

Date: 12/05/2011



Environmental Management Consolidated Business Center (EMCBC)

Subject: Cyber Security – Account Management and User Responsibilities

Implementing Procedure

APPROVED: (Signature on File)

EMCBC Director

Office of Information Resource Management

1.0 PURPOSE

The purpose of this procedure is to establish the process for managing user accounts, rights, access to specialized applications, and define users training requirements.

2.0 SCOPE

This procedure is limited to general user access to 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 REQUIREMENTS

4.1 Energy Program Cyber Security Plan (PCSP)

- 4.1.1 AC-1 Access Control Policy and Procedures
- 4.1.2 AC-2 Account Management
- 4.1.3 AC-3 Access Enforcement
- 4.1.4 AC-5 Separation of Duties
- 4.1.5 AC-6 Least Privilege
- 4.1.6 AC-17 Remote Access
- 4.1.7 AT-1 Security Awareness and Training Policy and Procedures
- 4.1.8 AT-2 Security Awareness
- 4.1.9 AT-4 Security Training Records
- 4.1.10 IA-1 Identification and Authentication Policy and Procedures
- 4.1.11 IA-2 User Identification and Authentication
- 4.1.12 IA-4 Identifier Management
- 4.1.13 IA-5 Authenticator Management
- 4.1.14 PL-4 Rules of Behavior
- 4.1.15 PS-1 Personnel Security Policy and Procedures
- 4.1.16 PS-3 Personnel Screening
- 4.1.17 PS-4 Personnel Termination
- 4.1.18 PS-5 Personnel Transfer
- 4.1.19 PS-7 Third-party Personnel Security

- 4.1.20 PS-8 Personnel Sanctions
- 4.1.21 SI-9 Information Input Restrictions

5.0 DEFINITIONS

- 5.1 Assistant Director: The Office Director of the specific department that is responsible for the Subject Matter Expert (SME) or Content Owner for a given application.
- 5.2 Content Owner: Also known as the Subject Matter Expert (SME), Non-IRM person assigned by their Assistant Director to be the point of contact for application development.
- 5.3 Domain: A single security boundary of one or more computers that form a computer network.
- 5.4 Federal Sponsor: A Federal EMCBC employee who requests specific access to the EMCBC system on behalf of a non-EMCBC user either Federal or contractor.
- 5.5 IRM: Office of Information Resource Management
- 5.6 Offsite User: Users who are not General Access Users under the EMCBC, but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office. These users are usually at a serviced site or at DOE Headquarters.
- 5.7 Sensitive Unclassified Information (SUI): Unclassified information requiring protection mandated by policy or laws, 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 SUI protection such as information identified under Cooperative Research and Development Agreements (CRADA).
- 5.8 Support Personnel: Individuals assigned by the Assistant Director of Information Resource Management (AD-IRM) to control access to the EMCBC domain or other services.
- 5.9 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 Administrators must ensure timely removal of access rights for all departed employees, especially in cases of employee termination.
- 5.10 System Security Plan: A formal document generated from the EM Program Cyber Security Plan to define all applicable EMCBC cyber security requirements.
- 5.11 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.

5.12 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.

6.0 RESPONSIBILITIES

6.1 Users: Read, sign, and follow Rules of Behavior for EMCBC Information Systems, Attachment A (user agreement).

6.2 Assistant Directors: Approve access to Specific Access Rights applications. Notify IRM when a user no longer needs special access rights.

6.3 IRM: The support personnel shall include the following responsibilities:

6.3.1 Create a new user account

6.3.2 Reset a user password

6.3.3 Copy a user account

6.3.4 Move a user account

6.3.5 Disable or enable a user account

6.3.6 Change a user's primary group

6.3.7 Delete a user account

6.3.8 Audit user accounts monthly for rights and access.

6.3.9 Enable or disable special access rights

6.4 Federal Sponsor: Requests access for a non-EMCBC user. The Federal Sponsor is also responsible for completing and signing the NON-EMCBC USER ACCOUNT ONLY section of the user agreement form, Attachment A, which includes providing an expiration date for the account.

