**KABARAK UNIVERSITY**

**UNIVERSITY EXAMINATIONS**

**MAIN CAMPUS**

**SECOND SEMESTER 2020/2021 ACADEMIC YEAR**

**EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SECURITY AND FORENSICS**

**COSF 411-INFORMATION SECURITY POLICY AND COMPLIANCE**

**STREAM: Y4S1, - REGULAR TIME: 9:00-11:00AM**

**EXAMINATION SESSION: MAY – AUGUST DATE: 24/08/2021**

**INSTRUCTIONS TO CANDIDATES**

1. **Answer Question 1 and any other two questions in the answer booklet provided.**
2. **Do not write on your question papers. All rough work should be done in your answer booklet.**
3. **Clearly indicate which question you are answering.**
4. **Write neatly and legibly.**
5. **Edit your work for language and grammar errors.**
6. **Follow all the instructions in the answer booklet**

**SECTION A: (COMPULSORY) TOTAL MARKS FOR THIS SECTION IS 30.**

**1.**

1. Under the Information Systems Acquisition, Development and Maintenance, Identify and discuss the FOUR major policies in correct processing for any Computer applications. **[8 Marks]**
2. RAID is applied in addressing fault tolerance in data security, Discuss RAID’s major characteristics. **[4 Marks]**
3. Analyze FOUR reasons why the increase in number of computer related security incidences in our society today. **[4 Marks].**
4. Describe the differences between COBIT and ITIL as relates to Information Security and compliance. **[6 Marks]**
5. Explain the major objectives in each of the following policy documents applied in most organizations listed below.
6. Network Policy **[2 Marks]**
7. Information systems strategy. **[2 Marks]**
8. Internet and Email Policy **[2 Marks]**
9. Anti-virus anti-spam Policy. **[2 Marks]**

**SECTION B. TOTAL MARKS FOR THIS SECTION IS 40.**

**ANSWER ANY TWO QUESTIONS FROM THIS SECTION. EACH QUESTION IN THIS SECTION CARRIES 20 MARKS.**

**2.**

1. Discuss THREE types of evidence in a modern working environment that would trigger the Security audit or forensic investigations. **[6 Marks]**
2. Discuss the following THREE Stages of System Intrusions.
3. Gaining Access. **[3 Marks]**
4. Maintaining Access. **[3 Marks]**
5. Clearing the logs. **[3 Marks]**
6. Demonstrate with examples why cyber law and ethicsis becoming increasingly important. **[5 Marks]**

**QUESTION THREE**

1. Define the following three types of hackers in our society today.
2. A Grey hat hacker. **[2 Marks]**
3. A White hat hacker. **[2 Marks]**
4. Suicide hackers. **[2 Marks]**
5. Discuss types of data backups available in safeguarding information.

**[8 Marks].**

1. Differentiate between Archiving and backup in data Security. **[6 Marks]**

**4.**

1. Analyze the THREE available circumstances where the general crime of copyright infringement provides for punishment. **[6 Marks]**
2. Salami Attacks and Phishing Email attacks are very common trending mechanisms in our society today, Analyze each of the attacks. **[4 Marks].**
3. Define the term Cryptography and why it is important in information security. **[4 Marks]**
4. Explain THREE major types of system back-ups conducted in systems security procedures. **[6Marks].**

**5.**

1. Analyze THREE major objectives of Corporate Governance. **[6 Marks].**
2. Differentiate between Brute force attacks and Packet replays as applied In Internet threats and security attack mechanisms. **[4 Marks].**
3. Compare and contrast between the following types of malwares within information systems. including worms, Trojan horses, and viruses.
4. Trojan horses. **[2 Marks]**
5. Viruses. **[2 Marks]**
6. Ransomwares. **[2 Marks]**
7. Rootkits **[2 Marks]**