1. What is information security?
   A) Protection of business vision, mission and values
   B) Protection of policy and procedures
   C) Protection of confidentiality, integrity and availability
   D) Protection of intellectual property

   Ans: C

2. Who is responsible for information security?
   A) Only the IT team
   B) Only management
   C) Every employee
   D) Only auditors

   Ans: C

3. Information security focuses only on technology, not people or processes.
   A) True
   B) False

   Ans: B

4. PCI - DSS stands for
   A) Payment Card Industry Data Security Standard
   B) Pay Card Industry Data Security Standard
   C) Payment Card Information Data Security Standard
   D) Pay Card Information Data Security Standard

   Ans: A

5. Which of the following is **not a Trust Services Criterion (TSC)** in SOC 2?
   A) Security
   B) Availability
   C) Confidentiality
   D) Profitability

   Ans: D

6. While creating new documented information
   A) It is essential that the document carries company logo as the watermark
   B) A copy of the new information must be created so that in case the information is destroyed by mistake, the same can be recovered easily
   C) It is mandatory to mark the information classification on the document, e.g., confidential, Internal Use, etc.
   D) It is important to call the CISO to monitor the information creation from the information security perspective

   Ans: C

7. Which of the following is a direct effect of a security breach?
   A) Increased system performance

B) Data loss or theft
C) Reduced electricity consumption
D) Improved employee morale

Ans: B

8. You receive an email from an unknown sender claiming to be from IT support, asking you to click a link to reset your password.

What should you do?

A. Click the link to check what it is

B. Forward it to your colleagues for awareness

C. Report it to the IT/security team and delete it

D. Reply asking if it's genuine

Answer: C

9. You're working from a café using public Wi-Fi. What is the best way to protect organizational data?

A. Connect directly to public Wi-Fi
B. Use VPN and ensure no confidential data is visible
C. Disable firewall for faster internet
D. Share hotspot with others

Answer: B

10. A person without a badge enters your office area, claiming to be from maintenance. What should you do?

A. Assume they're authorized and ignore
B. Escort them to your manager's cabin
C. Politely verify their identity or report to security
D. Let them proceed since they seem harmless

Answer: C

11. You mistakenly send an internal confidential document to an external recipient. What should you do first?

A. Ignore; they may not notice
B. Inform the recipient to delete the email and notify ISMS immediately
C. Delete it from Sent Items
D. Wait until someone asks about it

Answer: B

12. You find a free tool online that would help in your work. Should you install it?

A. Yes, if it helps productivity
B. No, unless approved by IT/security
C. Yes, if downloaded from a known website
D. Yes, if others use it too

Answer: B

13. If an employee is caught doing an offense like abusing the internet, he/she will instantly receive an Incident report instead of a mere warning.

A) True
B) False
Ans: A

14. What is social engineering?
A) A group planning for social activity in the organization
B) Creating a situation wherein a third party gains confidential information from you
C) The organization is planning an activity for the welfare of the neighborhood
D) None

Ans: B

15. Before leaving for the day, what should you ensure?

A. Leave system unlocked for updates
B. Clear desk of all confidential papers and lock system
C. Keep printed data for tomorrow
D. Keep system logged in for convenience

✅ **Answer: B**

16. Your company laptop containing project data is stolen from your car. What should you do?

A. Try to locate it yourself
B. Inform the police only
C. Immediately report to IT/security team and management
D. Wait a day to see if it turns up

✅ **Answer: C**

17. How often should you change your password as per ISMS best practices?

A. Only when you forget it
B. Every 45 days or as per organizational policy
C. Once a year
D. Never, if it's strong

Answer: B

18. A colleague says they've never read the ISMS policy. What should you do?

A. Ignore—it's not your responsibility
B. Remind them to review the ISMS awareness material or policy
C. Report them to HR
D. Share your copy with them

✅ **Answer: B**

19. An employee leaves the company. What should be ensured as part of ISMS?

A. Leave access active for handover
B. Disable all system and physical access immediately
C. Wait for IT's next monthly audit
D. Do nothing if they were trustworthy

✅ **Answer: B**

20. A friend visits your office and wants to see your workspace. What should you do?

A. Allow them to enter freely
B. Get visitor pass and escort them
C. Let them wait in your cubicle
D. Give your badge temporarily

✅ **Answer: B**