



Environmental Management Consolidated Business Center (EMCBC)

Subject: Cyber Security Master Policy

POLICY, PROCEDURE
and PLAN

APPROVED: (Signature on File)
EMCBC Director

1.0 PURPOSE

Title III (§301) of the E-Government Act (Public Law 107-347), passed November 15, 2002, is known as the Federal Information Security Management Act (FISMA) of 2002. This act requires that all federal agencies (U.S. civilian departments, agencies, and their contractors) develop and implement an agency-wide information security program to safeguard the Information Technology (IT) assets and data of the respective agency.

In 2004 and 2005, the National Institute of Standards and Technology (NIST) released a series of new guidance documents that restructured the certification and accreditation process (NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*) by requiring demonstrations of the processes and controls used to ensure a defense-in-depth computer security architecture. NIST is specific in its requirements and stipulates that the information security program must include documentation and reports that clearly describe the following:

- Periodic risk assessments
- Information security policies and procedures
- An assessment of threats, including their likelihood and impact
- Policies and procedures for detecting security vulnerabilities
- Evaluation and periodic testing of how well security policies are working
- An inventory of software and hardware assets
- Security awareness training and expected rules of behavior for end-users
- An evaluation of the technical, management, and operational security controls
- Procedures for reporting and responding to security incidents
- A process for addressing any deficiencies reported
- Contingency plans to ensure continuity of operations during a disaster

Federal Information Processing Standard (FIPS) 199 offers a standardized methodology to assess the risks to the confidentiality, integrity, and availability (CIA) of unclassified systems. NIST SP 800-60 provides guidance for mapping types of information systems to recommended baseline CIA security categories. NIST SP 800-53 sets out the baseline management, operational, and technical controls that systems must incorporate into a system to minimally ensure the security of low, moderate, and high risk systems. This set of documents is reflected in the first draft of FIPS 200. FISMA requires that Federal agencies report their cyber security programs in accordance with this new guidance, which highlights all laws and regulations on Cyber Security.

This policy document outlines the requirements of NIST 800-53 for cyber security policies. It is not intended to be a substitute for the EM Program Cyber Security Plan (PCSP), but rather is a policy statement of requirement for security controls.

2.0 SCOPE

This policy applies to all unclassified cyber systems and networks which are part of EMCBC cyber systems accreditation boundary and associated enclaves. This policy is intended to identify and outline the computer security policy statements implemented and or to be implemented in consonance with the referenced documents below. It specifically identifies the management, operational, and technical controls that must be incorporated into the EMCBC accreditation boundary to ensure the security of low and moderate risk systems. This policy specifies the responsible EMCBC department(s) and/or responsible official for the implementation of the control policies.

3.0 APPLICABILITY

This EMCBC policy applies to all entities, Federal or contractor that collects, create, process, transmit, store, and disseminate information for EMCBC Headquarters Organization and its Small Site Offices.

This policy applies to any information systems that collects, creates, processes, transmits, stores, and disseminates unclassified or classified DOE information. This policy applies to any information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system" or "system" is used to mean any information systems and/or networks that are used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of EMCBC or DOE.

4.0 REQUIREMENTS AND REFERENCES

4.1 Requirements:

Requirements are Performance based approaches and must be used to evaluate and verify the effectiveness of cyber security measures, as well as to identify areas requiring improvement and to validate implemented improvements. Protection measures for all EMCBC information systems must conform to the protection measures described in the EM PCSP, and the information System Security Plan (SSP). As a minimum, the protection afforded to the information and information system, on which it resides, is based on a risk-based graded protection approach as defined by the EM PCSP. Protection measures may be strengthened based on an assessment of unique local threat(s) or the local evaluation of Consequence of Loss.

All government information and any non-government information on an EMCBC information system must be considered when determining the systems' protection measures.

4.2 References:

- 4.2.1 Federal Information Security Management Act (FISMA);
- 4.2.2 Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors;
- 4.2.3 NIST SP 800-53 - Recommended Security Controls for Federal Information Systems;
- 4.2.4 NIST SP 800-53A – Guide for Assessing the Security Controls in the Federal Information Systems;
- 4.2.5 NIST SP 800-26 – Security Self-Assessment Guide for Information Technology Systems;
- 4.2.6 FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems;
- 4.2.7 NIST SP 800-30 - Risk Management Guide IT Systems;
- 4.2.8 NIST SP 800-37 – Security Certification and Accreditation;
- 4.2.9 NIST SP 800-27A Engineering Principles for Information Technology Security;
- 4.2.10 DOE Order 205.1A – Department of Energy Cyber Security Management Program;
- 4.2.11 DOE Manual 205.1-4 National Security Controls Manual (for classified AIS)
- 4.2.12 EMCBC Computer Security Gap Assessment;
- 4.2.13 EMCBC Computer Security Threat and Vulnerabilities Statement;
- 4.2.14 EMCBC Computer Security Risk Assessment and Mitigation;
- 4.2.15 EMCBC Computer Security Policies; EMCBC System Security Plan (SSP);
- 4.2.16 Contingency Plan for the EMCBC's Computer Accreditation Boundary;
- 4.2.17 EMCBC Certification and Accreditation Document;
- 4.2.18 EMCBC POA&M; and
- 4.2.19 Draft Security Assistance Team Evaluation of Cyber Security at the Environmental Management Consolidated Business Center.

5.0 DEFINITIONS

The following are terms and definitions used in this policy that are not found in National Security Telecommunications and Information Systems Security (NSTISSC) 4009, National Information Systems Security (INFOSEC) Glossary, dated 5 June 1992. "

- 5.1 Accreditation - Formal declaration by the Designated Approving Authority (DAA) that an information system is accredited to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

5.2 Architecture - The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.

5.3 Assurance - Measure of confidence that the security features, practices, procedures and architecture of an information system accurately mediate and enforce the security policy.

5.4 Accreditation Boundary - The conceptual limit of an information system that extends to all directly and indirectly connected users who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.

5.5 Certification and Accreditation (C&A) - All components of a system that are to be accredited by the DAA and excluding separately accredited systems to which the system is connected.

5.6 Confidentiality - A security objective that seeks to assure that information is not disclosed to unauthorized persons, processes, or devices. (NSTISSI No. 4009: Assurance that information is not disclosed to unauthorized persons, processes, or devices.)

5.7 Consequence of Loss (CoL) – Methodology used to determine the consequence, if any, that might occur if the asset was lost, using the impact factors.

5.8 Information System Site Manager (ISSM) - The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements, and ensuring the approved security configuration is maintained.

5.9 Information System Security Officer (ISSO) - Person responsible to the system owner and designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.

5.10 Integrity - Existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

5.11 Data Owner - The person responsible for having information reviewed for sensitivity and classification. This person is responsible for its generation, management, and destruction.

5.12 Data Custodian - The person acting on behalf of the data owner for the generation, management, and destruction of data and to ensure the review of information sensitivity and classification.

5.13 Defense-in-depth - Represents the use of multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be on different vectors within the network, helping prevent a shortfall in any one defense leading to a wider failure

5.14 Designated Approving Authority (DAA) - Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

5.15 Access Approval - Access to information is authorized in writing with justification. Documented approval by a data or system owner to allow user access to information.

5.16 Authority to Operate (ATO) - The system meets the requirements as stated in the System Security Plan.

5.17 General Support System - An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [From Office of Management and Budget (OMB) Circular A-130, Appendix III.]

5.18 Information Integrity -The preservation of unaltered states as information is transferred through the system and between components.

5.19 Information System - The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Any telecommunication or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [Office of Management and Budget, Circular A-130, Nov. 30, 2000: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.]

5.20 Information Technology (IT) - The hardware, firmware, and software used as part of the information system to perform information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management,

movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.

5.21 Integrity - Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. It is composed of data integrity and system integrity.

5.22 Legacy Information System - An operational information system that existed prior to the implementation of the C&A process.

5.23 Major Application- A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [From Appendix III, OMB A-130]

5.24 Mission - The assigned duties to be performed by an information system.

5.25 Perimeter - All components of an information system that are to be accredited as one entity.

5.26 Personally Owned - An item that is owned by an individual and is intended solely for his/her personal use.

5.27 Portable Computing Device - Any portable devices that provides the capability to collect, create, process, transmit, store, and disseminate information. They include (but are not limited to) Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-web-enabled cell phones, web based enhanced cell phones, two-way pagers, and wireless e- mail devices.

5.28 Privileged User - A user with access to control, monitoring, or administration functions of the information system (e.g., system administrator, system security officer, maintainers, system programmers, etc.). NOTE: It is often convenient to refer to a user who is NOT a privileged user as a power user.

5.29 Protection Profile - An implementation- independent set of security requirements for a category of information systems that meet specific protection measures for specific information groups.

