

Date 12/16/2015



Environmental Management Consolidated Business Center (EMCBC)

Subject: Cyber Security – Account Management and User Responsibilities

Information Management Procedure APPROVED:

[Signature]
EMCBC Director 12/16/15

Office of Information Resource Management

1.0 PURPOSE

The purpose of this procedure is to establish the process for managing user accounts, rights, and access to specialized applications; and to define users training requirements in accordance with the Environmental Management Consolidated Business Center (EMCBC) Cyber Security – System Security Plan for General Support Systems, PP-IRM-240-08.

2.0 SCOPE

This procedure is limited to general user access of EMCBC systems and applications.

3.0 APPLICABILITY

This procedure is applicable to all users accessing EMCBC Information Systems, whether they are EMCBC Federal employees, EMCBC contract employees, other Federal Agency employees, or have a contractual need to access these systems.

4.0 REFERENCES

- 4.1 DOE O 142.3A, Unclassified Foreign Visits and Assignments Program
- 4.2 DOE O 203.1, Limited Personal Use of Government Office Equipment including Information Equipment
- 4.3 Risk Management Approach Implementation Plan (RMAIP)
- 4.4 EMCBC PP-IRM-240-08 – Cyber Security–System Security Plan for General Support System:
 - AC-1 Access Control Policy and Procedures
 - AC-2 Account Management
 - AC-3 Access Enforcement
 - AC-5 Separation of Duties
 - AC-6 Least Privilege
 - AC-17 Remote Access
 - AC-20 Use of External Information Systems
 - CM-1 Configuration Management Policy and Procedures
 - CM-5 Access Restrictions for Change

- AT-1 Security Awareness and Training Policy and Procedures
- AT-2 Security Awareness
- AT-4 Security Training Records
- IA-1 Identification and Authentication Policy and Procedures
- IA-2 User Identification and Authentication
- IA-4 Identifier Management
- IA-5 Authenticator Management
- IA-8 Identification and Authentication (Non-Organizational Users)
- MA-1 System Maintenance Policy and Procedures
- MA-4 Nonlocal Maintenance
- MA-5 Maintenance Personnel
- PE-1 Physical and Environmental Protection Policy and Procedures
- PE-5 Access Control for Output Devices
- PL-4 Rules of Behavior
- PS-1 Personnel Security Policy and Procedures
- PS-2 Position Risk Designation
- PS-3 Personnel Screening
- PS-4 Personnel Termination
- PS-5 Personnel Transfer
- PS-7 Third-party Personnel Security
- PS-8 Personnel Sanctions

4.5 Homeland Security Presidential Directive 12 (HSPD-12)

5.0 DEFINITIONS

- 5.1 Domain: A single security boundary of one or more computers that form a computer network.
- 5.2 Foreign National: A citizen of a nation other than the United States.
- 5.3 General Access Rights: Access to applicable shared drives, individual user drives, and EMCBC general applications (e.g., Correspondence Control and Tracking Systems [CCTS], EMCBC Management System Description [MSD]) based on organizational permissions. General Access applications are designated at deployment and controlled under IRM configuration management.
- 5.4 Homeland Security Presidential Directive 12 (HSPD-12): Issued on August 12, 2004 by President George W. Bush, HSPD-12 calls for a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and employees of federal contractors for access to federally-controlled facilities and networks. Based upon this directive, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication (FIPS Pub) 201 including a description of the minimum requirements for a Federal personal identification verification (PIV) system.

- 5.5 IRM: Office of Information Resource Management
- 5.6 Remote Access: The ability to access the EMCBC Information System through public channels or the internet (e.g., home internet, hotel Wi-Fi, wireless hotspot, etc.).
- 5.7 Controlled Unclassified Information (CUI): Unclassified information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring CUI protection such as information identified under Cooperative Research and Development Agreements (CRADA).
- 5.8 Specific Access Rights: Access to information system resources that are beyond general user rights, such as support services with elevated privileges, administrators, server managers, restricted drives, etc. Certain applications have limited access due to the sensitivity of their data. Access to these applications requires specific permission by the Cognizant Assistant Director, Federal Project Director or Content Owner.
- 5.9 System Security Plan: A formal document generated from the EM Risk Management Implementation Plan (RMAIP) to define all applicable EMCBC cyber security requirements.
- 5.10 User: Identity of an employee (EMCBC user) or other individual (visitor/non-EMCBC user) having a legitimate business need to access the EMCBC Information System, or other EMCBC services through local network, web or remote access protocols.
- 5.11 User Identifiers: The credentials (user name and password) by which a user identifies himself/herself to the system and by which the system authenticates the user's access. This also includes Personal Identity Verification (PIV) directed by HSPD-12.

