



Chief Information Officer  
Office of Information Services  
Centers for Medicare & Medicaid Services

# CMS POLICY FOR THE INFORMATION SECURITY PROGRAM

**FINAL**  
**Version 4.0**  
**August 31, 2010**

Document Number: CMS-CIO-POL-SEC02-04.0

**(This Page Intentionally Blank)**

## NATURE OF CHANGES

**Version SEC02-04:** This is a revision to the December 31, 2008 issuance of the *CMS Policy for the Information Security Program* in response to changes in NIST special publications mandated by FIPS 200. Scope of control descriptions was reduced and relegated to the *CMS Information Security Acceptable Risk Safeguards*.

- 1) Section 1, Purpose, has been modified to update the statement that this version of the policy supersedes the previous version dated June 25, 2008.
- 2) Section 2, Background
  - a) Section 2.1, Information Security Control Organization, has been modified to update the NIST SP 800-53 version to remove version information.
  - b) Section 2.2, Information Security Program Activities, has been modified to reflect changes to the NIST Risk Management Framework.
- 3) Section 3, Scope, has been modified to address the addition of the Program Management (PM) control family by NIST.
- 4) Section 4, Policy
  - a) Section 4.1, Security Controls, has been updated to reduce the specificity of policy statements and to relegate specific control requirement to be addressed in the ARS.
  - b) Section 4.2, Organizational Security Program Management, added section to address Program Management family of controls from NIST SP 800-53.
- 5) Removed Glossary and added reference in Section 10, Associated Resources.

**Version SEC02-03.2:** This is a revision to the June 25, 2008 issuance of the CMS Policy for the Information Security Program in response to providing the CIO or his/her designated representative authority in accordance with Department policy to approve alternate mitigations when encryption of desktops is not feasible and physical controls and other management controls are in place. Also the Scope was enhanced to include that this policy applies to business partners and sub-contractors “doing work on behalf of CMS”. All changes, other than modifications to Section 4.1.3 and Scope, are editorial in nature. The changes to this policy can be found in the following sections:

- 1) Section 1, Purpose, has been modified to update the statement that this version of the policy supersedes the previous version.
- 2) Section 2, Background, has been modified to update the NIST SP 800-53 version to NIST SP 800-53 Rev. 2 to indicate the current version.
- 3) Section 3, Scope, has been modified to state that this policy also applies to Business Partners and sub-contractors “doing work on behalf of CMS.”

- 4) Section 4, Policy, has been modified to update the NIST SP 800-53 version to NIST SP 800-53 Rev. 2 to indicate the current version.
  - a) Section 4.1.3, last sentence, has been modified to require CIO or designate approval to employ alternate controls.
  - a) Section 4.4.4, has been modified to capitalize “Business Owners” for document consistency.
  - b) Section 4.17.3, has been modified to capitalize “Business Owners” for document consistency.
- 5) Section 6, Applicable Laws/Guidance, has been modified to include “Change Notice 2” to the FIPS 140-2 reference to clarify the reference date. The NIST SP 800-53 reference has been modified to NIST SP 800-53 Rev.2 with a date of December 2007 to reflect the current version.
- 6) Section 10, Associated Resources, removed trailing “/” from the CMS CIO Directives hyperlink.
- 7) Glossary, All Glossary references to NIST SP 800-53R1 have been modified to NIST SP 800-53R2 to reflect the current version. All Glossary references to NIST SP 800-53 have been modified to NIST SP 800-53R2 to reflect the current version.

**Version SEC02-03.1:** This is a revision to the April 24, 2008 issuance of the CMS Policy for the Information Security Program, in response to CMS modifying this policy to comply with the HHS Chief of Staff memo on Mandatory Protection of Sensitive Information on Computers, Mobile Devices and Portable Media, dated May 19, 2008. Modifications can be found in the following sections:

- 1) Section 1, Purpose, has been modified to add a statement that this version of the policy supersedes the previous version dated April 24, 2008.
- 2) Section 4, Policy, has been modified as follows:
  - a) Section 4.1.3 Access Enforcement (AC-3) was modified to add “In addition, encryption as access enforcement extends to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers.” to include the desktop encryption requirement.
  - c) Section 4.12.4 Rules of Behavior (PL-4) was changed from “ROBs shall be established and made readily available...” to “ROBs shall be established in alignment with HHS requirements <http://hhs.gov/ocio/policy/2008-0001.003s.html>, and made readily available...” to meet the requirement that all CMS employees and contractors review and sign the HHS ROB.