5.30 Risk Assessment - Process of analyzing threats to and vulnerabilities of an information system and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is a basis for identifying appropriate and cost-effective countermeasures.

5.31 Risk Management - The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.

5.32 Security - Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

5.33 Security Documentation - All documents which describe the security requirements, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system or major application (or update to either) meets the protection requirements.

5.34 Site Manager - The person responsible for management of all activities at an element.

5.35 System - The set of interrelated components consisting of mission, environment, and architecture as a whole.

5.36 System Owner - The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

5.37 System Security Plan (SSP) - Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

5.38 User - An individual who can receive information from, input information to, or modify information on an information system without an independent human review.

5.39 Vulnerability Assessment - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

6.0 RESPONSIBILITIES

EMCBC's organizational structure is listed below and the responsibilities are identified to implement the computer security controls.

6.1 Designated Approving Authority (DAA)

The DAA is a senior management official with budget and oversight authorities that is a federal employee within the organization who assumes the responsibility for EMCBC information systems and is held accountable for ensuring the information system is operating at an acceptable level of risk.

The DAA is responsible for;

- Approving system security requirements, system security plans (SSP) and memorandums of agreement and/or memorandums of understanding;
- Assuming full responsibility for the residual risk of an information system's operation;
- Certifying and Accrediting that all requirements have been mitigated to an acceptable level for the EMCBC Accreditation Boundary on all information systems.
- Approving operation of information systems through a Authority to Operate letter (ATO);
- Denying authorization to operate the information system (or if system is already operational, halt operations) if an unacceptable security risk exist.
- Possessing a clearance to the highest classification level of the systems to be accredited; and
- Receiving educational training specific to the role within six months of appointment.

6.2 Designated Approving Authority Representative (DAA Rep.)

The DAA Rep. is a management official who is appointed by the DAA to carry out the day-to-day implementation of the duties tasked to the DAA. The DAA Rep. is required to be a federal employee.

The DAA Rep. is responsible for:

- Day-to-day implementation of duties tasked to the DAA;
- Certifying to the DAA that all requirements have been met and that the information systems in EMCBC accreditation boundary are ready for accreditation;
- Recommending policies, standards, procedures and guidelines be adopted in EMCBC accreditation boundary for DAA signature;
- Reviewing current technology for more effective security practices;
- Securing funding for EMCBC cyber security program;
- Providing coordination and interface with other aspects of security;
- Overseeing training activities and security awareness;
- Developing publications and bulletins on a as needed basis;
- Performing independent validations and verification; and
- Performing and maintaining CIAC and EM cyber security incidents are promptly and properly reported.

6.3 Cyber Security Program Manager (CSPM)

The CSPM must be an Office of the Under Secretary of Energy employee and be knowledgeable in cyber security.

The CSPM is responsible for;

- Ensuring the implementation of the Office of the Under Secretary of Energy Program Cyber Security Plan (PCSP);
- Serving as the primary point of contact for cyber security for EMCBC;
- Developing and reviewing (at least annually) PCSP (if applicable), and approved System Security Plans (SSP);

- Reviewing DOE Risk and Threat statements as they become available;
- Approving minimum information system configurations for sites;
- Ensuring adequate cyber security training, education, and awareness is available, that employees receive training according to policy, and that training records are maintained;
- Evaluating incident reports and ensure that designated individuals are regularly monitoring sources (such as SANS) for new vulnerabilities;
- Monitoring PCSP and SSP compliance through program reviews, budget reviews, self-assessments, management assessments, performance metrics analysis, and analysis of the results of peer reviews, vulnerability assessments, and independent oversight evaluation;
- Ensuring the development and coordination of corrective actions plans in response to issues identified by OCIO, OIG, HSS, peer reviews, and self-assessments; and,
- Evaluating system changes to determine if they are significant and require re-certification and advises the DAA in this capacity.

6.4 Information Systems Site Manager (ISSM)

The Information System Security Manager (ISSM) is considered the lead security personnel in the field sites within any Program Office. This individual is responsible for conducting testing, as well as performing all “local” responsibilities designated by the field site. The ISSM is appointed by the field site manager in conjunction with concurrence from the DAA and DAA representative. The ISSM can serve as the Certification Agent (CA) in cases where duties are operationally separate. The ISSM is also responsible for maintaining the records related to C&A packages and Plan of Action & Milestones (POA&M).

The ISSM is responsible for:

- Establishing, implementing, and monitoring the PCSP for EM and assuring that EMCBC is in compliances with DOE policies, standards, and procedures for certified and accredited systems within the EMCBC accreditation boundary;
- Evaluating security measures and plans;
- Reviewing and updating risk and threat;
- Distribution of the guidelines for system security plan mission essential resource determination;
- Coordinating development of a site self-assessment program in accordance with DOE Order 205.1A, EM PCSP and SSP;
- Coordinating self-assessment of the sites’ SSP which will be performed between DOE periodic security surveys;
- Identifying and documenting threats unique to cyber security and communicating the requirements for risk assessments to Information Systems Security Officer (ISSO) and management;
- Identifying any known hardware/software vulnerabilities and determining if the countermeasures required by DOE Order 205.1A, PCSP, and 800-53 are satisfactory to mitigate the vulnerabilities and meet the security requirements;
- Determining the adequacy of protection of cyber systems as specified in software/hardware acquisition specification;
- Ensuring all documentation is complete, and all requirements of the DOE and EM PCSP

- (if applicable) and EMCBC SSP are met before approving risk assessments;
- Reviewing and posting all DOE orders, manual and guidance to all ISSO's and users;
 - Reviewing security plans for accuracy, completeness, and compliance with PSCP security program requirements;
 - Transmitting security plans to DAA Rep for DAA approval;
 - Approving the ISSO certification Technical Instruction Document (TID) or test plan;
 - Ensuring that all ISSO develop and implement a certificated TID or test plan for each SSP for which he/she is the ISSO as required by DOE Order 205.1A and the DAA;
 - Participating in educational classes on policies and practices within one year of appointment;
 - Ensuring that information systems are monitored and periodically evaluated to prevent or detect computer security incidents including instances of waste, fraud, or abuse;
 - Notifying appropriate DAA, and DAA Rep. of computer security incidents;
 - Investigating computer security incidents to ensure that adverse impact to site operations and national security is minimized and corrective action taken to preclude recurrence;
 - Completing appropriate documentation for each computer security incident for DAA Rep. review; and
 - Ensuring technical support is available to assist site personnel with the approved clearing and sanitization of media.

6.5 Certification Agent (CA)

The Certification Agent (CA) is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system. The purpose of this assessment is to determine the extent to which controls exist, are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the system. Once the system assessment is complete, the CA provides any recommended corrective actions to reduce or eliminate vulnerabilities in the information system to the DAA.

To ensure the integrity of the certification assessment, the CA must be independent of system development and operations teams as well as those individuals responsible for correcting security deficiencies identified during the certification. The independence of the CA ensures the DAA receives the most objective information possible in order to make an informed, risk-based, accreditation decision.

6.6 Information Systems Security Officer (ISSO)

The ISSO serves as the appropriate point of contact for inquiries related to C&A processes. The ISSO is responsible for complying with the following program requirements.

- Ensures the implementation of protection measures that are documented in SSP for each information system under ISSO jurisdiction;
- Ensures that users are granted access to information systems' resources based on the least privilege principle;

- Identifies unique threats to information systems and documents threats in the System Security Plan (SSP);
- Documents any special protection requirements identified by the application owner, data owner, or data steward and ensure that these requirements are included within the protection measures implemented in the information system;
- Ensures each information system under ISSO jurisdiction is covered by a SSP;
- Maintains a copy of the SSP for each information system under ISSO jurisdiction;
- Ensures the implementation of site procedures;
- Ensures that the organization's cyber security manager is notified when an information system is no longer needed or when the changes occur that might affect the accreditation of the information system;
- Ensures that information access controls and cyber protection measures are implemented for each information system as described by its SSP;
- Ensures that users and systems administrators are properly trained in information system security by identifying cyber security training needs and the personnel who need to attend the cyber security training program;
- Conducts cyber security reviews and tests to ensure that the cyber security features and controls are functioning and effective;
- Ensures the performance of a risk assessment to determine if additional countermeasures beyond those identified in the SSP are required and whether an identified unique local threat exists;
- Communicates individual incident reports to the ISSM;
- Ensures the implementation of all applicable protection measures for each information system; and,
- Ensures that unauthorized personnel are not granted use of, or access to, the information system.

