 5 Plan of Action and Milestones (POA&M) (Moderate)	
Control The organization: a. Develops and submits a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates and submits existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. **Implementation Standards** For FTI: The agency must submit an updated Corrective Action Plan (CAP) twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date. (Pub 1075, Ref. 7.5)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 5(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CA 6 Security Authorization (Moderate)	
Control The organization updates the security authorization: - At least every three (3) years; - When substantial changes are made to the system; - When changes in requirements result in the need to process data of a higher sensitivity; - When changes occur to authorizing legislation or federal requirements; - After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and - Prior to expiration of a previous security authorization. For FTI: Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the authorization. (Pub 1075, Ref 9.5) Note: For Federal agencies that receive FTI, a NIST compliant systems certification (C&A) is required in accordance with FISMA. For state agencies that receive FTI, a third-party accreditation is not required. Instead, these agencies may internally attest in writing that the security controls have been adequately implemented to protect FTI. The accreditation shall occur every three (3) years or whenever there is a significant change to the control structure. (Pub 1075, Ref. 9.5)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CA 7 Continuous Monitoring (Moderate)	
Control The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 7(1) Enhancement (Moderate)	
Control The use of independent security assessment agents or teams to monitor security controls is not required. However, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CA 7(2) Enhancement (Moderate)	
Control plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all information systems and information systems that are processing data on behalf of or directly for including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Security Assessment and Authorization Family (CA) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Configuration Management (CM) – *Operational*

CM 1 Configuration Management Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 2 Baseline Configuration (Moderate)	
Control The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 2(1) Enhancement (Moderate)	
Control The organization reviews and updates the baseline configuration of the information system: (a) At least once every three hundred sixty-five (365) days; (b) When required due to major system changes/upgrades; and (c) As an integral part of information system component installations and upgrades.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CM 2(3) Enhancement (Moderate)	
Control The organization retains older versions of baseline configurations as deemed necessary to support rollback.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 2(4) Enhancement (Moderate)	
Control The organization: (a) Develops and maintains a list of software programs authorized (white list) or unauthorized (black list) to execute on the information system; and (b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CM 3 Configuration Change Control (Moderate)	
Control The organization: a. Determines the types of changes to the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through change request forms which must be approved by an organizational and/or change control board which meets frequently enough to accommodate proposed change requests, and other appropriate organization officials including, but not limited to, the System Developer/Maintainer and information system support staff.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 3(2) Enhancement (Moderate)	
Control The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 4 Security Impact Analysis (Moderate)	
Control The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Activities associated with configuration changes to the information system are audited.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	Responsible for Control Implementation *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
CM-4(1) – Enhancement (Moderate)	
Control The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	Responsible for Control Implementation *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-4(2) – Enhancement (Moderate)	
Control The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM-5 – Access Restrictions for Change (Moderate)	
Control The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Records reflecting all such changes shall be generated, reviewed, and retained.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CM 6 Configuration Settings (Moderate)	
Control The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration guidelines listed in Implementation Standard 1 that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. For FTI: Establish mandatory configuration settings for systems that receive, store, process and transmit FTI using the Safeguards Computer Security Evaluation Matrices (SCSEMs). (Pub 1075, Ref 9.6) **Implementation Standard(s)** 1. Security configuration guidelines may be developed by different agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or guideline. To resolve configuration conflicts among multiple security guidelines, the hierarchy for implementing all security configuration guidelines is as follows: (a) NIST (b) DISA (c) OMB For FTI: SCSEMs – All agency information systems used for receiving, processing, storing and transmitting FTI must be hardened in accordance with the requirements of Publication 1075. Agency information systems include the equipment, facilities, and people that collect, process, store, display and disseminate information. This includes computers, hardware, software, and communications, as well as policies and procedures for their use. Safeguard Computer Security Evaluation Matrices (SCSEMs) provide hardening guidance for specific technologies and are publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 6(3) Enhancement (Moderate)	
Control The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 7 Least Functionality (Moderate)	
Control The organization configures the information system to provide only essential capabilities and specifically disables, prohibits, or restricts the use of system services, ports, network protocols, and capabilities that are not explicitly required for system or application functionality. A list of specifically needed system services, ports, and network protocols will be maintained and documented in the SSP; all others will be disabled.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 7(1) Enhancement (Moderate)	
Control The organization reviews the information system within every three hundred sixty-five (365) days to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CM 8 Information System Component Inventory (Moderate)	
Control The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes manufacturer, model/type, serial number, version number, location (i.e., physical location and logical position within the information system architecture), and ownership; and e. Is available for review and audit by designated organizational officials.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 8(1) Enhancement (Moderate)	
Control The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CM 8(5) Enhancement (Moderate)	
Control The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CM 9 Configuration Management Plan (Moderate)	
Control The organization develops, documents, and implements a configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Configuration Management Family (CM) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Contingency Planning (CP) – *Operational*

CP 1 Contingency Planning Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 2 Contingency Plan (Moderate)	
Control The organization: a. Develops a Contingency Plan (CP) for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the CP plan to key contingency personnel (identified by name and/or by role) and organizational elements; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the CP for the information system annually; (Pub 1075, Ref 9.7) e. Revises the CP to address changes to the organization, information system, or environment of operation and problems encountered during CP implementation, execution, or testing; and f. Communicates CP changes to key contingency personnel (identified by name and/or by role) and organizational elements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 2(1) Enhancement (Moderate)	
Control The organization coordinates contingency plan development with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 2(2) Enhancement (Moderate)	
Control The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 3 Contingency Training (Moderate)	
Control The organization trains operational and support personnel (including managers and users of the information system) in their contingency roles and responsibilities with respect to the information system and provides refresher training within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP-4 – Contingency Plan Testing and Exercises (Moderate)	
Control The organization: a. Tests and/or exercises the contingency plan for the information system within every three hundred sixty-five (365) days using defined tests and exercises, such as the tabletop test in accordance with the current CMS contingency plan procedure to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Documents and reviews the contingency plan test/exercise results and initiates reasonable and appropriate corrective actions to close or reduce the impact of contingency plan failures and deficiencies.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-4(1) – Enhancement (Moderate)	
Control The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP-5 – Contingency Plan Update (Moderate)	
Control [Withdrawn: Incorporated into CP-2].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 6 Alternate Storage Site (Moderate)	
Control The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. For FTI: The agency must identify alternative storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups and ensure the alternative storage sites meet FTI secure storage requirements. (Pub 1075 section 9.7)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 6(1) Enhancement (Moderate)	
Control The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 6(3) Enhancement (Moderate)	
Control The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 7 Alternate Processing Site (Moderate)	
Control The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the time period specified in Implementation Standard 1 when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the time period for resumption specified in Implementation Standard 1. **Implementation Standard(s)** 1. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one (1) week of contingency plan activation.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 7(1) Enhancement (Moderate)	
Control The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 7(2) Enhancement (Moderate)	
Control The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 7(3) Enhancement (Moderate)	
Control The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 7(5) Enhancement (Moderate)	
Control The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 8 Telecommunications Services (Moderate)	
Control The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the resumption time period specified in Implementation Standard 1 when the primary telecommunications capabilities are unavailable. **Implementation Standard(s)** 1. Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 8(1) Enhancement (Moderate)	
Control The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's	