6.0 ROLES AND RESPONSIBILITIES

- 6.1 Cognizant Assistant Director: The EMCBC Office Assistant Director of the specific department that is responsible for content for a given application. The Cognizant Assistant Director or designee is also the Content Owner of the given application.
- 6.2 Content Manager: Individual assigned by the Content Owner to be the point of contact for the development of the application and to ensure the integrity of the data.
- 6.3 Content Owner: The Cognizant Assistant Director, or designee, responsible for the content and functionality within the given application or system. The Content Owner approves access to Specific Access Rights applications and shall notify IRM when a user no longer needs special access rights.
- 6.4 EMCBC Federal Sponsor: A Federal EMCBC employee that verifies the need for and requests specific access to the EMCBC Information System on behalf of a non-EMCBC user either Federal or contractor. The Federal Sponsor is responsible for

completing and signing the Requesting New User Account form (IMP-IRM-8308-01-F1) for non EMCBC-based users, which includes providing an expiration date for the account.

- 6.5 IRM Support Personnel: Individuals assigned by the Assistant Director of Information Resource Management (ADIRM) to control access to the EMCBC Information System or other services. Support personnel are responsible for assisting in the completion of all required documentation related to the development and maintenance of applications, the EMCBC Information System, and managed hardware. Responsibilities shall include the following:
- Create a new user account
 - Reset a user password
 - Copy a user account
 - Move a user account
 - Disable or enable a user account
 - Change a user's primary group
 - Performs monthly user account audits
 - Enable or disable special access rights
- 6.6 System Administrator: The individual(s) responsible for maintaining and operating the systems and networks within an organization. The System Administrator typically manages user accounts including the deletion, creation, and modification of user privileges. The System Administrator must ensure timely removal of access rights for all departed employees, especially in cases of employee termination.
- 6.7 System Owner: The lead IRM individual that has overall implementation responsibility for any given application, usually the ADIRM.
- 6.8 User Types:
- 6.8.1 General Users: EMCBC-based users, Federal and contractor, that access the EMCBC Information System via the local network. General users must read, sign and follow the IRM Rules of Behavior for EMCBC Information Systems (RoB) (IMP-IRM-8308-01-F2). They must also complete initial cyber security awareness training within 30 days of start date and annual cyber security refresher training as required.
- 6.8.2 External Application Users: Users that are not EMCBC employees, but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office (usually at a serviced site or DOE Headquarters). These users must have an EMCBC Federal Sponsor. To request the account, the EMCBC Federal Sponsor must fill out the Requesting New User Account form (IMP-IRM-8308-01-F1) and submit it to IRM.
- 6.8.3 Non-EMCBC Employee User: Any individual who is not based at the EMCBC or the serviced sites but requires general access to the EMCBC Information System to accomplish his or her job function. Often, these are

Federal employees temporarily working at the EMCBC or contractors supporting a specific task for a limited time frame. These accounts are managed similarly to those for EMCBC employees with the following difference: Non-EMCBC Employee Users shall have an EMCBC Federal Sponsor. To request the account, the EMCBC Federal Sponsor must fill out the New User Account form, IMP-IRM-8308-01-F1, and submit it to IRM.

7.0 GENERAL INFORMATION

This procedure defines the process by which all users are made aware of and acknowledge their responsibilities as employees when interfacing with the information systems. The procedure sets requirements for access to EMCBC information systems and applications and provides criteria for user indoctrination and training.

8.0 PROCEDURE

Note: Foreign Nationals are citizens of a nation other than the United States. In the event business needs dictate that a specific Foreign National be granted access to the EMCBC Information Systems, the ADIRM will develop a specific plan, in accordance with Unclassified Foreign Visits and Assignments Program, DOE Order 142.3A, to address the needs of the organization for the individual in question. No access to the EMCBC Information System will be provided to a Foreign National without such a plan in place. EMCBC does not allow foreign nationals remote access to the EMCBC Information System or networks that contain CUI.

