

## Appendix A: Rules of Behavior

### Rules of Behavior

---

<b>Security Rules of Behavior</b>	
1. Official Business	Employees shall use FOIAonline 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.
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 or quality of information.
6. Availability	Employees shall protect the availability of information or systems.
7. Passwords and User-IDs	Employees shall protect information security through effective use of user IDs and passwords.
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.
11. Reporting	Employees shall promptly report security violations and vulnerabilities to proper authorities.

## **Rules of Behavior - Continued**

### **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 logon 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.

Shred all unneeded sensitive documentation.

Mark all sensitive documentation.

### **Password Rules:**

Do not share your password with anyone.

Password should be at least 8 characters long, include at least 1 number (but not in the first position), 1 uppercase letter, 1 lowercase letter and 1 special character. Try to create complex password (do not common English dictionary 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.

## **Rules of Behavior - Continued**

### **Rules for Using Confidentially-Sensitive Data:**

Do not leave information on your desk or your screen while away from your desk.

Ensure that only authorized personnel are allowed to view confidential data on your desk or your computer screen.

Use a screen saver with a password.

Position computer screens away from doors, windows and heavy traffic areas.

### **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 your agency's applications and data.

Logout and turn off your computer at the end of the workday.

Report any potential security violations to your manager immediately.