availability requirements. And b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 8(2) Enhancement (Moderate)	
Control The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 9 Information System Backup (Moderate)	
Control The organization: a. Conducts backups of user-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; b. Conducts backups of system-level information contained in the information system in accordance with the frequency specified in Implementation Standard 1; c. Conducts backups of information system documentation including security-related documentation and other forms of data, including paper records; and d. Protects the confidentiality and integrity of backup information at the storage location. **Implementation Standard(s)** 1. Perform full backups weekly to separate media. Perform incremental or differential backups daily to separate media. Backups to include user-level and system-level information (including system state information). Three (3) generations of backups (full plus all related incremental or differential backups) are stored off-site. Off-site and on-site backups must be logged with name, date, time and action. 2. (For PII only) Ensure that a current, retrievable, copy of PII is available before movement of servers. For FTI: Back-up tapes must be labeled as containing FTI, must be logged, must be transported securely using two barriers and a transmittal, and must be inventoried on a semi-annual basis. (Pub 1075 sections 3.0, 4.0)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 9(1) Enhancement (Moderate)	
Control The organization tests backup information following each backup to verify media reliability and information integrity.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

CP 10 Information System Recovery and Reconstitution (Moderate)	
Control The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. **Implementation Standard(s)** 1. Secure information system recovery and reconstitution includes, but not limited to: (a) Reset all system parameters (either default or organization-established), (b) Reinstall patches, (c) Reestablish configuration settings, (d) Reinstall application and system software, and (e) Fully test the system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 10(2) Enhancement (Moderate)	
Control The information system implements transaction recovery for systems that are transaction-based. Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
CP 10(3) Enhancement (Moderate)	
Control The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Contingency Planning Family (CP) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

IA 1	Identification and Authentication Policy and Procedures (Moderate)
Control	The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A security identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Identification and Authentication (IA) – *Technical*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 2 Identification and Authentication (Organizational Users) (Moderate)	
Control The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). **Implementation Standard(s)** 1. Require the use of system and/or network authenticators and unique user identifiers. 2. Help desk support requires user identification for any transaction that has information security implications. For FTI: Complete section 2.10 (e-Authentication level) in the SSP Template.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 2(1) Enhancement (Moderate)	
Control The information system uses multifactor authentication for network access to privileged accounts. For FTI: Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via agency's web portal by an employee or contractor.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 2(2) Enhancement (Moderate)	
Control The information system uses multifactor authentication for network access to non-privileged accounts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]
IA 2(3) Enhancement (Moderate)	
Control The information system uses multifactor authentication for local access to privileged accounts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 2(8) Enhancement (Moderate)	
Control The information system uses replay resistant authentication mechanisms for network access to privileged accounts. Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 3 Device Identification and Authentication (Moderate)	
Control The information system uniquely identifies and authenticates specific and/or types of devices before establishing a connection.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 4 Identifier Management (Moderate)	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Control	
The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier but not before a period of at least three hundred sixty-five (365) days has expired; and e. Disabling the user identifier after the time period of inactivity specified in Implementation Standard 1 and deleting disabled accounts during the annual re-certification process. **Implementation Standard(s)** 1. Disable user identifiers after one hundred eighty (180) days of inactivity. For FTI: Disable user identifier after ninety (90) days of inactivity.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 5 Authenticator Management (Moderate)	
Control The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing password authenticators as defined in IA-5(1); h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IA 5(1) Enhancement (Moderate)	
Control The information system, for password-based authentication: (a) Automatically forces users (including administrators) to change user account passwords every sixty (60) days and system account passwords every one hundred eighty (180) days; (b) Prohibits the use of dictionary names or words; (c) Enforces minimum password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lower-case letters, and numbers) and/or special characters; (d) Enforces at least a minimum of four (4) changed characters when new passwords are created; (e) Encrypts passwords in storage and in transmission; (f) Enforces password minimum and maximum lifetime restrictions of one (1) day for the minimum, and sixty (60) days for a user account and one hundred eighty (180) days for a system account maximum; and (g) Prohibits password reuse for six (6) generations prior to reuse. For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users. (Pub 1075, Ref Exhibit 8)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 5(2) Enhancement (Moderate)	
Control The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 5(3) Enhancement (Moderate)	
Control	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

The organization requires that the registration process to receive hardware tokens be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).
Fully explain control implementation *(or fully explain why control requirement is not applicable)* — **Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 6 Authenticator Feedback (Moderate)
Control The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
Fully explain control implementation *(or fully explain why control requirement is not applicable)* — **Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 7 Cryptographic Module Authentication (Moderate)
Control The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
Fully explain control implementation *(or fully explain why control requirement is not applicable)* — **Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IA 8 Identification and Authentication (Non Organizational Users) (Moderate)
Control The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
Fully explain control implementation *(or fully explain why control requirement is not applicable)* — **Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Identification and Authentication Family (IA) Security Controls Detail and Comment

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Incident Response (IR) – *Operational*

IR 1 Incident Response Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. For FTI: Policies and procedures must cover both physical and information security relative to the protection of FTI. For FTI: Complete SPR section 9.11.1	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR 2 Incident Response Training (Moderate)	
Control The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and For FTI: Provides refresher training prior to access of FTI and annually thereafter on incident response policy and procedure regarding FTI. (Pub 1075, section 6.2, 9.9) **Supplemental Guidance**: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. For FTI: Complete SPR section 9.11.2	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IR 3 Incident Response Testing and Exercises (Moderate)	
Control The organization tests and/or exercises the incident response capability for the information system annually using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. For FTI: Include procedures to exercise responding o unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA. (Pub 1075, Ref 9.9) Complete SPR section 9.11.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