**Version SEC02-03:** This is a revision to the November 15, 2007 issuance of the CMS Policy for the Information Security Program, in response to CMS modifying this policy and the CMS Information Security Acceptable Risk Safeguards (ARS) to align the CMS organizationally

defined variables to the current CMS processes. Modifications to this policy can be found in the following sections:

- 1) Section 1, Purpose, has been modified to add a statement that this version of the policy supersedes the previous version dated November 15, 2007.
- 2) Section 4, Policy, has been modified to correct an inaccuracy in the November 15, 2007 issuance of this policy and to apply a global change to replace the terms “annually” or “annual” with “every 365 days”. Section 4.6.6 which originally stated “Agreements with an alternate processing site shall...” should read “Agreements with an alternate storage site...” Section 4.12.4 originally stated “Before authorizing access to the information system and its resident information...”) and has been changed to “Before authorizing access to the information system and / or information and annually thereafter ...” to cover access to information even if no access to a CMS information system exists.

TABLE OF CONTENTS

**1** PURPOSE.....1

**2** BACKGROUND .....1

**2.1** Information Security Control Organization ..... 1

**2.2** Information Security Program Activities ..... 2

    2.2.1 Security Categorization..... 3

    2.2.2 Select..... 3

    2.2.3 Implement ..... 4

    2.2.4 Assess..... 4

    2.2.5 Authorize..... 5

    2.2.6 Monitor ..... 5

**3** SCOPE .....5

**4** POLICY .....5

**4.1** Security Controls ..... 6

    4.1.1 Access Control (AC)..... 6

    4.1.2 Awareness and Training (AT) ..... 7

    4.1.3 Audit and Accountability (AU) ..... 7

    4.1.4 Security Assessment and Authorization (CA) ..... 7

    4.1.5 Configuration Management (CM) ..... 7

    4.1.6 Contingency Planning (CP) ..... 7

    4.1.7 Identification and Authentication (IA)..... 7

    4.1.8 Incident Response (IR) ..... 8

    4.1.9 Maintenance (MA)..... 8

    4.1.10 Media Protection (MP) ..... 8

    4.1.11 Physical and Environmental Protection (PE)..... 8

    4.1.12 Planning (PL) ..... 8

    4.1.13 Personnel Security (PS) ..... 9

    4.1.14 Risk Assessment (RA) ..... 9

    4.1.15 System and Services Acquisition (SA)..... 9

    4.1.16 System and Communications Protection (SC)..... 10

    4.1.17 System and Information Integrity (SI)..... 10

**4.2** Organizational Security Program Management (PM)..... 10

    4.2.1 Security Program Plan ..... 11

    4.2.2 Chief Information Security Officer..... 11

    4.2.3 Information Security Resources..... 11

    4.2.4 Plan of Action and Milestones Process..... 11

    4.2.5 Information System Inventory ..... 12

    4.2.6 Information Security Measures Of Performance ..... 12

    4.2.7 Enterprise Architecture ..... 12

    4.2.8 Critical Infrastructure Plan..... 12

    4.2.9 Risk Management Strategy ..... 12

4.2.10 Security Authorization Process ..... 12

4.2.11 Mission/Business Process Definition..... 13

**5 ROLES AND RESPONSIBILITIES.....13**

**5.1 CMS Administrator ..... 13**

**5.2 CMS Chief Information Officer (CIO)..... 14**

**5.3 Chief Information Security Officer (CISO) ..... 14**

**5.4 Component ISSO ..... 15**

**5.5 Business Owner ..... 15**

**5.6 System Administrator ..... 15**

**5.7 System Developer/Maintainer ..... 16**

**5.8 CMS/Business Partner/Contractor Employees..... 16**

**5.9 Users ..... 16**

**6 APPLICABLE LAWS/GUIDANCE .....16**

**7 INFORMATION AND ASSISTANCE .....17**

**8 EFFECTIVE DATE/IMPLEMENTATION .....18**

**9 APPROVED .....18**

**10 ASSOCIATED RESOURCES .....18**

**11 GLOSSARY.....18**

**LIST OF TABLES**

Table 1 Table 1: NIST SP 800-53 IS Control Families and Classes ..... 6

**LIST OF FIGURES**

Figure 1 CMS IS Risk Management Process ..... 3

**(This Page Intentionally Blank)**

---

# 1 Purpose

This document establishes the policy for the information security (IS) program at the Centers for Medicare & Medicaid Services (CMS). The formation of the *CMS Policy for the Information Security Program (PISP)* is driven by many factors, the key one being **Risk**. This policy sets the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk, and minimize the effect of security incidents.

