ICT205 CYBER SECURITY T324 Brief

All information in the Subject Outline is correct at the time of approval. KOI reserves the right to make changes to the Subject Outline if they become necessary. Any changes require the approval of the KOI Academic Board and will be formally advised to those students who may be affected by email and via Moodle.
Information contained within this Subject Outline applies to students enrolled in the trimester as indicated

1. General Information

1.1 Administrative Details

Associated HE Award(s)	Duration	Level	Subject Coordinator
Bachelor of Information Technology (BIT)	1 trimester	Level 2	Dr Shuvashis SAHA shuvashis.saha@koi.edu.au P: +61 (2) 9283 3583 L: Level 1-2, 17 O'Connell St. Consultation: via Moodle or by appointment.

1.2 Core / Elective

Core subject for BIT

1.3 Subject Weighting

Indicated below is the weighting of this subject and the total course points.

Subject Credit Points	Total Course Credit Points
4	BIT (96 Credit Points)

1.4 Student Workload

Indicated below is the expected student workload per week for this subject

No. Timetabled Hours/Week*	No. Personal Study Hours/Week**	Total Workload Hours/Week***
4 hours/week (2 hour Lecture + 2 hour Tutorial)	6 hours/week	10 hours/week

* Total time spent per week at lectures and tutorials
** Total time students are expected to spend per week in studying, completing assignments, etc.
*** Combination of timetable hours and personal study.

1.5 Mode of Delivery Classes will be face-to-face or hybrid. Certain classes will be online (e.g., special arrangements).

1.6 Pre-requisites ICT106 Data Communications and Networks

1.7 General Study and Resource Requirements

- Dedicated computer laboratories are available for student use. Normally, tutorial classes are conducted in the computer laboratories.

 ABN: 72 132 629 979 CRICOS 03171A

- Students are expected to attend classes with the requisite textbook and must read specific chapters prior to each tutorial. This will allow them to actively take part in discussions. Students should have elementary skills in both word processing and electronic spreadsheet software, such as Office 365 or MS Word and MS Excel.
- Computers and WIFI facilities are extensively available for student use throughout KOI. Students are encouraged to make use of the campus Library for reference materials.
- Students will require access to the internet and email. Where students use their own computers, they should have internet access. KOI will provide access to required software.

Resource requirements specific to this subject: MS Imagine, Office 365, Virtual Box.

1.8 Academic Advising

Academic advising is available to students throughout teaching periods including the exam weeks. As well as requesting help during scheduled class times, students have the following options:

- Consultation times: A list of consultation hours is provided on the homepage of Moodle where appointments can be booked.
- Subject coordinator: Subject coordinators are available for contact via email. The email address of the subject coordinator is provided at the top of this subject outline.
- Academic staff: Lecturers and Tutors provide their contact details in Moodle for the specific subject. In most cases, this will be via email. Some subjects may also provide a discussion forum where questions can be raised.
- Head of Program: The Head of Program is available to all students in the program if they need advice about their studies and KOI procedures.
- Vice President (Academic): The Vice President (Academic) will assist students to resolve complex issues (but may refer students to the relevant lecturers for detailed academic advice).

2 Academic Details

2.1 Overview of the Subject

As the Internet becomes more pervasive, so do security threats to our computer systems and communications. Cybersecurity affects the social and economic health of the world. This subject provides students with a grounding in security technology and the fundamentals of encryption systems. Students will learn about types of attacks, access control and authentication, firewalls, wireless network security, intrusion detection systems, and cryptographic techniques and their applications.

2.2 Graduate Attributes for Undergraduate Courses

Graduates of Bachelor courses from King's Own Institute (KOI) will achieve the graduate attributes expected under the Australian Qualifications Framework (2nd edition, January 2013). Graduates at this level will be able to apply a broad and coherent body of knowledge from their major area of study in a range of contexts for professional practice or scholarship and as a pathway for further learning.

King's Own Institute's generic graduate attributes for a bachelor's level degree are summarised below:

	KOI Bachelor Degree Graduate Attributes	**Detailed Description**
	Knowledge	Current, comprehensive, and coherent and connected knowledge
	Critical Thinking	Critical thinking and creative skills to analyse and synthesise information and evaluate new problems

	KOI Bachelor Degree Graduate Attributes	Detailed Description
	Communication	Communication skills for effective reading, writing, listening and presenting in varied modes and contexts and for transferring knowledge and skills to a variety of audiences
	Information Literacy	Information and technological skills for accessing, evaluating, managing and using information professionally
	Problem Solving Skills	Skills to apply logical and creative thinking to solve problems and evaluate solutions
	Ethical and Cultural Sensitivity	Appreciation of ethical principles, cultural sensitivity and social responsibility, both personally and professionally
	Teamwork	Leadership and teamwork skills to collaborate, inspire colleagues and manage responsibly with positive results
	Professional Skills	Professional skills to exercise judgement in planning, problem solving and decision making

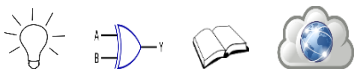
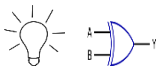
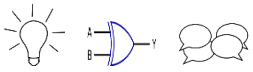
Across the course, these skills are developed progressively at three levels:

- **Level 1 Foundation** – Students learn the basic skills, theories and techniques of the subject and apply them in basic, standalone contexts
- **Level 2 Intermediate** – Students further develop the skills, theories and techniques of the subject and apply them in more complex contexts, and begin to integrate this application with other subjects.
- **Level 3 Advanced** – Students demonstrate an ability to plan, research and apply the skills, theories and techniques of the subject in complex situations, integrating the subject content with a range of other subject disciplines within the context of the course.