IR 4 Incident Handling (Moderate)	
Control The organization: a. Implements an incident handling capability using Information Security Incident Handling and Breach Notification Procedures; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. For FTI: The agency's incident response policy and procedures must include specific guidance relative to a data incidents involving FTI. (Pub 1075 Section 9.9) **Implementation Standard(s)** 1. Document relevant information related to a security incident according to Information Security Incident Handling and Breach Notification Procedures. 2. Preserve evidence through technical means, including secured storage of evidence media and "write" protection of evidence media. Use sound forensics processes and utilities that support legal requirements. Determine and follow chain of custody for forensic evidence. 3. Identify vulnerability exploited during a security incident. Implement security safeguards to reduce risk and vulnerability exploit exposure. For FTI: Complete SPR section 9.11.4	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IR 4(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to support the incident handling process. Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR 5 Incident Monitoring (Moderate)	
Control The organization tracks and documents information system security incidents. Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. For FTI: Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. (Pub 1075 section 10.3) For FTI: Complete SPR section 9.11.5	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IR 6 Incident Reporting (Moderate)	
Control The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current Information Security Incident Handling and Breach Analysis/Notification Procedure; and b. Reports security incident information to designated authorities. For FTI: Any data incident potentially involving FTI must immediately be reported to the Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards immediately, but no later than 24-hours after identification of a possible issue involving FTI. (Pub. 1075, Ref 9.9, 10.4) Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5. For FTI: Complete SPR section 9.11.6	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR 6(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to assist in the reporting of security incidents.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IR 7 Incident Response Assistance (Moderate)	
Control The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents. Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. For FTI: Complete SPR section 9.11.7	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
IR 7(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to increase the availability of incident response-related information and support. Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

IR 8 Incident Response Plan (Moderate)	
Control The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to incident response personnel and organizational elements; c. Reviews the incident response plan within every three hundred sixty-five (365) days; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to incident response personnel and organizational elements. Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability. For FTI: Complete SPR section 9.11.8.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Incident Response Family (IR) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Maintenance (MA) – *Operational*

MA 1 System Maintenance Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MA 2 Controlled Maintenance (Moderate)	
Control The organization: a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. **Implementation Standard(s)** 1. (For PII only) In facilities where PII is stored or accessed, document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MA 2(1) Enhancement (Moderate)	
Control the organization maintains maintenance records for the information system that include: - date and time of maintenance; - name of the individual performing the maintenance; - name of escort, if necessary; - a description of the maintenance performed; - a list of equipment removed or replaced (including identification numbers, if applicable).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA 3 Maintenance Tools (Moderate)	
Control The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MA 3(1) Enhancement (Moderate)	
Control The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.	
Fully explain control implementation (or fully explain why control requirement is not applicable)	**Responsible for Control Implementation** [Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]
MA 3(2) Enhancement (Moderate)	
Control The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA 4 Non Local Maintenance (Moderate)	
Control The organization prohibits non-local system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Monitors and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. **Implementation Standard(s)** 1. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
MA 4(1) Enhancement (Moderate)	
Control The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA 4(2) Enhancement (Moderate)	
Control The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA 4(3) Enhancement (Moderate)	
Control The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MA 5 Maintenance Personnel (Moderate)	
Control The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MA 6 Timely Maintenance (Moderate)	
Control The organization obtains maintenance support and/or spare parts for critical systems and applications (including Major Applications [MA] and General Support Systems [GSS] and their components) within twenty-four (24) hours of failure.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Maintenance Family (MA) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Media Protection (MP) – *Operational*

MP 1 Media Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. **Implementation Standard(s)** 1. (For PII only) Semi-annual inventories of magnetic tapes containing PII are conducted. The organization accounts for any missing tape containing PII by documenting the search efforts and notifying the tape initiator of the loss.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 2 Media Access (Moderate)	
Control The organization restricts access to sensitive digital and non-digital media to authorized individuals using automated mechanisms to control access to media storage areas.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 2(1) Enhancement (Moderate)	
Control The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MP 3 Media Marking (Moderate)	
Control The organization: a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment. For FTI: The agency must label removable media and information system output containing FTI. IRS Notice 129-A or Notice 129-B are available for this purpose. (Pub. 1075, Ref. 9.11)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

MP 4 Media Storage (Moderate)	
Control The organization: a. Physically controls and securely stores digital and non-digital media within controlled areas using safeguards prescribed for the highest system security level of the information ever recorded on it; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **Implementation Standard(s)** 1. (For PII only) Evaluate employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance. 2. (For PII only) If PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MP 5 Media Transport (Moderate)	
Control The organization: a. Protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and (i) if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or (ii) if shipped, trackable with receipt by commercial carrier; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. For FTI: All FTI transported through the mail or courier/messenger service must be double sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double sealing and prevents anyone from viewing the contents thereof. (Pub 1075, Ref 4.5) **Implementation Standard(s)** 1. (For PII only) Protect and control PII media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. PII must be in locked cabinets or sealed packing cartons while in transit.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 5(2) Enhancement (Moderate)	
Control The organization documents activities associated with the transport of information system media. For FTI: All shipments of FTI (including electronic media and microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. (Pub 1075, Ref 4.5) **Implementation Standard(s):** For FTI: Describe the permanent record(s) (logs) used to document requests for, receipt of, distribution of (if applicable), and disposition (return to IRS or destruction) of the FTI (including tapes, cartridges or other removable media) (e.g. FTI receipt logs, transmission logs, or destruction logs in electronic or paper format) (Please include a sample of the agency logs as an attachment).	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 5(4) Enhancement (Moderate)	
Control The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g.,notebook/laptop computers, personal digital assistants, cellular telephones).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