7.0 GENERAL INFORMATION

This procedure defines the process by which 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 AD-IRM will develop a specific plan to address the needs of the organization for the individual in question. No access to the EMCBC network will be provided to a Foreign National without such a plan in place.

8.1 New Users – EMCBC Employees: Upon notification from OHR (and verification that the person is not a Foreign National), IRM will establish new user accounts; EMCBC issues accounts to individual users only. User identifiers are provided directly to the individual, not through email. These accounts will be disabled until the start date of the user. A User may be granted access to EMCBC systems prior to their official start

date if they are a current government employee and have approval by their Assistant Director. Non-government employees who are identified as having access needs prior to their start date will need approval from both their Assistant Director and the EMCBC Security Officer.

- 8.1.1 Rules of Behavior for EMCBC Information Systems (User Agreement): Each user will be given a user agreement (Rules of Behavior for EMCBC Information Systems, Attachment A, IP-240-01-F1,) that establishes the uses of the EMCBC Information Technology systems. Before the user is granted access, the user will sign and acknowledge that they understand their responsibilities under the agreement. This user agreement allows users General Access to the system. Additional system access may be documented on the original user agreement, or by separate agreement. All user agreements will be maintained by IRM.
- 8.1.2 General Access Rights: All general users are granted access to shared drives, individual user drives and access to EMCBC general applications. New Users are given general access rights to EMCBC general applications, such as Correspondence Control and Tracking Systems (CCTS) and Policies, Procedures and Plans, based on their organization permissions by the EMCBC Intranet and EMCBC Web Based Applications access process. All users have access to the general tools such as Phonebook, Traffic, Forms, Training, Manuals, etc. General Access applications are designated at deployment and controlled under IRM configuration management.
- 8.1.3 Specific Access Rights: Certain applications have limited access due to the sensitivity of their data. These applications require specific permission by the Assistant Director, Federal Project Director or Content Owner for access. These permissions are documented on the user agreement or a supplemental agreement as user access is changed. See Attachment C, Example of General and Special Access List.
- 8.1.4 Desktop, Laptop Rights and Assignment: Office desktop or laptop computers and/or remote access tokens are made available to users as determined by their Assistant Director and the AD-IRM. Each system is issued a numbered property asset tag, which is recorded for inventory control. Users will be granted limited rights on their desktops/laptops. Distribution and addition of system privileges on all EMCBC personal computers software will be controlled by the System Administrators.
- 8.1.5 Offsite Access: All users are granted offsite access to their email accounts through the use of web-mail. All other remote access to data and applications is defined through the users Specific Access Rights. Offsite access is limited to an as needed basis. EMCBC does not allow foreign nationals offsite access EMCBC system or networks that contain Sensitive Unclassified Information (SUI) Completion of User Acknowledgement Agreement (UAA) for Two-Factor Authentication and Remote Access Connection Services, Attachment B

(IP-240-01-F2) is required before access to two factor authentication systems will be granted.

- 8.1.6 Special Software: Certain users may require software that goes beyond that supplied in the Basic DOE Common Operating Environment package installed on each computer. This software is typically Off the Shelf (OTS) software such as Adobe Acrobat, MS Project, Primavera, etc. Such software may be made available with the concurrence of the individual's Assistant Director or Team Leader.
- 8.2 New Users: Attached Sites: New users at sites that receive IT support from EMCBC will follow the protocol for EMCBC Employee users with the exception that the Federal Project Director may approve in lieu of their EMCBC Assistant Director. However, access to Specific Access Applications will require the approval of the Federal Project Director **and** their EMCBC Assistant Director or Content Owner, including verification that the individual is not a Foreign National.
- 8.3 Offsite Users: Offsite Users are those users who are not General Access Users under the EMCBC, but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office. (These users are usually at a serviced site or at DOE Headquarters.) These users will be given Specific Access Rights without General Access Rights. The offsite user will be required to sign an access form to acknowledge their responsibilities for the sensitivity of the data they are accessing and obtain the permission of the Assistant Director or Content Owner for the application they are accessing.
- 8.4 New Users: Visitors/non-EMCBC Employees: A Visitor is any individual who is not based at EMCBC or the attached sites but requires General Access to the EMCBC system to accomplish their 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:
 - 8.4.1 The user agreement must be signed by the Federal Sponsor who must indicate the expected end date for the account as well as the specific rights required for the user. The specified account will be set to automatically disable on that date or one year from the activation date, whichever is less. IRM must be notified in writing (email is acceptable) by the Federal Sponsor with a new end date prior to re-activation.
- 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 a user agreement. However, vendors given any long term access allowing for un-escorted access will be required to:
 - 8.5.1 Present documentation from their company verifying that they are a U. S. Citizen.

