Course Title:	**Information Security Technologies**
Course Code:	**COMP607**
Descriptor Start Date:	**28/02/2025**
POINTS:	**15.00**
LEVEL:	**6**
PREREQUISITE/S:	**COMP501**
COREQUISITE/S:	**None**
RESTRICTION/S:	**None**

LEARNING HOURS

Hours may include lectures, tutorials, online forums, laboratories. Refer to your timetable and course information in Canvas for detailed information.

Total learning hours: 150

PRESCRIPTOR

Addresses security technology and systems; basic crypto-graphy and public key infrastructure, physical security, logical security, access controls, securing networks, network operations, systems, databases and applications, mobile and wireless security, web-services security, and security strategies for e-commerce. The intrinsic relationship between security technologies, ethics, legal and regulatory requirements, forensics and fraud, business strategy, and risk management is addressed.

LEARNING OUTCOMES

1. Discuss the building blocks of IT security
2. Critically analyse and evaluate the ethical and legal requirements for IT security.
3. Compare models designed to meet the fundamental principles of security.
4. Discuss physical and logical security requirements for IT systems.
5. Propose suitable technical, operational and managerial controls for securing networks, network operations, systems, databases and applications.
6. Explain mobile and wireless security and web-services security issues, and suggest security strategies for e-commerce.
7. Describe the relationship between security technologies forensics and fraud, business strategy, and risk management.

CONTENT

- Analyse and evaluate the operating systems role in Computer System Structures.
- Apply models, concepts and theories of:
- Building blocks of IT security
- Examples of legal and ethics frameworks
- Electronic crime and forensic computing
- Basic cryptography and public key infrastructure
- Securing networks and hosts
- Securing network and systems operations, databases and applications
- Strategies for e-commerce security
- Mobile and wireless security
- Security of web-services
- Current and emerging issues in IT security

LEARNING & TEACHING STRATEGIES

Will include:
- Readings, Exercises
- Lectures
- Student presentations
- Class discussion
- Guest speaker/lecturer, site visit if appropriate
- Laboratory sessions
- Online learning modes: online tutorial(s)
- Student self study

ASSESSMENT PLAN

Assessment Event	Weighting %	Learning Outcomes
Laboratory Portfolio	20.00	1, 4, 6, 7
Written assignment	40.00	5
Online problem-solving questionnaire	40.00	1 - 7

Grade Map **MAP1**

A+ A A- Pass with Distinction
B+ B B- Pass with Merit
C+ C C- Pass
D Fail

Overall requirement/s to pass the course:

To pass this course, students must attempt all summative assessments and achieve a minimum overall grade of C-.

LEARNING RESOURCES

Recommended reading lists will be provided.

For further information, contact: Te Ara Auaha - Faculty of Design & Creative Technologies

Principal Programme:	**AK3697, Bachelor of Computer and Information Sciences**
Related Programme/s:	**AK1302** **AK3698** **AK3756** **ICE1** **INEXCH1** **SABRD1**

Disclaimer: Course descriptors may be amended between teaching periods/semesters