MP 6 Media Sanitization (Moderate)	
Control The organization: a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. For FTI: 1. FTI furnished to the user and any paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating. (See Pub 1075, Ref 8.3 for detailed procedures) 2. FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Generally, destruction should be witnessed by an agency employee. **Implementation Standard(s)** 1. Finely shred, using a minimum of cross-cut shredding, hard-copy documents, using approved equipment, techniques, and procedures. 2. (For PII only) Authorized employees of the receiving entity must be responsible for securing magnetic tapes/cartridges before, during, and after processing, and they must ensure that the proper acknowledgment form is signed and returned. Inventory records must be maintained for purposes of control and accountability. Tapes containing PII, any hard-copy printout of a tape, or any file resulting from the processing of such a tape will be recorded in a log that identifies: - date received - reel/cartridge control number contents - number of records, if available - movement, and - if disposed of, the date and method of disposition. For FTI, complete SPR section 8.1.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 6(1) Enhancement (Moderate)	
Control The organization tracks, documents, and verifies media sanitization and disposal actions.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 6(2) Enhancement (Moderate)	
Control The organization tests sanitization equipment and procedures to verify correct performance periodically.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 6(5) Enhancement (Moderate)	
Control The organization sanitizes information system media containing sensitive information using National Security Agency (NSA) guidance (www.nsa.gov/ia/government/mdg.cfm) and NIST SP 800-88, Guidelines for Media Sanitization. For FTI: Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. If reuse is not intended, the electronic media should be destroyed. Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be cleared completely by overwriting all data tracks a minimum of three times. (Pub 1075 section 8.4)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP 6(6) Enhancement (Moderate)	
Control The organization destroys media containing sensitive information that cannot be sanitized. For FTI: Paper FTI may be burned, cross-cut shredded to 5/16” wide or small strips or pulped.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
MP ACA 1 Media Related Records (Moderate)	
Control Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach. **Implementation Standard(s)** 1. The media records must, at a minimum, contain: (a) The name of media recipient; (b) Signature of media recipient; (c) Date/time media received; (d) Media control number and contents; (e) Movement or routing information; and (f) If disposed of, the date, time, and method of destruction.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Media Protection Family (MP) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Physical and Environmental Protection (PE) – *Operational*

PE 1 Physical and Environmental Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 2 Physical Access Authorizations (Moderate)	
Control The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials in accordance with the frequency specified in Implementation Standard 1, removing from the access list personnel no longer requiring access. For FTI: A visitor access log containing specific data elements will be used to authenticate and authorize visitor's access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached. (See IRS Pub. 1075, sections 4.3.2) **Implementation Standard(s)** 1. Review and approve lists of personnel with authorized access to facilities containing information systems at least once every one hundred eighty (180) days. 2. (For PII only) Create a restricted area, security room, or locked room to control access to areas containing PII. These areas will be controlled accordingly. 3. (For FTI) Complete SPR section 5.2.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 3 Physical Access Control (Moderate)

Control

The organization:
a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);
b. Verifies individual access authorizations before granting access to the facility;
c. Controls entry to the facility containing the information system using physical access devices and/or guards;
d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;
e. Secures keys, combinations, and other physical access devices;
f. Inventories physical access devices within every three hundred sixty-five (365) days; and
g. Changes combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

For FTI:
h. Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. This may be achieved through secured perimeter/locked container, locked perimeter/secured interior or locked perimeter/security container. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access after-hours. (See IRS Pub. 1075, sections 4.2)
i. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room. (See IRS Pub. 1075, sections 4.2)
j. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist. (See IRS Pub. 1075, sections 4.2)
k. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization. (See IRS Pub. 1075, sections 4.3)
l. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted access. . (See IRS Pub. 1075, sections 4.6)

Implementation Standard(s)
1. Control data center/facility access by use of door and window locks, and security personnel or physical authentication devices, such as biometrics and/or smart card/PIN combination.
2. Store and operate servers in physically secure environments, and grant access to explicitly authorized personnel only. Access is monitored and recorded.
3. Restrict access to grounds/facilities to authorized persons only.
4. (For PII only) Require two barriers to access PII under normal security: secured perimeter/locked container, locked perimeter/secured interior, or locked perimeter/security container. Protected information must be containerized in areas where other than authorized employees may have access after-hours.

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

For FTI: Complete SPR sections 5.3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE 4 Access Control for Transmission Medium (Moderate)

Control

The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Implementation Standard(s)
1. Permit access to telephone closets and information system distribution and transmission lines within organizational facilities only to authorized personnel.
2. Disable any physical ports (e.g., wiring closets, patch panels, etc) not in use.

For FTI: Complete SPR section 5.4.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PE 5 Access Control for Output Devices (Moderate)

Control

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

For FTI: Output from printers and fax machines should be in a controlled area and secured when not in use. Physical access to monitors displaying FTI should be controlled to prevent unauthorized access to the display output. (Pub. 1075, Ref 4.3, 4.3.2)

For FTI: Complete SPR section 5.5.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
PE 6 Monitoring Physical Access (Moderate)	
Control The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs in accordance with the frequency specified in Implementation Standard 1; and c. Coordinates results of reviews and investigations with the organization's incident response capability. **Implementation Standard(s)** 1. Review physical access logs every at least once every two (2) months. For FTI: Complete SPR section 5.6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 6(1) Enhancement (Moderate)	
Control The organization monitors real-time physical intrusion alarms and surveillance equipment.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 7 Visitor Control (Moderate)	
Control The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. For FTI: A restricted area visitor log will be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. The entry control monitor should verify the identify of visitors by comparing the name and signature entered into the register with some type of photo identification card. For FTI: Complete SPR section 5.7.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 7(1) Enhancement (Moderate)	
Control The organization escorts visitors and monitors visitor activity, when required.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 8 Access Records (Moderate)	
Control The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records monthly. For FTI: The restricted area visitor log shall include the visitor's name, signature, assigned work area, escort, purpose of entry, and time and date of entry. For FTI: Complete SPR section 5.8.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 9 Power Equipment and Power Cabling (Moderate)	
Control The organization protects power equipment and power cabling for the information system from damage and destruction. **Implementation Standard(s)** 1. Permit only authorized maintenance personnel to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 10 Emergency Shutoff (Moderate)	
Control The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in a location that does not require personnel to approach the equipment to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 11 Emergency Power (Moderate)	
Control The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 12 Emergency Lighting (Moderate)	
Control The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 13 Fire Protection (Moderate)	
Control The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 13(1) Enhancement (Moderate)	
Control The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 13(2) Enhancement (Moderate)	
Control The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 13(3) Enhancement (Moderate)	
Control The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
PE 14 Temperature and Humidity Controls (Moderate)	
Control The organization: a. Maintains temperature and humidity levels within the facility where the information system resides within acceptable vendor-recommended levels; and b. Monitors temperature and humidity levels. **Implementation Standard(s)** 1. Evaluate the level of alert and follow prescribed guidelines for that alert level. 2. Alert component management of possible loss of service and/or media. 3. Report damage and provide remedial action. Implement contingency plan, if necessary.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 15 Water Damage Protection (Moderate)	
Control The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 16 Delivery and Removal (Moderate)	
Control The organization authorizes, monitors, and controls the flow of information system-related components entering and exiting the facility and maintains records of those items. For FTI: All transportation or shipments of FTI (including electronic media or microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designed official or delegate is authorized to open it. (Pub. 1075, sections 4.5) For FTI: Complete SPR section 5.9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PE 17 Alternate Work Site (Moderate)	
Control The organization: a. Employs appropriate security controls at alternate work sites to include, but not limited to, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems. For FTI: Describe the policies and procedures for meeting the minimum protection standards for alternative work sites (e.g. employee's homes or other non-traditional work sites). (Pub 1075, Ref 5.3). For FTI: Complete SPR section 5.10.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PE 18 Location of Information System Components (Moderate)	
Control The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. For FTI: Complete SPR section 5.11.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Physical and Environmental Protection Family (PE) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Planning (PL) – *Management*

