ICT205 CYBER SECURITY T325 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) Diploma in Information Technology (DIT)	1 trimester	Level 2	Dr Babur Jalal babur.jalal@koi.edu.au P: +61 (2) 9283 3583 L: 7-11, 11 York St. Consultation: via Moodle or by appointment.

1.2 Core / Elective

Core subject for BIT
Elective subject for DIT

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) DIT (32 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.
- 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 the 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 continues to expand, so do the security threats targeting computer systems and communications. Cybersecurity plays a crucial role in maintaining the social and economic stability of the world. This subject equips students with a foundational understanding of security technologies and encryption systems. Students will explore various cyber threats, access control mechanisms, authentication protocols, firewalls, wireless network security, intrusion detection systems, and cryptographic techniques along with their practical applications. By the end of this subject, students will be prepared to identify, evaluate, and mitigate security risks while ensuring compliance with relevant regulations and industry standards.

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
	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

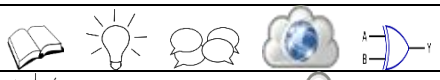
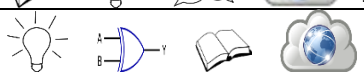
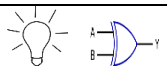
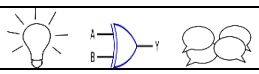
Across the course, these skills are developed progressively at three levels:

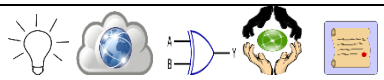
- **Level 1 Foundation** – Students learn the basic skills, theories and techniques of the subject and apply them in basic, standalone contexts
- **Level 2 Intermediate** – Students further develop the skills, theories and techniques of the subject and apply them in more complex contexts, and begin to 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.	

e) Identify and understand ethical, legal, and professional standards and regulations in cybersecurity.	
f) Demonstrate an understanding of professional ethics, privacy regulations, and security standards relevant to ICT practice.	

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
Week 1 27 Oct	Network Security, industry cybersecurity standards and Frameworks	Ch. 1	In this tutorial, students will install Kali Linux in VirtualBox, explore the Kali Linux environment, and learn essential Linux commands for cybersecurity applications. They will also complete exercises on the challenges of securing information and types of attackers.
Week 2 03 Nov	Malware and social engineering attacks	Ch. 2	In this tutorial, students will explore different types of malware (viruses, worms, trojans, ransomware, spyware), and learn basic Kali Linux commands for security analysis. **Biweekly activity 0%**
Week 3 10 Nov	Applications and network attacks, Risk mitigation. Personal, Legal, Ethical, and Social Issues	Ch. 15 Recommended Readings [5]	In this tutorial, students will examine risk identification methods, risk assessment techniques, and risk mitigation strategies, apply risk control frameworks, and analyse practical case studies on ethical decision-making using the ACS Code of Professional Conduct.
Week 4 17 Nov	Vulnerability assessment and data security; Data Credentials and Privacy	Ch. 13 Recommended Readings [4]	In this tutorial, students will gain an understanding of TCP/IP, the OSI model, and network ports, analyse network traffic using Wireshark, and perform basic network scanning. They will also complete exercises on web-server attacks and analyse

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
			privacy regulations through scenarios involving Australian businesses to discuss compliance requirements. Additionally, the Case Study for Assessment 2 will be discussed. **Biweekly activity 5%**
Week 5 24 Nov	Networking-based and web server attacks; Data Security	Ch. 5 Recommended Readings [6]	In this tutorial, students will learn about network-based and server-based attacks. They will also perform a SQL Injection attack using Kali Linux, learning to identify vulnerable web applications, extract sensitive database information, and use automated tools like sqlmap for exploitation. Students will also evaluate data protection strategies and compare security solutions for compliance with ACSC and NIST standards.
Week 6 01 Dec	Network security devices, technologies, and design	Ch. 6	In this tutorial, students will clone a target website to demonstrate how attackers capture user credentials through phishing. They will analyse social engineering tactics and explore defense strategies to prevent credential theft. Case Study for Assessment 4 will be discussed. **Biweekly activity 5%** **Assessment 4 (Group Formation)**
Week 7 08 Dec	Administering a secure network and systems and application security	Chs. 7, 9	In this tutorial, students will explore network design elements, standard network protocols, and network administration and security principles. They will use Nmap in Kali Linux to perform port scanning, identify open ports, and analyse network vulnerabilities. **Assessment 2 due date (30%)**