6.7 Application/Data Owner

All Application/Data Owners are responsible for complying with the following program requirements:

- Determining and declaring the classification level of the information prior to the information being processed, stored, transferred, or accessed on EMCBC information systems;
- Determining and documenting the mission essentiality of the information for which he or she is custodian and informing the ISSO;
- Providing the ISSO and System Administrator with any special security requirements for the information to be processed on information system;
- Defining appropriate data sets in order to be processed, stored, transferred, or accessed on the appropriate information system;
- Determining if disaster recovery and contingency plans are needed for information systems which they are responsible;
- Identifying and documenting unique threats to information system and reporting them to ISSO and/or ISSM;
- Advising the ISSO of any special confidentiality, integrity, or availability protection requirements for the information; and,

- Ensuring that the information is processed only on a system that is approved at a level to protect the information.

6.8 System Administrator

The System Administrator is responsible for maintaining and operating the systems and networks within an organization. Duties include day-to-day support, and are often wide-ranging. The System Administrator can expect to be charged with installing, supporting, and maintaining or other computer systems, and planning for and responding to service outages and other problems. The System Administrator typically manages user accounts including the deletion, creation, and modification of user privileges. System Administrators must ensure timely removal of access rights for all departed employees, especially in cases of employee termination. All DOE System Administrators must sign and abide by *DOE EM PCSP Appendix K, Privileged User Rules of Behavior (RoB)*.

- Ensuring authorized personnel compliance with computer security requirements;
- Ensuring that the end user has read and sign the Rules of Behavior User Agreements before access is granted;
- Ensuring that all information systems are properly patched in a timely manner;
- Ensuring that information processed is properly protected;
- Ensuring that general end user are properly trained on computer security requirements;
- Ensuring that disaster recovery and contingency plans defined by Data Owner and Line Managers for EMCBC information systems are being complied;
- Ensuring that information systems are monitored and periodically evaluated to prevent or detect computer security incidents including instances of waste, fraud, or abuse;
- Reviewing SSP and TID for compliance prior to submitting them to the ISSO;
- Report all suspicious or abnormal activities to ISSO and/or ISSM within 30 minutes of event or incident finding.

6.9 Line Managers

Line Managers are responsible for complying with the following program requirements:

- Concurring with the determination of critical resource within their organization, if they are found as mission essential, and information systems and associated networks, whether they are found as mission essential or non-mission essential;
- Notifying the system administrator and ISSO when a user should be removed from the system (i.e., in the case of termination, transfer, etc.);
- Ensuring that their employees are aware of site computer security procedures and the consequences of not adhering to those procedures;
- Ensuring that authorized personnel are appropriately screened and cleared to a level commensurate with the sensitivity of the data to be accessed or handled and the risk and magnitude of loss or harm that could be caused by the individual;
- Determining if disaster recovery and contingency plans are needed for information systems which they are responsible;
- Making, documenting, and signing a decision concerning the need for a disaster recovery and contingency plan for the systems within EMCBC accreditation boundary;

- Ensuring that disaster recovery and contingency plans are developed when applicable, and that they are reasonable and sufficient; and
- Supporting the ISSM and ISSO personnel in the investigation of computer security incidents and in the implementation of corrective actions.

6.10 Users

All information system users and owners/originators of documents and information are responsible for complying with the following program requirements:

- Obtaining classification review by their Line Manager;
- Remaining aware of and knowledgeable about their responsibilities in regard to cyber security;
- Being accountable for their actions when using government-owned computer equipment;
- Ensuring that authentication mechanisms issued for the control of their access to information systems are not shared and are protected at the highest classification level and most restrictive category of information to which they permit access;
- Reading and signing a Computer Security Code of Conduct statement before initially accessing any information system. Such a statement is included in the Rules of Behavior for EMCBC Computer Systems form;
- Ensuring all computer equipment and media assigned is properly inventoried and labeled;
- Providing protection for all media assigned is maintained at all times to at least the level commensurate with the sensitivity or classification level and category of the information stored on the media;
- Ensuring that all media is properly sanitized and destroyed when it is no longer needed;
- Complying with the computer system security requirements identified in the IP-240-01-F1 Rev. 1 User Agreement Form and Annual Cyber Security Awareness Training;
- Remaining alert for any adverse event that could have an impact the Department of Energy and EMCBC; and
- Reporting all suspected computer security incidents and taking actions to mitigate the effects of the incident by contacting your line manager, data owner and/or system administrator.

7.0 **GENERAL INFORMATION**

This policy defines the roles and responsibilities on how the core cyber security functions are to be performed for all EMCBC unclassified accreditation boundary. The implementation of stated policy is the responsibility of both federal employees, as well as associated support service contractors, and their individual understanding of and involvement in the EMCBC cyber security program is critical to its success.

8.0 **RECORDS MAINTENANCE**

8.1 Records generated as a result of implementing this policy are identified as follows:

8.1.1 IP-250-01-F1, EMCBC Procedure Change Request (Attachment A)

8.1.2 IP-250-01-F2, EMCBC Document Review Record Sheet (Attachment B)

8.1.3 IP-250-01-F3, EMCBC Record of Revision (Attachment C)

9.0 FORMS USED

9.1 DOE EM PCSP Appendix K, Privileged User Rules of Behavior (RoB)

9.2 IP-240-01-F1, Rev. 1 User Agreement Form

10.0 ATTACHMENTS

Computer Master Security Policy Statements Attached:

Attachment Number	Class	Policy	Identifier
10.1	Management	Risk Assessment	RA
10.2	Management	Security Planning	PL
10.3	Management	System and Services Acquisition	SA
10.4	Management	Certification, Accreditation, and Security Assessment	CA
10.5	Operational	Personnel Security	PS
10.6	Operational	Physical and Environmental Protection	PE
10.7	Operational	Contingency Planning	CP
10.8	Operational	Configuration Management	CM
10.9	Operational	Maintenance	MA
10.10	Operational	System and Information Integrity	SI
10.11	Operational	Media Protection	MP
10.12	Operational	Incident Response	IR
10.13	Operational	Awareness and Training	AT
10.14	Technical	Identification and Authentication	IA
10.15	Technical	Access Control	AC
10.16	Technical	Audit and Accountability	AU
10.17	Technical	System and Communications Protection	SC

ATTACHMENT 10.1

Computer Security Policy: Risk Assessment (RA) Policy

Purpose:

To ensure that cost effective mitigation strategies are applied to the environment to implement a defense posture commensurate with the risk of compromise or destruction of the information being developed, transmitted, or stored. These strategies must ensure that the missions of EMCBC are protected, not just its information assets.

Security controls will be assessed for effectiveness and applicability to the EMCBC environment and will be placed at the most critical or beneficial points. Controls shall be selected to cost effectively maximize the reduction in risk. Risk assessment is a continuous process, incorporating both a formal risk analysis and ongoing reassessment. The methods outlined in NIST SP 800-30 will be used for risk analysis. Mitigation strategies will be based on the degree of risk as well as the cost-effectiveness of the strategy and implemented through a POA&M to correct / reduce the vulnerabilities identified.

Scope:

This policy covers all information systems within the EMCBC environment, including General Support Systems, Major Applications, and Minor Applications. All EMCBC information systems must undergo a formal risk assessment process as part of Certification and Accreditation.

Roles and Responsibilities:

Role	Responsibilities
DAA, DAA Rep.	<ul style="list-style-type: none"> • Ensuring that all systems are reviewed and provided the appropriate DOE policies, orders and guidance to ensure they have security controls that are cost effective and sufficient to protect the information and information system based upon the operational risks • Reviewing and approving all FIPS 199 sensitivity classifications for all EMCBC accreditation boundary systems or enclaves.

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> • Development and implementation of risk assessment procedures, to include ensuring they are: <ul style="list-style-type: none"> ○ Documented; ○ Disseminated to appropriate persons within the organization; ○ Reviewed by responsible parties at least annually; and ○ Updated to maintain an accurate description of system operations. • Reviewing and approving the POA&M
ISSO	<ul style="list-style-type: none"> • Reviewing all risk assessments to ensure the risk mitigation strategies selected are appropriate and that the system owners have developed and maintain an appropriate set of documentation
System Administrator, Application/Data Owners, Line Managers	<ul style="list-style-type: none"> • Implementation of this policy, including the preparation and timely maintenance of all required documentation; • Reviewing risk assessments annually or if a major change to the environment occurs; and • that risks with an unacceptable level of mitigation are identified • Ensuring for further security controls and that these are included and tracked to resolution in the POA&M

Compliance

This Risk Assessment Control policy will be implemented through the preparation of an EMCBC Risk Assessment Policy and supported by documented procedures. Procedures shall:

- Be reviewed annually and updated to address any new risk factors,
- Be consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance,
- Include categorization of the information system and the information being processed, stored, or transmitted by the system in accordance with FIPS 199; and document the results (including supporting rationale) in the system security plan.
- Address assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the laboratory.
- Ensure that risk assessments are updated annually or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.
- Establish for vulnerability assessment techniques on a recurring basis to detect new vulnerabilities in the information system.