PL 1 Security Planning Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PL 2 System Security Plan (SSP) (Moderate)	
Control The organization: a. Develops a security plan for the information system that: - Is consistent with the System Security Plan (SSP) Procedure; - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security categorization of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system within every three hundred sixty-five (365) days; and c. Updates the plan, minimally every three (3) years, to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. For FTI: 1. When FTI is incorporated into a Data Warehouse, the controls described in IRS Pub. 1075, Exhibit 11 are to be followed, in addition to those specified in other controls. 2. Develop and submit a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). The SAR advises the IRS of minor changes to the procedures or safeguards described in the SPR. It also advises the IRS of future actions that will affect the organization's safeguard procedures, summarizes the organization's current efforts to ensure the confidentiality of FTI, and finally, certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted. (See IRS Pub. 1075, sections 7.0 and 9.13) **Implementation Standard(s)** 1. (For PHI only) Retain documentation of policies and procedures relating to HIPAA 164.306 for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. (See HIPAA 164.316(b).)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
PL 3 System Security Plan Update (Moderate)	
Control [Withdrawn: Incorporated into PL-2].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PL 4 Rules of Behavior (ROB) (Moderate)	
Control The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information, information system, and network use; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PL 5 Privacy Impact Assessment (PIA) (Moderate)	
Control The organization conducts a Privacy Impact Assessment (PIA) on the information system in accordance with OMB policy.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PL 6 Security Related Activity Planning (Moderate)	
Control The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on operations (i.e., mission, functions, image, and reputation), assets, and individuals. **Implementation Standard(s)**	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Planning Family (PL) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Personnel Security (PS) – *Operational*

PS 1 Personnel Security Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS 2 Position Categorization (Moderate)	
Control The organization: a. Assigns a criticality/sensitivity risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position criticality/sensitivity risk designations within every three hundred sixty-five (365) days.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PS 3 Personnel Screening (Moderate)	
Control The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals periodically, consistent with the criticality/sensitivity rating of the position. For FTI: Individuals must be screened before authorizing access to information systems and devices containing FTI. (Pub 1075, Ref. 9.12) **Implementation Standard(s)** 1. Perform criminal history check for all persons prior to employment. 2. Require appropriate personnel to obtain and hold a moderate-risk security clearance as defined in the DHHS Personnel Security/Suitability Handbook.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PS 4 Personnel Termination (Moderate)	
Control The organization, upon termination of individual employment: a. Revokes system and physical access immediately following employee termination; b. Conducts exit interviews; c. Retrieves all security-related information system-related property; d. Retains access to information and information systems formerly controlled by terminated individual; and e. Immediately escorts employees terminated for cause out of the organization. **Implementation Standard(s)** 1. System access must be revoked prior to or during the employee termination process.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PS 5 Personnel Transfer (Moderate)	
Control The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates the following transfer or reassignment actions during the formal transfer process: a. Re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes); b. Notification to security management; c. Closing obsolete accounts and establishing new accounts; and d. Revocation of all system access privileges (if applicable).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PS 6 Access Agreements (Moderate)	
Control The organization: a. Ensures that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements as part of the system security authorization or when a contract is renewed or extended. For FTI: Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization. (See IRS Pub. 1075, sections 9.12)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PS 7 Third Party Personnel Security (Moderate)	
Control The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance. **Implementation Standard(s)** 1. Regulate the access provided to contractors and define security requirements for contractors. Contractors must be provided with minimal system and physical access, and must agree to and support the information security requirements. The contractor selection process must assess the contractor's ability to adhere to and support information security policies and standards.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PS 8 Personnel Sanctions (Moderate)	
Control The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Personnel Security Family (PS) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Risk Assessment (RA) – *Management*

RA 1 Risk Assessment Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

RA 2 Security Categorization (Moderate)	
Control The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

RA 3 Risk Assessment (Moderate)	
Control The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in accordance with the Information Security (IS) Risk Assessment (RA) Procedures; c. Reviews risk assessment results within every three hundred sixty-five (365) days; and d. Updates the risk assessment within every three (3) years or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
RA 4 Risk Assessment Update (Moderate)	
Control [Withdrawn: Incorporated into RA-3].	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

RA 5 Vulnerability Scanning (Moderate)	
Control The organization: a. Scans for vulnerabilities in the information system and hosted applications within every ninety (90) days and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities based on the Business Owner's risk prioritization in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization on a "need to know" basis to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). For FTI: At a minimum, systems containing FTI shall be scanned quarterly to identify any vulnerability in the information system. (Pub. 1075, Ref 9.13) **Implementation Standard(s)** **1.** Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three hundred sixty-five (365) days, in accordance with IS procedures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
RA 5(1) Enhancement (Moderate)	
Control The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Risk Assessment Family (RA) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Services Acquisition (SA) – *Management*