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 8 15 Dec	Wireless network security and mobile and embedded devices	Chs. 8, 10	In this tutorial, students will learn penetration testing techniques for FTP servers (port 21) using brute-force password guessing attacks. They will explore common vulnerabilities in FTP authentication and understand countermeasures to prevent unauthorised access. Additionally, they will examine different types of wireless network attacks, vulnerabilities in IEEE 802.11 security, and solutions for securing wireless networks **Biweekly activity 5%**
Week 9 05 Jan	Access management fundamentals	Ch. 11	In this tutorial, students will follow a step-by-step guide to set up a basic firewall using UFW (Uncomplicated Firewall) in Kali Linux. They will learn how to configure rules, manage traffic, and enhance network security by controlling inbound and outbound connections. **Assessment 3: Quiz (20%)**
Week 10 12 Jan	Authentication and account management	Ch. 12	In this tutorial, students will explore incident response strategies, including identifying, analysing, and mitigating cybersecurity threats. They will learn best practices for handling security breaches, incident reporting, and recovery procedures to minimise damage and restore systems efficiently.
Week 11 19 Jan	Cryptography: hash; symmetric; and asymmetric algorithm	Chs. 3, 4	The tutorial exercises on cryptographic algorithms (hash, symmetric, and asymmetric), risk control, and the role of security policies in reducing risk. **Assessment 4 due: Report (20%)** **Assessment 4 due: Presentation & Interview (15%)**

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
Week 12 27Jan (Tue)	Business continuity	Ch. 14	Discussion and exercises based on business continuity, Revision **Assessment 4 due: Presentation & Interview (Cont.) (15%)**
Week 13 02 Feb	Study review week and Final Exam Week		
Week 14 09 Feb	Examinations Continuing students - enrolments for T126 open		Please see exam timetable for exam date, time and location
Week 15 16 Feb	Student Vacation begins New students - enrolments for T126 open		
Week 16 23 Feb	• Results Released • Review of Grade Day for T325 – see Sections 2.6 and 3.2 below for relevant information. • Certification of Grades NOTE: More information about the dates will be provided at a later date through Moodle/KOI email.		
T126 2 Mar 2026			
Week 1 02 Mar	Week 1 of classes for T126		

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

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: Individual Biweekly Reflection (Week 2,4,6, and 8) Week 2: Reflection on Network and Industry Cybersecurity Standards and Frameworks with Practical Examples. Week 4: Reflection on the application of ACS and BCS Codes of Ethics using real-world examples. Week 6: Reflection on Data Privacy Compliance by Integrating APP, GDPR, and CDR Principles with Cybersecurity Measures to Address Real-World Challenges. Week 8: Reflection on Applying ACSC Small Business Cyber Security Guidelines and NIST Risk Management Standards to Real-World Security Issues.	Weeks 2- 0% Weeks 4- 5% Weeks 6- 5% Weeks 8- 5%	5% each submission Total: 15%	a, e, f

** Case Study will be discussed in the Tutorial Class.			
Assessment 2: Individual Written Report (1500 words) on ICT Ethics and Compliance with Australian Privacy Laws	Week 7	30%	b, e and f
Assessment 3: Quiz	Week 9	20%	a, c, e and f
Assessment 4: Group Case Study Report Group Case Study Presentation and Interview	Report: Week 11 Presentation and Interview: Week 11 and Week 12	Report: 20% Presentation and Interview: 15%	a, b, c, d, and e

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:

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

***Recommended Readings**:*

[1] McDermid, D. (ed.) 2008, *Ethics in ICT: An Australian perspective*, Pearson Education, Frenchs Forest, NSW.