2.3 Subject Learning Outcomes

This is a Level 2 subject.

On successful completion of this subject, students should be able to:

Subject Learning Outcomes	Contribution to Graduate Attributes
a) Analyse and evaluate the organisational adoption of security controls	
b) Design solutions for concrete security problems for distributed applications	
c) Formulate and evaluate security countermeasures to reduce potential security risks	
d) Analyse emerging security threats and controls.	

 ABN: 72 132 629 979
CRICOS 03171A

2.4 Subject Content and Structure

Below are details of the subject content and how it is structured, including specific topics covered in lectures and tutorials. Reading refers to the text unless otherwise indicated.

Weekly Planner:

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
1 28 Oct	Network Security and industry cybersecurity standards and frameworks	Ch. 1	Complete exercises in Tutorials on challenges of securing information, information security and types of attackers. Tutorial not graded
2 04 Nov	Malware and social engineering attacks	Ch. 2	Complete exercises in Tutorials on basic steps of an attack and principles of defence and different types of malware and payloads of malware. Tutorial Graded 1%
3 11 Nov	Applications network attacks and risk mitigation	Ch. 15	Complete exercises in Tutorials on client-side attacks, overflow attacks and different types of networking-based attacks. Tutorial Graded 1% **Assessment 2 due: Quiz.**
4 18 Nov	Vulnerability assessment and data security	Ch. 13	Complete exercises in Tutorials on web-server attacks. Graded 1%
5 25 Nov	Networking-based and web server attacks	Ch. 5	Complete exercises in Tutorials on securing a host computer and application security. How to secure data. Tutorial Graded 1%
6 02 Dec	Network security devices, technologies, and design	Ch. 6	Complete exercises in Tutorials on network security devices and their uses, network technologies and security. Tutorial Graded 1%
7 09 Dec	Administering a secure network and systems and application security	Chs. 7, 9	Complete exercises in Tutorials on network design elements, functions of common network protocols, principles of network administration and how they can be secured. Tutorial Graded 1%

ABN: 72 132 629 979
CRICOS 03171A

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
8 16 Dec	Wireless network security and mobile and embedded devices	Chs. 8, 10	Complete exercises in Tutorials on different types of wireless network attacks and the vulnerabilities in IEEE 802.11 security. Solutions for securing a wireless network. Tutorial Graded 1%
9 06 Jan	Access management fundamentals	Ch. 11	Complete exercises in Tutorials on four access control models, how to implement access control and the different types of authentication services. Tutorial Graded 1%
10 13 Jan	Authentication and account management	Ch. 12	Complete exercises in Tutorials on authentication credentials and account management procedures for securing passwords. Tutorial Graded 1%
11 20 Jan	Cryptography: hash; symmetric; and asymmetric algorithm	Chs. 3, 4	Complete exercises in Tutorials on cryptography, hash, symmetric, and asymmetric cryptographic algorithms. Tutorial Graded 1% Complete exercises in Tutorials on how to control risk, ways in which security policies can reduce risk **Assignment 3 due: Report**
12 28 (Tue) Jan	Business continuity	Ch. 14	Discussion and exercises based on business continuity, Revision **Assignment 3 due: Demonstration**
13 03 Feb	Study Review Week and Final Exam Week		
14 10 Feb	Examinations Continuing students - enrolments for T125 open		Please see exam timetable for exam date, time and location
15 17 Feb	Student Vacation begins New students - enrolments for T125 open		
16 24 Feb	• Results Released • Review of Grade Day for T324 – see Sections 2.6 and 3.2 below for relevant information. • Certification of Grades		

 ABN: 72 132 629 979 CRICOS 03171A

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
	NOTE: More information about the dates will be provided at a later date through Moodle/KOI email.		
T125 3 Mar 2025			
1 03 Mar	Week 1 of classes for T125		

2.5 Teaching Methods/Strategies

Briefly described below are the teaching methods/strategies used in this subject:

- *Lectures* (2 hours/week) are conducted in seminar style and address the subject content, provide motivation and context and draw on the students' experience and preparatory reading.
- *Tutorials* (2 hours/week) include class discussion of case studies and research papers, practice sets and problem-solving and syndicate work on group projects. Tutorials often include group exercises and so contribute to the development of teamwork skills and cultural understanding. Tutorial participation is an essential component of the subject and contributes to the development of many of the graduate attributes (see section 2.2 above). Tutorial participation contributes towards the assessment in many subjects (see details in Section 3.1 for this subject). Supplementary tutorial material such as case studies, recommended readings, review questions etc. will be made available each week in Moodle.
- *Online* teaching resources include class materials, readings, model answers to assignments and exercises and discussion boards. All online materials for this subject as provided by KOI will be found in the Moodle page for this subject. Students should access Moodle regularly as material may be updated at any time during the trimester
- *Other contact* - academic staff may also contact students either via Moodle messaging, or via email to the email address provided to KOI on enrolment.