ATTACHMENT 10.2

Computer Security Policy: Security Planning (PL) Policy

Purpose:

The security planning policy provides guidance for developing the documentation for an information or information system as required by the Federal Information Systems Management Act (FISMA) and NIST. The system security plan provides the basis by which the DAA will assess the security controls and make a decision on the operational status that should be granted.

Scope:

This policy covers the processes and procedures that will be used by [ACRO] to develop, maintain, and update each Computer Security Program Plan (CSPP). The CSPP is the DOE equivalent of what NIST refers to as a system security plan. In general, the content of all SSP's will be constructed in accordance with the DOE Office of Environmental Management Program Cyber Security Plan (PCSP).

This policy describes the process for developing a SSP. Once the SSP has been developed it must be tested to validate that the security controls designated in the PCSP are operational and functioning as planned. Once that testing has been accomplished the entire package will be compiled and presented to the DAA who will make an operational decision for the system or enclave.

This policy prescribes review and update processes for the SSP when a significant change has occurred or when other operational requirements may dictate the need for reviewing the system/enclave's operational status. In addition, all EMCBC SSP's will be reviewed at least annually to ensure the protection of all computing resources that correspond to EMCBC accreditation boundary.

Roles and Responsibilities:

Role	Responsibilities
DAA	<ul style="list-style-type: none"> • Review and approval of the operational status of the cyber systems in EMCBC accreditation boundary. • Making appropriate changes to the operational status based upon the risk factors associated with continued operations whenever there is a change to the security status of the system.
DAA Rep.	<ul style="list-style-type: none"> • Approval of the SSPs and providing the DAA with an operational recommendation for the accreditation boundary.

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> • Review of each SSP for completeness and accuracy. • Providing the DAA Rep. with a recommendation relating to approval of the SSP created by the Application/Data Owner. • Independently assessing the implementation of security controls for all systems/enclaves to provide assurance that the systems are being operated as documented. • Developing a standard “Rules of Behavior User Agreement” document and ensure that all personnel have read and understand their responsibility concerning the rules of behavior. • Determining if any systems collect information that necessitates the completion of a privacy impact assessment (PIA). If any systems collect this information the PIA will be conducted and included with the SSP.
ISSO	<ul style="list-style-type: none"> • Working with the system administrator, application/data owner and line managers in developing their system/enclave security plan. • Developing, documenting and implementing the SSP for their systems. • Reviewing the plan and documenting weaknesses. • Monitoring the operations of systems/enclaves to verify they are being operated in accordance with their SSP.
System Administrator, Application/Data Owners, Line Managers	<ul style="list-style-type: none"> • Reporting any configuration change in operational status or implementation in security controls that may modify the risk factors for the system. • Reporting any time a significant change is made to the operational status of the system.

Compliance:

This Security Planning Policy will be implemented through a formal EMCBC procedures document and supported by detailed documented procedures. Documentation will include:

- Development and maintenance of a SSP document in accordance with the DOE EM PCSP.
- Development of procedures that define a significant change and the activities required when such a change is planned.
- Documentation of procedures for review and processing of a SSP to obtain approval and the appropriate authority to operate from the DAA.
- Development of procedures for validating the implementation of security controls. This validation can include a variety of techniques, how the examiner verifies the control is operational (the artifact(s) that should be available) and the documentation needed to validate the control.

- Development of guidance for the use and operation of systems within the EMCBC accreditation boundary. This document (Rule of Behavior User Agreement) shall be distributed to all users and users shall acknowledge that they have read, understand, and will follow the requirements.
- Identifying data that requires the preparation of a Privacy Impact Assessment and preparation of a PIA if required.

ATTACHMENT 10.3

Computer Security Policy: System and Services Acquisition (SA) Policy

Purpose:

EMCBC will obtain systems and services that fully comply with public law and DOE’s guidance. Systems and service acquisition will be based on a life-cycle total cost of ownership model that is subject to Capital Planning and Investment Control (CPIC) review.

Scope:

IRM develops, disseminates and periodically reviews and updates formal documentation of system and services acquisition policy that addresses the purpose, scope, roles, responsibilities, and compliance to new standards. This policy applies to all acquisitions of information systems and services by EMCBC under the auspices of the IRM policies.

Roles and Responsibilities:

Role	Responsibilities
DAA Rep.	Development, dissemination, and periodic review and update of a formal, documented, system and services acquisition policy in compliance with IRM policy.
ISSM	Development and maintenance of an overall acquisition policy

Compliance:

This System and Services Acquisition Policy will be implemented through the preparation of System and Services Acquisition procedures. These procedures shall be:

- Reviewed annually and updated to address any new risk factors.
- Consistent with EMCBC’s missions, functions, directives, policies, regulations, standards, and guidance.
- Consistent with DOE capital planning and investment control processes for adequately and cost effectively protecting the information and information system.
- Consistent with a structured information systems development life cycle methodology that includes computer security considerations.
- Consistent with the assessment of risk. System procurements shall include devices or software necessary to ensure that the device will meet EMCBC security control specifications.
- Completed to ensure that EMCBC complies with all software usage restrictions.

System owners shall develop procedures that:

- Enforce explicit rules governing the downloading and installation of software by users.
- Ensure that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The system owner and third party organization shall monitor security control compliance.
- Ensure that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.

ATTACHMENT 10.4**Computer Security Policy: Certification, Accreditation and Security Assessment (CA) Policy****Purpose:**

The certification and accreditation (C&A) process certifies that EMCBC's information systems meet documented security requirements and will continue to maintain them throughout the system's life cycle. The C&A process ensures that every system encompasses a minimum level of security is appropriated to the information that is being stored, processed or transmitted within the C&A accreditation boundary. These common protection requirements create a common baseline for security in all EMCBC systems for each specific type. Accreditation provides EMCBC with the authority to operate (ATO) their information systems in the manner described by the CSPP.

Scope:

All EMCBC information systems must undergo a Certification and Accreditation process prior to initial operation. Reauthorization is required every three years or when a major change is made to the systems. EMCBC uses an accreditation boundary (a.k.a Enclave) for certification and accreditation.

EMCBC applies NIST guidance to determine the category of risk of all computing assets in accordance with FIPS 199. Those with the same category of risk are grouped together into an accreditation boundary henceforth called enclaves. A description of the enclaves is located in the SSP. Recommended management, operational, and technical controls are applied to provide the level of security required for the information and computer resources as determined by the risk categorization. An independent group will audit these controls to determine if they provide appropriate protection and that their state of application provides the necessary protection across the enclave. Enclaves with controls applied and working should be granted an authority to operate (ATO) by the designated approving authority (DAA).

Roles and Responsibilities:

Role	Responsibilities
DAA Rep.	<ul style="list-style-type: none"> • Ensuring that all systems are reviewed and provided appropriate guidance to ensure they have security controls that are cost effective and sufficient to protect the information and information system based upon their purpose and the operational risks
ISSM	<ul style="list-style-type: none"> • Defining security assessment, certification, and accreditation procedures that are: <ul style="list-style-type: none"> ○ Documented; ○ Disseminated to appropriate elements within the organization, including the DAA & DAA Rep.;

	<ul style="list-style-type: none"> ○ Reviewed by responsible parties at least annually; and ○ Updated in a timely manner to maintain an accurate description of system operations ● Ensuring that all systems are maintained and operated in accordance with their authority to operate ● Review and approval of the Computer Security POA&M
ISSO	<ul style="list-style-type: none"> ● Ensuring that the controls selected are appropriate ● Ensuring that system owners have developed and maintain an appropriate set of C&A documentation.
System Administrator, Application/Data Owners, Line Managers	<ul style="list-style-type: none"> ● Implementation of this policy, including the preparation and timely maintenance of all required documentation. ● Ensuring the system is operated within the approval to operate provided by the DAA. ● Ensuring all identified deficiencies are included and tracked to resolution in the POA&M.

Compliance:

The security assessment shall address:

- Purpose, scope, roles, responsibilities, and compliance for security assessment, certification, and accreditation activities.
- Procedures are sufficient to address all areas identified in:
 - Federal law and applicable NIST publications;
 - DOE Order 205.1A;
 - The EM PCSP and SSP;
 - Certification and accreditation policy; and
 - All associated security assessments.
- Procedures to ensure that policies and procedures are updated periodically, especially when organizational reviews indicate updates are required.
- Processes for an assessment of the system's security controls are conducted at least annually.
- Development of security assessment reports to document the system's security controls to ensure they are implemented properly, operating as intended, and providing the appropriate protection to meet the security requirements and all policies and procedures.
- Procedures for system administrator, application/data owners, and line managers to ensure their activities are consistent with EMCBC's security assessment procedures.
- Maintenance of records or documents to demonstrate: (i) security assessments are being consistently conducted on the information system on an ongoing basis; and (ii) if anomalies or problems encountered during security assessments are being documented and the resulting information used to actively improve security assessment policy, procedures, and processes on a continuous basis.

