

# Monthly Quizzes

## January Quiz

1. T F The more difficult the password the better.
2. T F Pneumonic aids can help in remembering passwords.  
**True** - pneumonic aids can be a big help in remembering password. For instance, a password such as "**MHALLWFWAWAS**" would be difficult to remember but a pneumonic such as "*Mary Had A Little Lamb Whose Fleece Was As White As Snow*" Would make remembering this password a lot easier.
3. T F Electronic Dictionaries can be adapted to identify passwords.
4. T F DOM required to keep your password a secret except for sharing it with your supervisor.
5. T F CDs can be cleaned with soapy water or solvents.
6. T F Fingerprints on the recording surface of a CD will make it unreadable.
7. T F I am allowed to make copies of Company licensed software for home use if I will be working on Company work.
  - A. Yes, provided I only use it for Company work
  - B. Yes, provided I delete the software from my home computer when the Company work is completed.
  - C. Not unless I get written approval from the vendor.
  - D. No, It is against COMPANY policy to copy Company Licensed software.
8. T F How can I protect my password?
  - A. Change your password every two years.
  - B. Use a long word with an embedded numeric
  - C. Write down the password so you won't forget it and tape it to the underside of the telephone handset
  - D. To make it easy for you to remember the password, use a family members name

E. All of the above

9. T F All bulleting Boards and Internet sites are free of viruses. Viruses can only be sent by E-mail.

10. T F Unauthorized access to a computer by using another persons USER-ID is reportable using an Incident Report

11. It is OK to leave confidential information on a desk in the administrative Building?

A. The administration Building is not in a secure area so there is not a problem.

B. Only Office staff are in the administrative building so security is not an issue.

C. Non-company employee's work throughout the company, therefore confidential information should never be left where it can be seen by anyone.

D. If the administrative area is not associated with an outside contractor it is OK to leave confidential on your desk.

E. None of the above.

### Answers to December quiz

1. T F Supervisors should require that passwords and logons be written down and placed in a vault place in case the employee is out ill.

**False - Passwords should not be written down anyplace. If a supervisor needs to logon to a computer of an employee who is out ill they should call an ASIA to establish a temporary password. The temporary password should be change immediatly on the employee's return.**

2. T F Passwords that are 3 to 5 characters in length are considered secure.

**False - Anything less than six characters is not considered secure. An industry recommendation for a secure password is eight characters and includes a numeric or special character. Industry also found that people will resist anything more than eight characters.**

3. T F Passwords should be comprised of both upper and lower case letters.

**True - It is true that mixed upper and lower will make a stronger password. However, mixing upper and lower case letters tends to cause typing errors. A password of 8 or more characters in either upper or lower case character is sufficient for most purposes.**

4. T F When changing passwords it is OK to repeat the same password every third time it is changed.

**False - No, a repetition cycle of three months is a fairly recognizable pattern. Most large systems will require you to use at least twelve different passwords before a password can be repeated.**

5. T F A good password to use is the same numeric character so long as it is more than 7 characters in length (i.e. 99999999).

**False - Entering a password by striking the same key six or seven times is not a very good password. It is simply too easy to determine the password by simply looking or listening. Testing repetitive character strings is one of the first tests a cracker will try.**

6. T F If my computer won't boot up I should call the Help Desk immediately.

**False - Well, almost immediately, first check to see if the power cord is plugged into the wall socket, and then check to make sure that a circuit breaker has not tripped. If everything is OK then call the help Desk.**

7. T F Refrigerator magnets and magnets on flashlights are too weak to harm data on a diskette.

**False - It depends on how far away from the diskette and how long they are there. If the magnet were lying on top of a diskette for a few hours I wouldn't bet the diskette is readable.**

8. T F Very strong magnets cannot erase data on a CD.

**True - The recording media on CD's is not magnetic so a magnet no matter how strong will not affect it.**

9. T F I can leave the same image on my computer monitor all day without harming the monitor.

**True - But if you leave the same image on the monitor for weeks at a time you run the risk of burning the image on the screen permanently.**

