

**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.

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.

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) _____	