2.6 Student Assessment

 ABN: 72 132 629 979 CRICOS 03171A

Assessment is designed to encourage effective student learning and enable students to develop and demonstrate the skills and knowledge identified in the subject learning outcomes. Assessment tasks during the first half of the study period are usually intended to maximise the developmental function of assessment (formative assessment). These assessment tasks include weekly tutorial exercises (as indicated in the weekly planner) and low stakes graded assessment (as shown in the graded assessment table). The major assessment tasks where students demonstrate their knowledge and skills (summative assessment) generally occur later in the study period. These are the major graded assessment items shown in the graded assessment table.

Final grades are awarded by the Board of Examiners in accordance with KOI's Assessment and Assessment Appeals Policy. The definitions and guidelines for the awarding of final grades within the BIT degree are:

- HD High distinction (85-100%) an outstanding level of achievement in relation to the assessment process.
- DI Distinction (75-84%) a high level of achievement in relation to the assessment process.
- CR Credit (65-74%) a better than satisfactory level of achievement in relation to the assessment process.
- P Pass (50-64%) a satisfactory level of achievement in relation to the assessment process.
- F Fail (0-49%) an unsatisfactory level of achievement in relation to the assessment process.

Provided below is a schedule of formal assessment tasks and major examinations for the subject.

Assessment Type	When assessed	Weighting	Learning Outcomes Assessed
Assessment 1: Tutorial Weekly	Weeks 2 - 11	1% each submission Total: 10%	a, b, c, d
Assessment 2: Quiz	Week 4	5%	a
Assessment 3: Practical and Written Assessment, Individual assignment (2000 words)	Week 11 Report Submission Week 12 Demonstration	35%	a, b, c, d
Assessment 4: Final examination On-campus: 2 hours + 10 mins reading time	Final exam period	50%	a, b, c, d

Requirements to Pass the Subject:

To gain a pass or better in this subject, students must gain a *minimum of 50%* of the total available subject marks.

2.7 Prescribed and Recommended Readings

Provided below, in formal reference format, is a list of the prescribed and recommended readings.

Prescribed Text:

 ABN: 72 132 629 979 CRICOS 03171A

Ciampa, M. (2024). CompTIA Security+ guide to network security fundamentals (8th ed.). Cengage Learning.

***Recommended Readings**:*

Easttom, W 2019. *Computer Security Fundamentals*, 4th Edition, Pearson.

Moschovitis, C 2018, *Cybersecurity Program Development for Business: The Essential Planning Guide*, John Wiley & Sons, Incorporated, Newark. Available from: ProQuest Ebook Central. [9 June 2020].

Whitman, M, & Mattord, H 2018, *Principles of Information Security,* Cengage Learning US, Mason, OH. Available from: ProQuest Ebook Central. [9 June 2020].

Journal Articles:

Furnell S., "The cybersecurity workforce and skills*", Elsevier Computers & Security*, Vol. 100, PP. 102080, 2021. ISSN 0167-4048.

Zhang D., Feng, G., Shi, Y. and Srinivasan, D., Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances," in *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319-333, 2021, doi: 10.1109/JAS.2021.1003820.

Zhang-Kennedy, L. and Chiasson, S., A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education, *ACM Computing Survey*, Vol. 54, No. 1, 2021. ISSN = 0360-0300.

ISO/IEC 27001 standards

NIST Cybersecurity Framework

COBIT for Information Security

Journals:

- Journal of Information System Security
- ACM Transactions on Information and System Security
- Computers and Security
- IEEE Transactions on Information Forensics and Security

Conference/ Journal Articles:

Students are encouraged to read peer reviewed journal articles and conference papers. Google Scholar provides a simple way to broadly search for scholarly literature. From one place, you can search across many disciplines and sources: articles, theses, books, abstracts and court opinions, from academic publishers, professional societies, online repositories, universities and other web sites.

Useful Websites:

The following websites are useful sources covering a range of information useful for this subject. However, most are not considered to be sources of Academic Peer Reviewed theory and research. If your assessments require ***academic peer reviewed journal articles*** as sources, you need to access such sources using the Library database, Ebscohost, or Google Scholar. Please ask in the Library if you are unsure how to access Ebscohost. Instructions can also be found in Moodle.

- https://www.cybersecurity-insiders.com/
- Kali Linux Official Documentation: The official documentation for Kali Linux (https://www.kali.org/docs/)
- Offensive Security courses and resources at their official website (https://www.offensive-security.com/).

- Metasploit Unleashed (https://www.metasploitunleashed.org/)

 ABN: 72 132 629 979 CRICOS 03171A