10. T F Modems can be moved from computer to computer without any special software.
- False - Modem requires software to operate properly. Simply moving the modem to another computer will not work without loading the software. To move a modem call the help Desk.**
11. T F The surface of a CD can be scratched without loss of data.
- False - Scratches can cause the CD to be skip or be unreadable. The scratch causes the laser beam to reflect off the surface rather than the data.**
12. T F E-mail is not as confidential as the mail handled by the U.S. Postal Service.
- True - The U.S. Postal Services is required to provide privacy of mail by an act of congress. No such legislation applies to e-mail or other mail carriers.**
13. T F I can say anything I want in my e-mail since the only person who will be seeing it is the person I am sending it to.
- False - Once you press the send button you have no control over who will see your e-mail. Your mail can be forwarded to all over the world and you would be powerless to stop it. Common sense dictates that you should write your e-mail in a professional manner.**
14. T F I don't have to worry about making e-mail look professional since it is considered as a casual way of communicating.
- False - You should be careful about making your email look professional. Those who see your e-mail will be drawing conclusions about you based on what they see. If your e-mail looks unprofessional you will judged as unprofessional.**
15. T F If after sending my e-mail I erase the message from my computer and the person I send the message to erases the message no one else will ever see it.
- False - For the protection of the user, servers that handle e-mail make backup copies of all e-mail. The backs up copies are sometimes kept for years. Examples of old e-mail resurfacing are the Microsoft antitrust action and the Iran Contra Investigation in Washington.**
16. T F The Company does not have a right to read my e-mail without a court order.

**False - The Company has every right to read your e-mail. The system belongs to COMPANY and only Company's business is to be conducted on its e-mail system. This does not mean that COMPANY reads all e-mail, only that COMPANY has the right to. If an incident occurred that required an investigation by your manager or Internal affairs it is reasonable to believe that they would look at any e-mail that might have a bearing on the investigation.**

17. T F The courts have said that all mail, including e-mail, is considered as private.

**False - The courts have held that e-mail systems are not covered by the same legislative act that covers the U.S. Postal System.**

18. T F It is considered good manners to write an e-mail message in all uppercase letters.

**False - In the electronic world a message that is written all in upper case is considered the same as shouting. Additionally, it is difficult to read.**

19. T F All Company information is public.

**False - The vast majority of information is public however the Records Management Act describes which information is confidential, when, and to whom it may be disclosed.**

### **Answers to November quiz**

1. T F Unit supervisors or their designee have responsibility for modems under their control

**True - User Responsibility: Unit supervisors or their designee have authority for modems under their control, and shall limit access to such modems to ensure their security at all times.**

2. T F It is recommended that a log be kept of modem use.

**True - User Responsibility: It is recommended that a log be kept for each modem itemizing usage by date, transmitting user, start time, time signed off, software used, data transmitted, and line speed.**

3. T F Each facility and Facility manager is to develop a policy to ensure the security of modems.

**True - Modem Security Policy within COMPANY:**

**(1) All modems are safeguarded when in use and protected from unauthorized access when not in use.**

**(2) The physical location of each modem is tracked at all times.**

**(3) An onsite evaluation of modem use is performed no later than 90 days after installation of each modem installed in the facility.**

4. T F When changing passwords it is OK to repeat the same password every third time it is changed.

**False - No, a repetition cycle of three months is a fairly recognizable pattern. Most large systems will require you to use at least twelve different passwords before a password can be repeated.**

5. T F A good password to use is the same numeric character so long as it is more than 7 characters in length (i.e. 99999999).

**False - Entering a password by striking the same key six or seven times is not a very good password. It is simply too easy to determine the password by simply looking or listening.**

6. T F It's OK to logon a terminal with my password in the morning and let my colleagues use the terminal anytime that they need to.

**False - No, The purpose of a unique logon and password is to identify you to the system and to provide accountability. If you logon to your system and allow others to use it you will be held accountable for any inappropriate activity that takes place on that terminal.**

7. T F It's OK to write down logons and passwords of my colleagues in a book in case someone is ill so long as I lock the book in my desk.

**False - No, you do not share your logon or password with anyone, that includes your supervisor. If your supervisor needs to get into your system when you are ill or on vacation they can go to the Help Desk and establish a new password that is then assigned to them.**

8. T F It's OK to use consecutive letters on the keyboard so long as the letters are random, as an example, QWERTY would be a good password.

**False - No, although the letters are alphabetically random they are consecutive on the keyboard. They are also easy to spot if you watch someone enter them on a keyboard.**

9. T F Any Operator who uses CLETS to make only inquires into the system requires one hour of training.
- False - Anyone who intends to use the CLETS system to make inquires must within six (6) months of appointment, receive four (4) hours of agency provided lecture and completion of a less than full Access Operators Workbook. Recertification: Every two (2) years, and within the DOJ windows of recertification completion of a Less than Access Operator Proficiency Exam.**
10. T F Very strong magnets can erase data on a CD.
- False - The recording media on CD's is not magnetic so a magnet not matter how strong will not affect it.**
11. T F Frayed power cords are not a danger if they are not near water or other liquids.
- False - Frayed power cords are dangerous at any time. If you have a frayed power cord call the Help Desk for a replacement immediately.**
12. T F I can leave the same image on my computer monitor all week
- True - But If you leave the same image on the monitor for weeks at a time you run the risk of burning the image on the screen permanently.**
13. T F Modems can be moved from computer to computer without any special software.
- False - Modem requires software to operate properly. Simply moving the modem to another computer will not work without loading the software. To move a modem call an ASIA.**

