NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Computer Science

QUALIFICATION : 08BHIS – BACHELOR OF COMPUTER SCIENCE HONOURS (INFORMATION SECURITY) 08BCHS – BACHELOR OF COMPUTER SCIENCE HONOURS (SOFTWARE DEVELOPMENT)	
QUALIFICATION CODE: 08BHIS; 08BHIS	**LEVEL: 8**
COURSE: Secure Systems	**COURSE CODE:** SSS810S
DATE: July 2022	**SESSION:** 2
DURATION: 2 hours	**MARKS: 60**

SECOND OPPORTUNITY/SUPPLEMENTARY EXAMINATION QUESTION PAPER	
EXAMINER(S)	**Mr. Mbaunguraije Tjikuzu**
MODERATOR:	**Mr. Ndangi Nashiku**

THIS QUESTION PAPER CONSISTS OF 2 PAGES
(Excluding this front page)

INSTRUCTIONS

1. Answer ALL the questions.
2. Write clearly and neatly.
3. Number the answers clearly.
4. When answering questions you should be guided by the allocation of marks. Do not give too few or too many facts in your answers.

PERMISSIBLE MATERIALS

1. None

Question 1

Complexity often accumulates inadvertently, but this can lead to tipping-point situations where a small and apparently innocuous change has major consequences for a system's reliability or security. Outline and explain four (4) architecture decisions you can take to make changes to your system easier? [10 marks]

Question 2

The following concepts are usually considered when designing for insider risk. Please explain what each concept means in the context of system design and outline how each concept is used in the mitigation of insider risk.

a. Three-Factor Authorization (3FA) [4 marks]

b. Zero Trust [4 marks]

c. Multi-Party Authorization [4 marks]

d. Business Justification [4 marks]

e. Auditing and Detection [4 marks]

Question 3

What benefit does threat intelligence provide to system defenders when defending against adversaries. Outline and explain three (3) forms of threat intelligence that one can find. [10 marks]

Question 4

Provide two examples of defence techniques you can implement at each of the following stages of a Cyber Kill Chain. *[2 Marks for listing, 4 Marks for an explanation of defence technique]*

a. Reconnaissance: *The attacker uses a search engine to find the email addresses of employees at a target organization.* [4 marks]

b. Entry: *Attacker sends phishing emails to employees that lead to compromised account credentials. The attacker then signs into the organization's virtual private network (VPN) service using those credentials.* [4 marks]

c. Lateral Movement: *Attacker remotely logs in to other systems using the compromised credentials.* [4 marks]

d. Persistence: *Attacker installs a backdoor on the newly compromised systems that provide them with remote access.* [4 marks]

e. Attacker Goals: Attacker steals documents from the network and uses the remote access backdoor to exfiltrate them. [4 marks]

**********END OF EXAM**********