The security certification shall ensure that:

- A certification process is defined that determines the completeness and effectiveness of each security control. This process shall validate that the security control is implemented properly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Procedures are consistent with NIST FIPS 199, FIPS 200, Special Publications (SP) 800-60, 800-53, 800-30, 800-37, 800-53A and other publications as deemed appropriate by the system owner.
- Development of security certification documentation to include a threat and risk analysis, system security plan (SSP), Independent Verification and Validation (IV&V) results, current Plan of Action and Milestones (POA&M) and system/enclave certification letter.

Plan of Action and Milestones (POA&M) shall:

- Verify that EMCBC develops and updates an action plan for the information system which identifies and tracks to completion shortfalls within the security controls.
- Identify deficiencies noted during any assessment or audit of the security controls. All discrepancies shall be identified and tracked using EMCBC's POA&M process. For each deficiency develop a corresponding plan of action to document EMCBC's plan to correct noted deficiencies and to reduce or eliminate known vulnerabilities in the system.
- Report quarterly to the DAA, DAA Rep. and CSPM by ISSM on progress in completing activities to correct each shortfall.

Accreditation procedures shall address:

- The DAA's process for accrediting each accreditation boundary and providing a written authority to operate in accordance with NIST SP 800-37. The DAA may authorize operations of a system or enclave up to 3 years based upon the level of risk and the operational status of security controls.
- Process for the DAA to revoke the authority to operate for an accreditation boundary based upon changes in risk or actions that may place the information or information system in jeopardy.

Continuous Monitoring shall include:

- Verification that the security controls are being monitored according to defined procedures on an ongoing basis.
- Security control monitoring procedures are consistent with NIST Special Publication 800-37.

- Maintenance of records to determine: (i) that designated security controls are assessed;

(ii) changes to or deficiencies in the operation of the security controls are analyzed for impact, documented, and reported; and (iii) adjustments are made to the information system security plan and plan of action and milestones, as appropriate.
- Verification that EMCBC personnel with security control monitoring responsibilities understand their roles and responsibilities and conduct operations within those guidelines.
- Reporting procedures to the DAA for any deficiency or shortfall that could reasonably be expected to impact the authority to operate or that substantially increases the risk associated with continued operations.

ATTACHMENT 10.5

Computer Security Policy: Personnel Security (PS) Policy

EMCBC will develop, disseminate, and periodically review and update a formal, documented, personnel security policy that addresses the purpose, scope, roles, responsibilities, and compliance with the policies and requirements of OMB, DOE, and the EM PCSP. EMCBC will ensure that Assistant Director of Information Resource Management (IRM) has formal, documented procedures to facilitate the hiring, management and termination of personnel as well as screening for all EMCBC personnel to implement the required defense-in-depth.

Scope:

This policy applies to all EMCBC employees as well as contractors with access to EMCBC computing resources are required to comply with this policy in accordance with the Rules of Behavior for EMCBC Computer Systems as well as HR policies . This policy covers hiring, screening, termination, transfer, and punishment of persons with access to EMCBC computing resources (as far as their actions or the actions of this policy impact on information and information systems). This policy is not intended to replace other EMCBC, DOE, or IRM personnel policies.

Roles and Responsibilities:

Role	Responsibilities
Site Manager	<ul style="list-style-type: none"> • Implementation of EMCBC Personnel policies to comply with this policy as well as Federal laws, directives and guidelines for personnel security.
Assistant Director, IRM	<ul style="list-style-type: none"> • Ensure that personnel positions with site administration access are identified and that appropriate pre-screening is required as a condition of employment. • Ensure that personnel positions with elevated system access to PII are identified and that appropriate pre-screening is required as a condition of employment. • Establishment of procedures for appropriate disposition of system access rights in conjunction with personnel transfer or termination policies.
Director, Human Resources	<ul style="list-style-type: none"> • Establishment of procedures for termination and transfer of personnel, to include notification of EMCBC for appropriate disposition of information system accounts. • Establishment of sanction procedures for personnel failing to comply with policies or procedures, in accordance with EMCBC's IRM and DOE policy
Line Managers	<ul style="list-style-type: none"> • Identify positions with site administration access or elevated system access to PII and assign a level of risk to that position description. • Review of risk designations in conjunction with annual performance reviews. • Screening of individuals in accordance with IRM policy.

Compliance:

This Personnel Security Control policy will be implemented through the preparation of and supported by documented procedures. The procedures shall be:

- Reviewed periodically (at least annually) and updated to address any new risk factors,
- Consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance,
- Created to address assigning a risk designation to all positions and establishes screening criteria for individuals filling those positions. EMCBC will review each position's risk designation annually in conjunction with annual performance reviews.
- Established to address individuals requiring screening prior to access to EMCBC information and information systems.
- Created to cover termination and transfer procedures that include appropriate disposition of information system access rights, and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.

ATTACHMENT 10.6

Computer Security Policy: Physical and Environmental Protection (PE) Policy

Purpose:

EMCBC will provide a safe and productive environment for personnel working on the EMCBC sites. Physical access to the information and information systems will negate many of the security controls that are being implemented. For this reason it is very important that the information and information system processing areas be properly protected. This policy puts for the requirements for protecting EMCBC’s information and information systems from physical and environmental threats.

Scope:

Physical access to the EMCBC sites is open to proper personnel. Access to individual sites are handled through Site Safeguards and Security and their functions are not included in this policy. This policy is focused on physical access to the data center and other areas that contain network infrastructure devices (e.g., routers, switches) information technology networking devices. The policy also covers the environmental controls, e.g. fire, water, heat, humidity, etc. that are necessary for the safe operation of these areas.

For some aspects of this policy the IRM relies upon the site security forces for completion of those functions. In those cases, IT responsibility is limited to the transfer of that responsibility and to validating the function is being completed appropriately to ensure the protection of the information and information systems.

Roles and Responsibilities:

Role	Responsibilities
Compliance & Project Support, Office of Logistics	<ul style="list-style-type: none"> • Identification of site security requirements for all functions required of the facility Safeguards and Security department functions
ISSO, System Administrators	<ul style="list-style-type: none"> • Annual review of security agreements and controls to ensure they effectively protect the information and information systems; • Development of procedures, in concert with the Safeguards and Security personnel, to limit access to protected areas to only authorized personnel; • Monitoring access to the controlled areas and ensure the procedures are being followed; • Monitoring the environmental controls to ensure they are operational and functioning as necessary

Role	Responsibilities
Application/Data Owners, Line Managers	<ul style="list-style-type: none"> • Identifying any system environmental or security requirements that may be unique to their systems and provide the requirements to the appropriate personnel for review.

Compliance:

This Physical and Environmental Protection Control policy will be implemented through a formal EMCBC procedures document and supported by detailed documented procedures. Documentation will include:

- The identification of all areas needing access control and coordinating a cost effective controls procedure for each area to ensure only authorized personnel have access.
- Developing and maintaining lists of personnel with authorized access to the data center or any otherwise designated limited access facility containing information systems.
- Designating the access approval process and the documentation or device (e.g., badges, identification cards, and smart cards) required to gain access.
- Designating officials within the organization who review and approve the access list and authorization credentials at least annually.
- Controlling all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities.
- Controlling physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
- Maintaining a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes:
 - Name and organization of the person visiting;
 - Signature of the visitor;
 - Citizenship;
 - Form of identification;
 - Escort;
 - Date of access;
 - Time of entry and departure;
 - Purpose of visit; and
 - Name and organization of person visited.
- Developing procedures to monitor physical access to information systems.
- Documenting the processes for shutting down the systems including
 - A controlled shutdown based upon any function that could potentially damage the device if it was allowed to continue to operate;

- An emergency shutdown (e.g. fire in a data center); and
 - A shutdown when systems have been transitioned to the UPS when local power is no longer available.
- Documenting the procedures in the event of a fire in areas occupied by IT. This includes data centers, telecommunication closets and any other area that contains information systems resources.
- Documenting the procedures for monitoring temperature and humidity in the data centers, including notification to service providers.
- Documenting procedures for monitoring for water leaks or other disruptions that would negatively impact the operations of the systems and devices in the data centers.
- Documenting the processes and procedures that will be followed during the receipt, transfer, or removal of any system or device from the data center. This procedure should include the verification of information contained on the information system and the potential that the computer storage media may require removal, sanitization, or destruction.

ATTACHMENT 10.7**Computer Security Policy: Contingency Planning (CP) Policy****Purpose:**

Contingency planning is focused on identifying and categorizing information and information systems to ensure they are appropriately protected. This policy has been developed to ensure that contingency plans appropriate to the risk and potential damage are developed and tested for each enclave/system.

