ICT740 APPLIED CYBERSECURITY 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
Master of Information Technology (MIT) Graduate Diploma of Information Technology (GDIT)	1 trimester	Postgraduate	Dr Prabhu Jyot Singh prabhu.singh@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

This subject is:
- an elective subject for the Master of Information Technology (MIT)
- an elective subject for the Graduate Diploma of Information Technology (GDIT) for students from a cognate background

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	MIT (64 Credit Points); GDIT (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***
3 hours/week plus supplementary online material	7 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 ICT722 Information Security

1.7 General Study and Resource Requirements

- Students are expected to attend classes with the weekly worksheets and subject support material provided in Moodle. Students should read this material before coming to class to improve their ability to participate in the weekly activities.
- Students will require access to the internet and their KOI email and should have basic skills in word processing software such as MS Word, spreadsheet software such as MS Excel and visual presentation software such as MS PowerPoint.
- 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.

Software resource requirements specific to this subject: MS Imagine, Office 365, Guided exploitation of attacks suites, Virtual Box with Kali Linux.

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

This subject provides students with practical techniques to help achieve digital security. The mechanisms and prominent techniques used to tackle sophisticated attacks will be highlighted. Digital security for operating systems, databases, and servers will be covered including designs, implementations, and configurations to apply security measures and principles to protect these systems. The subject also examines the framework of cybersecurity, safety principles and guidelines. Practical experience will be gained using a range of tools designed to enforce security and privacy. Students will perform guided exploitation attacks in practical sessions to experiment with popular practices in hacking.

2.2 Graduate Attributes for Postgraduate Courses

Graduates of postgraduate courses from King's Own Institute will achieve the graduate attributes expected from successful completion of a postgraduate degree under the Australian Qualifications Framework (2nd edition, January 2013). Graduates at this level will be able to apply advanced 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 master's level degree are summarised below:

	KOI Postgraduate Degree Graduate Attributes	Detailed Description
	Knowledge	Current, comprehensive and coherent knowledge, including recent developments and applied research methods
	Critical Thinking	Critical thinking skills to identify and analyse current theories and developments and emerging trends in professional practice
	Communication	Communication and technical skills to analyse and theorise, contribute to professional practice or scholarship, and present ideas to a variety of audiences
	Research and Information Literacy	Cognitive and technical skills to access and evaluate information resources, justify research approaches and interpret theoretical propositions
	Creative Problem Solving Skills	Cognitive, technical and creative skills to investigate, analyse and synthesise complex information, concepts and theories, solve complex problems and apply established theories to situations in professional practice
	Ethical and Cultural Sensitivity	Appreciation and accountability for ethical principles, cultural sensitivity and social responsibility, both personally and professionally
	Leadership and Strategy	Initiative, leadership skills and ability to work professionally and collaboratively to achieve team objectives across a range of team roles Expertise in strategic thinking, developing and implementing business plans and decision making under uncertainty
	Professional Skills	High level personal autonomy, judgement, decision-making and accountability required to begin professional practice

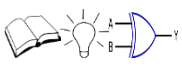
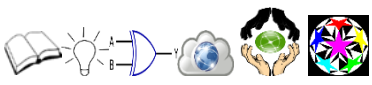
Across the courses, these skills are developed progressively at three levels:

- **Level 1 Foundation –** Students learn the skills, theories and techniques of the subject and apply them in stand-alone contexts
- **Level 2 Intermediate –** Students further develop skills, theories and techniques of the subject and apply them in more complex contexts, beginning to integrate the application with other subjects
- **Level 3 Advanced** – Students have a demonstrated 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

Generally, skills gained from subjects in the Graduate Certificate and Graduate Diploma are at levels 1 and 2 while other subjects in the Master's degree are at level 3.

2.3 Subject Learning Outcomes

Listed below, are key knowledge and skills students are expected to attain by successfully completing this subject:

Subject Learning Outcomes	Contribution to Graduate Attributes
a) Investigate computer security systems, and generate and present a proposal to address security problems	
b) Identify and analyse security vulnerabilities and propose justifiable technical solutions and potential remedy actions based on findings	

c) Compare different types of security systems on the basis of functionalities, architectures, configurations, and ethical challenges	
d) Communicate cybersecurity vulnerabilities and solutions to non-technical audiences to make informed decisions	

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	Introduction of cyberspace security and safety; network security, implementation security, IoT security, cloud security	Reading material provided on Moodle	Tutorial activities on virtual machine installation and lab environment configuration. Practical questions Formative not graded
2 04 Nov	Cyberspace security and safety	Reading material provided on Moodle	Practical question on enterprise risk management and NIST cybersecurity framework. Formative not graded
3 11 Nov	Cyberspace security and safety: ethical considerations in cybersecurity	Ch. 11 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L]	Case study on cyber security and safety ethical considerations Formative not graded
4 18 Nov	OS security	Ch.5 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L] Ch. 12 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on Set-UID Formative not graded
5 25 Nov	User Authentication, Access Control and Buffer Overflow	Ch. 2 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L] Ch. 3,4,10 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on buffer overflow vulnerability Formative not graded **Assessment 1: due**
6 02 Dec	Network security	Ch. 6 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L]	Practical questions. Tutorial activities on network security Formative not graded

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
		Ch. 22 [Stallings, W, & Brown, L]	
7 09 Dec	Software security	Ch. 3 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L] Ch. 11 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on Format String vulnerability Formative not graded
8 16 Dec	Cloud and IoT Security	Ch.8 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L] Ch. 13 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on Shellshock Vulnerability Formative not graded **Assessment 2: due**
9 06 Jan	Intrusion Detection	Reading material provided on Moodle Ch..8 [Stallings, W, & Brown, L].	Practical questions. Tutorial activities on Meltdown Attack. Formative not graded
10 13 Jan	Firewalls and Intrusion Prevention Systems	Reading material provided on Moodle Ch. 9 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on Cross-site Request Forgery Attack. Formative not graded
11 20 Jan	Database and Data Center Security	Ch.7 [Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L] Ch. 5 [Stallings, W, & Brown, L]	Practical questions. Tutorial activities on Android Repackaging.
12 28 (Tue) Jan	Review	All chapters	Revision **Assessment 3 due**
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		

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* (1 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 assessments (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 are:

- *HD High distinction* (85-100%): an outstanding level of achievement in relation to the assessment process.
- *D Distinction* (75-84%): a high level of achievement in relation to the assessment process.
- *C 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.
- *FW:* This grade will be assigned when a student did not submit any of the compulsory assessment items.

