Appendix A: Rules of Behavior for IOME – Internet Operations, Maintenance, & Enhancements

Security Rules of Behavior for IOME	
Purpose / Affected users	These rules of behavior formally establish the expected behaviors of all content providers for www.epa.gov, both federal employees and contractor personnel who post content to the web site.
1. Official Business	Employees shall use EPA computer systems and information for official business only.
2. Access	Employees shall access and use only information for which they have official authorization.
3. Accountability	Employees shall be accountable for their own actions and responsibilities related to information resources entrusted to them. Each is expected to: • Behave in an ethical and trustworthy manner. • Do not attempt to perform actions or processing for which you do not have authorization. • Do not attempt to view, change or delete data unless you are authorized to do so. • Do not use your system privileges to obtain information for anyone who is not authorized to do so. • Do not allow another user to logon using your user ID and password. • Be alert to threats to EPA applications and data. • Logout of IOME at the end of each work session; do not leave telnet or ftp sessions open.
4. Confidentiality	Employees shall protect confidentially sensitive information about employees and others from disclosure to unauthorized individuals or groups. Employees shall protect Privacy Act Information (personal information about individuals).
5. Integrity	Employees shall protect the integrity and quality of information.
6. Availability	Employees shall protect the availability of information and systems.
7. Passwords and User-IDs	Employees shall protect information security through effective use of user IDs and passwords. • Do not share your password with anyone. • Password must be a minimum 8 characters in length, with at least one numeric and at least one alpha character, one capital, and one special character (!@#$%^&*.:-). Try to create complex password (do not use words). • Do not use family names, birthdays or other easily solved passwords. • Password must be changed every ninety days. • Password should be memorized, not written down**.**
8. Hardware	Employees shall protect computer equipment from damage, abuse, and unauthorized use.
9. Software	Employees shall use software in a safe manner that protects it from damage, abuse, and unauthorized use.

10. Awareness	Employees shall stay abreast of security policies, requirements, and issues, including completing annual security awareness training and reading distributed security information.
11. Reporting	Employees shall promptly report security violations and vulnerabilities to proper authorities, including the EPA CSIRC at 1-866-411-4EPA (4372). See http://cfint.rtpnc.epa.gov/otop/security/csirc/incident_how.cfm

Last updated: September 28, 2011