

- 1) To whom is the FSA Information Security and Privacy Policy document applicable?
 - a. Police officers, dentists, and taxi drivers
 - b. FSA employees and contractors
 - c. FSA employees and school officials
 - d. Only FSA employees
- 2) How can an exemption from an FSA IT Security and Privacy policy be created?
 - a. The System Owner must approve the exemption in writing and notify the CSO
 - b. The System Security Officer must approve the exemption in writing and notify the System Manager
 - c. The System Owner must approve the exemption in writing
 - d. President Bush must approve the exemption in writing and notify the First Lady
- 3) How often should workstation passwords be changed?
 - a. At least every 30 days
 - b. At least every 60 days
 - c. At least every 90 days
 - d. Passwords need to be changed?
- 4) What should you do if you suspect a security weakness in an FSA system?
 - a. Prove the weakness exists
 - b. Call the National Guard
 - c. Notify the System Manager and/or System Administrator
 - d. Send an email message to the FBI
- 5) When should FSA identification badges be worn at work?
 - a. Only when entering or exiting the UCP facility
 - b. Badges? We don't need no stinking badges!
 - c. Only in high security areas
 - d. At all times, regardless of the areas sensitivity
- 6) What must be verified before an System Security Officer may grant access to a user? (Choose all that apply)
 - a. The user has authorization from the system owner to access the system
 - b. The level of access is appropriate for the user's business purpose.
 - c. The access will not compromise segregation of duties
 - d. The user has a valid Social Security Number
- 7) What is the minimum length for a password?
 - a. 4 characters
 - b. 6 characters
 - c. 8 characters
 - d. 10 characters
- 8) What is required before a user may install personal software on an FSA computer for processing FSA business?
 - a. Document each instance and inform the supervisor in writing
 - b. Verbally inform the supervisor
 - c. Register the software in the Federal Register
 - d. Document each instance

- 9) What information is not required to be stored in an audit trail?
- a. Type of event
 - b. User ID associated with the event
 - c. When the event occurred
 - d. Name of the person accessing the system
- 10) A Rules of Behavior document must include which of the following? (Choose all that apply)
- a. Consequences for violating the rules of behavior
 - b. Protection of Privacy Act information
 - c. Individual accountability
 - d. Who yields at a four-way stop
- 11) (T/F) In general, users can access systems without filling out appropriate background clearance forms.