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 Assessment	Week 5	15%	a, d
Assessment 2: Individual - Report 2000 words	Week 8	20%	b, c
Assessment 3: Individual Report	Week 12	15%	b, c
Assessment 4: Final examination On-campus: 2 hours + 10 mins reading time Online: 2 hours + 30 mins technology allowance	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:

Pfleeger, C. P., Pfleeger, S. L., Coles-Kemp, L 2023. Security in Computing. Netherlands: Addison Wesley Professional.

Recommended Readings:

Stallings, W, & Brown, L 2024, Computer Security: Principles and Practice, 5th edition, Pearson Education Limited, Harlow, United Kingdom. Available from: ProQuest Ebook Central. [06 Junruary 2021].

Ahmadi, S., 2024. Challenges and Solutions in Network Security for Serverless Computing. International Journal of Current Science Research and Review, 7(01), pp.218-229.

Conklin, W. A., White, G. B., Cothren, C., Williams, R., and Davis, R. 2022. Principles of Computer Security: CompTIA Security+ and Beyond. 6th ed. New York: McGraw-Hill Education.

Easttom, C. 2023. Computer Security Fundamentals. 5th ed. Indianapolis: Pearson IT Certification.

Ciampa, M. 2022. CompTIA Security+ Guide to Network Security Fundamentals. 7th ed. Boston: Cengage Learning.

Wong, A.Y., Chekole, E.G., Ochoa, M. and Zhou, J., 2023. On the security of containers: Threat modeling, attack analysis, and mitigation strategies. Computers & Security, 128, p.103140.

Butt, U.A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M.T. and Albaqami, N., 2023. Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), pp.387-413.

Omotunde, H. and Ahmed, M., 2023. A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. Mesopotamian Journal of CyberSecurity, 2023, pp.115-133.

Momand, A., Jan, S.U. and Ramzan, N., 2023. A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: deep learning, datasets, and attack taxonomy. Journal of Sensors, 2023.

Alatawi, M.N., Alsubaie, N., Ullah Khan, H., Sadad, T., Alwageed, H.S., Ali, S. and Zada, I., 2023. Cyber security against intrusion detection using ensemble-based approaches. Security and Communication Networks, 2023.

Khan, A.R., Kashif, M., Jhaveri, R.H., Raut, R., Saba, T. and Bahaj, S.A., 2022. Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions. *Security and Communication Networks*, *2022*.

Atlam, H.F. and Wills, G.B., 2020. *IoT security, privacy, safety and ethics. Digital twin technologies and smart cities*, pp.123-149.

Calder, A., 2020. Cyber security : Essential principles to secure your organisation. ProQuest Ebook Central https://ebookcentral.proquest.com

Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, 2018. *Cybersecurity Essentials*

Gupta, C. P., & Goyal, K. K., 2020. *Cybersecurity: A self-teaching introduction*. ProQuest Ebook Central https://ebookcentral.proquest.com

Le, D, Kumar, R, Chatterjee, JM, Khari, M, & Mishra, BK (eds), 2019, *Cyber Security in Parallel and Distributed Computing : Concepts, Techniques, Applications and Case Studies*, John Wiley & Sons, Incorporated, Newark. Available from: ProQuest Ebook Central. [1 July 2020].

Schreider, T., 2020. *Cybersecurity law, standards and regulations*, 2nd edition. ProQuest Ebook Central https://ebookcentral.proquest.com

Useful Websites :

Simmons, A. 2024. Internet of Things (IoT) Examples by Industry in 2024. [online] Dgtlinfra. Available at: https://dgtlinfra.com/internet-of-things-iot-examples/.

Lauzier, J. 2020. Industrial IoT Security: Challenges and Solutions. [online] www.machinemetrics.com. Available at: https://www.machinemetrics.com/blog/industrial-iot-security.

Suggested Periodicals:

- IEEE journals and magazines: http://www.ieee.org/web/publications/journmag/index.html
- ACM Transactions and Information and System Security: https://dl.acm.org/citation.cfm?id=J789
- ACM Computing Surveys: https://csur.acm.org/
- IEEE Security and Privacy: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
- National Institute of Standards and Technology (NIST). Cybersecurity Framework. Available at: https://www.nist.gov/cyberframework
- OWASP Foundation. OWASP Top Ten Project. Available at: https://owasp.org/www-project-top-ten
- SecurityWeek. Cybersecurity News and Information. Available at: https://www.securityweek.com

Conference/ Journal Articles:

Arogundade, O.R., 2023. Network security concepts, dangers, and defense best practical. Computer Engineering and Intelligent Systems, 14(2).

Basholli, F., Daberdini, A. and Basholli, A., 2023. Detection and prevention of intrusions into computer systems. Advanced Engineering Days (AED), 6, pp.138-141.

Allahrakha, N., 2023. Balancing cyber-security and privacy: legal and ethical considerations in the digital age. Legal Issues in the digital Age, (2), pp.78-121.

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.