Scope:

This policy covers all systems/enclaves identified in the EMCBC SSP. A contingency plan will be documented to include the necessary recovery timeframes and the primary methods that will be used to recover operations for each system. A test or verification process should be included with each plan to verify that the plan is realistic and that it can be executed.

Most of the business functions performed at EMCBC use commercially available computing resources and are all completed on commercial systems. While EMCBC has no servers or systems that meet the criteria for a Continuity of Operations Plan (COOP), EMCBC does have contingency plans in place to backup, replace, and recover systems.

Roles and Responsibilities:

Role	Responsibilities
ISSO	<ul style="list-style-type: none"> Validating the contingency plan has been developed and testing is accomplished
System Administrators, Application/Data Owners, Line Managers	<ul style="list-style-type: none"> Developing a contingency plan for their systems Review, approval, and test the contingency plan at least annually to ensure that it cost effectively protects the information and information system

Compliance:

Contingency plans will be maintained for all EMCBC information systems within an accreditation boundary.

- The Contingency Plan will be coordinated as applicable with other organizations, such as IRM to ensure inclusiveness of other related plans as required (e.g., emergency services, natural disasters, business systems recovery plans, etc.),
- Contingency Planning training will be conducted at least annually for personnel in their roles and responsibilities with respect to the EMCBC information systems.

- The plan will be tested at least annually. Actual exercise of the plan (such as a major power loss) may be substituted for an annual test, provided it is documented as such. Table top exercises may not be used as a test more than once every two years.
- IRM shall ensure alternate storage sites are maintained and lists of personnel authorized to deliver or pickup tapes is current.

ATTACHMENT 10.8**Computer Security Policy: Configuration Management (CM) Policy****Purpose:**

A configuration management program is designed to ensure that system components are installed and maintained using standards that maximize the protection for all components of the network. The purpose of this policy is to establish a baseline policy that will define the minimum application of security controls that will be used for each element type. In addition, this policy establishes guidance for devices that either will not or can not conform to EMCBC baseline configuration management baselines.

Scope:

This policy is applicable to all devices that are part of, or connect to the EMCBC accreditation boundary. Configuration guidelines for devices may vary between enclaves; however, any device in the EMCBC accreditation boundary must conform to EMCBC IRM's Technical Instruction Documents (TID) configuration management guidelines. Use of personal computer equipment or electronic devices in EMCBC accreditation boundary is strictly forbidden, unless it is approved by Assistant Director, IRM and EMCBC configuration management team.

Roles and Responsibilities:

Role	Responsibilities
ISSO	<ul style="list-style-type: none"> • Validation of configuration baselines for each type of device • Review of scans and other available information to ensure that configuration guidelines are being maintained on the network • Mediation of any request for exemption from the configuration guidelines
System Administrators	<ul style="list-style-type: none"> • Development of procedures to ensure each device on the network is configured, maintained and operated within EMCBC configuration guidelines • Removal of any system that fails to conform with the guidelines • Deployment and support of their systems with the appropriate configurations
Users	<ul style="list-style-type: none"> • Ensuring they do not remove, modify or otherwise tamper with system configurations or remove security settings

Compliance:

Assistant Director, IRM shall:

- Develop and maintain an inventory of device types, operating systems and other critical elements necessary for defining configuration standards.
- Develop an approved configuration baseline for each device, operating system or other element to ensure each device is operating in a manner to protect the information and information systems.
- Develop procedures for ensuring each device has the baseline configuration standards implemented.
- Develop processes to rapidly identify when a system configuration has been changed and to return that system to the approved baseline configuration.
- Develop procedures for systems owned by EMCBC to be used on the EMCBC accreditation boundary. These procedures shall include ensuring that the systems are maintained and operated in a manner consistent with EMCBC policies and to ensure that they present no additional threat to the environment.
- Work with the system administrator and application/data owners to identify any system that increases the risk to the EMCBC accreditation boundary to remediate the deficiency. This authority includes the immediate removal of any system that may be conducting activities in violation of EMCBC policy, e.g. scanning or other nefarious activity.
- Conduct scans to validate and verify device configurations. Provide an automated function to return devices found to have configuration modifications to the approved setting.

ATTACHMENT 10.9

Computer Security Policy: Maintenance (MA) Policy

Purpose:

The maintenance program is established to provide a standard based system for the long term support of all devices connected to the EMCBC accreditation boundary. By providing appropriate maintenance the long term reliable operations of each device can be ensured. In addition, by following the maintenance polices the security configuration of the device will be maintained.

Scope:

The maintenance policy is applicable to all EMCBC owned devices that connect to the accreditation boundary. In addition, the policy applies to devices that support the operations of IRM. Most of these devices are under the control the Office of Logistics Management at EMCBC, however, responsibilities to ensure that these services are appropriate to the continued operation of the IRM functions do exist.

The maintenance policy also includes contracts for software and software related functions at EMCBC. Contracts for all maintenance functions are included in this policy.

Roles and Responsibilities:

Role	Responsibilities
Assistant Director, IRM	<ul style="list-style-type: none"> • Review of maintenance contracts to ensure EMCBC computer security policies are incorporated within the contract terms and conditions
System Administrators	<ul style="list-style-type: none"> • Development of procedures that maintain the security controls structure while allowing maintenance personnel required access; • Monitoring of maintenance activities with respect to computer security principles; • Tracking the use of maintenance contract personnel and their access to site devices; • Using appropriate processes to maintain the security controls for all devices during maintenance.

Compliance:

This system maintenance policy will be implemented through a formal EMCBC Procedures Document and supported by documented procedures. Procedures will:

- Be developed, disseminated, and periodically reviewed/updated to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
- Schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.
- Approve, control, and monitor remote and locally executed maintenance and diagnostic activities.
- Maintain a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.
- Ensure the organization maintains a maintenance log for the information system that includes: (I) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) citizenship; (iv) name of escort, if necessary; (v) a description of the maintenance performed; and (vi) a list of equipment removed or replaced (including identification numbers, if applicable).

ATTACHMENT 10.10

Computer Security Policy: System and Information Integrity (SI) Policy

Purpose:

EMCBC will provide a safe and secure computing environment that is free from viruses, spam, and spy ware to the maximum extent possible. Assistant Director IRM ensures that software patches and upgrades are applied promptly consistent with level of risk and local mission requirements and that anti-virus and malicious code threats are blocked to the maximum extent possible.

Scope:

This policy covers all devices connected to the EMCBC accreditation boundary, whether directly or remotely, including devices connected internally and those connected to the Visitor enclave. This policy covers the areas of patching, anti-virus, spy ware, malicious code, and vulnerability scanning and assessments.

Roles and Responsibilities:

Role	Responsibilities
Assistant Director, IRM	<ul style="list-style-type: none"> • Development and implementation of the System and Information Integrity procedures.
ISSM	<ul style="list-style-type: none"> • Monitoring the internet security environment through subscriptions to mailing lists and security forums to ensure that new threats are identified and countermeasures implemented as quickly as possible • Implementation of processes and techniques for intrusion detection and monitoring of critical network segments and servers • Scanning for common vulnerabilities and patch levels on all accessible systems at least once per week.
ISSO, System Administrators	<ul style="list-style-type: none"> • Ensuring all government-owned systems have anti-virus or anti-spy ware installed as part of the baseline configuration as prescribed in EMCBC Rim's TID. • Providing anti-virus updates to users at least once per week • Implement spam filtering on email servers • Ensuring all anti-virus software is updated regularly, not less than once per week • Implementation and administration of patching and update procedures and ensuring systems have appropriate patches and updates applied. • Identify and correct information system flaw and share information with ISSM.
Users	<ul style="list-style-type: none"> • Ensuring that all anti-virus software is updated regularly, not less than once per week • Ensuring all systems have appropriate patches applied

Compliance:

This System and Information Integrity Control policy will be implemented through the preparation of and supported by documented procedures. The procedures shall:

- Be reviewed periodically (at least annually) and updated to address any new risk factors.
- Be consistent with EMCBC missions, functions, directives, policies, regulations, standards, and guidance.
- Address monitoring of connected systems for compliance to include installation and updating of anti-virus software and application of critical patches.

IRM shall

- Implement malicious code protection that includes a capability for automatic updates.
- Receive and review information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.
- Employ tools and techniques to monitor events on information systems, detect attacks, and provide identification of unauthorized use of the systems.

ATTACHMENT 10.11

Computer Security Policy: Media Protection (MP) Policy

Purpose:

EMCBC will enforce activities to safeguard physical media and the information on that media from unauthorized disclosure.

Scope:

This policy applies to the transfer, disposal, or any other activity that may result in the unauthorized release of information. This policy applies to all information produced, stored, processed, or otherwise contained within any device that connects to the EMCBC accreditation boundary. This policy also covers printed matter that is generated from information contained or processed on an EMCBC information system.