8.5.2 Sign Rules of Behavior for EMCBC Information Systems form.

8.5.2.1 IRM will annotate the form with the product the vendor is maintaining and give the document an expiration date a maximum of one year from the nearest current month. The AD-IRM may renew the access without generating a new form by annotating the user agreement.

8.6 Termination of Account and Access: Upon notification from OHR, the Assistant Director, or the Federal Sponsor, account access will be terminated as required.

8.6.1 General Account Access will be disabled until such time as the disposition of the user's files and emails has been determined. Users leaving EMCBC, but staying in the government service may be allowed access to the email accounts for up 30 days with approval of their Assistant Director. Users leaving government service will be allowed to generate an "Out of Office" email giving out details of their new location and access to their email account will be terminated.

8.6.2 Specific Account Access may be terminated by notification of an Administrator of the application and will be terminated once the employee has left the EMCBC.

8.6.3 Accounts are automatically disabled after 90 days of inactivity. If there is a need to re-enable the account, current EMCBC based employees may contact the Help Desk directly. For Visitor/Non-EMCBC accounts, an EMCBC based 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 Maintenance Log.

8.7.2 IRM will coordinate semi-annual audits of Specific Access Rights by the Content Owner.

8.8 Training:

8.8.1 Initial Training: All users will take cyber security awareness training within 30 days of being issued a User ID. All new accounts are set up to be automatically disabled after 30 days from date of creation or on the end date specified by the Federal Sponsor, whichever is sooner. Once the automatic notification from the training system notifies support personnel that the security awareness training has been completed, the account is set for the appropriate end date or not to expire, as appropriate. Extensions may be granted by the Assistant Director with concurrence by the AD-IRM for extenuating circumstances.

- 8.8.2 Annual Training: All users will take a cyber security refresher training annually to maintain their access rights to the network. Users will be notified when this training is due. Users may operate up to two months beyond the training due date with the permission of the AD-IRM.
- 8.8.3 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 in accordance with the Office of Information Resource Management File Plan:
 - 9.1.1 ADM 01-29.2-A3 Administrative Training Records – Cyber Security Training
 - 9.1.2 ADM 20-01-C Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications or Electronic Records – System Usage Agreements
 - 9.1.3 GRS 24-03-B1 Information Technology Asset and Configuration Management Files – Access and Assignment Information
 - 9.1.4 GRS 24-08-C Information Technology Operations Records – IRM Maintenance Log