SA 1 System and Services Acquisition Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls. Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM-9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SA 2 Allocation of Resources (Moderate)	
Control The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; c. Includes information security requirements in mission/business case planning, and d. Establishes a discrete line item in programming and budgeting documentation for the implementation and management of information systems security.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 3 Life Cycle Support (Moderate)	
Control The organization: a. Manages the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the Integrated IT Investment & System Life Cycle Framework (ILC); b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 4 Acquisitions (Moderate)	
Control The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems. **Implementation Standard(s)** 1. Each contract and Statement of Work (SOW) that requires development or access to information must include language requiring adherence to security policies and standards, define security roles and responsibilities, and receive approval from officials. For FTI: 1. Whenever information systems contain FTI, the agency shall include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for the acquisition must contain Exhibit 7 language. (Pub 1075 section 9.15) 2. Agencies using a consolidated data center must implement appropriate controls to ensure the protection of FTI, including a Service Level Agreement (SLA) between the agency authorized to receive FTI and the data center. (Pub 1075, section 5.5.2)	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 4(1) Enhancement (Moderate)	
Control The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SA 4(4) Enhancement (Moderate)	
Control The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 5 Information System Documentation (Moderate)	
Control The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. **Supplemental Guidance:** The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls. **Implementation Standard(s)** 1. Develop system documentation to describe the system and to specify the purpose, technical operation, access, maintenance, and required training for administrators and users. 2. Maintain an updated list of related system operations and security documentation. 3. Update documentation upon changes in system functions and processes. Must include date and version number on all formal system documentation.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SA 5(1) Enhancement (Moderate)	
Control The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SA 5(3) Enhancement (Moderate)	
Control The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SA 6 Software Usage Restrictions (Moderate)	
Control The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. **Supplemental Guidance:** Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 7 User Installed Software (Moderate)	
Control The organization prohibits users from downloading or installing software, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, explicit rules govern the installation of software by users. **Supplemental Guidance:** If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2. **Implementation Standard(s)** 1. If user installed software is authorized, ensure that business rules and technical controls enforce the documented authorizations and prohibitions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SA 8 Security Engineering Principles (Moderate)	
Control The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. **Supplemental Guidance:** The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]

SA 9 External Information System Services (Moderate)

Control

The organization:
a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
c. Monitors security control compliance by external service providers.
d. Prohibits service providers from outsourcing any system function outside the U.S. or its territories.

For FTI: FTI may not be accessed by agency employees, agents, representatives or contractors located "off-shore", outside of the United States or its territories. FTI may not be received, stored, processed or disposed via information technology systems located off-shore.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Implementation Standard(s)
1. (For PHI only) A covered entity under HIPAA may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with HIPAA regulations. Such assurances must be documented and meet the requirements set forth in HIPAA regulations. (See HIPAA 164.308(b) and 164.314(a).)

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
SA 10 Developer Configuration Management (Moderate)	
Control The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution. **Supplemental Guidance:** Related controls: CM-3, CM-4, CM-9	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SA 11 Developer Security Testing (Moderate)	
Control The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan in accordance with, but not limited to the, current procedures; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security control assessment process; and c. Document the results of the security control assessment and flaw remediation processes. For FTI: The agency must submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the FTI over the Internet to a customer (Pub 1075, Ref. 9.18.8) **Supplemental Guidance:** Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2. **Implementation Standard(s)** 1. If the security control assessment results are used in support of the security authorization process for the information system, ensure that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. 2. Use hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Services Acquisition Family (SA) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Communications Protection (SC) – *Technical*

SC 1 System and Communications Protection Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. **Supplemental Guidance:** This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 2 Application Partitioning (Moderate)	
Control The information system separates user functionality (including user interface services [e.g., web services]) from information system management (e.g., database management systems) functionality. **Supplemental Guidance:** Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 4 Information in Shared Resources (Moderate)	
Control The information system prevents unauthorized and unintended information transfer via shared system resources. **Supplemental Guidance:** The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role. **Implementation Standard(s)** 1. Ensure that users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. Ensure that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure. For FTI: When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 5 Denial of Service Protection (Moderate)	
Control The information system protects against or limits the effects of the following types of denial of service attacks defined on the following sites or in the following documents: - SANS Organization www.sans.org/dosstep; - SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and - NIST CVE List http://checklists.nist.gov/home.cfm. **Supplemental Guidance:** A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 7 Boundary Protection (Moderate)	
Control The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of automated boundary protection devices arranged in accordance with a organizational security architecture. **Supplemental Guidance:** Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in effective security architecture (e.g., routers protecting firewalls and application gateways residing on protected subnetworks commonly referred to as a demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5. **Implementation Standard(s)** 1. Ensure that access to all proxies is denied, except for those hosts, ports, and services that are explicitly required. 2. Utilize stateful inspection/application firewall hardware and software. 3. Utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(1) Enhancement (Moderate)	
Control The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(2) Enhancement (Moderate)	
Control	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(3) Enhancement (Moderate)	
Control	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(4) Enhancement (Moderate)	
Control The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(5) Enhancement (Moderate)	
Control The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(6) Enhancement (Moderate)	
Control The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 7(7) Enhancement (Moderate)	
Control The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 8 Transmission Integrity (Moderate)	
Control The information system protects the integrity of transmitted information. **Implementation Standard(s)** 1. Employ appropriate approved mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of data while in transit from source to destination outside of a secured network (see SC-13). 2. For FTI: All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, fiber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. (Pub 1075, ref. 9.18.2) 3. For FTI: FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. (Pub. 1075, Ref 9.18.5) 4. For FTI: The agency must follow specific precautions when faxing FTI. (Pub 1075 section 9.18.6) **Supplemental Guidance:** This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 8(1) Enhancement (Moderate)	
Control The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 9 Transmission Confidentiality (Moderate)	
Control The information system protects the confidentiality of transmitted information. For FTI: 1. All FTI in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). If encryption is not used, the agency must use other compensating mechanisms (e.g. switched VLAN technology, fiber optic medium, etc.) to ensure FTI is not accessible to unauthorized users. (Pub 1075, ref. 9.18.2) 2. FTI should not be transmitted or used on the agency's internal e-mail systems. If transmittal of FTI within the agency's e-mail system is necessary, specific precautions must be taken to protect the FTI. FTI must not be transmitted outside of the agency, either in the body of an e-mail or as an attachment. (Pub. 1075, Ref 9.18.5) 3. The agency must follow specific precautions when faxing FTI. (Pub. 1075, Ref. 9.18.6) **Supplemental Guidance:** This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4. **Implementation Standard(s)** 1. (For PII only) When sending or receiving faxes containing PII: (i) fax machines must be located in a locked room with a trusted staff member having custodial coverage over outgoing and incoming transmissions or fax machines must be located in a secured area; (ii) accurate broadcast lists and other preset numbers of frequent fax recipients must be maintained; and (iii) a cover sheet must be used that explicitly provides guidance to the recipient that includes: a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone the sender (collect if necessary) to report the disclosure and confirm destruction of the information.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 9(1) Enhancement (Moderate)	
Control The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. **[*Assignment: organization-defined alternative physical measures*].**	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 10 Network Disconnect (Moderate)	
Control The information system automatically terminates the network connection associated with a communications session at the end of the session, or: a. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and b. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity. For FTI: Forcibly disconnects inactive VPN connections after 15 minutes of inactivity. (Pub 1075 section 9.16) **Supplemental Guidance:** This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 12 Cryptographic Key Establishment and Management (Moderate)	
Control When cryptography is required and used within the information system, the organization establishes and manages cryptographic keys for required cryptography employed within the information system. **Supplemental Guidance:** Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 13 Use of Cryptography (Moderate)	
Control When cryptographic mechanisms are used, the information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 13(1) Enhancement (Moderate)	
Control When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 14 Public Access Protections (Moderate)	
Control The information system protects the integrity and availability of publicly available information and applications. **Supplemental Guidance:** The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls. **Implementation Standard(s)** 1. Ensure that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. 2. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
SC 15 Collaborative Computing Devices (Moderate)	
Control The organization prohibits running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used. The information system: a. Prohibits remote activation of collaborative computing devices; and b. Provides an explicit indication of use to users physically present at the devices. **Supplemental Guidance:** Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 15(1) Enhancement (Moderate)	
Control If collaborative computing is authorized, the information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 17 Public Key Infrastructure Certificates (Moderate)	
Control The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. **Supplemental Guidance:** For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC 18 Mobile Code (Moderate)	
Control The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system. **Supplemental Guidance:** Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 19 Voice Over Internet Protocol (Moderate)	
Control The organization prohibits the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization: a. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system. For FTI: The agency must meet specific technical requirements to utilize a VoIP network that provides FTI to a customer (Pub 1075, Ref. 9.18.13) For FTI: Complete SPR section 9.28.3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 20 Secure Name /Address Resolution Service (Authoritative Source) (Moderate)	
Control The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. **Supplemental Guidance:** This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 20(1) Enhancement (Moderate)	
Control The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 22 Architecture and Provisioning for Name /Address Resolution Service (Moderate)	
Control The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. **Supplemental Guidance:** A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 23 Session Authenticity (Moderate)	
Control The information system provides mechanisms to protect the authenticity of communications sessions. **Supplemental Guidance:** This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SC 28 Protection of Information at Rest (Moderate)	
Control The information system protects the confidentiality and integrity of information at rest. **Supplemental Guidance:** This control is intended to address the confidentiality and integrity of information at rest in non-mobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SC 32 Information System Partitioning (Moderate)	
Control The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. **Supplemental Guidance:** Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SC ACA 1 Electronic Mail (Moderate)		
Control Controls shall be implemented to protect ACA sensitive information (such as FTI or Privacy Act protected information) that is sent via email. **Implementation Standard(s)** **1.** Prior to sending an email, place all ACA sensitive information in an encrypted attachment.		
Guidance A good place to obtain recommended security practices for handling sensitive information via e-mail is NIST SP 800-45 (as amended), Guidelines on Electronic Mail Security.		
Applicability: All	**Reference(s):**	**Related Controls Requirement(s):**
ASSESSMENT PROCEDURE: SC-ACA-1.1		
Assessment Objective Determine if: (i) the organization effectively implements protections for ACA sensitive information that is sent via e-mail;		