#### Answers for October Quiz

1. T F As long as I don't share my password I don't need to change it.
- False - No, passwords tend to become known over time even if we don't intentionally mean to share them.**
2. T F I can be held responsible for anything that happens if someone else used my password.
- True - the system only knows you by your logon and password. If someone else used your logon and password the systems thinks it is you and any inappropriate action is attributed to you.**

3. T F A good password to use is the same numeric character so long as it is more than 7 characters in length (i.e. 99999999).
- False - Entering a password by striking the same key six or seven times is not a very good password. It is simply too easy to determine the password by simply looking or listening.**
4. T F It's OK to logon a terminal with my password in the morning and let my colleagues use the terminal anytime that they need to.
- False - No, The purpose of a unique logon and password is to identify you to the system and to provide accountability. If you logon to your system and allow others to use it you will be held accountable for any inappropriate activity that takes place on that terminal.**
5. T F If I drop water on the magnetic surface of diskette I can just wipe it off with my finger.
- False - No, using your fingers to wipe away water may remove the water but it will leave oil from your fingers. Use a very soft cloth to blot the water off the surface.**
6. T F CDs can be cleaned with mild soapy water, rinsed, and dried with a soft cotton cloth.
- True - CD's are made of plastic and are read using a laser beam. They can be washed provide use a soft cloth to gently wipe them dry**
7. T F Fingerprints will not harm the magnetic surface of a diskette.
- False - Fingerprints on the recording surface of a magnetic media can make it unreadable.**
8. T F The tray for CDs cannot be used as a cup holder if it isn't being used to play a CD.
- True - The CD tray is not a cup holder, it is much too fragile.**
9. T F Surge protectors will help prevent the loss of information if we have a spike in the power or unexpected loss of power.
- False - Surge protectors will help protect your system in the event of spike in the electrical power, they will not protect you system in the event of a power loss. For power loss protection you will need an Un-interruptable Power Supply (UPS)**
10. T F E-mail is as confidential as the mail handled by the U.S. Postal Service.

**False - The U.S. Postal Services is required to provide privacy of mail by an act of congress. No such legislation applies to e-mail.**

11. T F I can say anything I want in my e-mail since the only person who will be seeing it is the person I am sending it to.

**False - Once you press the send button you have no control over who will see your e-mail. Your mail can be forwarded to all over the world and you would be powerless to stop it. Common sense dictates that you should avoid foul language. Be careful in what you say in e-mail, you really don't know who will be reading it.**

12. T F I don't have to worry about making e-mail look professional since it is considered as a casual way of communicating.

**False - You should be careful about making your email look professional. Those who see your e-mail will be drawing conclusions about you based on what they see. If your e-mail looks unprofessional you will be judged as unprofessional.**

13. T F Passwords should be comprised of both upper and lower case letters.

**True - It is true that mixed upper and lower will make a stronger password. However, mixing upper and lower case letters tends to cause typing errors. A password of 8 or more characters in either upper or lower case character is sufficient provided it contain a numeric or special character.**

14. T F Special characters such as a period(.) or / can be imbedded in a password.

**False - No, these particular characters are reserved for systems use.**

15. T F A good way to pick a password is to randomly pick a word out of the dictionary.

**False - A common practice among those seeking to break passwords is to use an electronic dictionary in searching for the correct password.**

16. T F All Company information is public.

**False - The Records Management Act describes which information is confidential. All other information is public.**

## Answers for September Quiz

1. T F You are not allowed to use Company owned equipment at home.  
**False - You are allowed to use Company owned equipment at home provided you obtain approval from your manager or supervisor.**
2. T F You are not allowed to work on confidential information at home.  
**False - You are allowed to work on confidential information at home provide you apply the appropriate security controls.**
3. T F System access cannot be protected when using a terminal.  
**False - log-off when you leave your immediate work area. Do not leave an unattended terminal.**
4. T F Use of the Internet can be used for any kind of research, including viewing anti-government sites.  
**False - Access to erotic, sexually oriented, or anti-government sites is prohibited.**
5. T F To completely erase you only have to delete the file.  
**False - Deleting a file only erases the address of the data. To totally erase the data you have to overwrite it.**
6. T F To pass along a diskette to that once contained confidential information you must first do a quick format.  
**False - A quick format only erases the addresses of data, just as pushing the delete key does. You still must overwrite the data.**
7. T F If the system administrator calls asking for my password for system maintenance it is OK to give it to him.  
**False - No, It is never OK to give your password to anyone.**
8. T F Social engineering is the intentional manipulation of an individual into believing that the caller is authorized and entitled to receive information.  
**True - Social engineers can be very convincing. Be careful of people calling asking for confidential information if there is any doubt ask for their name and phone number. If you believe some one is using social engineering tell your supervisor.**