This policy supersedes the previous version that was signed by the CMS Chief Information Officer (CIO) on December 31, 2008.

---

## 2 Background

### 2.1 Information Security Control Organization

As the Agency charged with administering the Medicare, Medicaid, and Children's Health Insurance Programs, CMS collects, generates, and stores financial, health care, and other sensitive information. Most of this information relates to the health care provided to the nation's Medicare and Medicaid beneficiaries and has access restrictions required by legislative and regulatory directives. As the information's trusted custodian, CMS must protect and ensure the confidentiality, integrity, and availability (CIA) of all its information regardless of how it is created, distributed, or stored.

To safeguard the CIA of its information and information systems effectively, CMS has established an enterprise-wide IS Program. As part of this program, security controls must be implemented to protect all information assets, including hardware, systems, software, and data. These controls must be designed to ensure compliance with all federal legislation, policies and standards (e.g., by managing risk; facilitating change control; reporting and responding to security incidents, intrusions, or violations; and formulating contracts.)

This policy addresses the reduction in risks to information resources through adoption of preventive measures and controls designed to detect any errors that occur. It also addresses the recovery of information resources in the event of a disaster. CMS has established three (3) classes of IS controls: Management, Operational, and Technical. This structure is consistent with the guidance established by the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*.

**Management** controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to CMS' assets and operations. There are five (5) families of policy within the Management class that address:

- Security Assessment and Authorization (CA);
- Planning (PL);

- Risk Assessment (RA);
- System and Services Acquisition (SA); and
- Program Management (PM).

**Operational** controls support the day-to-day procedures and mechanisms to protect CMS' information and information systems. There are nine (9) families of policy within the Operational class that address:

- Awareness and Training (AT);
- Configuration Management (CM);
- Contingency Planning (CP);
- Incident Response (IR);
- Maintenance (MA);
- Media Protection (MP);
- Physical and Environmental Protection (PE);
- Personnel Security (PS); and
- System and Information Integrity (SI).

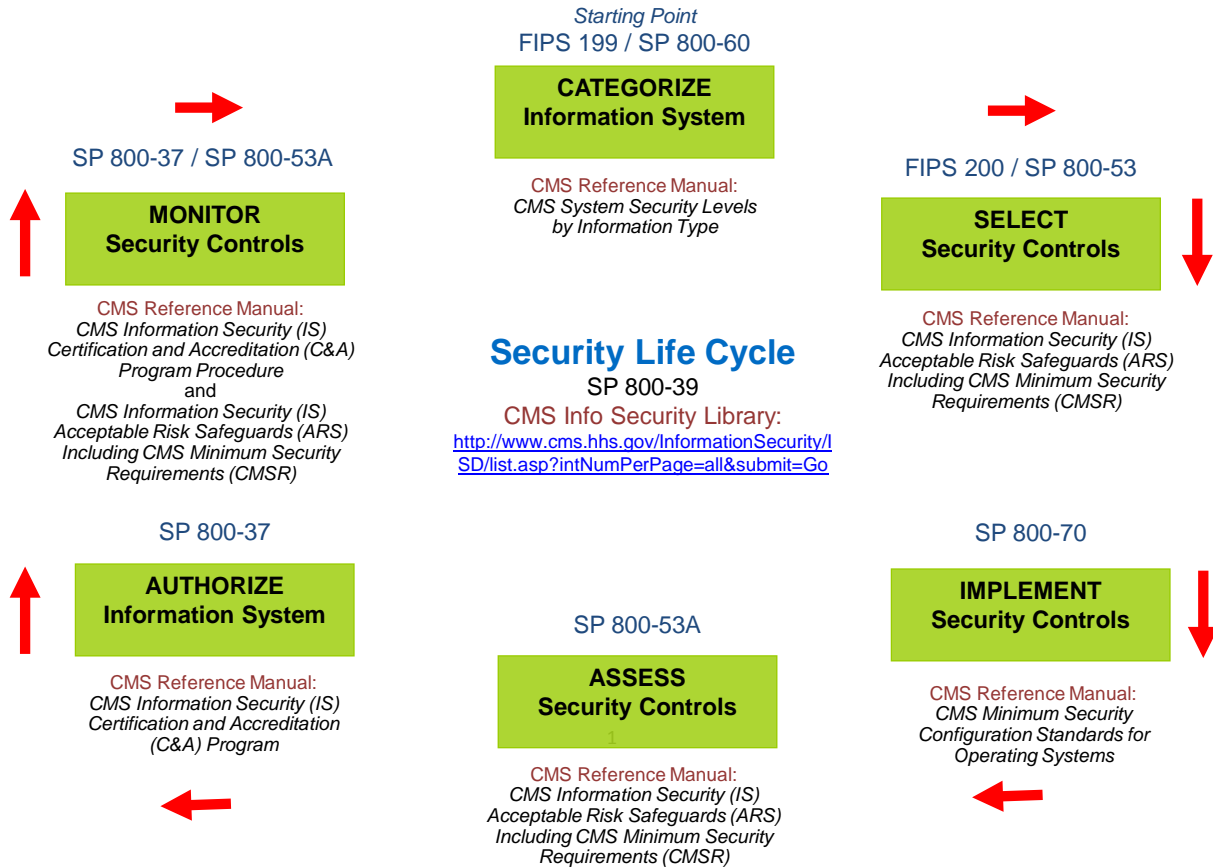
**Technical** controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are four (4) families of policy within the Technical class that address:

