MODULE SPECIFICATION PROFORMA

Module Code:	COM645

Module Title:	Network Security

Level:	6	**Credit Value:**	20

Cost Centre(s):	GACP	JACS3 **code**:	I120

Faculty:	Arts, Science and Technology	**Module Leader:**	Dr. Paul Comerford

Scheduled learning and teaching hours	24 hrs
Guided independent study	176 hrs
Placement	0 hrs
Module duration (total hours)	200 hrs

Programme(s) in which to be offered (not including exit awards)	Core	Option
BSc (Hons) Computer Networks and Security	✓	☐
BSc (Hons) Cyber Security	✓	☐
BSc (Hons) Applied Cyber Security	✓	☐

Pre-requisites
None

Office use only
Initial approval: 30/08/2018 Version no:2
With effect from: 01/09/2018
Date and details of revision: Jan 22: addition of BSc Applied Cyber Security Version no:

Module Aims

The aim of this module is to provide students with a critical understanding of security threats against network and cloud computing systems and the security measures designed to protect such systems. The module will explicitly develop students' knowledge and experience in the design and application of network and cloud security solutions. The module will also equip students for further academic study and future employability in the area of computer security.

The curriculum provides an introduction to the core security concepts and skills needed for the installation, troubleshooting, and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices.

Intended Learning Outcomes

Key skills for employability

KS1	Written, oral and media communication skills
KS2	Leadership, team working and networking skills
KS3	Opportunity, creativity and problem solving skills
KS4	Information technology skills and digital literacy
KS5	Information management skills
KS6	Research skills
KS7	Intercultural and sustainability skills
KS8	Career management skills
KS9	Learning to learn (managing personal and professional development, self-management)
KS10	Numeracy

At the end of this module, students will be able to		Key Skills	
1	Critically analyse security threats in the digital world within a professional and ethical context.	KS1, KS2, KS3, KS4, KS5, KS6	
2	Model and design a range of modern symmetric and asymmetric encryption problems appropriate to modern communication systems.	KS1, KS2, KS3, KS4, KS5, KS6	
3	Apply a range of security tools and algorithms related to computer security.	KS4, KS5	
4	Design and synthesise security protocols and algorithms.	KS1, KS2, KS3, KS4, KS5, KS6	

5	Critically analyse ethical issues relating to privacy and anonymity in today's digital society.	KS1, KS2, KS3, KS4, KS5, KS6	
6	Justify the selection of appropriate standards in the context creating appropriate security policies.	KS1, KS2, KS3, KS4, KS5, KS6	

Transferable skills and other attributes

- Personal motivation, organisation and time management
- Ability to collaborate and plan
- Written and verbal communication skills
- Research and analytical skills

Derogations

None

Assessment:

Indicative Assessment Tasks:

Assessment 1 will comprise of a written assignment covering the syllabus topics. This will be in the form of a case study with a research element. Assessment 2 is a practical test to be completed on the lab and will assess a student's ability to design and configure an appropriate network security solution for a given scenario including configuration of firewalls, VPNs and other network security measures. Assessment 3 will be an in-class test hosted on the University VLE and will assess students on their knowledge and understanding of the course content.

Assessment number	Learning Outcomes to be met	Type of assessment	Weighting (%)	Duration (if exam)	Word count (or equivalent if appropriate)
1	1-6	Coursework	40		2500
2	1-6	Practical	30	2 hours	
3	1-6	In-class test	30	1.5 hours	

Learning and Teaching Strategies:

The learning on this module will be through a series, on-line learning materials and tutorial supports. Teaching and learning will be delivered through (a) lectures (b) tutorials/workshops (c) laboratory and group assignments (d) self-directed study and research: self-selected reading, workshop preparation, literature searching. Each topic will be

introduced in lectures, followed by tutorials/workshops to deepen the theoretical principles with practical applications. Some of the tutorials will be group based and some individual.

Syllabus outline:

• Elements of applied cryptography
• Information security concepts
• Securing the network.
• Network security applications:
•Authentication applications
•IP security
•Web security
•E-Mail security
Systems security
•Intruders
•Malicious software
•Firewalls
•Strategies of developing and maintaining a network security
• Cloud computing fundamentals
• Cloud computing architecture
• Cloud computing software security
• Risk issues of cloud computing
• Cloud computing security architecture

Indicative Bibliography:

Essential reading

Pfleeger, C.P., Pfleeger, S.L., and Marguiles, J. (2015). *Security in Computing*. 5th ed. Prentice-Hall.

Stallings, W. (2017), *Cryptography and Network Security: Principles and Practices*. 7th ed. Upper Saddle River, NJ: Pearson/Prentice Hall.

Santos, O. and Stuppi, J. (2015), *CCNA Security 210-260 Official Cert Guide*. Indianapollis IN: Cisco Press.

Other indicative reading

Shostack, A. (2014), *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons.

Engebretson, P. and Kennedy, D. (2013), *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. 2nd ed. Waltham, USA: Syngress.