8.1 New Users – EMCBC Employees: Upon completion of the Requesting New User Account form (IRM-IMP-8308-01-F1), IRM will establish new user accounts by creating a username/password and issuing an EMCBC smart card. The EMCBC issues accounts to individual users only. Group accounts are prohibited. User identifiers are provided directly to the individual, not through email. These accounts will be disabled until the start date of the user.

8.1.1 IRM Rules of Behavior for EMCBC Information Systems: Each user will be given the IRM Rules of Behavior for EMCBC Information Systems (RoB) (IMP-IRM-8308-01-F2) which establishes the rules that govern appropriate use of the EMCBC Information Systems. All users shall read, print, and sign the RoB prior to account activation and as required thereafter. Signing the form indicates acknowledgment and acceptance of responsibilities under the RoB. This will allow users General Access Rights to the system, and the applicable resources (printers, share drives, SharePoint page, etc). Additional Access Rights require separate written approval from the appropriate entity (email is acceptable). All completed RoBs will be submitted to and maintained by IRM.

The RoB shall be reviewed by IRM annually for updates.

- 8.1.1.1 If there are revisions to the RoB, it must be printed and re-signed by all active users.
- 8.1.1.2 Annually, in conjunction with the annual cyber security training requirement (Section 8.8.2), all active users shall re-certify that they have read and understand the RoB. If there have been no revisions to the RoB, electronic re-certification that the employee has read and understands the RoB will be acceptable.
- 8.1.2 Position Categorization: All persons shall be screened prior to obtaining network access. Positions requiring access above that of a general user must meet the appropriate screening criteria requirements (National Agency Check with Inquiries [NACI], Sponsor Certification or Authorizing Official Designated Representative (AODR) Approval, Contractor Employment Screening).
- 8.1.3 Desktop Rights and Assignment: Office desktop computers are made available to users as determined by their Assistant Director and the ADIRM. Each system is issued a numbered property asset tag, which is recorded for inventory control. Users will be granted limited rights on their desktops. Distribution and addition of system privileges on all EMCBC personal computer software will be controlled by the System Administrators.

NOTE: Laptops shall be issued in accordance with the Policy for Issuing Specialized Information Technology Equipment, PO-IRM-205-10.
- 8.1.4 Remote Access: All EMCBC users are granted remote access through the use of two-factor authentication.
- 8.1.5 Special Software: Certain users may require software that goes beyond that supplied in the Basic DOE Common Operating Environment (DOECO) package installed on each computer. This software is typically Commercial-Off-the-Shelf (COTS) software such as Adobe Acrobat, MS Project, Primavera, etc. Such software may be made available with the concurrence of the individual's Cognizant Assistant Director or Team Leader and in accordance with software licensing.
- 8.2 New Users - Serviced Sites: New users at sites that receive IT support from the EMCBC will follow the same protocol as users at the EMCBC (see Section 8.1). However, access to Specific Access Applications will require the approval of the Federal Project Director and the Content Owner, after verification that the individual is not a Foreign National.
- 8.3 External Application Users: Users who are not employees of the EMCBC but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office (usually at a serviced site or at DOE Headquarters) will be given Specific Access Rights without General Access Rights. The non-EMCBC user will be required to sign an RoB to acknowledge his or her responsibilities for the

sensitivity of the data he or she is accessing and obtain the permission of the Cognizant Assistant Director or Content Owner for the application he or she is accessing.