9. T F It is OK to be casual in your e-mail.

**False - You should not be casual when writing e-mail because once you send it you have lost all control over who will see it. What ever you write can reflect on you.**

10. T F E-mail is private just as any other mail.

**False - E-mail is not private. The privacy of e-mail is governed by the policies of the organization you work for.**

11. The Company telephone system is owned by the Phone Company and telephone security is their problem.

- A. The Company telephone system is owned by the phone company but telephone security is managed by the Company.
- B. The Company owns the Company telephone system but the Phone Company manages telephone security.
- C. The Company owns the Company telephone system and telephone security is a Company problem.
- D. Telephone security is not a serious problem.
- E. None of the above.

**Ans: C The Company telephone system is owned by the Company and telephone security is a Company problem.**

12. Are cell phones safe?

- A. Yes, all cell phones use radio signals that can't be listened to.
- B. Yes, confidential information can be safely disclosed over a cell phone.
- C. No, cell phones are used all anywhere you are never sure someone is not overhearing your conversation.
- D. No, all telephone conversations can be picked up by radio frequency scanner.
- E. None of the above.

**Ans: C No, cell phones are used everywhere. You are never sure someone is not in a position to overhearing your conversation.**

13. Having Visitors in the work area are OK, right?

- A. Only relatives that you can rely on to keep information confidential.
- B. With former COMPANY employee's information security is not a concern.

- C. Consultant and contractors that have been hired by the Company are cleared to view confidential information.
- D. Former coworkers that have transfer to another unit have been cleared to receive information.
- E. None of the above.

**Ans: E None of the above. Unless the person is a current worker in your unit they are not cleared to receive confidential information.**

**14.** How can I protect the information in my office?

- A. Back up your information daily.
- B. Clear your desk at the end of the day.
- C. Dispose of confidential or sensitive information properly.
- D. Never leave a terminal unattended.
- E. All of the above.

**Ans: E All of the above.**

**15.** Are there Legal reasons for protecting Information?

- A. Yes, the Company Policy provides for individual privacy.
- B. Yes, It is COMPANY policy to protect confidential information.
- C. Yes, The Records Management Act requires the confidentiality of certain information.
- D. Yes, Violation of individual privacy is a violation of certain Federal Laws.
- E. All of the above.

**Ans: E All of the above**

**16.** The consequences of information security violations:

- A. Written reprimand
- B. Suspension with out pay.
- C. Reduction in pay.
- D. Demotion
- E. All of the above.

**Ans: E All of the above. Any of the above adverse actions may be taken.**

### **Answers for August Quiz**

1. T F Do not write down you password and lock it in your desk.  
**True - Do not write down your password. Pick a password that you can remember without writing it down.**
  
2. T F With respect to viruses, it is safe to download software from bulletin Boards and off the Internet.  
**False - It is not safe to download software off of the Internet or Bulletin Board. If you do, download the program to a disk then subject the disk to a virus scan.**
  
3. T F If you detect a virus in your computer attempt to remove it yourself, if you can't call an ASIA.  
**False - Call the help desk or Security immediately, do not try and remove it yourself.**
  
4. T F Reportable security incidents of destruction, damage include deliberate, or through negligence, damage to or destruction of manual or computerized information.  
**True - Damage or destruction of manual or computerized information that occurs through deliberate actions or negligence are reportable.**
  
5. T F It is the policy of the Department that the incidents, such as, incidents involving a virus or other such malicious computer code should be reported to the ISO through the chain of command.  
**True - Policy does require incident of virus or virus or malicious code be reported to the ISO.**
  
6. T F Unauthorized Access to computer via another persons USER-ID is reportable.  
**True - Use of a computer system, which is logon with another users ID, is reportable. Anytime an employee uses a computer that has been logged on under another persons ID they are making an unauthorized access.**
  
7. T F An unauthorized access is access by a person whose job duties do not require such access.

**True - If your job duties do not require specific access to COMPANY information assets you are not authorized.**

8. Microcomputer that are used by inmates can't be used for any other purpose unless:

- A. The authorized for inmate use is removed.
- B. Communication is added to the computer.
- C. The computer is removed from the secured area.
- D. Until the help Desk reformats all the storage, reload need software, puts a new authorization label on it, and certifies it for general use.
- E. All of the above.