- Access Control (AC);
- Audit and Accountability (AU);
- Identification and Authentication (IA); and
- System and Communications Protection (SC).

## 2.2 Information Security Program Activities

This section describes some of the key activities of CMS' IS risk management process, as they are conducted within the System Developmental Life Cycle (SDLC). See Figure 1 below.

**Figure 1 CMS IS Risk Management Process**



2.2.1 Security Categorization

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires that for all federal systems must be associated with a system security level by evaluating the potential impact value (High, Moderate or Low), for each of the three security objectives of confidentiality, integrity and availability (CIA). CMS has pre-determined, using FIPS Publication 199 and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, all of the applicable CMS System Security Levels for the various information types processed by CMS information systems. This security categorization is the basis for selecting appropriate security controls for CMS information systems as well as assessing the risks to CMS operations and assets.

2.2.2 Select

Annually, CMS performs a review of the current baseline controls established in the CMS Information Security (IS) Acceptable Risk Safeguards (ARS) - CMS Minimum Security Requirements (CMSR). Adjustments, with senior agency management concurrence, are applied

to the PISP and ARS to reflect the current IS requirements established by NIST SP 800-53 and any other DHHS or OMB directives. Tailoring guidance for the CMS enterprise has already been established during this review and no additional tailoring is permitted.

- Each Business Owner must select the applicable security controls from the appropriate High, Moderate or Low CMSR.
- In exceptional circumstances, deviations from the CMSR can be requested with explicit justification in respect to specific mission and business processes, organizational requirements, and environments of operation along with alternate risk mitigations through the CMS risk acceptance process to obtain written approval from the CMS CISO.
- Each Business Owner should select additional security controls based on an assessment of risk and local conditions including specific and credible threat information, organization-specific security requirements, cost-benefit analyses, and special circumstances.

### 2.2.3 Implement

The implementation of security controls to protect CMS' mission and business processes is tightly coupled to the enterprise architecture and integrated into the SDLC. Knowledgeable individuals within the organization (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists) shall determine which personnel, processes, hardware, software, firmware, facilities, or environmental components within the defined information system boundary are providing specific security functionality. There should be close coordination and collaboration among organizational personnel to ensure that the needed security functions are allocated to the appropriate information systems and supporting infrastructure. For common security controls, the organization should allocate the controls to entities, either internal or external to the organization, with the responsibility for their development, implementation, and assessment. Certain security controls employed within CMS information systems require that security configuration settings be established during implementation. For many technologies, CMS defines mandatory configuration settings for information technology products that are used within CMS information systems to comply with configuration settings-related legislation, directives, and policy requirements. Mandatory security configuration settings shall be enforced across CMS, including all information systems that are supporting organizational mission/business processes.

### 2.2.4 Assess

The security controls must be tested and evaluated prior to system deployment to ensure that the controls are effective. A Security Test and Evaluation (ST&E) plan is developed and executed for each system to test the security controls. This test provides feedback as to the effectiveness of implemented security controls to Business Owners and System Developers/Maintainer, and is one of the factors that may affect the ATO decision. Satisfactory completion of the ST&E is an essential milestone for the security authorization of new systems to assure compliance with CMS IS policy and standards as well as providing the desired functionality.

### 2.2.5 Authorize

In accordance with the provisions of Office of Management and Budget (OMB) Circular A-130, a security authorization of an information system to process, store, or transmit information is required. This authority to operate (ATO) is granted by the CMS CIO or their designee and is based on the verified effectiveness of the security controls to CMS policy and standards together with an identified risk to the organization's operation or assets.