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

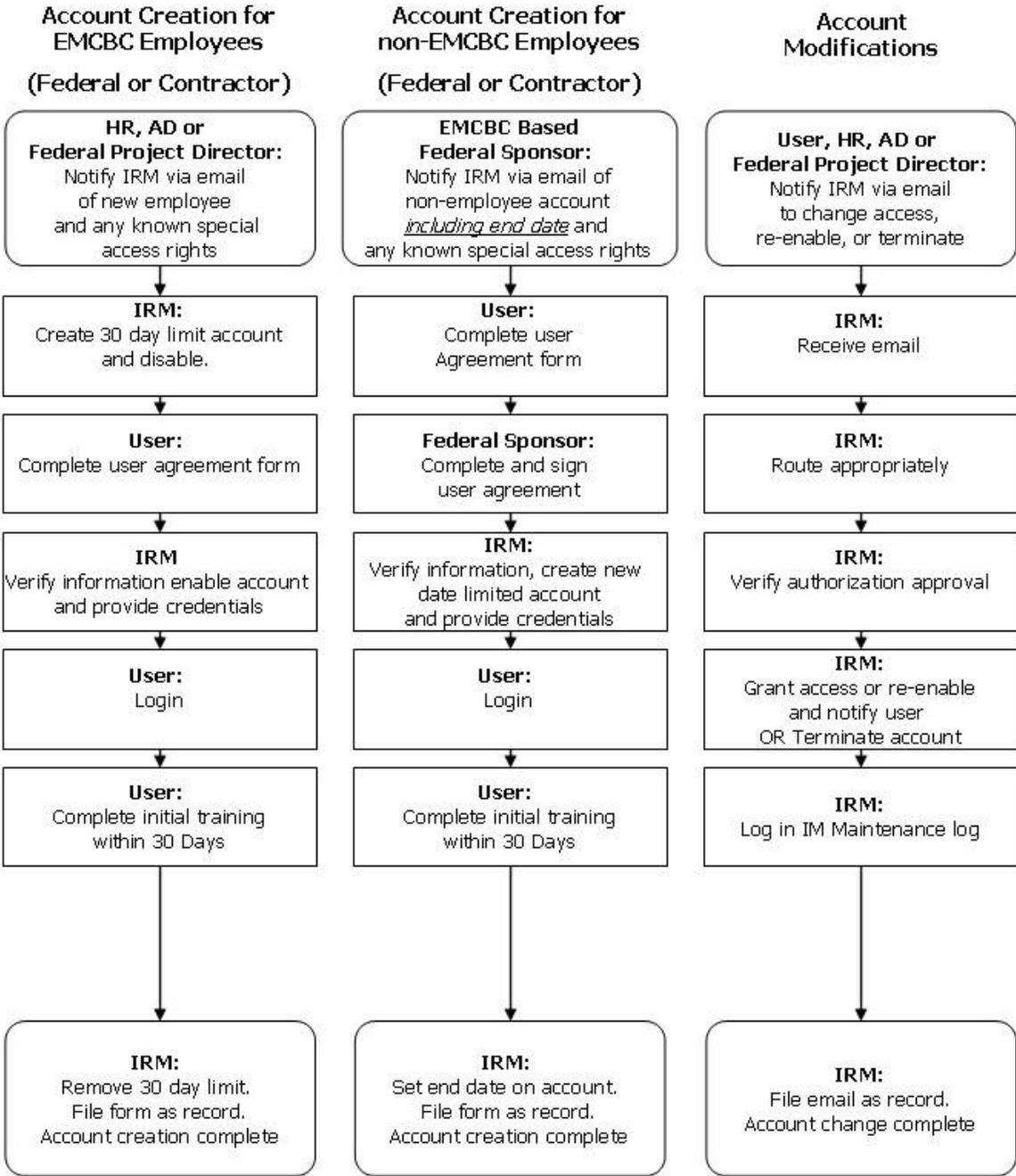
- 10.1 ‘Rules of Behavior for EMCBC Information Systems’ IP-240-01-F1
- 10.2 ‘User Acknowledgement Agreement for Two-Factor Authentication and Remote Access Connection Services’ IP-240-01-F2

11.0 ATTACHMENTS

- 11.1 Attachment A - Rules of Behavior for EMCBC Information Systems, IP-240-01-F1
- 11.2 Attachment B - User Acknowledgement Agreement for Two-Factor Authentication and Remote Access Connection Services, IP-240-01-F2
- 11.3 Attachment C - Example of General and Special Access list

12.0 FLOWCHART

EMCBC Cyber Security User Account Management



**DEPARTMENT OF ENERGY
OFFICE OF ENVIRONMENTAL MANAGEMENT
PROGRAM CYBER SECURITY PLAN**

RULES OF BEHAVIOR FOR EMCBC INFORMATION SYSTEMS

In compliance with the requirements of OMB Circular A-130, Appendix III, as required by law under the Clinger-Cohen Act, all users of a Government Information System are required to be apprised of the rules that govern the appropriate use of such data processing resources. This applies to both the computer that has been issued to them as well as any computer they are authorized to use apart from what has been issued to them.

To ensure compliance with regulations in this regard, the following conditions of use apply. These conditions form the Rules of Behavior that shall establish evidence of such compliance on an individual basis. As a condition of system access, you are required to read the following and concur at the bottom of this document with a signature by your hand.