**Ans: D Until the help Desk reformats all the storage, reloads needed software, puts a new authorization label on it, and certifies it for general use.**

9. It is OK to use any group of characters, as long as:

- A. More than three characters and a number are used.
- B. The only criteria is that the password is eight characters in length.
- C. Names of pets are OK as passwords.
- D. Words like QWERTY or 66666666 are OK long as they are eight characters in length.
- E. None of the Above

**Ans: E None of the above. A password should be at least six characters in length and contain a number or none reserved special character.**

13. It is all right to give my password to another trusted friend.

- A. It's never all right to give my password to anyone.
- B. It's OK if supervisor asks for my logon and password in case I am sick.
- C. It's OK to share my password with my coworkers provided we are in a locked secure area, such as, records.
- D. I cannot be held responsible for anything that happens if someone else uses my password.
- E. None of the above.

**Ans: A It's never all right to give my password to anyone.**

**14.** It is OK to leave confidential information on a desk in the administrative Building?

- A. The administration Building is not in a secure area so there is not a problem.
- B. Only Office staff are in the administrative building so security is not an issue.
- C. Contractors work throughout the institution, therefore confidential information should never be left where and contractor can view it.
- D. If the administrative area is not associated with a contractor it is OK to leave confidential on your desk.
- E. None of the above.

**Ans: C It is never OK to leave confidential information out where a curious inmate or parolee can view it in any building regardless of the location.**

**15.** Can I bring my home computer to the office?

- A. Yes, if you insure it.
- B. Yes, the Company will insure it.
- C. Provided you lock it inn your car when not using it.
- D. Yes, provided it does not have a modem.
- E. None of the above.

**Ans: E It is not recommended, since the Company does not assume any liability for personal property brought to the job site.**

### **Answers for the July Quiz**

**Select the most correct answer.**

**1.** The key to good information security is:

- A. Security awareness training.
- B. Good technical security (firewalls, virus scans, etc).
- C. Good passwords.
- D. Employee awareness

E. All of the above.

**Ans: D. All of the above**

2. Practices for backing up data that everyone should follow:

A. Back up data when it is changed, daily if necessary.

B. Keep back up diskette in your desk in case it is needed.

C. It is not necessary to test backup diskettes

D. It is only necessary to keep one generation of backed-up data [i.e. 1 days worth]

E. All of the above.

**Ans: A. Back up data when it is changed, daily if necessary.**

3. What data should I backup?

A. Data that you can't afford to lose.

B. Only when there are large volumes of data.

C. Only when the original documents are not available.

D. Only when the time to recreate the file would require a lengthy period of time.

E. All of the above.

**Ans: A. Data that you can't afford to lose.**

4. What are the symptoms of a virus?

A. Unusual error messages appear.

B. Files change size, date, and content.

C. Disk access seems excessive for simple tasks

D. All of the above.

**Ans: D. All of the above.**

5. All viruses must be sent as executable files.

A. Yes, all virus must be sent as executable files

B. No, some viruses can be sent as attachments to e-mail.

C. Viruses that are in attachments are not executable.

- D. All viruses are designed to cause damage to files.
- E. All of the above.

**Ans: B. No, some viruses can be sent as attachments to e-mail.**

6. Steps that can be taken to reduce the chance of getting a virus.
- A. Update you virus-scanning software at least once a year.
  - B. Make periodic backup copies of your files.
  - C. Avoid using "shareware or freeware"
  - D. Set virus scanning software to search only files with and EXE extension.
  - E. All of the above

**Ans: C. Avoid using "shareware or freeware"**

7. Can I make copies of Company-licensed software?
- A. Yes, provided I only use it at home
  - B. Yes, provided I only use it for Company work.
  - C. Not unless I write to the vendor and get an OK for home use.
  - D. No, it is against COMPANY policy
  - E. All of the above.

**Ans: D. No, it is against COMPANY policy**

8. Can I make copies of software that I wrote?
- A. No, Yes if you wrote the entire program.
  - B. B Not if it is being used by the Company
  - C. Not it you wrote it at work.
  - D. Only it does not pertain to any Company operation.
  - E. All of the above

**Ans: C. Not it you wrote it at work.**

9. How can I protect my password?
- A. Change your password frequently, at least every 90 days.
  - B. Use a long word (8 or more characters) found in the dictionary.

- C. Write it down and tape it to the bottom of your keyboard.
- D. Make it easy for you to remember, use your children's or husband's name.
- E. All of the above.