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

(ii) the organization meets all the requirements specified in the applicable implementation standard(s).

Assessment Methods And Objects

Examine: Email policy and procedures; other relevant documents or records.

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Communications Protection Family (SC) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Information Integrity (SI) – *Operational*

SI 1 System and Information Integrity Policy and Procedures (Moderate)	
Control The organization develops, disseminates, and reviews/updates within every three hundred sixty-five (365) days: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. **Supplemental Guidance:** This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 2 Flaw Remediation (Moderate)	
Control The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. **Supplemental Guidance:** The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US CERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11. **Implementation Standard(s)** 1. Correct identified information system flaws on production equipment in a timeframe based on the National Vulnerability Database (NVD) Vulnerability Severity Rating of the flaw: flaws rated as High severity within seven (7) calendar days; Medium severity within fifteen (15) calendar days; and all others within thirty (30) calendar days. (a) Evaluate system security patches, service packs, and hot fixes in a test bed environment to determine the effectiveness and potential side effects of such changes, and (b) Manage the flaw remediation process centrally.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 2(1) Enhancement (Moderate)	
Control The organization centrally manages the flaw remediation process and installs software updates automatically. Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 2(2) Enhancement (Moderate)	
Control The organization employs automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 3 Malicious Code Protection (Moderate)	
Control The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform critical system file scans during system boot, information system scans using the frequency specified in Implementation Standard 1, and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - Block and quarantine malicious code and send alert to administrator in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. **Supplemental Guidance:** Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7. **Implementation Standard(s)** 1. Desktop malicious code scanning software is configured to perform critical system file scans every twenty (24) hours.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 3(1) Enhancement (Moderate)	
Control The organization centrally manages malicious code protection mechanisms.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 3(2) Enhancement (Moderate)	
Control The information system automatically updates malicious code protection mechanisms (including signature definitions).	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 3(3) Enhancement (Moderate)	
Control The information system prevents non-privileged users from circumventing malicious code protection capabilities.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 4 Information System Monitoring (Moderate)	
Control The organization: a. Monitors events on the information system in accordance with Information Security Incident Handling and Breach Analysis/Notification Procedure and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. **Supplemental Guidance:** Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7. **Implementation Standard(s)** 1. Install IDS devices at network perimeter points and host-based IDS sensors on critical servers.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 4(1) Enhancement (Moderate)	
Control The organization interconnects and configures individual intrusion detection tools into a system wide intrusion detection system using common protocols.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 4(2) Enhancement (Moderate)	
Control The organization employs automated tools to support near real-time analysis of events.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 4(4) Enhancement (Moderate)	
Control The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 4(5) Enhancement (Moderate)	
Control The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: (a) Presence of malicious code, (b) Unauthorized export of information, (c) Signaling to an external information system, or (d) Potential intrusions.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI 4(6) Enhancement (Moderate)

Control

The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

SI 5 Security Alerts, Advisories, and Directives (Moderate)

Control

The organization:
a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;
b. Generates internal security alerts, advisories, and directives as deemed necessary;
c. Disseminates security alerts, advisories, and directives to appropriate personnel; and
d. Implements security directives in accordance with established time frames, or notifies the degree of noncompliance.