[2] https://www.standards.org.au/documents/pacific-islands-cyber-security-standards-cooperation-agenda

[3] Student Insights on Cybersecurity Careers: https://www.nist.gov/blogs/cybersecurity-insights/student-insights-cybersecurity-careers

[4] Emerging Threats: Cybersecurity Forecast 2025: https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025/

[5] Pacific Islands Cyber Security Standards Cooperation Agenda: https://www.standards.org.au/documents/pacific-islands-cyber-security-standards-cooperation-agenda

[6] Student Insights on Cybersecurity Careers: https://www.nist.gov/blogs/cybersecurity-insights/student-insights-cybersecurity-careers

[7] Top Resources to Learn Ethical Hacking: https://medium.verylazytech.com/top-resources-to-learn-ethical-hacking-a-curated-guide-for-intermediate-to-advanced-learners-c3235a2f2bb1

[8] Journal of Cybersecurity: https://academic.oup.com/cybersecurity?login=false

[9] Ethics References:

- Australian Privacy Principles (APP): Reference the Office of the Australian Information Commissioner (OAIC) website. (https://www.oaic.gov.au/privacy/australian-privacy-principles)
- GDPR: Include the GDPR official regulation link (https://www.dfat.gov.au/sites/default/files/nixora-group-eufta-submission.pdf).

[10] Security References:

- Australian Cyber Security Centre (ACSC): Official ACSC guidelines for implementing ICT security measures(https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines).
- NIST Cybersecurity Framework: Reference the NIST website for guidelines (https://www.nist.gov/cyberframework).

[11] Cyber Security Best Practices

- Australian Cyber Security Centre (ACSC) Small Business Cyber Security Guide (https://www.cyber.gov.au/sites/default/files/2023-07/acsc_small_business_cyber_security_guide.pdf)
- Australian Cyber Security Centre (ACSC) Cybersecurity Best Practices for Smart Cities (https://www.cyber.gov.au/sites/default/files/2023-04/Joint-guidance-cybersecurity-best-practices-for-smart-cities.pdf)
- NIST SP 800-100, Information Security Handbook: A Guide for Managers (2024) (https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-100.pdf)

[12] ACSC Guidelines for cybersecurity roles. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-roles

[13] ACSC Guidelines for cybersecurity incidents. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cybersecurity-roles

[14] ACSC Guidelines for physical security. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-physical-security

[15] ACSC Guidelines for networking. https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-networking

Journal Articles:

[1] Gupta, M., Akiri, C., Aryal, K., Parker, E. & Praharaj, L. 2023, From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy, *IEEE Access*, vol. 11, pp. 80218–80245, doi: https://doi.org/10.1109/ACCESS.2023.3300381

[2] Liu, L. & Xu, M. 2025, 'A network intrusion detection method based on contrastive learning and Bayesian Gaussian Mixture Model', *Cybersecurity*, vol. 8, no. 1., doi: https://doi.org/10.1186/s42400-025-00364-7

[3] River Publishers 2023, 'Vulnerability assessment for applications security through penetration simulation and testing', *River Publishers Journals & Magazine*, doi: https://ieeexplore.ieee.org/document/10251051

[4] Neels, D., Ezhilazhagan, D.C. & Prabha, K.L. 2024, *Ethical hacking*, doi: https://doi.org/10.59646/eh/182

[6] ISO/IEC 27001 standards

[7] NIST Cybersecurity Framework

[8] COBIT for Information Security

[9] General Data Protection Regulation (GDPR)

[10] Australian Privacy Principles guidelines

Journals:

- Journal of cybersecurity https://academic.oup.com/cybersecurity
- Journal of Information System Security https://www.jissec.org/
- ACM Transactions on Information and System Security https://dl.acm.org/toc/tissec/2015/17/4
- IEEE Transactions on Information Forensics and Security https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=10206

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://cybercx.com.au/blog/
- https://www.cybersecurity-insiders.com/
- Cybersecurity Standards in Australia: https://www.standards.org.au/engagement-events/strategic-initiatives/critical-and-emerging-technologies/cybersecurity-standards
- Examine data breaches—Visual: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (If you are no longer able to access the site through this web address, use a search engine to search for *Information Is beautiful World's biggest data breaches & hacks*.")
- 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/)