# MODULE SPECIFICATION PROFORMA

| | |
|---|---|
| **Module Code:** | COM538 |

| | |
|---|---|
| **Module Title:** | Cyber Security and Forensics |

| | | | |
|---|---|---|---|
| **Level:** | 5 | **Credit Value:** | 20 |

| | | | |
|---|---|---|---|
| **Cost Centre(s):** | GACP | JACS3 **code**: | I190 |

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

| | |
|---|---|
| Scheduled learning and teaching hours | 30 hrs |
| Guided independent study | 170 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 Science | ✓ | ☐ |
| 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 DA programme title Version no:

**Module Aims**

This module will give students a broad grounding in the basics of security and digital forensics. It will introduce students to technological security basics, beginning with physical and environmental security factors and the identification and management of risks to security and privacy. Upon competition of the module, students will be competent in discussing and analysing security threats by evaluating the potential business impact, and be competent in determining appropriate interventions and techniques to mitigate and monitor these risks. The module also deals with forensics and provides students with exposure to data recovery techniques that could be used in criminal investigation and data recovery scenarios.

**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 | Discuss the computer security and forensic investigation landscape | KS1 | KS4 |
| | | KS5 | KS7 |
| | | KS8 | KS10 |
| 2 | Recognise and manage security and privacy threats using technological solutions | KS3 | KS4 |
| | | KS5 | KS10 |
| | | | |
| 3 | Apply forensic investigation tools to recover and collate lost and hidden data | KS1 | KS4 |
| | | KS5 | KS6 |
| | | KS10 | |

**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 is formed of two components: a class test, which will validate student acquisition and understanding of theoretical principles that relate to computer security and forensics; and a practical test, which will require students to demonstrate proficiency in configuring and testing security mechanisms as well as applying forensic investigation skills to recover lost data and form a case or profile under time-limited conditions. As such, the assignment strategy supports the intentions of the learning outcomes: to ensure students have a competent knowledge and understanding in Cyber Security and Forensic principles, but with greater emphasis being placed upon their ability to implement these techniques and technologies.

| Assessment number | Learning Outcomes to be met | Type of assessment | Weighting (%) | Duration (if exam) | Word count (or equivalent if appropriate) |
|---|---|---|---|---|---|
| 1 | 1 | In-class test | 30% | 1 hour | N/A |
| 2 | 2, 3 | Coursework | 70% | N/A | 3 hours |

**Learning and Teaching Strategies:**

This module has an emphasis in the practical issues related to Cyber Security and Forensics and will be delivered using a combination of formal lecturers, tutorials, practical demonstrations and lab sessions. The split between theory and practical teaching and learning is approximately 40% and 60% respectively. The formal delivery will be supplemented by reading materials, such as academic papers and industry technology reports, which will be made available via the University’s VLE.

**Syllabus outline:**

Threats and risks
Asset management and physical security
Risk management and security standards
Predictive business impact analysis
Viruses, malware and other nasty software
Authentication
Access control
Cryptography
Software security
Operating systems security
Phishing and email privacy
Security management
Forensic investigation
Data recovery and file analysis
Email and web forensics
Legal issues, cyber crime and ethics

**Indicative Bibliography:**

**Essential reading**

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

Stallings, W. and Brown, L. (2017). *Computer Security: Principles and Practice*. 4th ed. Boston: Pearson.

**Other indicative reading**

Howard, M., LeBlanc, D. and Viega, J. (2009). *The 24 Deadly Sins of Software Security*. California: McGraw-Hill/Osborne.

Davis, C., Cowen, D. and Philipp, A. (2009), *Hacking Exposed Computer Forensics: Secrets & Solutions*. 2nd ed. London: McGraw-Hill/Osborne.

Nestlet, V.J., Harrison, K., Hirsch, M.P., and Conklin, W.A. (2014), *Principles of Computer Security Lab Manual*. 4th ed. London: McGraw-Hill/Osborne.