### 2.2.6 Monitor

In accordance with the provisions of FISMA, periodic or continuous testing and evaluation of security controls in an information system are required on an on-going basis to ensure that the controls continue to be effective in their application. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures is a critical activity conducted by the organization or by an independent third party on behalf of the organization. The on-going monitoring of security control effectiveness is accomplished in a variety of ways including security reviews, self-assessments, ST&Es, and various audits.

---

## 3 Scope

This policy applies to all CMS information, information systems, IT activities, and IT assets owned, leased, controlled, or used by CMS, CMS' agents, contractors, or other business partners on behalf of CMS. This policy applies to all CMS employees, contractors, sub-contractors, and their respective facilities supporting CMS business missions, wherever CMS data is stored or processed. Some policies are explicitly stated for persons with a specific job function (e.g. the System Administrator); otherwise, all personnel supporting CMS business functions shall comply with the policies. CMS operating departments shall use this policy or may create a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy.

This policy does not supersede any other applicable law or higher level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

---

## 4 Policy

CMS' policies and controls have a well-defined organization and structure. Security policies and controls are organized into classes and families for ease of use in the control selection and specification process. There are three (3) general classes of security policies and controls (i.e., Management, Operational, and Technical) and eighteen (18) security policy and control families as specified in NIST SP 800-53.

Each family contains security policies and controls related to the security functionality of the family. A two character identifier is assigned to uniquely identify each policy and control family. The following table summarizes the classes and families in the security control catalog and the associated family identifiers, as well as the order of the included policies.

Table 1 Table 1: NIST SP 800-53 IS Control Families and Classes

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Organizational Security Program Management	Management

Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog in the ARS, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family (Program Management [PM] family) provides controls for information security programs. This family provides security controls at the organizational level rather than the information-system level.

The program management (PM) controls, complement the other 17 families of security controls for an information system by focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. The PM family of controls is addressed in full by Section 4.2 of this policy.

## 4.1 Security Controls

Security requirements for all information systems, using the ARS CMSR, shall be used and effectively implemented. The minimum CMSR shall include:

### 4.1.1 Access Control (AC)

Information system access must be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

#### 4.1.2 Awareness and Training (AT)

Managers and users of information systems must be made aware of the security risks associated with their activities and of the applicable federal and agency requirements related to the security of CMS information systems. Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities.

#### 4.1.3 Audit and Accountability (AU)

Information system audit records must be created, protected, and retained to the extent needed to: (i) enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

#### 4.1.4 Security Assessment and Authorization (CA)

Information systems must: (i) be assessed at least every three years or whenever a significant change occurs to the information system to determine if security controls are effective in their application; (ii) have plans of action with milestones designed to correct deficiencies and reduce or eliminate vulnerabilities; (iii) be authorized for processing including any associated information system connections by a designated senior agency official; and (iv) be monitored on an ongoing basis to ensure the continued effectiveness of the controls.

#### 4.1.5 Configuration Management (CM)

Baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) must be established and maintained throughout the respective system life cycles; and security configuration settings for information products employed in information systems must be established and enforced.

#### 4.1.6 Contingency Planning (CP)

Contingency plans for emergency response, backup operations, and disaster recovery for organizational information systems must be established, maintained, and effectively implemented to ensure the availability of critical information resources and continuity of operations in emergency situations.

#### 4.1.7 Identification and Authentication (IA)

Information system users, processes acting on behalf of users, or devices must be identified and the identities authenticated (or verified), as a prerequisite to allowing access to information systems.

#### 4.1.8 Incident Response (IR)

An operational incident handling capability for information systems must be established that includes preparation, detection, analysis, containment, recovery, and user response activities. Incidents must be tracked, documented, and reported.

#### 4.1.9 Maintenance (MA)

Periodic and timely maintenance on organizational information systems must be performed. Effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance must be established.

#### 4.1.10 Media Protection (MP)

Information system media, both digital and non-digital must be protected by: (i) limiting access to information on information system media to authorized users; and (ii) sanitizing or destroying information system media before disposal or release for reuse.

#### 4.1.11 Physical and Environmental Protection (PE)

Physical access to information systems, equipment, and the respective operating environments must be limited to authorized individuals.

4.1.11.1 The physical plant and support infrastructure for information systems must be protected.

4.1.11.2 Supporting utilities for information systems must be provided.

4.1.11.3 Information systems must be protected against environmental hazards.

4.1.11.4 Appropriate environmental controls must be provided in facilities containing information systems.

#### 4.1.12 Planning (PL)

System security plans for information systems that describe the security controls in place for the information systems and the rules of behavior for individuals accessing the information systems must be developed, documented, implemented, and updated at least every three years, whenever a significant change occurs to the information system, whenever a change in the threat environment occurs, whenever a significant data breach occurs, or the accreditation has expired.

