Information Security Awareness: Exam 1

1. Which of the following is NOT something privileged account holders are required to do?
   ○ a. Abide by the provisions of the USDA IT/IS Rules of Behavior for General Users except those variations required to perform authorized privileged user activities.
   ○ b. Limit the performance of privileged user activities to privileged user account(s).
   ○ c. Consent to monitoring and search of any IT/IS equipment used while in or brought into or removed from USDA owned, controlled, or leased facilities.
   ○ d. Change the privileged user account password every sixty (60) days, or as required for security reasons.
   ○ e. None of the above.

2. Edna wants to create a strong password. She should avoid all of the following except:
   ○ a. Family or pet names
   ○ b. Birthdays
   ○ c. Special characters
   ○ d. Sports teams

3. Which term refers to a secure systems ability to protect against the unauthorized modification or destruction of information?
   (circle one)
   ○ a. Confidentiality
   ○ b. Availability
   ○ c. Integrity
   ○ d. Nonrepudiation

4. This high-tech scam that uses email or web sites to deceive you into disclosing your credit card numbers, bank account information, Social Security Number, passwords, or other sensitive information is known as:
   (circle one)
   ○ a. Spyware
   ○ b. Social engineering
   ○ c. A virus
   ○ d. Phishing
5. For Official Use Only (FOUO) and Controlled Unclassified Information (CUI) may include all of the following except: (circle one)
   - a. Secret information
   - b. Personnel information
   - c. Payroll information
   - d. Sensitive information

6. Denise found a volume of documents in the trash bin that contained individuals, names, social security numbers and years of birth. After additional inspection, she realized it was an extra report from one of their file systems that had been discarded. What should Denise do? (circle one)
   - a. Contact the Freedom of Information Act Officer for the agency.
   - b. Submit an agency trouble ticket.
   - c. Contact the PII Hotline number and report to Information Security Center.
   - d. Contact her agency Privacy Officer and Information Systems Security Program Manager.
   - e. Selection A and B
   - f. Selection C and D
   - g. Selection B and D
   - h. All of the above

7. Protecting your identity is essential, even on your personal or home computer. You should consider doing all of the following except: (circle one)
   - a. Respond to emails asking you to verify your personal information.
   - b. Ask how information will be used before giving it out.
   - c. Pay attention to credit card and bank statements.
   - d. Avoid common names/dates for passwords and PINs.
8. Which of the following vulnerabilities is most likely to be exploited by an external threat to the infrastructure? (circle one)
   ○ a. Floods
   ○ b. Software flaws
   ○ c. Insufficient cooling
   ○ d. Disgruntled employees

9. Cookies contain information about you. This information, if not encrypted, could be viewed by a third party. The best practice to prevent this from happening is: (circle one)
   ○ a. Visit only web sites that use ActiveX or JavaScript code
   ○ b. Do not visit non-government web sites
   ○ c. Ensure your browser is set to not accept cookies.
   ○ d. Install spyware software

10. All of the following are examples of malicious code except: (circle one)
    ○ a. Cookies
    ○ b. Viruses
    ○ c. Trojan horses
    ○ d. Worms

11. Which of the following will help reduce your risk of identity theft when engaging in e-commerce? (circle one)
    ○ a. Confirm the site you are using uses an encrypted link.
    ○ b. Respond to email inquiries only from institutions you do business with regularly.
    ○ c. Use e-commerce for all transactions.
    ○ d. Click on links sent to you from trusted providers.
12. To keep your mobile device secure, you should do all of the following except: (circle one)

- Download apps from unknown app stores.
- Set a personal identification number (PIN) or password on your phone’s home screen.
- Do not open unsolicited email messages.
- Do not open or follow links in unsolicited text messages.
- Keep your mobile device updated and patched to the latest revisions.

13. Unlocking your smart phone removes security protections that protect your mobile device from malicious applications. (select True or False)

- TRUE
- FALSE

14. To ensure the physical security of USDA information, you should do all of the following except: (circle one)

- Allow people to enter the facility by following others.
- Secure your office at night and during emergency procedures.
- Know your organization’s security policy.
- Challenge people who don’t follow physical security policies.