1. DOE computers and Information Systems are provided for the processing of official U.S. Government information.
2. Accessing Government work files to which I have been given access permission, whether by issued computer or privately owned computer, requires that I abide by the Rules of Behavior described herein.
3. I have no expectation of privacy on any information entered, stored, or transferred through DOE computers, host systems or networks.
4. Use of DOE computers, host systems and networks are restricted to authorized users and I am responsible for all actions taken under my user account or identity.
5. I have attended training and have been instructed on Remote Access security concepts and best practices. If using a privately owned computer to access a Government computer network, I will not circumvent the protections that such access may be subject to.
6. I will use the DOE computer, host system and network only as authorized. I understand that I am permitted to use this system for limited personal use as described in the appropriate use policy elements that I have reviewed.
7. If I have been authorized to process classified information, I will not enter classified data into a classified system if that data is of a higher classification level than the classified computer system is authorized to process.

Attachment A

(Page 2 of 4)

8. Under no circumstances will I ever enter classified data into an unclassified system or permit anyone to do so. If I do so accidentally or otherwise receive by email or acquire such information unexpectedly from anyone, I will immediately notify my supervisor.
9. If I observe anything that indicates inadequate security, misuse of this system or virus infection, I will immediately notify my supervisor and IRM.
10. I will follow office security procedures, official regulations, and policies applicable to Information Systems operation, to include applicable password policy.
11. I will not use any DOE computer and/or the host system to gain unauthorized access, or attempt to gain unauthorized access, to other computers or Information Systems. Further, I will not use any DOE computer and/or the host system to launch denial of service, or attempt to launch denial of service, attacks against other computers or Information Systems.
12. I understand that the host system and network is monitored to ensure information security, system integrity, and the limitation of use for official purposes. By using the host system and network, I am expressly consenting to such monitoring and agree that any and all information derived from such monitoring, including connection logs between computers and my subscriber information may be used as a basis for administrative, disciplinary, or criminal proceedings.
13. I understand that my supervisor may instruct me to reduce my level of personal usage based on monitoring reports of such activity.
14. I also hereby consent to the opening of any stored filed and/or electronic mail that may be stored either on the host system or on any DOE computer workstation by my supervisor, chain of command or any individual duly authorized under color of law. If such information has been encrypted by me, I shall freely provide the means of decryption to provide such access.
15. I hereby expressly authorize the system administrator to provide my supervisors and law enforcement personnel with any and all information pertaining to my alleged misuse and abuse of any DOE computer and/or the host system and/or network.
16. I further certify that I am not a Foreign National.
17. I have been provided a copy of this Agreement and understand that the EMCBC IRM Department will maintain the original.

Attachment A
(Page 3 of 4)

- 18. I certify that I will follow all requirements for the protection of sensitive data such as Personally Identifiable Information, Sensitive Agency Information, Source Selection Information, etc.

- 19. I understand that the following activities on DOE computer resources are prohibited and constitute misuse or abuse and can lead to disciplinary action up to removal:
 - a. Activities that include, but not limited to hate language; material that ridicules others on the basis of race, creed, religion, sex, disability, national origin, or sexual orientation; and harassment or threats.
 - b. The creation, downloading, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.
 - c. Use for commercial purposes or in support of “for-profit” activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services) with which an employee is associated.
 - d. Any personal use of government resources that may mislead someone into believing that the employee is acting in an official capacity.
 - e. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
 - f. The above inappropriate activities are not all inclusive and employees must abide by DOE directives on appropriate use of Information Systems.
 - g. Employees will not disseminate government e-mail addresses on flyers, personal business publications, Internet websites or anything that would cause a significant increase in the number of e-mail messages received.

Levels of Access:
 Access Authorized for General Use, as defined by the General Use Access Protocol.