#### 4.1.13 Personnel Security (PS)

CMS information systems shall employ personnel security controls consistent with applicable laws, Executive Orders, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.

4.1.13.1 Individuals occupying positions of responsibility within organizations (i.e., including third-party service providers) must be trustworthy and meet established security criteria for those positions.

4.1.13.2 Information and information systems must be adequately protected when personnel actions are enacted such as initial employment, terminations and transfers.

4.1.13.3 Formal sanctions for personnel failing to comply with organizational security policies and procedures must be employed.

#### 4.1.14 Risk Assessment (RA)

The risk to organizational operations (i.e., including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information must be assessed and an risk assessment developed, documented, implemented, and updated at least every three years, whenever a significant change occurs to the information system, whenever a change in the threat environment occurs, whenever a significant data breach occurs, or the accreditation has expired.

#### 4.1.15 System and Services Acquisition (SA)

Documented procedures shall be developed and implemented effectively to facilitate the implementation of the system and services acquisition security controls in all system and services acquisitions. Procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4.1.15.1 Sufficient resources to adequately protect organizational information systems must be allocated by the responsible organization.

4.1.15.2 System development life cycle processes that incorporate required information security considerations must be employed.

4.1.15.3 Software usage and installation restrictions must be employed.

4.1.15.4 Security specifications, either explicitly or by reference, shall be included in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal requirements and industry best practices.

4.1.15.5 Security measures consistent with applicable federal requirements and industry best practices to protect information, applications, and/or services outsourced from the organization are required of third party vendors and must be verified.

#### 4.1.16 System and Communications Protection (SC)

Technical controls shall be developed, documented, and implemented effectively to ensure the CIA of CMS information systems and the protection of the CMS information system communications. Procedures shall be developed, documented, and implemented effectively to guide the implementation and management of such technical controls. The technical controls and procedures shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance; and shall be reviewed periodically, and, if necessary, updated.

4.1.16.1 Communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems must be monitored, controlled, and protected.

4.1.16.2 Architectural designs, software development techniques, and systems engineering principles that promote effective information security within information systems must be employed.

#### 4.1.17 System and Information Integrity (SI)

4.1.17.1 Information and information system flaws must be identified, reported, and corrected in a timely manner.

4.1.17.2 Protection from malicious code must be provided at appropriate locations within organizational information systems.

4.1.17.3 Information system security alerts and advisories issued shall be monitored and appropriate action taken in response.

4.1.17.4 Minimum security controls shall be supplemented, as warranted, based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analysis, or special circumstances.

## 4.2 Organizational Security Program Management (PM)

Organizational security program management controls are required of CMS, CMS' agents, contractors, sub-contractors or other business partners performing work on behalf of CMS and they apply to their respective facilities that support CMS business missions, wherever CMS data is stored or processed. These security requirements focus on organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. These controls are subject to the approval,

evaluation, review, monitoring, and correction processes for information systems, but are done separately from and are inherited by information systems. Minimum security controls include:

#### 4.2.1 Security Program Plan

The CIO shall develop, disseminate, review (at least annually), and update as needed an organizational security program plan that contains, at a minimum:

- 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.
- 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.
- Roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Approval 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, CMS, other organizations, and the Nation.

#### 4.2.2 Chief Information Security Officer

The CMS CIO shall appoint a chief information security officer with the mission and resources to coordinate, develop, implement, and maintain a CMS-wide information security program.

#### 4.2.3 Information Security Resources

CMS Business Owners shall, at a minimum:

- Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.
- Record the resources required. CMS Business Owners shall use a business case/Exhibit 300/Exhibit 53 to record the resources required.
- Ensure that information security resources are available for expenditure as planned.

#### 4.2.4 Plan of Action and Milestones Process

CMS Business Owners shall implement the CMS CIO-specified 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

(from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

#### 4.2.5 Information System Inventory

Organizations shall develop and maintain an inventory of information systems as directed by the CMS CIO.

#### 4.2.6 Information Security Measures Of Performance

Organizations shall develop, monitor, and report on the results of information security measures of performance as directed by the CMS.

#### 4.2.7 Enterprise Architecture

A CMS enterprise architecture shall be developed, and maintained, by the CMS CIO; with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Contractors of CMS and Business Partners shall design, develop, implement, and operate CMS related information systems in accordance with the CMS enterprise architecture.

