Rules of Behavior for the Federal Docket Management System (FDMS)

These Rules are intended to supplement Agency mandatory computer use Rules of Behavior.

Security Rules of Behavior for FDMS	
1. Access	Users shall access and use only information for which they have official authorization.
2. Accountability	Users shall be accountable for their own actions and responsibilities related to information resources entrusted to them.
3. Confidentiality	Users shall protect controlled unclassified information (CUI) from disclosure to unauthorized individuals or groups. Users shall protect Privacy Act Information (personal information about individuals).
4. Integrity	Users shall protect the integrity or quality of information.
5. Availability	Users shall protect the availability of information or systems.
6. Passwords and User-IDs	Users shall protect information security through effective use of user IDs and passwords.
7. Software	Users shall use software in a safe manner that protects it from damage, abuse, and unauthorized use.
8. Awareness	Users shall stay abreast of security policies, requirements, and issues. Users shall successfully complete required annual agency security training.
9. Reporting	Users shall promptly report security violations and vulnerabilities to proper authorities.

General Use Rules:

- Do not leave information on your desk or your screen while away from your desk.
- 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 log on using your user ID and password.
- To prevent unauthorized use on your PC, log off whenever you will be away from your PC for an extended period of time.
- Use a screen saver with a password.

Password Rules:

- Do not share your password with anyone.
- Password requires 12-20 characters with at least: one upper case letter, one lower case letter, one number, and one of the following special characters: ~ ! @ # $ % & * = + < > / ?
- Try to create a complex password (do not use common English dictionary words).
- Do not use family names, birthdays or other easily solved passwords.
- Password must be changed every thirty days.
- Password should be memorized, not written down.

Rules for Using Controlled Unclassified Information (CUI):

- Do not leave information on your desk or your screen while away from your desk.
- Ensure that only authorized personnel are allowed to view Controlled Unclassified Information (CUI) on your desk or your computer screen.

Rules for Accountability:

- Behave in an ethical and trustworthy manner.
- Do not attempt to perform actions or processing for which you do not have authorization.
- Be alert to threats to Federal Agency applications and data.
- Logout and turn off your computer at the end of the workday.
- Report any potential security violations to your manager immediately.