	User’s Signature	Date:
	Printed Name	
	Organization	

Federal Employee? Yes No

Additional Specific Access Rights for EMCBC Drives, Systems and Applications:	
Drive, System or Application	Access Type (Read, Write, Update)

NON-EMCBC USER ACCOUNT ONLY
Will this user require? <input type="checkbox"/> Assigned Phone <input type="checkbox"/> Email account <input type="checkbox"/> Assigned workstation
Other specific access rights or limitations:
Planned expiration date for this account: (Date account will be disabled. EMCBC Federal Sponsor may extend or re-enable by contacting the Help Desk.) _____
EMCBC Federal Sponsor Name: _____ Organization: _____ Signature: _____ Date: _____

<u>THIS SECTION TO BE COMPLETED BY IRM</u>
<input type="checkbox"/> EMCBC/SLA Customer User Account Setup completed _____ (initial) List Exceptions to Standard Setup _____
<input type="checkbox"/> Non-EMCBC User Account Setup completed _____ (initial) List Exceptions to Standard Setup _____
<input type="checkbox"/> Email request(s) attached
Authorizations for specific rights were: <input type="checkbox"/> Verified and completed (list) _____ <input type="checkbox"/> Forwarded to appropriate individual for authorization (list) _____

Attachment B

(Page 1 of 2)

USER ACKNOWLEDGEMENT AGREEMENT (UAA)
For Two-Factor Authentication and Remote Access Connection Services

U. S. Department of Energy (DOE) employees, contractors, and affiliates are responsible for acknowledging this user agreement when requesting, accepting, and/or using a DOE assigned identity token. Employees will be bound to the terms of this user agreement upon cessation of need or employment, whichever comes first.

As an EMCBC Remote Access Connection (RAC) user, you must agree to the following prior to using the EMCBC RAC:

- Use Restricted to Official DOE Business and Unclassified Data:
The EMCBC RAC user license, software, and identity token that are issued to you are the property of the U. S. Department of Energy and should only be used exclusively for legal, authorized, and legitimate DOE business only.
- Accuracy of Representation:
Make true representation at all times of identification and authentication information. Not only should you provide accurate representation initially to receive an identity token, but you should also notify the EMCBC IRM Department if your personal information changes (name change, organization change, email address change, etc.) throughout the duration of use so the identity information is updated in the directory.
- Notification of Identity Token Loss, Disclosure, or Compromise:
Upon any actual or suspected loss, disclosure, or compromise of your identity token or authentication information, you must immediately notify the EMCBC IRM Department .
- Non-Transference of License and Cessation of Operation:
You may not transfer your EMCBC RAC user license to anyone else. If you no longer need the EMCBC RAC, notify the EMCBC IRM Department which will provide you with instructions for returning your identity token.
- Export of EMCBC RAC Prohibited:
Please consult with your local Security Officer if you have a requirement involving any foreign nationals.

Attachment B
(Page 2 of 2)

AS AN EMCBC RAC USER, YOU AGREE TO USE EMCBC RAC SERVICES IN ACCORDANCE WITH THE TERMS FOUND IN THE ATTACHED AGREEMENT.

You demonstrate your knowledge and acceptance of the terms of this agreement by signing this user agreement form. This agreement is valid for the identity token lifetime or until cessation of need or employment, whichever comes first.

_____	_____	_____	_____
User First Name	User MI	User Last Name	User Signature
_____		_____	_____
User Email Address		User Site ID	Date
SECRET KEYWORD			
Please answer <u>ALL</u> of the questions listed below. The question(s) will be asked of you if you need to contact the EMCBC IRM Department for any reason regarding your identity token (forgotten passwords, departmental changes, or name / email changes).			
What was the make and model of your first car?	_____		
What year you graduated from high school?	_____		
In what city or town was your first job?	_____		

