Subject Description Form

Subject Code	COMP3335
Subject Title	Database Security
Credit Value	3
Level	3
Pre-requisite / Co-requisite / Exclusion	**Pre-requisite**: COMP2411 or equivalent introductory database subject
Objectives	The objectives of this subject are to: 1. introduce to students about security threats with respect to database applications; 2. equip students with knowledge of security measures and understanding on the concepts in protecting data; and 3. equip students with skills to design and implement secure database applications with respect to the security requirements.
Intended Learning Outcomes	Upon completion of the subject, students will be able to: *Professional/Academic Knowledge and Skills* (a) identify security threats in database systems; (b) understand the concepts and security mechanisms in the protection of data; (c) design and implement secure database systems; *Attributes for All-Roundness* (d) develop skills in problem-solving; and (e) solve complex problems in team and function effectively in a team environment to achieve a common goal.
Contribution of the Subject to the Attainment of the Programme Outcomes	Programme Outcome 3: this subject contributes to developing students' understanding in security requirements in modern database systems. Programme Outcome 4: this subject empowers the students to design and implement database applications to meet the security requirements Programme Outcome 6: this subject contributes to cultivating teamwork spirit through group project.

Subject Synopsis/ Indicative Syllabus	**Topic**
	1. Overview of Database Concepts Common database technologies and database application architectures, including ER modelling and existing relational database management systems such as MySQL and Oracle; advanced database technologies, including object-oriented databases and distributed databases.
	2. Introduction to Database Security Threats to databases; commonly accepted security goals (integrity, availability and confidentiality); kinds of security control measures.
	3. Access Control Database authorisation, including discretionary security mechanisms and mandatory security mechanisms.
	4. File System Security FAT, NTFS, HFS, disk encryption.
	5. Inference Control Nature of statistical database and the inference control mechanism to prevent detailed confidential information.
	6. Advanced Topics Including security threats with respect to SQL injection attacks, virtual private databases and database auditing, searchable encryption, blockchain and decentralised storage.
Teaching/ Learning Methodology	During the lectures, students will come across the common concepts and theories in database security issues. Those concepts and theories would be explained with reference to real database systems such as Oracle and MySQL. Hands-on exercises in tutorial/laboratory will be included to allow students to explore and analyse practical problems and topics. Group project to solve database security problems will help students to integrate and apply what they have learnt.

Specific assessment methods/tasks	% weighting	Intended subject learning outcomes to be assessed				
		a	b	c	d	e
Continuous Assessment	**55%**	✓	✓	✓	✓	✓
Examination	**45%**	✓	✓	✓	✓	
Total	100%					

Types of assessments include assignments, project, test and examination. Assignments are designed to reinforce the concepts and mechanisms learned in the lecture and laboratory, by solving bigger problems. Project is used to develop students' analytic and problem-solving skills by developing a practical database security policy. Test and examination are used to assess independent problem solving and critical thinking skills.

Student Study Effort Expected	Class contact:	
	▪ Lecture	39Hrs.
	Other student study effort:	
	▪ Assignments, Projects, Self-study, Test and Exam Preparation	66 Hrs.
	Total student study effort	105 Hrs.

Reading List and References

Reference Books:

1. Vinicius M. Grippa and Sergey Kuzmichev, Learning MySQL (2nd Edition), O'Reilly Media, Inc., 2021

2. Ettore Galluccio, Edoardo Caselli, Gabriele Lombari, SQL Injection Strategies, 2020

3. Afyouni, Hassan A., *Database Security and Auditing: Protecting Data Integrity and Accessibility*, Course Technology, ISBN 0619215593, 2006.

4. Basta, Alfred and Zgola, Melissa, *Database Security*, Cengage Learning, ISBN 1435453905, 2011.