This includes personally identifiable information (PII) and other information that the information owner deems as needing additional controls. This policy covers those systems and ensures that the media is appropriately protected when transferred or removed.

Roles and Responsibilities:

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> • Reviewing media protection procedures to validate that they appropriately protect EMCBC information • Developing procedures for the sanitization or destruction of computer storage devices to ensure the protection of all EMCBC information types • Monitoring the procedures to ensure they are being applied appropriately
Application/Data System Owners, Line Managers	<ul style="list-style-type: none"> • Identifying the type of information stored on each system
System Administrators	<ul style="list-style-type: none"> • Following EMCBC policy when transferring or accessing any system or device and validate the device has been properly sanitized

Compliance:

This Media Protection Control policy will be implemented through a formal EMCBC Procedures Document and be supported by documented procedures. Documentation will include:

- Ensuring unauthorized users do not have access to information in printed form or on digital media removed from information systems.

- A formal statement that EMCBC follows the DOE sanitization standard (DOE 471.2.1C and CS-11) and its *Material Control Policy* and procedures concerning the destruction of media.
- A process that sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media. (note: physical destruction is preferred for any device leaving EMCBC)
- Requiring external labels on removable computer storage media and information system output indicating the distribution limitations and handling caveats of the information, based on a risk assessment of the information.
- Requiring physical controls and secure storage of information system media based on the highest FIPS 199 security category of the information recorded on the media.
- Requiring controls for information system media that restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.
- Requiring sanitization of information system digital media using approved equipment, techniques, and procedures.

ATTACHMENT 10.12

Computer Security Policy: Incident Response (IR) Policy

Purpose:

Incident response controls provide those security controls that protect EMCBC's information and information systems by properly responding to security incidents. This policy defines the roles and responsibilities for individuals and organizations that may be involved in an incident. This policy also provides direction for assessing and reporting on that incident to allow others to rapidly identify and correct a similar incident.

Scope:

This policy covers all EMCBC information and information systems. This includes all networks and devices that may connect to the EMCBC accreditation boundary. EMCBC has the responsibility to put in place policies and procedures that include identifying, controlling, eliminating, investigating, and reporting on all computer security related incidents.

Roles and Responsibilities:

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> • Review of incident reports to validate their completeness and assess the need for updates to policies or procedures • Forwarding of incident reports in accordance with EM PCSP • Development of an incident response program and identify an incident response team in writing
ISSO	<ul style="list-style-type: none"> • Validation that vulnerabilities identified as part of an incident have been removed or mitigated
System Administrators and Users	<ul style="list-style-type: none"> • Identifying potential incidents and reporting incidents to the computer security group.
Incident Response Team	<ul style="list-style-type: none"> • Maintaining expertise to handle all types of information security incidents • Identifying, correcting, tracking and documenting the incident. • Supporting application/data owners and system administrators in recovering from the incident. • Tracking the incident through to conclusion and completing the applicable reports

Compliance:

This Incident Response Control policy will be implemented through a formal EMCBC Procedures Document/Manual. The incident response procedures shall:

- Validate that EMCBC follows DOE Manual 205.1A and EM PCSP.
- Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, recovery, and follow-up.
- Define the steps to be taken, and by whom, when a computer attack poses a major threat.
- Document training requirements for personnel in their incident response roles and responsibilities. This shall include annual refresher training.
- Define incident response testing and exercises, and document those used to determine incident response program effectiveness.
- Track and document computer security incidents on an ongoing basis.
- Employ mechanisms to increase the availability of incident response information and support.

ATTACHMENT 10.13

Computer Security Policy: Security Awareness and Training (AT) Policy

Purpose:

To ensure that personnel receive information and skills appropriate to their system access rights (e.g. users, administrators, domain administrators, and computer security professionals) to properly use and protect the information and information systems which they have access and that all personnel are aware of their responsibilities under *EMCBC's Computer Security policies and procedures*.

Scope:

This policy is applicable to all users granted access to EMCBC resources, whether directly or remotely. All users must undergo basic security awareness training prior to being granted access to EMCBC information systems resources. At a minimum, basic awareness training must incorporate acceptable use of resources, basic security procedures (such as password choice), and incident reporting procedures.

Roles and Responsibilities:

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> • Development and implementation of the EMCBC Computer Security Training Program • Ensuring training material is current, relevant and appropriate to the EMCBC personnel
Director, Human Resources	<ul style="list-style-type: none"> • Ensuring new employees take the Computer Security Awareness Training when first logging EMCBC network.
ISSO, System Owners, Line Managers	<ul style="list-style-type: none"> • Ensuring personnel compliance with policy
Users	<ul style="list-style-type: none"> • Completion of required computer security training, including both basic and refresher training

Compliance:

As a minimum, training requirements shall:

- Be reviewed at least annually and updated to address any new risk factors.
- Be consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance.
- Ensure all users (including managers and senior staff) are exposed to basic information system security awareness before they are allowed access to the system.

- Provide refresher training for all personnel at least annually.
- Include identification of personnel with elevated system privileges and responsibilities, document those privileges and responsibilities, and provide appropriate information system security training before authorizing access to the system and at least annually thereafter.
- Include documentation and monitoring of individual information system security training activities, including basic security awareness training and specific information system security training, to ensure compliance with this policy.

ATTACHMENT 10.14

Computer Security Policy: Identification and Authentication (IA) Policy

Purpose:

To implement an identification and authentication process such that all users of EMCBC Information systems are appropriately identified and authenticated. Authentication services verify an individual's authorization to receive information or validate the authenticity of a transmission. This policy will establish authentication services that appropriately protect the information and information systems within each enclave.

Scope:

This policy applies to all personnel that use EMCBC information or information systems resources. This policy applies to any device that connects to the EMCBC accreditation boundary.

Roles and Responsibilities:

Role	Responsibilities
ISSM	<ul style="list-style-type: none"> Review of the identification and authentication processes at least annually to determine that the policy effectively protects EMCBC's information and information systems
ISSO	<ul style="list-style-type: none"> Development of procedures to effectively implement the identification and authentication policy Routine monitoring of identification and authentication procedures to validate that all devices and individuals usage is monitored in accordance with this policy
Application/Data Owners	<ul style="list-style-type: none"> Implementation of identification and authentication processes
System Administrators	<ul style="list-style-type: none"> Implementation and support of all identification and authentication processes for their systems Reporting any attempt to bypass or circumvent identification and authentication processes to the ISSO and/or ISSM.
Users	<ul style="list-style-type: none"> Compliance with authentication and identification procedures

Compliance:

This identification and authentication policy will be implemented through an *EMCBC Procedures Document/Manual* defining full compliance. This procedure will include requirements addressing every user of an EMCBC information system. The procedures shall be:

- Reviewed at least annually and updated to address any new risk factors.
- Consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance.
- Inclusive of all users of the EMCBC network and services and define the identification and authentication processes for each class of user or administrator based upon risk to EMCBC's information resources.
- Designed and established to ensure that individuals are accountable for their actions and that anyone abusing the services can be rapidly identified and isolated. Group and shared credentials are not encouraged. Anyone abusing this policy shall have their credentials removed immediately and be forwarded for administrative action.
- Developed to reasonably allow personnel access to services based upon their need and the risk they present to EMCBC.
- Established to ensure all personnel understand their responsibilities and limitations and require a signature, including electronic signatures, to these limitations.
- Established to limit the ability of users to continually attempt to access a system. This includes locking systems after a limited number of unsuccessful login attempts or continuous monitoring or alerts when these types of activities are attempted.
- Developed to ensure that approved protocols do not allow the use of reusable passwords or credentials be transmitted in the clear.

ATTACHMENT 10.15

Computer Security Policy: Access Control (AC) Policy

Purpose:

The purpose of the access control policy is to ensure that access to systems is provided only to authorized users and devices. Access controls provide those security controls that protect the EMCBC information systems by properly authenticating the user/device before providing access to the information or information system.

This policy defines the procedures that are required to support access control. This includes the requirement for validation of the access requirement, completion of security awareness training, agreement to work within EMCBC policy, and validation of the individual's identity when credentials are issued.

Application/data owners as well as system administrators are responsible for establishing procedures for granting, maintaining, and removing access from information systems, applications, and resources.

Scope:

The DOE and EMCBC provide staff with the computing resources needed to support official government business. Access to EMCBC resources is a privilege granted based upon the needs of DOE, EMCBC, and the user. Each person with authorized access to EMCBC computing resources must agree to comply with all applicable policies and regulations.

This policy includes access for foreign nationals which is granted in accordance with EMCBC's procedures that follow the DOE Notice 205.2, Foreign National Access to DOE Computer Systems. Specific requirements are outlined in the EM PCSP.

This policy includes all users requiring access to EMCBC's information systems inclusive of whether functions are performed locally or through remote access.