Do not write below this line

IDENTITY PROOFING

Date: _____

Type of identification presented: _____

Identification Number: _____

Person's name as it appears on identification: _____

Identity Token Serial Number Assigned: _____

Registration Authority Name: _____

Registration Authority Signature: _____

Attachment C

Example of General and Special Access List

Application Name	Security
Blackberries & Cell Accts	Yes
Bomb Threat Checklist	No
CCTS	Yes
CCTS MOAB	Yes
CCTS_OAKLAND	Yes
Congressional Directed Activities	Yes
Copier Count	Yes
Dictionary / Thesaurus	No
DOE Acronyms	No
DOE Weblinks	No
DOENet Sites	No
E-CLPS	Yes
ECP	Yes
ECP Upgrade Team	Yes
EEOICPA	Yes
EMCBC Weekly Reports to EM HQ	No
File Plans	No
Flexiplace Accomplishment Tracking	No
FOIA / PA	Yes
Forms	No
IM Maintenance Log	Yes
jTrac for Finance	Yes
jTrac for IRM	Yes
Maintenance Request	No
Manuals	No
Moodle	No
MS Project Viewer	No
Newsletter	No
PCard	Yes
Pegasus	Yes
Permissions	No
Phonebook	No
Policies, Procedures & Plans	No
Printer Management	Yes
Property Tracking	Yes
Purchasing	Yes
Recovery Toolbox	Yes
REDS	Yes
SEB Resource Management	Yes
Selected EMCBC Process Flowcharts	No
Site Profiles	No
Traffic Conditions	No
Training	No

EMCBC RECORD OF REVISION

DOCUMENT – IP-240-01 Rev 3 Cyber Security Account Management and User Responsibilities

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	Original Procedure	Entire Document	1/22/07
2	Updated references	1	6/16/08
2	Spelled out SSP	2	6/16/08
2	Clarified Foreign Nationals cannot get accounts	3, 8	6/16/08
3	Periodic Review	Entire Document	12/05/11
3	Revised Attachment A, Rules of Behavior for EMCBC Information Systems to include IRM Section	Attachment A	12/05/11
3	Added Attachment B, User Acknowledgement Agreement	Attachment B	12/05/11
3	Added title “Example of General and Special Access List” to Attachment C (formerly Attachment B)	Attachment C	12/05/11
3	Revised the Flow Chart	Section 12.0	12/05/11
3	Changed text “User Agreement Form” to “Rules of Behavior for EMCBC Information Systems”	Entire Document	12/05/11
3	Corrected spelling and grammar errors	Entire Document	12/05/11
3	Added Office of Information Resource Management to header of document	Document Header	12/05/11
3	Changed text from “directly employed by EMCBC” to “EMCBC Federal employees, EMCBC contract employees, other Federal Agency employees.”	Section 3.0	12/05/11
3	Changed PL-240-08 Cyber Security – Systems Security Plan for General Support System to Energy Program Cyber Security Plan	Section 4.1	12/05/11
3	Alphabetized the definitions. Also deleted Application Sponsor, changed Cognizant Assistant Director to Assistant Director, and changed Domain Administrator to Support Personnel. Also added Content Owner, Federal Sponsor, Offsite User, Sensitive Unclassified Information, System Administrator and User Identifiers	Section 5.0	12/05/11
3	Changed Assistant Director to Office Director of the specific department responsible for SME.	Section 5.1	12/05/11
3	Changed “Special” to “Specific”	Section 6.2	12/05/11
3	Changed “domain administrators group” to “support personnel” and added 6.3.9 Enable or Disable special access rights.	Section 6.3	12/05/11
3	Added “information” and “criteria”	Section 7.0	12/05/11
3	Changed Office of Human Resources to OHR	Sections 8.1, 8.6	12/05/11

3	Included Federal Project Directors and Content Owners to approve access rights to applications in addition to AD. Also, removed limited administrator rights to users when offsite or on travel. Also added “accounts” and “offsite” and clarified offsite access for foreign nationals. Also, removed requirement to document special access rights on the user agreement form when these are granted after the initial account creation. Also, removed requirement that ADs or Federal Project directors need to sign for EMCBC Employees.	Sections 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.2, 8.3	12/05/11
3	Added section for non-EMCBC employees and clarified that these accounts require signature from employee and federal sponsor. Non-EMCBC employees’ rights may be more restricted than EMCBC employees.	Section 8.4	12/05/11
3	Clarified vendor access rights.	Section 8.5	12/05/11
3	Added Federal Sponsor as an individual who can make notification to terminate a user’s account for visitor/non-EMCBC account holder or vendor.	Section 8.6	12/05/11
3	Removed text pertaining to specific account access regarding former EMCBC employees in new functions.	Section 8.6.2	12/05/11
3	Added clarification about how disabled accounts are re-enabled.	Section 8.6.3	12/05/11
3	Changed monthly to semi-annual for special rights review.	Section 8.7	12/05/11
3	Clarified that new accounts are only authorized for 30 days until training is completed.	Section 8.8.1	12/05/11