THE CATHOLIC UNIVERSITY OF EASTERN AFRICA

A. M. E. C. E. A

MAIN EXAMINATION

AUGUST – DECEMBER 2018 TRIMESTER

FACULTY OF SCIENCE

DEPARTMENT OF COMPUTER AND LIBRARY SCIENCE

REGULAR PROGRAMME

DIT 018: FUNDAMENTALS OF SYSTEM SECURITY

Date: DECEMBER 2018	**Duration: 2 Hours**
INSTRUCTIONS: Answer Question ONE and any other TWO Questions	

Q1.a)   Briefly explain what you understand by the term Information Systems
        Security   **(2 Marks)**

   b)   Information Security performs four important functions for an organization.
        Briefly explain those four functions   **(4 Marks)**

   c)   An effective information security program is essential to the
        protection of the integrity and value of the organizations data. Briefly
        explain what you understand by the term data   **(2 Marks)**

   d)   There are various threats to Information security in an institution. Briefly
        explain the term threat and highlight four categories of threats to
        information Security in an institution   **(6 Marks)**

   e)   The organization's systems depends on the successful operation of many
        interdependent support systems including but not limited to power grids,
        telecom networks, parts suppliers, service providers etc. Briefly explain
        three sets of service issues that can affect the availability of information
        and systems   **(6 Marks)**

   f)   Briefly explain the following terms as used in computer security
                        i)   Cracker
                        ii) Phreaker   **(4 Marks)**

ISO 9001:2008 Certified by the Kenya Bureau of Standards

g) Deliberate software attacks occur when an individual or group designs software to attack an unsuspecting system. Most of this software is referred to as malicious code or malicious software. Give a brief description of any six malicious code **(6 Marks)**

Q2. a) Briefly explain the following terms as used in security

    I.   Information extortion
    II.   Sabotage/ vandalism
    III.   Virus
    IV.   Worm
    V.   Backdoors/rootkits   **(10 Marks)**

b) Briefly differentiate between Spyware and Adware as used in systems security. **(4 Marks)**

c) Briefly explain two ways in which an organization or institution can protect itself against deliberate software attacks. **(4 Marks)**

d) Give a brief description of the term intellectual property as used in systems security **(2 Marks)**

Q3. a) Forces of Nature or acts of God post the most dangerous threats to Systems security, because they are unexpected and can occur with very little warning. Briefly explain five forces of nature **(10 Marks)**

b) Write short notes on what you understand by Technical hardware failures or errors **(4 Marks)**

c) What are some of the consequences of Technological obsolescence **(6 Marks)**

Q4. a) Briefly explain the term Attack and then differentiate between Exploit and vulnerability **(6 Marks)**

b) Write short notes on what is meant by malicious code **(4 Marks)**

c) Give a brief description of the following forms of attacks
    I.   Backdoors
    II.   Brute force
    III.   Password Crack
    IV.   Dictionary
    V.   Hoaxes   **(10 Marks)**
    VI.

Q5. a) Briefly differentiate the following terms in respect to security

ISO 9001:2008 Certified by the Kenya Bureau of Standards

I. Distributed Denial Of Service Attack and Buffer Overflow
        II. Spoofing and Spam.   **(8 Marks)**
        III.

b) Copyrights, Patents and Trade secrets   are legal devices that can protect
    computers, programs and data. Briefly explain how the above are used in
    computing   **(10 Marks)**

c) What do you understand by the term information   **(2 Marks)**

END

ISO 9001:2008 Certified by the Kenya Bureau of Standards