Roles and Responsibilities:

Role	Responsibilities
Assistant Director, IRM	<ul style="list-style-type: none"> • Implementation and oversight of Access Control Policy
ISSO	<ul style="list-style-type: none"> • Verification and validation that only approved individuals have access to EMCBC information and information systems
System Administrators, Line Managers	<ul style="list-style-type: none"> • Establishment and maintenance of procedures for access control of users and systems,

Application/ Data Owners, Line Managers	<ul style="list-style-type: none"> Ensuring only personnel with a valid requirement are provided access, access is removed when the need no longer exists, and any violation of access is immediately reported to the ISSO.
Users	<ul style="list-style-type: none"> Completion of required actions and complying with EMCBC access control policies

Compliance:

This Access Control policy will be implemented through a [ACRO] Procedures Document/Manual defining full compliance. Procedures shall:

- Be reviewed at least annually and updated to address any new risk factors.
- Be consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance.
- Be developed to ensure personnel are assigned, and given both the responsibility and authority, to ensure that access is granted on a need basis and when that need no longer exists the access is removed.
- Be consistent with the needs of the application/data system owner, user, and EMCBC. These procedures shall be consistent with the level of risk that has been accepted by the DAA in C&A process.
- Include periodic review of access control lists and the removal or suspension of accounts that are no longer required for near term access.
- Train all authorized EMCBC personnel, with access control responsibilities, to ensure they document and report any anomalies or problems discovered within their systems. Anomalies shall be reported in accordance with the incident reporting procedures.
- Define reasonable use of the computer resources (including limited personal use). This should be reflective of The Rules of Behavior for EMCBC Computer System document, which outlines the criteria for reasonable use, limited personal use, and inappropriate use.

ATTACHMENT 10.16

Computer Security Policy: Audit and Accountability (AU) Policy

Purpose:

To ensure that all appropriate information is collected on the actions of devices and users to allow for efficient system management and to assist in the identification and investigation of potential security incidents.

Scope:

This policy applies to all persons and devices that operate on the [ACRO] network. The precise auditing and other functions that will be used to ensure accountability are dependent upon the operating system capability. This policy is established to provide the information that may be required to investigate an incident or to analyze the activities of a specific user. This policy includes retention periods for audit information.

Roles and Responsibilities:

Role	Responsibilities
ISSO	<ul style="list-style-type: none"> • Ensuring that audit logs are reviewed and actions are taken to address anomalies or potential issues. • Review of the activities being logged and ensure that they are sufficient to investigate potential events.
System Administrators	<ul style="list-style-type: none"> • Development of procedures to review and respond to information provided from audit log reviews. • Ensuring that systems have auditing activated and that audit logs are reviewed in a timely manner. • Providing access to central log servers for the maintenance and archival of system logs. • Providing log parsing and reduction tools. • Enabling and maintenance of auditing on all systems in accordance with the guidance in the SSP. • Reviewing logs on a daily basis for security events and reporting of suspected security events.
Users	<ul style="list-style-type: none"> • Not removing, modifying or otherwise tampering with audit logs or log settings

Compliance:

The Assistant Director, IRM shall perform audits as identified in the list of auditable events specified in the PCSP, TMR, and SSP. These auditable events will be generated and log reports produced in the timeframes specified by the Assistant Director, IRM. Audit procedures shall ensure:

- Appropriate data is captured providing traceability back to the event occurrence and the event outcome.
- Auditable events are stored for an appropriate time period as defined by this policy, the PCSP, SSP, DOE policy, or by IRM. The period shall be sufficient to provide the necessary information for incident investigations.
- The information system provides the capability to include detailed information in the audit records for audit events identified by user, time, type, location, and activity.
- Logs are regularly reviewed for inappropriate or unusual activity. Activity is investigated, reported, and action taken.
- All networked systems must provide consistent time stamps using a network time synchronization function for audit records.

ATTACHMENT 10.17

Computer Security Policy: System and Communications Protection (SC) Policy

Purpose:

EMCBC will implement system and communications protection security controls consistent with the accreditation boundaries and a defense-in-depth, segmentation, and isolation strategy consistent with the risk mitigation strategy.

Scope:

This policy covers all devices authorized for use in EMCBC accreditation boundary. This policy covers the areas of network segmentation, boundary protection, transmission integrity and all other components of the protection and transmission of information.

Roles and Responsibilities:

Role	Responsibilities
Assistant Director, IRM	<ul style="list-style-type: none"> Ensuring appropriate resources (including hardware, software, and personnel) are available to implement the network security architecture
ISSM, ISSO	<ul style="list-style-type: none"> Development and implementation of a network security architecture that meets the requirements of this policy Review of changes to the network architecture design for security compliance Implementation of monitoring solutions to detect attacks on the network Validate the system and communications procedures effectively protect the information and information systems
System Administrators	<ul style="list-style-type: none"> Ensuring network devices and hosts are configured in accordance with baseline security standards to facilitate prevention and early detection of attacks

Compliance:

This System and Communications Protection policy will be implemented through the preparation of EMCBC *System and Communications Protection procedures*. The System and Communication Protection procedures shall:

- Be reviewed annually and updated to address any new risk factors.
- Be consistent with EMCBC's missions, functions, directives, policies, regulations, standards, and guidance.

- Include monitoring and controlling communications at the external boundary of the information system and at key internal boundaries within the accreditation boundary. The architecture shall provide a means of isolating a group of devices or an enclave to limit security incidents.
- Address the issue of denial of service attacks and how the architecture will address this activity.
- Prioritize the information systems to facilitate a return to service in the event of a situation that will require restarting all or a major number of systems.
- Ensure that information is transmitted in a manner that will validate the integrity of the transmission and limit the potential of data being modified in transit.
- Address the generation, distribution or use of mobile code (java, ActiveX controls, or applets) in applications used or developed at EMCBC.
- Developed that address the use of voice over IP or voice over data technologies.
- Assess the risk and include detailed procedures for inter-connecting the EMCBC information and information systems as part of a collaborative computing environment.
- Define and address the use of cryptography at EMCBC. Use of cryptographic devices shall be consistent with DOE orders and guidance as well as NIST standards including FIPS 140-2.
- Address publicly accessible system components (e.g., public web servers)

PROCEDURE CHANGE REQUEST	
DATE: <u>06/25/07</u>	
INITIATOR: <u>W. Best</u>	
INITIATOR PHONE NUMBER: <u>60530</u>	
DOCUMENT AFFECTED: _____	
SECTION: _____	PARAGRAPH #: _____
IP NUMBER : _____	PARAGRAPH #: _____
NEW IP: <u>PS-563-01</u>	
PROPOSED REVISION: _____	

JUSTIFICATION: <u>Establish policy</u>	

Requested by: <u>W. Best</u>	DATE: _____
Approval: _____	DATE: _____
Associate Director	
Assigned to: <u>M. Cahill</u>	DUE DATE: _____

Document Review Record Sheet				
Document Title	Cyber Security Master Policy			
IP Number PS-563-01	Revision No. 1	Date Issued for Review		
The subject document is being submitted for your review, approval or comments. Since this review is controlled, a response is required from all reviewers. Therefore, please return the review sheet with or without comments				
To: M. Cahill	Extension:	By:		
Additional Instructions:				
Reviewer	Approve	Approve w/Comments	Do Not Approve	Signature of Reviewer
Ward Best				
B. Fain				
R. Nelson				
M. Roy				
P. Vent				
L. Schlag				
T. Brennan				
R. Holland				
R. Everson				
T. J. Jackson				
C. Anderson				
F. Lockhart				
D. Metzler				
J. Rampe				
R. Schassburger				
B. Bower				
J. Craig				
Comments may be attached to a separate sheet of paper				
APPROVE: Signifies the reviewer's acceptance of the document issued for review.				
APPROVE w/comments: Signifies the reviewer's overall acceptance of the document regarding concept, practice, implementation, provisions and assigned responsibilities. However, the reviewer has suggestions as to the organization of its contents or helpful additions and/or deletions. These comments are termed "non-mandatory comments" and do not require formal resolution between the reviewer and preparer.				
DO NOT APPROVE: Signifies that the reviewer has identified significant problems regarding concept, practice, implementation or responsibilities that render the document unacceptable and/or not in conformance with stated requirements. Such problem areas must be clearly identified by the reviewer. It is mandatory for the preparer to resolve these comments with the reviewer, document the resolution and obtain the reviewers concurrence for the resolution. The reviewer's written concurrence with the resultant change in disposition shall be documented on this form.				
General Review Comments:				

When review is delegated, the designated reviewer shall review and indicate concurrence with the designee's review comments and recommend disposition:				
Designated Reviewer	Concur	Do Not Concur	Signature	Date

IP-250-01-F2, Rev.2

EMCBC RECORD OF REVISION

DOCUMENT

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- I Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- I Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Initial Policy	All	08/27/07