**Ans: A. Change your password frequently, at least every 90 days.**

### **Answers for June Quiz**

1. **T F** Following an Information Security incident, the incident must be reported to the Information Security Officer within 10 working days.  
**False - The following information concerning each incident shall be reported to the department ISO within five working days of any awareness of the occurrence of the incident."**
2. **T F** Once a new system is fully developed and is ready for implementation an Information Security layer must be added.  
**False -By establishing security requirements as an integral part of system development process, system designers, with the help of the information system coordinators (ISC) can insure that adequate information security is always provided."**
3. **T F** The owners of information are responsible for classifying, defining precautions of it's integrity, disposing of information, defining level of access, and identifying the levels of acceptable risk.  
**True The owners of information are responsible for classifying the information, defining precautions for its integrity, disposing of the information, defining initial level of access need, filing security incident reports, securing signed agreements and forwarding then to the Access Management Group (AMG), and identifying for the ISO the level of acceptable risk."**
4. **T F** Separation of duties is a concept which refers to fiduciary responsibilities not information security.  
**False -Segregation of duties, similar to that required in manual systems shall be implemented in computerized systems."**
5. **T F** For administrative purposes, all information residing on Company's computers that is considered sensitive or confidential shall be treated as such by those who periodically use it.

**False For administrative purposes, all information residing on Company's computers that is considered to be sensitive or confidential, shall be treated as such by all persons who have access to it and shall be protected from unauthorized access."**

12. T F No confidential information or sensitive information shall be faxed, reproduced, operated on within email or transmitted by telephone to any entity without appropriate security controls in place.

**True - Additionally, no confidential or sensitive information shall be faxed, reproduced (e.g. photocopied) operated on within email or transmitted by telephone to any entity without appropriate security controls in place."**

13. T F User ID's shall never be shared.

**True User IDs shall never be shared.**

14. T F The password owner shall not leave an active terminal session.

**False. Not leave an active terminal session."**

15. T F If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to their Security

**False If anyone asks for a password, the owner shall refuse to provide it and shall refer the person to a supervisor.**

16. T F All employees are accountable for the implementation of information security policies and procedures within their areas of responsibility.

**True - All employees are accountable for the implementation of information security policies and procedures within their areas of responsibility.**

17. T F Dialup access to Company's mainframe is not allowed.

**True -Dialup access to the Department's mainframe database is not allowed.**

18. T F All persons who have access to any COMPANY information shall be provided security awareness training at the time such access begins, and at least bi-annually thereafter.

**False All persons who have access to COMPANY information shall be provided security awareness training at the time of such access begins, and at least annually thereafter.**

19. T F Decentralized terminals (and as much as possible all terminals) shall be locked, the keys removed, and the screen intensity turned all the way down (or off) when the terminal is unattended.

**True Decentralized terminals (and as much as possible, all terminals) shall be locked, the keys removed and the screen intensity turned all the way down when the terminal is unattended.**

20. T F Backup files of confidential data shall be maintained in a locked cabinet away from the location of the microcomputer containing the program providing access to such files.

**True Backup files of confidential data shall be maintained in a locked cabinet away from the location of the microprocessor containing the program providing access to such files.**

### Answers for the May Quiz

1. T F All Company information is public.

**False - The Records Management Act describes which information is confidential. All other information is public.**

2. T F Sensitive and confidential information can be disposed of by tearing the pages in half and putting them in the trash.

**False - All departments have containers especially for recycling paper. The Company contracts with recyclers that are certified to handle confidential information. Some departments require that confidential information be run through a shredder before placing in a recycling bin. Never just throw confidential information in the trash.**

3. T F Diskettes and CDs can be destroyed by simply putting them in the trash. They will be buried at the dump.

**False - Information on diskettes and CDs is not destroyed when buried in a dump. Anyone finding the CDs or Diskettes may be able to clean them sufficiently to retrieve the information.**

4. T F Reformatting hard disks erases all the data that was on the diskette.

**False - Reformatting a disk erases the main address file (FAT file) on the disk, not the data. There are programs that can**

**read the erased area of the disk and make the information readable.**

5. T F Completed travel expense forms are considered confidential.
- True - Travel expense forms are considered as confidential. They contain name and address, social Security number, and the amount of money that is to be reimbursed. All together this information is considered as confidential.**
6. T F Recycled paper is processed by a company that has been certified to handle confidential information.
- True - The Company contracts with recycling companies that are certified to handle confidential information.**
7. T F Computer printouts should be considered as confidential and disposed of in recycle bins.
- True - Quite frequently computer printouts carry confidential information. Unless you are absolutely sure that the information is not confidential make sure they go in the recycle bin. Also, computer printouts are printed on a higher quality paper that gets a higher price from the recycler.**
8. T F Sensitive information may or may not be confidential.
- True - Sensitive information may be either Confidential or public information.**
- 9 T F When we talk about the confidentiality of information we are referring to the manner of disclosure.
- True - Privacy of information refers to the issues surrounding the disclosure of information.**
10. T F When we say that information is "sensitive" we are saying that because of the nature of the information it requires a greater degree of protection.
- True - When we say that information is "sensitive" we are saying that because of the nature of the information it requires a grater degree of security.**
11. T F When information is copyrighted it is the same thing as saying that it is confidential.
- False - Copyright refer to ownership of the information or intellectual property and how the information can be used. For**

**instance, books have a copyright and they are not confidential, but you must have to have permission of the owner to reprint the book or any part of the book.**

12. T F Security of information and privacy of information mean the same thing; that is, information that cannot be shown to a third party without permission.

