ICT722 INFORMATION 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
Master of Information Technology (MIT) Graduate Diploma of Information Technology (GDIT)	1 trimester	Postgraduate	Dr Muhammad Sajjad Akbar sajjad.akbar@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)

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 Nil

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

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

Information is a critical asset for every business and needs to be protected. This subject presents security activities, methods and procedures which protect information assets in an organisation. The key issues related to the protection of these assets include identification of the need for security, levels of protection, response to security incidents, and the design of effective information security systems. The subject will examine legal, ethical and professional issues related to the inspection and protection of information assets. The subject covers the detection of and reaction to information security threats to enable students to develop an information security plan to protect an organisation.

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 Master’s 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) Analyse the information assets and security needs of an organisation	📖 💡 A B ⊃ Y
b) Articulate ethical and legal issues relating to information security	📖 💡 A B ⊃ Y 🌍
c) Apply security techniques and technologies to secure information assets according to an organisation's requirements	📖 💡 💬 🌐 A B ⊃ Y 📜
d) Devise an information security plan to reduce risk to an organisation's information assets based on security threats and vulnerabilities	📖 💡 💬 🌐 A B ⊃ Y 📜

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 to information security	Ch.1	Group Project introduced in the class. Chapter review questions on components and approaches to Information Security are discussed. Formative not graded
2 04 Nov	The need for security	Ch.2	Discussion of Group Project Activities, exercises and chapter review questions on business drivers behind the security analysis design process and the needs for security are discussed. Formative not graded

Week (beginning)	Topic covered in each week's lecture	Reading(s)	Expected work as listed in Moodle
3 11 Nov	Legal, ethical, and professional issues in information security	Ch.3	Discussion of Group Project Activities, exercises and chapter review questions on law and code of ethics for information security are discussed. Formative not graded
4 18 Nov	Security Management	Ch.4	Discussion of Group Project Activities, exercises and chapter review questions on security management. Formative not graded.
5 25 Nov	Incident Response and Contingency Planning.	Ch.5	Discussion of Group Project Activities, exercises and chapter review questions on incident response and contingency planning. Formative not graded. **Assessment 1 due: Quiz**
6 02 Dec	Risk Management	Ch. 6	Discussion of Group Project Activities, exercises and chapter review questions on risk identification, assessment and control are discussed. Formative not graded.
7 09 Dec	Security technology: Firewalls, VPNs, and Wireless	Ch.7	Discussion of Group Project Activities, exercises and chapter review questions on technical controls for both network and system access are discussed. Formative not graded
8 16 Dec	Security technology: Intrusion detection and prevention systems and other security tools	Ch.8	Activities, exercises and chapter review questions on the use and deployment of intrusion detection and prevention systems are discussed. Formative not graded.

Week (beginning)	Topic covered in each week’s lecture	Reading(s)	Expected work as listed in Moodle
9 06 Jan	Cryptography Part 1	Ch 9	Discussion of Group Project Activities, exercises and Chapter review questions on cryptography-based protocols used in secure communications are discussed. Formative not graded
10 13 Jan	Cryptography Part 2	Ch 9 and 10	Discussion of Group Project Activities, exercises and chapter review questions on advanced cryptography are discussed. Formative not graded **Assessment 3 due**
11 20 Jan	Implementation of Information Security	Ch 10 and 11	Discussion of Group Project Activities, exercises and chapter review questions on information security Formative not graded
12 28 (Tue) Jan	Security Personnel and Maintenance	Ch 11 and 12	Activities, exercises, chapter review questions. Formative not graded **Assessment 4 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: Quiz	Week 5	10%	a
Assessment 2: Individua Report (Disaster Recovery Planning)	Week 7	30%	a, b
Assessment 3: Individual Report (Risk Management Process)	Week 10	30%	a, b, c
Assessment 3: Group Report (Development of Information Security Policy Process)	Week 12	30%	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:

Whitman, M, & Mattord, H 2021, Principles of Information Security. 7th ed. Cengage Learning US, Mason, OH

Recommended Readings:

Alqarawi, G., Alkhalifah, B., Alharbi, N. and El Khediri, S., 2023. Internet-of-Things Security and Vulnerabilities: Case Study. *Journal of Applied Security Research*, *18*(3), pp.559-575.

