UNIVERSITY OF GHANA

B.SC INFORMATION TECHNOLOGY, FIRST SEMESTER EXAMINATIONS 2017/2018

CSIT 311: INFORMATION SECURITY PRINCIPLES - (3 CREDITS)

TIME ALLOWED: *TWO AND A HALF (2½) HOURS*

INSTRUCTION:

Section A: *Answer ALL Questions in the Answer Booklet*

Section B: *Answer ALL Questions in the Answer Booklet*

Section C: *Answer Question C1 and Any other THREE (3) Questions from this section*

SECTION A (40 Marks)

Answer all questions in this section in the answer booklet. **1 Mark Each**

1. The ____ is a methodology for the design and implementation of an information system in an organization.
    a. DSLC
    b. SDLC
    c. LCSD
    d. CLSD

1. The ____ model consists of six general phases.
    a. pitfall
    b. 5SA&D

c. waterfall

d. SysSP

1. During the ____ phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design.

a. investigation

b. implementation

c. analysis

d. physical design

1. Which of the following phases is the longest and most expensive phase of the systems development life cycle?

a. investigation

b. logical design

c. implementation

d. maintenance and change

1. Which of the following functions does information security perform for an organization?

a. Protecting the organization’s ability to function.

b. Enabling the safe operation of applications implemented on the organization’s IT systems.

c. Protecting the data the organization collects and uses.

d. All of the above.

1. _____ is an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure of an organization.

   a. SSL
   b. PKI
   c. PKC
   d. SIS

1. _____ are software programs that hide their true nature, and reveal their designed behaviour only when activated.

   a. Viruses
   b. Worms
   c. Spam
   d. Trojan horses

1. Which of the following is an example of a Trojan horse program?

   a. Netsky
   b. MyDoom
   c. Klez
   d. Happy99.exe

1. As frustrating as viruses and worms are, perhaps more time and money is spent on resolving virus_____.

a. false alarms

b. power faults

c. hoaxes

d. urban legends

1. Web hosting services are usually arranged with an agreement providing minimum service levels known as a(n)_____.

a. SSL

b. SLA

c. MSL

d. MIN

1. ____ is the predecessor to the Internet.
    a. NIST
    b. ARPANET
    c. FIPS
    d. DES

1. A famous study entitled “Protection Analysis: Final Report” was published in ____.
    a. 1868
    b. 1978
    c. 1988
    d. 1998

1. ____ was the first operating system to integrate security as its core functions.
    a. UNIX
    b. DOS
    c. MULTICS
    d. ARPANET

1. ____ security addresses the issues necessary to protect the tangible items, objects, or areas of an organization from unauthorized access and misuse.

a. Physical
b. Personal
c. Object
d. Standard

1. A(n) ____ attack is a hacker using a personal computer to break into a system.
    a. indirect
    b. direct
    c. software
    d. hardware

1. A computer is the ____ of an attack when it is used to conduct the attack.
    a. subject
    b. object
    c. target
    d. facilitator

1. ____ of information is the quality or state of being genuine or original.
    a. Authenticity
    b. Spoofing
    c. Confidentiality
    d. Authorization

1. In file hashing, a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a ____ value.

a. key
b. hashing
c. hash
d. code

1. An information system is the entire set of ____, people, procedures, and networks that make possible the use of information resources in the organization.

a. software
b. hardware
c. data
d. All of the above

1. The most successful kind of top-down approach involves a formal development strategy referred to as a ____.

a. systems design
b. development life project
c. systems development life cycle
d. systems schema

SECTION B (20 Marks)

Answer All Questions from this Section

B1. Has the implementation of networking technology created more or less risk for businesses that use information technology? Discuss. **[5 Marks]**

B2. Why is the identification of risks, by listing assets and their vulnerabilities, so important to the risk management process? **[5 Marks]**

B3. Who is responsible for risk management in an organization? Explain. **[5 Marks]**

B4. State any five (5) of the Ten Commandments of Computer Ethics. **[5 Marks]**

SECTION C (60 Marks)

Answer C1 and Any Other THREE (3) Questions from this Section. (15 Marks Each)

C1. Answer the following questions regarding your respective groupings formed in class during the course of the semester:

a. State the name of your company and the kind of information that is processed in its operations. [2 Marks]

b. Why is data the most important asset your organization possesses? [3 Marks]

c. What other assets in the organization require protection? Explain. [3 Marks]

d. State two (2) information security principles that governs your company's information use. [2 Marks]

e. State the laws in Ghana that govern the operation of your company? [5 Marks]

C1.

a. Outline any five (5) of the information security principles that the University of Ghana as academic institution uses to govern its information circulation.

[10 Marks]

b. Discuss any five (5) principles that governs Information Security as a nation, in

its Information Security Policy document? [5 Marks]

C1.

a. Discuss four (4) reasons why it is important to study Information Security?

[4 marks]

a. Briefly explain the following Security goals and how your companies created this semester enforces them:

I. Confidentiality? [2 Marks]

II. Integrity? [2 Marks]

III. Availability? [2 Marks]

b. What is a mantrap? When should it be used? [5 Marks]

C1.

a. Your organization is planning to have a server room that functions without human beings— in other words, the functions are automated (such a room is

often called a lights-out server room). Describe the fire control system(s) you would install in that room. [8 Marks]

b. You have been asked to review the power needs for a standalone computer system which processes important but noncritical data and does not have to be online at all times, and which stores valuable data that could be corrupted if the power to the system were suddenly interrupted.

I. Which UPS features are most important to such a system? [3 Marks]

II. Which type of UPS do you recommend for this system? [2 Marks]

c. What can you do to reduce the risk of laptop theft? [2 Marks]

C1.

a. Describe a physical firewall that is used in buildings. List the reasons why an organization might need firewalls for physical security controls. [3 Marks]

b. What is considered the most serious threat within the realm of physical security? [2 Marks]

I. Why is it valid to consider this threat the most serious? [2 Marks]

c. List and describe the three fire detection technologies covered in the physical security chapter. [6 Marks]

I. Which is currently the most commonly used? [2 Marks]

C1.

a. If you were setting up an encryption-based network, what size key would you choose and why? [3 Marks]

b. What is the average key size of a strong encryption system in use today?

[1 Mark]

c. What is the standard for encryption currently recommended by NIST?

[2 Marks]

d. How does Public-Key Infrastructure protect information assets? [3 Marks]

e. What are the six components of PKI? [3 Marks]

f. What is the difference between digital signatures and digital certificates?

[3 Marks]