**False - Security refers to how information will be protected. Privacy refers to the disclosure of information.**

13. T F Confidential information and private information mean the same thing when it comes to how the information will be disclosed.

**False Confidential information refers to information restricted to the use of a particular person, or group.**

14. T F All e-mail is private.

**False - There is no privacy of email. An individual may consider e-mail as private, which is not the same thing as saying that there is privacy of e-mail. It is important to understand the distinction.**

### March

1. T F It is OK to put my coffee cup on the computer so long as I don't spill it.

**False - NO! No! no!, The oils, acids, sugar, cream in coffee can cause damage and are extremely difficult to remove if it should spill. Even if you are very careful others are not.**

2. T F If I drop water on the magnetic surface of diskette I can just wipe it off with my finger.

**False - No, using your fingers to wipe away water may remove the water but it will leave oil from your fingers. Use a very soft cloth to blot the water off the surface.**

3. T F CDs can be cleaned with mild soapy water, rinsed, and dried with a soft cotton cloth.

**True - CD's are made of plastic and are read using a laser beam. They can be washed provide use a soft cloth to gently wipe them dry**

4. T F Fingerprints will not harm the magnetic surface of a diskette.

**False - Fingerprints on the recording surface of a magnetic media can make it unreadable.**

5. T F The tray for CDs can be used as a cup holder if it isn't being used to play a CD.

**False - No! The CD tray is not a cup holder.**

6. T F Surge protectors will help prevents the loss of information if we have a spike in the power or unexpected loss of power.

**False - Surge protectors will help protect your system in the event of spike in the electrical power, they will not protect you system in the event of a power loss. For power loss protection you will need an Uninterruptible Power Supply (UPS)**

7. T F If I spill a can on soda on the keyboard it might be a little sticky but it will not hurt it.

**False - Not only will the keyboard be sticky, but it is doubtful that it will ever work properly again.**

8. T F If my computer won't boot up I should call the ASIA immediately.

**False - Almost immediately, first check to see if the power cord is plugged into the wall socket, and then check to make sure that a circuit breaker has not tripped. If everything is OK then call an ASIA.**

9. T F Refrigerator magnets and magnets on flashlights are two weak to harm data on a diskette.

**False - It depends on how far away form the diskette and how long they are there. If the magnets were lying on top of a diskette I wouldn't bet the diskette is readable.**

10. T F Very strong magnets can erase data on a CD.

**False - The recording media on CD's is not magnetic so a magnet not matter how strong will not affect it.**

11. T F Frayed power cords are not a danger if they are not near water or other liquids.

**False - Frayed power cords are dangerous at any time. If you have a frayed power cord call your ASIA for a replacement immediately.**

12. T F I can leave the same image on my computer monitor all week without harming the monitor.

**True - But If you leave the same image on the monitor for weeks at a time you run the risk of burning the image on the screen permanently.**

13. T F Modems can be moved from computer to computer without any special software.

**False - Modem requires software to operate properly. Simply moving the modem to another computer will not work without loading the software. To move a modem call an ASIA.**

14. T F The surface of a CD can be scratched without loss of data.

**False - Scratches can cause the CD to be unreadable. The scratch causes the laser beam to reflect off the surface rather than the data.**

15. T F Computer monitor screens can be cleaned with Windex or special monitor cleaning products.

**True - Monitor screens are made of glass and can be cleaned with Windex or other glass cleaner and a soft cloth. Use only special cleaners for the screens on laptops. Do not use any cleaner that will leave any wax or other residue.**

16. T F Microcomputer screens can be cleaned with Ajax or Borax cleaning products.

**False - No, do not use any abrasive cleaner or cleaning material that will leave a residue.**

17. T F Spilling water or a soda on a microcomputer will not hurt it.

**False - The minerals in water may harm a computer. The sugars in a soda are definitely not good for a computer.**

18. T F Microcomputers are strong enough to be dropped on a concrete floor without being harmed.

**False - If you try dropping a laptop on the floor be prepared to cough up about \$2000 for a new one.**

19. T F Microcomputers do not have modems.

**False - Virtually all computers now on the market come with modems, although it is possible to order one without a modem.**