#### 4.2.8 Critical Infrastructure Plan

Business Owners shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

#### 4.2.9 Risk Management Strategy

Organizations shall:

- Develop 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.
- Implement that strategy consistently across the organization.

#### 4.2.10 Security Authorization Process

Organizations shall:

- Manage (i.e., document, track, and report) the security state of organizational information systems through the security authorization processes.
- Fully integrate the security authorization processes into an organization-wide risk management program.

#### 4.2.11 Mission/Business Process Definition

Organizations shall:

- Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, CMS, other organizations, and the Nation.
- Determine information protection needs arising from the defined mission/business processes and revise the processes as necessary, until an achievable set of protection needs is obtained.

---

## 5 Roles And Responsibilities

The following entities have responsibilities related to the implementation of this program policy.

### 5.1 CMS Administrator

The CMS Administrator has the overall responsibility for the implementation of an agency-wide IS Program as required by the laws and regulation as directed by the Department of Health and Human Services (DHHS) for ensuring compliance with all government-wide legal and policy requirements.

The CMS Administrator shall be responsible for the following duties, in accordance with provisions of FISMA:

- Providing information security protections commensurate with this policy, the CMS IS program and federal regulations;
- Ensuring that senior agency officials provide information security for the information and information systems that support the operations and assets under their control;
- Delegating to the CMS CIO the authority to ensure compliance with the requirements imposed on CMS under sub-section 3544 of FISMA, Federal Agency Responsibilities;
- Ensuring that CMS has trained personnel sufficient to assist CMS in complying with the requirements of this policy and related procedures, standards and guidelines; and
- Ensuring that the CMS CIO, in coordination with other senior CMS officials, reports annually to the CMS Administrator on the effectiveness of the CMS IS Program, including progress of remedial actions.

## 5.2 CMS Chief Information Officer (CIO)

The CMS CIO is responsible for the following:

- Ensuring there is an appropriate level of protection for all CMS information resources, whether retained in-house or under the control of contractors, including the establishment of operational, management and technical safeguards;
- Assisting Business Owners in understanding their security responsibilities and ensuring that they incorporate an acceptable level of protection for all CMS IT Systems;
- Developing, implementing and administering the CMS IS Program, as well as DHHS and government-wide security directives;
- Designating a Chief Information Security Officer (CISO);
- Developing and maintaining this policy, information security procedures, and control techniques to address federal requirements;
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
- Assisting senior agency officials concerning their responsibilities regarding information and information systems that support operations and assets under their realm of responsibility.

## 5.3 Chief Information Security Officer (CISO)

The CMS CISO is responsible for the following activities:

- Developing and implementing an information system security training and orientation program in accordance with the requirements from the FISMA of 2002;
- Developing, evaluating and providing information about the CMS IS Program, and communicating CMS IS Program requirements and concerns to CMS management and personnel;
- Ensuring that SSPs are developed, reviewed, implemented, and revised;
- Maintaining documentation used to establish systems security level designations for all SSPs within CMS;
- Ensuring that IS RAs are developed, reviewed, and implemented for the SSP process;
- Providing leadership & participating in IS incident response and reporting IS incidents in accordance with reporting procedures developed and implemented by Federal mandates, HHS, and CMS;
- Mediating and resolving systems security issues that arise between two CMS organizations, CMS and other federal organizations, or CMS and States or contractors;

- Assuring that CMS business Component Information System Security Officers (ISSOs) are appointed and trained;
- Assisting CMS business Component ISSOs in developing local systems security; and
- Researching state-of-the-art systems security technology and disseminating information material in a timely fashion.

## **5.4 Component ISSO**

Component ISSOs are responsible for the following activities:

- Assisting the CISO in ensuring the component adheres to Laws, Executive Orders, Directives, Regulations, Policies, Standards, and CMS IS Program Requirements;
- Serving as the primary point of contact in the component for IS issues; and
- Participating in the technical certification of component RAs and SSPs.

## **5.5 Business Owner**

CMS Business Owners are responsible for the following activities:

- Assessing the risk to the information and information systems over which they have responsibility;
- Ensuring, through system certification, that the CMS information systems over which they have responsibility are developed, implemented, operated, and documented according to the requirements of this policy;
- Certifying that CMS information systems fully comply with CMS IS requirements; and
- Ensuring appropriate security measures and supporting documentation are maintained.