Xue, B., Warkentin, M., Mutchler, L.A. and Balozian, P., 2023. Self-efficacy in information security: A replication study. *Journal of Computer Information Systems*, *63*(1), pp.1-10.

Pinto, A., Herrera, L.C., Donoso, Y. and Gutierrez, J.A., 2023. Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. Sensors, 23(5), p.2415.

Macas, M., Wu, C. and Fuertes, W., 2022. A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. Computer Networks, 212, p.109032.

Dasgupta, D., Akhtar, Z. and Sen, S., 2022. Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), pp.57-106.

Kilincer, I.F., Ertam, F. and Sengur, A., 2021. Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188, p.107840.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. and Xu, M., 2020. A survey on machine learning techniques for cyber security in the last decade. IEEE access, 8, pp.222310-222354.

Veiga, Ad., Astakhova, L. V., Botha, A. and Herselman, Marlien., 2020, Defining Organisational Information Security Culture – Perspectives from Academia and Industry. *Computers & Security* vol. 92, 2020.

Jeong, C.Y., Lee, S-Y.T. and Lim, J-H., 2019, Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information & Management*, vol.56, no. 5, pp.681-695.

Haquf, H. and Koyuncu, M., 2018, Understanding Key Skills for Information Security Managers, *International Journal of Information Management*, vol. 43, pp. 165-172.

Buczak, A.L. and Guven, E., 2015. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), pp.1153-1176.

ISC2 CISSP Certified Information Systems Security Professional Official Study Guide Paperback – 3 July 2024 by Mike Chapple (Author), James Michael Stewart (Author), Darril Gibson (Author)

Useful Websites:

Information Security Management: Computer Security: https://www.youtube.com/watch?v=IkJ7x6yI8W0
Information Security Management in your Workplace: https://www.youtube.com/watch?v=aigeZvxbRZ0
Information Technology Management (Information Security): https://www.youtube.com/watch?v=tKyk2vb5oPk
Kerbs on Security: https://krebsonsecurity.com
SANS Institute: https://www.sans.org
Security Week: https://www.securityweek.com
The Hacker News: https://thehackernews.com
Dark Reading: https://www.darkreading.com

Suggested Periodicals:

International Journal of Information Security: https://link.springer.com/journal/10207
Journal of Information Security and Applications: https://www.journals.elsevier.com/journal-of-information-security-and-applications
Information Security Journal: A Global Perspective: https://www.tandfonline.com/loi/uiss20

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.

Khaustova, V., Tirlea, M. R., Dandara, L., Trushkina, N., & Birca, I. (2023). Development Of Critical Infrastructure From The Point Of View Of Information Security. Strategic Universe Journal/Univers Strategic, (1).

AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. Electronics, 12(17), 3629.

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security, 124, 102974.

Abrahams, T. O., Farayola, O. A., Amoo, O. O., Ayinla, B. S., Osasona, F., & Atadoga, A. (2024). Continuous improvement in information security: A review of lessons from superannuation cybersecurity uplift programs. International Journal of Science and Research Archive, 11(1), 1327-1337.

Li, W. W., Leung, A. C. M., & Yue, W. T. (2023). Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. MIS Quarterly, 47(1), 317-342.

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 information security management standard: how to extract value from data in the IT sector. Sustainability, 15(7), 5828.

Yas, N., Elyat, M. N. I., Saeed, M., Shwedeh, F., & Lootah, S. (2024). The Impact of Intellectual Property Rights and the Work Environment on Information Security in the United Arab Emirates. Kurdish Studies, 12(1), 3931-3948.

.