1.	Name of Course/Module	Password Authentication and Biometrics
2.	Course Code	TPA3421
3.	Status of Subject	Major for B.IT Security Technology
4.	MQF Level/Stage	Bachelor Degree – MQF Level 6
5.	Version (state the date of the last Senate approval)	June 2012
6.	Requirement for Registration	TSC2211 Computer Security
7.	Name(s) of academic/teaching staff	Ooi Shih Yin Chong Siew Chin Ong Thian Song
8.	Semester and Year offered	Trimester 1 (Delta Level)

9.	Objective of the course/module in the programme :	
	To introduce the fundamentals of computer authentication, including password, token and biometrics based authentications.	
10.	Learning Outcomes :	
	At the completion of the subject, students should be able to: LO1: Describe the various techniques and algorithms underlying password authentication and biometric technology (Cognitive, Level 1) LO2: Identify the advantages and disadvantages of applying password authentication and biometrics in different security systems (Cognitive, Level 4) LO3: Plan and design the practical security solutions for real-world applications using password authentication and biometrics (Cognitive, Level 5) LO4: Evaluate the various industry standards available for biometric implementation (Cognitive, Level 6)	
11.	Synopsis:	
	This course prepares the students with the knowledge on computer authentication methodology, including password, token and biometrics based authentications. After learning this course, students shall be able to evaluate the techniques mentioned above by looking at the situations where different techniques succeed or fail, and examining ways to strengthen them.	
	Kursus ini memperkenalkan pengesahan komputer yang merangkumi teknik pengesahan yang berdasarkan kata laluan, token dan biometrik. Pelajar-pelajar akan dapat menilai teknik pengesahan yang disebutkan dengan melihat kepada keadaan di mana teknik tertentu berjaya atau gagal dan juga cara untuk memperkuatkannya.	
12.	Mapping of Subject to Programme Outcomes :	
	Programme Outcomes	**% of Contribution**
	PO1: Apply soft skills in work and career related activities	40

	PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to security technology	40
	PO8: Apply principles and knowledge of security technology in relevant areas	20

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written Test	15%
Assignment	Case Study, and Report	15%
Quiz	Written Quiz	10%
Final Exam	Written Exam	60%

14. Details of Subject

Topics	Mode of Delivery	
	Lecture	Tutorial
1. Introduction to Authentication Authentication Definition. The Importance of Authentication to Today Computer Security System. Element of an Authentication System. Various Kind of Authentication: Password, Token, and Biometrics. Two or Multiple Factor Authentication.	2	1
2. Password and Token Based Authentication UserID and Static Passwords. Dynamic Passwords: One-Time Password, Challenge Response Schemes, X9.9, S/Key. Password Management. Token Based Authentication: Passive and Active Tokens, One Time Password Keys, Attacks on One Time Password, Smartcard, Digital Signature etc.	2	1
3. Automatic Identification System Card technologies: Optical cards, IC cards, magnetic stripe cards. Coercivity. Contactless smart cards. Radio-Frequency Identification.	2	1
4. Introduction to Biometrics Definition and Biometric Technology Overview. Biometric Authentication Modes: Identification and Verification. Architecture of Biometric Systems. Evaluation Schemes: FAR, FRR, ROC, etc.	2	1
5. Physiological Based Biometrics – Face Recognition Face Recognition Overview. Devices, Algorithms, and Applications on Face Recognition in Industry.	2	1
6. Physiological Based Biometrics – Fingerprint Recognition Fingerprint Recognition Overview. Devices, Algorithms, and Applications on Fingerprint Recognition in Industry.	2	1
7. Physiological Based Biometrics - Others Iris, Retina, Hand Geometry, Palmprint, Thermal Imaging, and Ear Biometrics Overview. Devices, Algorithms, and Applications on Iris, Retina, Hand Geometry, Palmprint, Thermal Imaging, and Ear Biometrics in Industry.	2	1

	8. Behavioural Based Biometrics Speech, Signature, and Keystroke Biometrics Overview. Devices, Algorithms, and Applications on Speech, Signature, and Keystroke Biometrics in Industry.	2	1
	9. Emerging Biometric Technologies Ear recognition. Odour recognition. Gait recognition. Footprint recognition.	4	2
	10. Practical Issues of Using Biometrics Biometric System Comparison. Biometric System Performance. Industry Standard: BioAPI, BAPI, CBEFF, HA-API. Identifying Law and Policy Concerns. Biometric Encryption.	2	1
	11. Case Studies Case Study on Commercial Authentication System: Kerberos, SSL, SSH, etc. Case Study on Biometric Encryption.	2	1
	Total	**24**	**12**

15. Tutorial

- Authentication using Password, Token, and Biometrics.
- Exploring the possible techniques in securing the password and token.
- Exploring the possible image processing, feature extraction, and classification techniques in face, fingerprint, iris, retina, hand geometry, palmprint, thermal imaging, ear, speech, signature, and keystroke biometrics.
- Evaluating the performance of different authentication techniques on different applications, including their deployment cost.
- Examining the recent related case studies in Malaysia.

16.

Total Student Learning Time (SLT)	Face to Face (Hour)	Total Guided and Independent Learning
Lecture	24	24
Tutorials	12	12
Laboratory/Practical	-	-
Presentation	-	-
Assignment	-	12
Mid Term Test	1	3
Lab Test	-	-
Final Exam	2	18
Quiz	9	9
Sub Total	48	78
Total SLT	126/40 = 3.15 => 3	

17.	Credit Value	3
18.	Reading Materials :	
	Textbook	Reference Materials

	1. David Salomon, “Elements of Computer Security (Undergraduate Topics in Computer Science)”, 1st Ed. Springer, 2010. ISBN-13: 978-0857290052	1. Anil K. Jain, Patrick Flynn, Arun A. Ross, “Handbook of Biometrics”, Springer, 2010. ISBN-13: 978-1441943750 2. Dobromir Todorov,“Mechanics of User Identification and Authentication: Fundamentals of Identity Management”, Auerbach Publications, 2007. ISBN-13: 978-1420052190 3. Mark Burnett, Dave Kleiman, “Perfect Password: Selection, Protection, Authentication”, Syngress, 2005. ISBN-13: 978-1597490412 4. Richard E. Smith, “From Password to Public Keys”, Addison-Wesley Professional, 2001. ISBN-13: 978-0201615999
19.	Appendix (to be compiled when submitting the complete syllabus for the programme) : 1. Mission and Vision of the University and Faculty 2. Mapping of Programme Objectives to Vision and Mission of Faculty and University 3. Mapping of Programme Outcome to Programme Objectives 4. Programme Objective and Outcomes (Measurement and Descriptions)	