

**OFFICE OF ENERGY EFFICIENCY AND RENEWABLE ENERGY (EERE)
FEMP Central End User and Privileged User Rules of Behavior**

1. INTRODUCTION

The Office of Management and Budget (OMB) has established the requirement to formally document website Rules of Behavior as set forth in OMB circular A-130¹. The Rules of Behavior contained in this document are to be followed by Federal employees, contractor users, and general system users of the EERE Centralize Website Hosting Environment (ECWHE), a combination of a website hosting environment and Content Management System (CMS), which hosts the Federal Energy Management Program's Central Program (FEMP Central). Users will be held accountable for their actions on the ECWHE and, by association, on FEMP Central. If a user violates DOE and/or EERE policy regarding the rules of the ECWHE and FEMP Central, the user may be subject to disciplinary action at the discretion of DOE, EERE, and/or their employer's management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation and the judgment of the appropriate authority. These Rules of Behavior do not apply to public users browsing the EERE web.

Rules of behavior establish ethical and practical standards in recognition that a knowledgeable staff is the single most critical element of a successful security program. Rules of behavior are not to be used in place of existing policy, but rather, they are intended to enhance and further define the specific rules each user must follow while accessing EERE HQ information systems.

2. APPROPRIATE USE OF THE ECWHE AND THE FEMP CENTRAL SYSTEM

- Users are not authorized to disable any security features or alter system configurations.
- Users are only authorized to enter content into the ECWHE or FEMP Central system that has received prior approval, or will receive approval by DOE/EERE or one of its authorized representatives, and is free from violations of: law, standards of conduct, and DOE and EERE policies.

3. INCIDENT HANDLING AND REPORTING

In the event that any ECWHE or FEMP Central users become aware of a security incident, such as those identified in the list below or the defacing of a website (specifically, FEMP Central), or any other malicious activity (actual or suspected), the user must contact the FEMP Help Desk and/or the EERE help desk, which has been trained to address security concerns.

Reportable cyber security incidents generally meet at least one of the following criteria:

- All attempts of unauthorized access, whether or not they are successful, even if unauthorized access is suspected but not yet proven.
- Instances of malicious code such as viruses, Trojan horses, or worms.
- Situations where a person who does not appear to be conducting legitimate business is acting in a manner that raises suspicion.
- Instances where a user is in violation of these Rules of Behavior, or exhibiting non-compliance with DOE, EERE, or FEMP policy.
- Instances where a user is seeking to use the ECWHE and FEMP Central system to publish information which is not related to, or is in opposition to, the Federal Energy Management Program, Office of Energy Efficiency and Renewable Energy, and/or Department of Energy mission and goals.

Upon the discovery of a security-related incident, the user should immediately stop work, report cyber security incidents (suspected or actual) to management, and contact the FEMP and/or EERE help desks immediately.

4. ACCESS CONTROLS

Password Generation.

- Passwords should contain at least eight non-blank characters consisting of a combination of letters (preferably a mixture of upper and lowercase), numbers, and at least one special character within the first seven positions.
- Passwords should contain non-numeric characters in the first and last position.
- Passwords should not contain the user ID, any common English dictionary word, spelled forward or backwards (except words of three or fewer characters); employ common names; or include the user's own or, to the best of his/her knowledge close friends—or relatives— names, user serial number, Social Security number, birth date, phone number, or any recognizable information associated with the user of the password. Passwords should not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx."²

For easy reference, these rules are repeated upon account and password creation and during any password reset process within FEMP Central.

Password Management.

- Individuals should change passwords at least every 90 days; immediately after sharing; as soon as possible, but at minimum within 1 business day, after a password has been compromised, or after one suspects that a password has been compromised; and on direction from management.
- Individuals should not: share passwords except in emergency circumstances or when there is an overriding operational necessity³; leave clear-text passwords in a location accessible to others or secured in a location whose protection is less than that required for protecting the information that can be accessed using the password; enable applications to retain passwords for subsequent reuse.

For easy reference, FEMP Central will present a reminder to reset passwords, starting within 14 days of expiration, until the password has been reset or expires (causing the individual to be locked out of his/her account). The reminder provides a quick link to the password reset page with the same password requirements as listed above.

5. REMOTE ACCESS

- Remote access users must be authorized for remote access and should access only the services for which they have been explicitly authorized.
- Anti-virus software must be used on all remote machines and must be updated with the latest virus definitions prior to initiating a remote session.

By utilizing the FEMP Central system in whatever capacity and with whatever permission currently granted to me, I acknowledge receipt of, understand my responsibilities, and will comply with these rules of behavior for the EERE ECWHE and FEMP Central Systems.

_____ *Signature and Date*

_____ *(Print Name)*

¹ <http://www.whitehouse.gov/omb/circular/a130/a130.html>, Appendix II, Section A3

² DOE G 205.1-3, Password Guide, <https://www.directives.doe.gov/pdfs/doe/doetext/restrict/neword/205/g2053-1.pdf>

³ As described in the approved and relevant Cyber Security Program Plan (CSPP)