MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

1.	Name of Course	Information Assurance and Security
2.	Course Code	TIA 2221
3.	Status of Course [Applies to (cohort)]	Specialisation Core for B.IT 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 – MQF Level 6
5.	Version (State the date of the Senate approval – history of previous and current approval date)	Date of previous version: - Date of current version: June 2014
6.	Pre-Requisite	None
7.	Name(s) of academic/teaching staff	Jaya Kumar Krishnan Rouzbeh Behnia
8.	Semester and Year offered	Trimester 2, Year 2
9.	Objective of the course in the programme: This course exposes students to an enterprise security policy relating to information assurance program development and implementation.	
10.	Justification for including the course in the programme: Information assurance and security is one of the major domains in computer security study, where it exposes students to the concepts and technology of current security products and protocols into scalable, practical working solutions for defending the enterprise.	

11.

Course Learning Outcomes :	Domain	Level
LO1 Describe of all the concepts and technical terms related to information assurance and security.	Cognitive	1
LO2 Explain the concepts of successful security applications current in business environment.	Cognitive	5
LO3 Describe the role of information security in creating a sustained strategic advantage.	Cognitive	6
LO4 Analyse the security of information assurance and security schemes.	Cognitive	4
LO5 Differentiate information assurance and security model or framework.	Cognitive	4

12. Mapping of Learning Outcomes to Programme Outcomes :

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

SUMMARY OF INFORMATION ON EACH COURSE

	LO3		X		X	X				
	LO4		X			X				
	LO5		X		X					

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Mid Test	Written test	30%
Assignment	Written assignment	15%
Quizzes	Written quizzes	5%
Final Examination	Written examination	50%

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

Assessment Components	LO1	LO2	LO3	LO4	LO5
Mid Test	35.29	35.29	35.29		
Assignment				100	100
Quizzes	5.88	5.88	5.88		
Final Examination	58.82	58.82	58.82		

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
Dynamic Modelling of the Cyber Security Threat Problem: The Black Market for Vulnerabilities Discusses the possible growth of black markets (BMs) for software vulnerabilities and factors affecting their spread.	2	1
Insider Threat Prevention, Detection and Mitigation Introduces the insider threat and discusses methods for preventing, detecting, and responding to the threat.	2	1
An Autocorrelation Methodology for the Assessment of Security Assurance Describes a methodology for assessing security infrastructure effectiveness utilizing formal mathematical models. The goal of this methodology is to determine the relatedness of effects on security operations from independent security events and from security event categories, identify opportunities for increased efficiency in the security infrastructure yielding time savings in the security operations and identify combinations of security	4	2

	events which compromise the security infrastructure.		
	Human Factors in Security: The Role of Information Security Professionals within Organizations Contributes to a better understanding of role conflict, skill expectations, and the value of information technology (IT) security professionals in organizations.	3	1
	Diagnosing Misfits, Inducing Requirements, and Delineating Transformations within Computer Network Operations Organizations Use Contingency Theory research to inform leaders and policy makers regarding how to bring their Computer Networked Operations (CNO) organizations and approaches into better fit, and hence to improve performance.	4	2
	An Approach to Managing Identity Fraud Outlines components of a strategy for government and a conceptual identity fraud management framework for organizations. Identity crime, related cybercrimes and information systems security breaches are insidious motivators for governments and organizations to protect and secure their systems, databases and other assets against intrusion and loss.	3	2
	A Repeatable Collaboration Process for Incident Response Planning Presents a repeatable collaboration process as an approach for developing a comprehensive Incident Response Plan for an organization or team.	3	2
	Server Hardening Model Development: A Methodology-Based Approach to Increased System Security Essential server security components and develop a set of logical steps to build hardened servers. The authors outline techniques to examine servers in both the Linux/UNIX and the Windows Environment for security flaws from both the internal and external perspectives.	4	2
	Trusted Computing: Evolution and Direction To effectively combat cyber threats, our network defences must be equipped to thwart dangerous attacks.	3	1

SUMMARY OF INFORMATION ON EACH COURSE

	However, our software-dominated defences are woefully inadequate. The Trusted Computing Group has embarked on a mission to use an open standards-based interoperability framework utilizing both hardware and software implementations to defend against computer attacks.		
	Total	**28**	**14**

	Total Student Learning Time (SLT)	Face to Face / Guided Learning	Independent Learning
	Lecture	28	28
	Tutorials	14	14
	Laboratory/Practical	0	0
	Presentation	0	0
	Assignment	0	10
	Mid Term Test	1	3
	Final Exam	2	18
	Sub Total	2 times	2
	Total SLT	**120**	
16.	Credit Value	**120/40 = 3**	

17. Reading Materials :

Textbooks

1.Corey Schou, Steven Hernandez (2014). Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, ISBN-13: 978-0071821650, McGraw Hill.

2. Kenneth J. Knapp (2009). Cyber Security and Global Information Assurance:
Threat Analysis and Response Solution, ISBN-10: 1605663263.Information Science Reference

Reference Material (including 'Statutes' for Law)

1.Kim, Michael G.Solomon (2013). Fundamentals of Information Systems Security (Jones & Bartlett Learning Information Systems Security & Assurance), 2nd edition, ISBN-13: 978-1284031621, Jones & Bartlett Learning.

2.Andrew Blyth, Gerald L.Kovacich (2008).
Information Assurance: Security in the Information Environment (Computer Communications and Networks), ISBN-10: ISBN-10: 1846282667. Springer.

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

1. Mission and Vision of the University and Faculty
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 :

MULTIMEDIA UNIVERSITY®

SUMMARY OF INFORMATION ON EACH COURSE

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