1.	Name of Course/Module	Network Security and Management
2.	Course Code	TNS2201
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	TCE 2321 Computer Networks, AND (TCD2221 Cryptography and Data Security, OR TAC2681 Applied Cryptography)
7.	Name(s) of academic/teaching staff	Hiew Bee Yan Goh Kah Ong Michael
8.	Semester and Year offered	Trimester 1 (Delta Level)
9.	Objective of the course/module in the programme :	
	This course focuses on the basic concepts of network security. It provides the students with an understanding of common problems faced and the mechanisms to protect information on the network.	
10.	Learning Outcomes :	
	By the end of the course, students should be able to: LO1: Define the network management components, its motivation, constraints and issues. (Cognitive, Level 1) LO2: Explain the different issues affecting the security of networks and relate the solutions to these issues. (Cognitive, Level 6) LO3: Identify the common areas and models currently in use to secure networks and networked applications. (Cognitive, Level 4) LO4: Compare and contrast the security algorithms used in the networked environment. (Cognitive, Level 6)	
11.	Synopsis:	
	This course introduces student to techniques in Computer Network Security Management and also highlights some security problems which arises as well as potential solution.	
	Kursus ini adalah untuk memperkenalkan pelajar kepada teknik pengurusan Keselamatan Rangkaian Komputer dan masalah keselamatan yang kerap dihadapi di dalam bidang ini serta penyelesaian kepada masalah ini.	
12.	Mapping of Subject to Programme Outcomes :	
	Programme Outcomes	**% of Contribution**
	PO1: Apply soft skills in work and career related activities	11.11
	PO7: Demonstrate knowledge and understanding of essential facts, concepts, principles, and theories relating to security technology	44.44
	PO8: Apply principles and knowledge of security technology in relevant areas	33.33

	PO9: Design, integrate, implement and manage information technology solutions and resources, and recognise the impact of technology on individuals, organisations and society	11.11

13. Assessment Methods and Types :

Method and Type	Description/Details	Percentage
Test	Mid term test	20%
Assignment	Report	20%
Final Exam	Final Exam	60%

14. Details of Subject

Topics	Mode of Delivery	
	Lecture	Tutorial
1. Overview of Network Security • Security attacks, security services, security mechanisms. • Model for Network Security	2	1
2. Conventional Encryption & Message Confidentiality • Overview of Cryptography • Conventional Encryption Principles • Conventional Encryption Algorithms • Cipher Block Modes of Operation • Location of Encryption Devices • Key Distribution	3	1.5
3. Public-Key Cryptography & Message Authentication • Approaches to Message Authentication • Secure Hash Functions and HMAC • Public-Key Cryptography Principles • Public-Key Cryptography Algorithms • Digital Signatures • Key Management	4	2
4. Authentication Applications • Security Concerns • Kerberos • X.509 Authentication Service	2	1
5. Electronic Mail Security • Pretty Good Privacy (PGP) • S/MIME	2	1
6. IP Security • IP Security Overview • IP Security Architecture • Authentication Header (AH) • Encapsulating Security Payload (ESP) • Combinations of Security Associations (SAs) • Key Management	2	1
7. Web Security • Web Security Considerations • Secure Socket Layer (SSL) • Transport Layer Security (TLS) • Secure Electronic Transaction (SET)	2	1

	8. Network Management Security • Basic Concepts of SNMP • SNMPv1 Community Facility • SNMPv3	2	1
	9. Intruders and Viruses • Intruders - Intrusion Techniques - Password Protection - Password Selection Strategies - Intrusion Detection • Viruses and Related Threats - Malicious Programs - The Nature of Viruses - Antivirus Approaches - Advanced Antivirus Techniques	2	1
	10. Firewalls • Firewall Design Principles • Firewall Characteristics • Types of Firewalls • Firewall Configurations • Trusted Systems - Data Access Control - The Concept of Trusted systems - Trojan Horse Defense	2	1
	11. Wireless Networks Security • IEEE 802.11 - WLAN Vulnerabilities - WEP Vulnerabilities - WLAN Security Solutions • Bluetooth - Security Architecture - Security Model - Authentication & Encryption - Risks & Limitations • GSM Security • UMTS Security	3	1.5
	12. Network Management • Introduction to Network Management: motivation and major components • Network management in the real world: External pressures and constraints, time issues, tools of the trade	2	1
	Total	**28**	**14**
15.	Tutorials		

<table>
<tr><td></td><td colspan="3">

- Overview of Network Security
- Conventional Encryption & Message Confidentiality
- Public-Key Cryptography & Message Authentication
- Authentication Applications
- Email Security
- IP Security
- Web Security
- Network Management Security
- Intruders and Viruses
- Firewalls
- Wireless Networks Security
- Network Management

</td></tr>
<tr><td rowspan="11">16.</td><td>Total Student Learning Time (SLT)</td><td>Face to Face (Hour)</td><td>Total Guided and Independent Learning</td></tr>
<tr><td>Lecture</td><td>28</td><td>28</td></tr>
<tr><td>Tutorials</td><td>14</td><td>14</td></tr>
<tr><td>Laboratory/Practical</td><td>-</td><td>-</td></tr>
<tr><td>Presentation</td><td>-</td><td>-</td></tr>
<tr><td>Assignment</td><td>-</td><td>10</td></tr>
<tr><td>Mid Term Test</td><td>1</td><td>5</td></tr>
<tr><td>Final Exam</td><td>2</td><td>20</td></tr>
<tr><td>Quizzes</td><td>-</td><td>-</td></tr>
<tr><td>Sub Total</td><td>45</td><td>77</td></tr>
<tr><td></td><td>Total SLT</td><td colspan="2">122/40 = 3.05 => 3</td></tr>
<tr><td>17.</td><td colspan="2">Credit Value</td><td>3</td></tr>
<tr><td rowspan="3">18.</td><td colspan="3">Reading Materials :</td></tr>
<tr><td colspan="2">Textbook</td><td>Reference Materials</td></tr>
<tr><td colspan="2">1. William Stallings, Cryptography and Network Security: Principles and Practice: International Version, 5th Edition, Prentice Hall, 2011. [ISBN: 013705632X]</td><td>1. William Stallings, Network Security Essentials: Applications and Standards, 4/E, Prentice Hall, 2011</td></tr>
<tr><td>19.</td><td colspan="3">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)</td></tr>
</table>