20. T F Microcomputers are very limited in the amount of data that they can store.

**False - Most microcomputer come with huge amount of storage. Most laptop computer has with as much storage as the average desktop computer**

### **Answers for February Quiz**

1. T F If there is a work related need it is all right to share my password with my colleagues.

**False - There is never a work related need to share your password with anyone. If there is a need to get into your computer when you are not available your supervisor can contact the Help Desk to establish a new password for that occasion.**

2. T F I have been using my password for over a year, as long as no one knows my password there is no need to change it.

**False - You should change your password at least every 90 days. Your password can be identified by someone if they watch you enter it often enough.**

3. T F It's all right to use my cat's name as a password since no one knows my cat.

**False - You should not use a family member's name, a pets name, the name of a hobby, consecutive letters on the keyboard (qwerty), etc. In normal casual conversation we will mention these names to our acquaintances. As a result, it is first thing a hacker will use to gain entry to your system.**

4. T F My password is comprised of alphabetic characters and a number so I know it is a good password.

**True - Mixing letters and numbers is a good habit to get into. When you mix letter and numbers a hacker can't use an electronic dictionary to try to find your password.**

5. T F It is easier to remember a password if you use a phrase or sentence as an aide.

**True - A pneumonic can be very helpful in remembering a password.**

6. T F It is OK to imbed special character, such as # & \$ in a password.

**True - Just as a number imbedded in a word will prevent the use of an electronic dictionary so will the use of special**

characters, such as, pound sign (#), carrot (^), ampersand (@,) right quote (, left quote), etc. Keep in mind that some special characters, such as, a period (.) or slash (/) are reserved for system use.

7. T F Passwords should be written down and placed in a secret place in case it is forgotten.

**False - Passwords should not be written down anyplace. Select words that are easy for you to remember but don't write it down.**

8. T F Passwords that are 3 to 5 characters in length are considered secure.

**False Anything less than six characters is not considered secure. An industry recommendation for a secure password is eight characters. Industry also found that people will resist anything more than eight characters.**

9. T F Passwords should be comprised of both upper and lower case letters.

**True - It is true that mixed upper and lower will make a stronger password. However, mixing upper and lower case letters tends to cause typing errors. A password of 8 or more characters in either upper or lower case character is sufficient.**

10. T F Special characters such as a period(.) or / can be imbedded in a password.

**False - No, these particular characters are reserved for systems use.**

11. T F A good way to pick a password is to randomly pick a word out of the dictionary.

**False - Selecting a word out of the dictionary is OK only if you imbed a number or special character.**

12. T F It's OK to use my logon name as my password.

**False - No, a logon name appears on the monitor screen each time you log on. Anyone standing near can read it. A logon name is also one of the first things a person who wants to break into your system will try.**

13. T F When changing passwords it is OK to repeat the same password every third time it is changed.

**False - No, a repetition cycle of three months is a fairly recognizable pattern. Most large systems will require you to use at least twelve different passwords before a password can be repeated.**

14. T F A good password to use is the same numeric character so long as it is more than 7 characters in length (i.e. 99999999).

**False - Entering a password by striking the same key six or seven times is not a very good password. It is simply too easy to determine the password by simply looking or listening.**

15. T F It's OK to logon a terminal with my password in the morning and let my colleagues use the terminal anytime that they need to.

**False - No, The purpose of a unique logon and password is to identify you to the system and to provide accountability. If you logon to your system and allow others to use it you will be held accountable for any inappropriate activity that takes place on that terminal.**

16. T F It's OK to write down logons and passwords of my colleagues in a book in case someone is ill so long as I lock the book in my desk.

**False - No, DOM 49020.9.2, requires that you do not share your logon or password with anyone, that includes your supervisor. If your supervisor needs to get into your system when you are ill or on vacation they can go to the ASIA and establish a new password that is then assigned to them.**

17. T F It's OK to use consecutive letters on the keyboard so long as the letters are random, as an example, QWERTY would be a good password.

**False - No, although the letters are alphabetically random they are consecutive on the keyboard. They are also easy to spot if you watch someone enter them on a keyboard.**

18. T F A good password would be the name of my husband, my child, my dog, or the street that I live on.

**False - Because these names tend to come up in casual conversation and are easy to remember by others they are considered to be very poor passwords.**

19. T F As long as I don't share my password I don't need to change it.

**False - No, passwords tend to become known over time even if we don't intentionally mean to share them.**

20. T F I can be held responsible for anything that happens if someone else used my password.

**True - the system only knows you by your logon and password. If someone else used your logon and password the systems thinks it is you and any inappropriate action is attributed to you.**