Supplemental Guidance: Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is essential due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

	Common; Indicate All Control Provider(s)]
SI 7 Software and Information Integrity (Moderate)	
Control The information system detects unauthorized changes to software and information. **Supplemental Guidance:** The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 7(1) Enhancement (Moderate)	
Control The organization reassesses the integrity of software and information by performing daily integrity scans of the information system.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 8 Spam Protection (Moderate)	
Control The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with configuration management policy and procedures. **Supplemental Guidance:** Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 8(1) Enhancement (Moderate)	
Control The organization centrally manages spam protection mechanisms.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 9 Information Input Restrictions (Moderate)	
Control The organization restricts the capability to input information to the information system to authorized personnel. **Supplemental Guidance:** Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
SI 10 Information Input Validation (Moderate)	
Control The information system uses automated mechanisms to check the validity of information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. **Supplemental Guidance:** Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 11 Error Handling (Moderate)	
Control The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel. For FTI: Generates error messages that provide information necessary for corrective actions in error logs and administrative messages. (Pub 1075 section 9.17) **Supplemental Guidance:** The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

SI 12 Information Output Handling and Retention (Moderate)	
Control The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. **Supplemental Guidance:** The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4. **Implementation Standard(s)** 1. Retain output, including, but not limited to audit records, system reports, business and financial reports, and business records, from the information system in accordance with Policy and all applicable National Archives and Records Administration (NARA) requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *[Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

System and Information Integrity Family (SI) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Project Management (PM) – *Management*

PM 1 INFORMATION SECURITY PROGRAM PLAN
Control
The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [Assignment: organization defined frequency]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments. **Supplemental Guidance**: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls. Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 2 SENIOR INFORMATION SECURITY OFFICER	
Control:	
The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. **Supplemental Guidance:** The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior Information Security Officer or Chief Information Security Officer. Control Enhancements: None.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 3 INFORMATION SECURITY RESOURCES	
Control:	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned. **Supplemental Guidance:** Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation**
	Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]

PM 4 PLAN OF ACTION AND MILESTONES PROCESS
Control:
The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5. Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM 5 INFORMATION SYSTEM INVENTORY
Control:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

The organization develops and maintains an inventory of its information systems. **Supplemental Guidance:** This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 6 INFORMATION SECURITY MEASURES OF PERFORMANCE	
Control:	
The organization develops, monitors, and reports on the results of information security measures of performance. **Supplemental Guidance:** Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program. Control Enhancements: None.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 7 ENTERPRISE ARCHITECTURE	
Control:	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. **Supplemental Guidance:** The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, a integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 8 CRITICAL INFRASTRUCTURE PLAN	
Control:	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan. Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

PM 9 RISK MANAGEMENT STRATEGY

Control:

The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and

b. Implements that strategy consistently across the organization. Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

PM 10 SECURITY AUTHORIZATION PROCESS	
Control:	
The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program. **Supplemental Guidance:** The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*
PM 11 MISSION/BUSINESS PROCESS DEFINITION	
Control:	
The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. **Supplemental Guidance:** Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.	

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Project Management (PM) Security Controls Detail and Comment

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 Protection of FTI in Virtual Environments
Control:
Notification Requirements • The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a virtual environment. • If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Virtualization Notification (see Exhibit 15), which will serve as an addendum to their SPR. • If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Virtualization Notification (see Exhibit 15). Technical Requirements • When FTI is stored in a shared location, the agency must have policies in place to restrict access to FTI to authorized users. • Programs that control the hypervisor should be secured and restricted to authorized administrators only. • FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods, provided by either the virtualization solution or third party-solution, such as a virtual private network (VPN) that encapsulates the management traffic. • Separation between virtual machines (VMs) must be enforced, and functions which allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled. • Virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment. This includes being able to monitor the movement of FTI into and out of the virtual environment. • The VMs and hypervisor/ host OS software for each system within the virtual environment that receives, processes, stores or transmits FTI must be hardened in accordance with the requirements of Publication 1075 and be subject to frequent vulnerability testing. • Special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM should be disabled. • Virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur. • Vulnerability assessment must be performed on systems in a virtualized environment prior to system implementation. • Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need to know. For FTI: Complete SPR section 9.28.2

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 Protection of FTI in Voice over IP (VOIP) Networks	
Control:	
• VoIP traffic that contains FTI should be segmented off from non-VoIP traffic via a virtual Local Area Network (vLAN) or other segmentation method. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied which restrict access to VoIP traffic which contains FTI. • When FTI is in-transit across the network (either Internet or state agency's network) the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode. • VoIP network hardware (servers, routers, switches, firewalls) must be physically protected in accordance with the minimum protection standards for physical security outlined in IRS Publication 1075, section 4.0, Secure Storage. • Each system within the agency's network that transmits FTI to an external customer through the VoIP network is hardened in accordance with the requirements of Publication 1075 and is subject to frequent vulnerability testing. • VoIP-ready firewalls must be used to filter VoIP traffic on the network. • Security testing must be conducted on the VoIP system prior to implementation with FTI and annually thereafter. • VoIP phones must be logically protected and agencies must be able to track and audit all FTI-applicable conversations and access For FTI: Complete SPR section 9.28.3	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*

ADDITIONAL CONTROLS REQUIRED BY IRS PUBLICATION 1075 Protection of FTI in Cloud Computing Environments
Control:
Notification Requirements • The agency must notify the IRS Office of Safeguards 45 days prior to putting FTI in a cloud environment. • If the agency's approved SPR is less than six years old and reflects the agency's current process, procedures and systems, the agency must submit the Cloud Computing Notification (see Exhibit 16), which will serve as an addendum to their SPR. • If the agency's SPR is more than six years old or does not reflect the agency's current process, procedures and systems, the agency must submit a new SPR and the Cloud Computing Notification (see Exhibit 16).

Document Date:

Document Version:

Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

Moderate Security Requirements SSP Workbook for Exchanges

System Name:

Technical Requirements • Data Isolation. Software, data, and services that receive, transmit, process, or store FTI must be isolated within the cloud environment so that tenants sharing physical space cannot access their neighbors' physically co-located data and applications. • Service Level Agreements (SLA). The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with their third party cloud provider. • Data Encryption in Transit. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA. • Data Encryption at Rest. FTI must be encrypted while at rest in the cloud. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing the FIPS 140-2 compliant module. This requirement must be included in the SLA. • Security Control Validation. Agencies must validate security control implementation claims made by cloud providers through a security plan and security control assessments. For FTI: Complete SPR section 9.28.4	
Fully explain control implementation *(or fully explain why control requirement is not applicable)*	**Responsible for Control Implementation** *Indicate System-specific, Hybrid, or Common; Indicate All Control Provider(s)]*