## **5.6 System Administrator**

System Administrators are responsible for the following activities:

- Verifying that system security requirements of their systems are being met;
- Establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; and
- Periodically reviewing and verifying that all users of their systems are authorized and are using the required systems security safeguards, in compliance with the CMS IS Program and all related standards, guidelines, and procedures.

## 5.7 System Developer/Maintainer

System Developers/Maintainers are responsible for the following activities:

- Developing and implementing the IS requirements throughout the SDLC; and
- Planning and implementation for the on-going maintenance of the information system, including updates, upgrades and patches in accordance with the SDLC and this policy.

## 5.8 CMS/Business Partner/Contractor Employees

CMS / Business Partner / Contractor employees have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the CMS IS "Virtual Handbook"<sup>1</sup>. Use of organization-owned or leased equipment and resources to accomplish work-related responsibilities will always have priority over personal use. In order to avoid capacity problems and to reduce the susceptibility of organization information technology resources to computer viruses and cyber attacks, employees shall comply with the following requirements:

- Personal files obtained via the Internet may not be stored on individual PC hard drives or on local area network (LAN) file servers;
- Official video and voice files may not be downloaded from the Internet except when they will be used to serve an approved organization function; and
- Internet and email etiquette, customs and courtesies shall be followed when using organization-owned or leased equipment or resources.

## 5.9 Users

Users have the responsibility to ensure the protection of CMS' information (data) and information systems by complying with the IS requirements maintained in this policy and in the CMS IS "Virtual Handbook". Users shall attend required information security and functional training. In addition, CMS employee-users shall adhere to the duties, requirements, and responsibilities as stated in the Master Labor Agreement (MLA) between CMS and the American Federation of Government Employees, Article 35, November 16, 2007 or any of its successors.

---

## 6 Applicable Laws/Guidance

The following public laws and federal guidance are applicable to this policy:

- FISMA Act of 2002, Public Law (P.L.) 107-347;

---

<sup>1</sup> The CMS IS "Virtual Handbook" is the collection of all CMS policies, procedures, standards, and guidelines which implement the CMS IS Program.

- HIPAA, 1996, P.L. 104-191;
- Medicare Modernization Act of 2003, P.L. 108-173;
- The Privacy Act of 1974, as amended (5 U.S.C. 552a);
- OMB Circular A-130, Management of Federal Information Resources, November 28, 2000;
- OMB Memorandum M-00-07, Incorporating and Funding Security in Information Systems Investments, February 28, 2000;
- OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003;
- OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 23, 2004;
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007;
- Federal Information Processing Standards (FIPS), Publication 140-2, Security Requirements for Cryptographic Modules, Change Notice 2, December 3, 2002;
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004;
- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006;
- Federal Preparedness Circulars (FPC) 65, June 15, 2004;
- Federal Preparedness Circulars (FPC) 67, April 30, 2001;
- National Security Presidential Directive (NSPD)-1, February 13, 2001;
- Homeland Security Presidential Directives (HSPD)-7, December 17, 2003;
- Homeland Security Presidential Directives (HSPD)-12, August 27, 2004;
- NIST SP 800-53 Rev. 3, Recommended Security Controls for Federal Information Systems, August 2009, and other NIST 800 Series Special Publications;
- CMS Information Security Policy, CMS-OA-POL-SEC01, April 12, 2006; and
- CMS Policy for Investment Management and Governance, May 17, 2007.

---

## 7 Information And Assistance

Contact the Chief Information Security Officer for further information regarding this policy.

---

## 8 Effective Date/Implementation

This policy becomes effective on the date that CMS' CIO signs it and remains in effect until officially superseded or cancelled by the CMS CIO.

---

## 9 Approved

\_\_\_\_\_ August 31, 2010

Julie C. Boughn Date of Issuance  
CMS Chief Information Officer and  
Director, Office of Information Services

---

## 10 Associated Resources

This policy is augmented by the:

- CMS Information Security "Virtual Handbook,"  
<http://www.cms.hhs.gov/InformationSecurity/>
- CMS Integrated IT Investment and System Lifecycle Framework  
<http://www.cms.hhs.gov/SystemLifecycleFramework/>
- CMS CIO Directives [http://www.cms.hhs.gov/InfoTechGenInfo/04\\_CIODirectives.asp](http://www.cms.hhs.gov/InfoTechGenInfo/04_CIODirectives.asp)

---

## 11 Glossary

The glossary of this document is provided in the below listed document:

- *CMS Information Security Terms, Definitions, and Acronyms*  
<http://www.cms.hhs.gov/InformationSecurity/downloads/termsdefinitions.pdf>