- 8.4 Non-EMCBC Employee: Federal employees temporarily working at the EMCBC or contractors supporting a specific task for a limited time frame that require General Access Rights to the EMCBC Information System to accomplish their job function are managed similarly to EMCBC employees with the following differences:
- 8.4.1 The Federal Sponsor must complete the Requesting New User Account form (IMP-IRM-8308-01-F1) and must indicate the expected end date for the account. The account will be set to automatically disable on that date. IRM must be notified in writing (email is acceptable) by the Federal Sponsor with a new end date before the account expires or prior to re-activation if the account has been disabled.
- 8.4.2 The RoB must be signed by the Non-EMCBC Employee prior to enabling the account.
- 8.5 Vendors: Vendors are given access to the network on an as-needed basis to perform IT related work under the supervision of IRM personnel only. Vendors escorted by IRM and not issued general access or an email address are not required to sign the RoB. However, vendors requiring long term and unescorted access will be managed similarly to the EMCBC employees with the following differences:
- 8.5.1 The ADIRM or designee must complete the Requesting New User Account form (IMP-IRM-8308-01-F1) and must indicate the expected end date for the account. The account will be set to automatically disable on that date. IRM will annotate the form with the product name. The ADIRM may renew the access without generating a new form by annotating the original form or via email.
- 8.5.2 The RoB must be signed by the vendor prior to enabling the account.
- 8.5.3 Remote access must be authorized by the ADIRM and will be monitored and logged in the IRM Project Management System, SharePoint, or equivalent. The remote session and network connection will be terminated when the maintenance is completed.
- 8.6 Termination of Account and Access: Upon notification from the Human Resources Advisory Office (HRAO), the Cognizant Assistant Director, or the Federal Sponsor, account access will be terminated as required.
- 8.6.1 All account access (General and Specific) will be disabled. Users leaving the EMCBC but staying in government service may be allowed access to their email accounts for no more than 30 days with approval from the Cognizant Assistant Director. Users leaving government service will be allowed to generate an "Out of Office" email giving out details of their new location but access to their email account will be terminated.

- 8.6.2 Specific Account Access will be terminated upon notification from the application Content Owner/Content Manager (or from HRAO if employment is terminated) by disabling or removing the account or access rights.
- 8.6.3 Accounts are automatically disabled after 60 days of inactivity. If there is a need to re-enable the account, current EMCBC-based employees may contact IT Support directly. For Visitor accounts, an EMCBC Federal Sponsor must make the request via email on behalf of the user and re-verify the required access rights.
- 8.7 Account Management:
- 8.7.1 IRM will conduct a monthly audit of General Account Access. Results of the audit will be documented in the IRM Project Management System.
- 8.7.2 IRM will provide a list of applications requiring Specific Access Rights to the Content Owner for verification semi-annually. Results of the audit will be documented in the Project Management System.
- 8.8 Training:
- 8.8.1 Initial Training: All users shall take cyber security awareness training within 30 days of being issued an account. All new accounts are set up to be automatically disabled after 30 days from date of creation. Failure to complete the training within 30 days will result in the account being disabled/locked. Users must inform IRM upon completion of the training for their accounts to be fully activated. Following confirmation that the user has completed the cyber security awareness training, his or her account will be set to the appropriate end date or not to expire, as applicable.
- 8.8.2 Annual Training: All users shall take cyber security refresher training annually to maintain their access rights to the network. Users will be notified when this training is due. DOE and contractor employees permanently assigned to other DOE sites with user access are assumed to have completed the required user training through their home-site's cyber security program.
- 8.8.3 Failure to complete the required training within the timeframe specified in the notification will result in the account being disabled. Users must then contact IT Support to schedule completion of the training at a computer located in a designated area. Accounts will be re-activated upon completion of the required training and a written request from the user's supervisor/Federal Sponsor to the ADIRM. Remote users' accounts will be reactivated for 24 hours upon authorization by their supervisor/Federal Sponsor to allow for completion of training. If an employee is on extended leave during the specified timeframe, the cognizant supervisor/Federal Sponsor should notify the ADIRM.
- 8.9 Updates and Alerts: IRM will periodically issue alerts to identify security issues to the EMCBC users. The purpose of the alerts is to inform the users of security threats

that may affect them in the workplace or at home and are issued at the discretion of IRM.

9.0 RECORDS MAINTENANCE

9.1 Records generated as a result of implementing this document are identified as follows and are maintained by the Office of Information Resource Management and managed in accordance with the EMCBC Organizational File Plan:

9.1.1 DAA-GRS-2013-0006-0003 – System Access Records – Information Systems Security Records

10.0 FORMS USED – All forms are the latest revision unless otherwise specified.

10.1 Requesting New User Account, IMP-IRM-8308-01-F1

10.2 EMCBC IRM Rules of Behavior, IMP-IRM-8308-01-F2

11.0 ATTACHMENTS - None

EMCBC RECORD OF REVISION

Document Title: Cyber Security Account Management and User Responsibilities

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate change:

I Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised, or

I Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are revised.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

| Rev. No. | Description of Changes | Revision on Pages | Date |
|-----------------|--|--------------------------|-------------|
| 0 | Initial Information Management Procedure supersedes IP-240-01, Rev 3 | Entire Document | 12/16/15 |