Below is the accredited information for this unit:

Unit Code	: HIT333
Unit Name	: Cyber Security
Year	: 2022
Semester	: Semester 2
Sector	: Higher Education
School/Discipline	: Information Technology
Credit Points	: 10
Equivalent Units	: BIS243
Pre-requisites	: NA
Assumed Knowledge	: HIT274

Unit Description:

This unit gives an overview of securing the organisations business assets based on risk management approach. Students will develop an understanding about the risks and defense mechanism for network, application, physical, and wireless security. Students will gain insight into the fundamental concepts of modern cryptography and its applications in cybersecurity. Foot printing, enumeration and social engineering aspects are also covered. Wireless networks, desktop and operating system vulnerabilities, Internet of Things security are covered. Students will gain an understanding of the steps and process of network defense. Access to highspeed broadband is highly recommended.

Learning Outcomes:

1. Plan for organisations information security through policies, technologies and risk management.
2. Evaluate Operating Systems and network level vulnerabilities and formulate appropriate countermeasures.
3. Evaluate application development vulnerabilities and recommend appropriate countermeasures.
4. Evaluate the effectiveness of Disaster Recovery techniques to safeguard information assets.
5. Apply effective communication methods to convey ideas and principles.

Assessment Items (3):

Assessment Task	**Value (of total mark)**	**Related Learning outcome/s**
Presentation slides (10 minutes) and notes (500 words) on current topics on security risk management, policies and vulnerability management.	20%	1,2,5
Presentation slides (15 minutes) and notes (750 words) on cutting-edge technologies and cybersecurity.	30%	3,4,5
Final examination (2 hours)	50%	1,2,3,4,5