MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Password Authentication and Biometrics
2.	Course Code	TPB 3141
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT (Hons) Security Technology
4.	MQF Level/Stage Note : *Certificate – MQF Level 3* *Diploma – MQF Level 4* *Bachelor – MQF Level 6* *Masters – MQF Level 7* *Doctoral – MQF Level 8*	Bachelor Degree – MQF Level 6
5.	Version (State the date of the Senate approval – history of previous and current approval date)	Date of previous version : June 2015 Date of current version : March 2016
6.	Pre-Requisite	TCS2251 Computer Security
7.	Name(s) of academic/teaching staff	Ooi Shih Yin
8.	Semester and Year offered	Trimester 1, Year 3
9.	Objective of the course in the programme : To introduce the fundamentals of computer authentication, including password, token and biometrics based authentications.	
10.	Justification for including the course in the programme : 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.	

11.	Course Learning Outcomes :		Domain	Level
	LO1	Describe the various techniques and algorithms underlying password authentication and biometric technology.	Cognitive	1
	LO2	Identify the advantages and disadvantages of applying password authentication and biometrics in different security systems.	Cognitive	4

SUMMARY OF INFORMATION ON EACH COURSE

	LO3	Plan and design the practical security solutions for real-world applications using password authentication and biometrics.	Cognitive	5
	LO4	Evaluate the various industry standards available for biometric implementation.	Cognitive	6

12. Mapping of Learning Outcomes to Programme Outcomes :

Learning Outcomes	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
LO1	X						X		
LO2	X						X		
LO3	X						X	X	
LO4	X						X	X	

13. Assessment Methods and Types :

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

14. Mapping of assessment components to learning outcomes (LOs)

Assessment Components	LO1	LO2	LO3	LO4
Mid Test	18	18		
Assignment			60	100
Quiz	12	12	40	
Final Exam	70	70		

15. Details of Course

Topics	Mode of Delivery (eg : Lecture, Tutorial, Workshop, Seminar, etc.) Indicate allocation of SLT (lecture, tutorial, lab) for each subtopic	
	Lecture	Tutorial
1. **Access Control Using Biometrics** Introduction. Biometric Methods. Biometric Security Environment. Access Control for Physical Facilities and Resources. Techniques for Preventing Theft and Destruction. Computer Authentication and Authorization.	2	2
2. **Biometric Traits and Modalities** Biometric Characteristics. Identification and Verification Concepts. Biometric Methodologies. Finger, Palm and Hand Biometrics. Iris Biometrics. Face Biometrics. Voice Biometrics. Signature Biometrics. Emerging Biometric	2	2

		Technologies. Biometric Method Advantages and Disadvantages.		
	3.	**Biometric Applications and Solutions** Legacy Applications Requirements. The Need for Secure Transactions. Biometric Application Environment. Using Biometric Methods and Applications. Biometric Applications and Vendors. Future Applications.	2	2
	4.	**Repositories for Database and Template Storage** Legacy Data and Database Primer. Database Management System. Major Features of a DBMS. Database and Repository Security. Biometric Databases.	2	2
	5.	**Legacy and Biometric Systems** Computer and Information System Basics. Security Systems Design. E-Commerce Security and Secure Protocols. Reactive and Proactive Security Systems. Biometric System Basics. Issues with Biometric Systems. Card Systems. Commercial and Government Biometric Systems. Biometric Products.	2	2
	6.	**Biometric Multi-Factor System Design** Multibiometrics Defined, Components, Systems Issues. Effects of Multibiometrics on the User. Production of Multibiometric Systems.	2	2
	7.	**Policy and Program Management** Corporate Security Policy. Identity Management. System Program Management. Biometrics Policies and Procedures. Biometric Methods Assessment. Biometric Security and Business Ethics. Governance. Electronic Access Control. Privacy Concerns.	2	2
	8.	**Security and Access Technologies** Authentication and Access Control Mechanism. Security Elements and Components. Computer and Network Resource Access Control. Digital Certificates and Signatures. Proven Biometric Technologies.	2	2
	9.	**System Integrity and Accessibility** Confidentiality and Integrity. Accessibility and Availability. Securing Mechanized Transactions. Enterprise Threats and Vulnerabilities. Performance Measures. Future Developments for Biometrics Data Integrity Assurance.	2	2
	10.	**Security and Privacy Issues** Computer Privacy Basics. Biometric Systems Security and Privacy. Barriers to Using Biometrics. Biometrics and Cryptography. Smart Card and RFID Issues.	2	2

SUMMARY OF INFORMATION ON EACH COURSE

	11. **Implementation and Operation Issues** Security Evaluation. Security Cost Justification. Security Implementation Issues. Evaluation Protocols. Physical Security Controls. Disaster Recovery Planning.	2	2
	12. **Standards and Legal Environment** Standards and Practices. Standards Organizations. Smart Card Standards and Interoperability. Security Standards. Biometric Standards. Engineering/ Specifications.	2	2
	Total	**24**	**12**

15.

Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
Lecture	24	24
Tutorials	12	12
Laboratory/Practical	0	0
Presentation	2	6
Assignment	0	11
Mid Term Test	2	6
Final Exam	2	15
Quizzes	4 times	4
Sub Total	42	78
Total SLT	**120**	
Credit Value	**120/40 = 3**	

16. Reading Materials :

Textbooks

1. Julian Ashbourn, (2015).Practical Biometrics: From Aspiration to Implementation. Springer. ISBN-13: 978-1447167167.
2. Robert Newman, (2010). Security and Access Control Using Biometric Technologies. Cengage Learning. ISBN-13: 978-1-4354-4105-7.

Reference Material (including 'Statutes' for Law)

1. Nathan Clarke, (2014). Transparent User Authentication: Biometrics, RFID and Behavioural Profiling. Springer. ISBN-13: 978-1447160113.
2. David Salomon, (2010). Elements of Computer Security (Undergraduate Topics in Computer Science), 1st Ed. Springer. ISBN-13: 978-0857290052
3. Anil K. Jain, Patrick Flynn, Arun A. Ross, (2010). Handbook of Biometrics, Springer. ISBN-13: 978-1441943750
4. Dobromir Todorov, (2007). Mechanics of User Identification and Authentication: Fundamentals of Identity Management, Auerbach Publications. ISBN-13: 978-1420052190

Appendix (to be compiled when submitting the complete syllabus for the programme) :

1. Mission and Vision of the University and Faculty

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

2. Programme Objectives or Programme Educational Objectives
3. Programme Outcomes (POs)
4. Mapping of POs to the 8 MQF domain
5. Summary of the Bloom's Taxonomy's Domain Coverage in all the Los in the format below :

Subject	Learning Outcomes (please state the learning 0utcomes)	Bloom's Taxonomy Domain		
		Affective	Cognitive	Psychomotor
ABC1234	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			
DEF5678	Learning Outcome 1			
	Learning Outcome 2			
	Learning Outcome 3			
	Learning Outcome 4			

6. Summary of LO to PO measurement
7. Measurement and Tabulation of result for LO achievement
8. Measurement Tabulation of result for PO achievement