Programme Specification

Computer Security and Forensics {Foundation} [GCET]

Version: 2022-23, v1.0, 11 Jan 2024

Contents

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Computer Security and Forensics {Foundation} [GCET]

Highest award: BSc (Hons) Computer Security and Forensics

Interim award: BSc Computer Security and Forensics

Interim award: DipHE Computer Security and Forensics

Interim award: CertHE Computer Security and Forensics

Awarding institution: UWE Bristol

Affiliated institutions: Global College of Engineering and Technology (GCET)

Teaching institutions: Global College of Engineering and Technology (GCET)

Study abroad: Yes

Year abroad: No

Sandwich year: No

Credit recognition: No

School responsible for the programme: FET Dept of Computer Sci & Creative Tech, Faculty of Environment & Technology

Professional, statutory or regulatory bodies: Not applicable

Modes of delivery: Full-time

Entry requirements: For the current entry requirements see the UWE public website.

For implementation from: 01 February 2019

Programme code: G4HC00

Section 2: Programme Overview, Aims and Learning Outcomes

Part A: Programme Overview, Aims and Learning Outcomes

Overview: The general aims of the programme are:

To prepare students for careers in computer security and computer crime-investigation (e.g.'forensic technician')

To develop problem-solving, communication and other transferable skills applicable to a variety of careers

To prepare students for study for higher degrees in related subjects.

Features of the programme: Professional Practice and Lab Facilities:

Students can access a suite of newly purchased PCs (I7 and I5), modern software, free printing facilities and an IT help desk/line. The General IT lab is open from 8am till 9pm.

Besides the College's plan of extending its IT facilities as the number of students grows, it also has a policy of upgrading 25% of its IT facilities every year.

Technology Enhanced Learning:

Staff members in the department are keen adopters of technology to support and enhance student learning. This includes:

Computer based e-assessment implemented in a number of modules, so that students can take regular short tests with automated computer generated feedback.

Recordings of some lectures (audio and video) which are made available after classes via the university's Virtual Learning Environment.

Mathematics Support:

The Math Support Centre provides drop-in one-to-one tuition each day and a website that provides a portal to a variety of on-line resources in mathematics and statistics.

Educational Aims: The specific aims of the programme are:

To develop knowledge of computer hardware and software systems

To provide an understanding of applicable law, court procedure and the role of the expert witness

To introduce a variety of approaches to both the analysis of the security requirements of computer systems and the investigation of computer crime.

Programme Learning Outcomes:

On successful completion of this programme graduates will achieve the following learning outcomes.

Knowledge and Understanding

A1.   Computer systems and networks Trusted computing base, threats and security policy. Computer security mechanisms in networks and computers at various layers and levels. Security technology innovations.

A2.   Information, data and its representation and organisation in computer systems.

A3.   National legal system and court procedure. Skills and responsibilities of a forensic computing practitioner and expert witness.

A4.   Law pertaining to computer crime and digital evidence and its investigation and legal and commercial aspects of Computer Security and Forensics.

A5.   Security management. Defining, modelling and describing the concepts of trust and security policy. Securing access to services and applications from various devices.

A6.   Tools and techniques for investigating computer crime such as data mining and profiling.

Intellectual Skills

B1.   Critical Thinking

B2.   Analysis

B3.   Synthesis of different types of information

B4.   Evaluation

B5.   Problem Solving

B6.   Appreciate problem contexts

B7.   Balance conflicting objectives

B8.   Construction of logical arguments

B9.   Discussion and debate about technical subjects

Subject/Professional Practice Skills

C1.   Understand a variety of computer systems, configurations and networking topologies

C2.   Understand the professional and legal obligations of forensic computing investigations and communicate with legal personnel at an appropriate level

C3.   Assess a computer crime scene and formulate a strategy for securing the evidence, investigating it impartially, and produce a report in appropriate language

C4.   Describe the key security mechanisms used in access control, authentication, encryption and digital signatures and perform systems analysis in terms of computer security

C5.   Use software libraries and toolkits to implement security aware applications conforming to appropriate designs

C6.   Employ a range of tools and notations to support the activities listed above

C7.   Know the limits of their knowledge and how to extend those limits through self-managed learning

Transferable Skills and other attributes

D1.   Communication skills: to communicate orally or in writing, including, for instance, the results of technical investigations, to peers and/or to "problem owners".

D2.   Self-management skills: to manage one's own time; to meet deadlines; to work with others having gained insights into the problems of team-based systems development.

D3.   IT Skills in Context (to use software in the context of problem-solving investigations, and to interpret findings).

D4.   Problem formulation: To express problems in appropriate notations.

D5.   Progression to independent learning: To gain experience of, and to develop skills in, learning independently of structured class work. For example, to develop the ability to use on-line facilities to further self-study.

D6.   Comprehension of professional literature: to read and to use literature sources appropriate to the discipline to support learning activities.

D7.   Working with Others: to be able to work as a member of a team; to be aware of the benefits and problems which teamwork can bring.

Assessment strategy: The assessment strategy has been designed to test the programme learning outcomes.

Student support: Academic Support:

Academic advice and support is the responsibility of the staff delivering the module in question. Staff are expected to be available outside normal timetabled hours, either by appointment or during published "surgery" hours, in order to offer advice and guidance on matters relating to the material being taught and on its assessment.

Pastoral Care The College offers pastoral care through two routes:

Academic Personal Tutors: All level 1 students are assigned a Personal Academic Tutor, who is an academic member of staff in their department. Students meet individually with their tutor at least twice a year and also participate in group sessions with the Personal Academic Tutor's tutor group (max size 15) during years 1 and 2.

In year 3 project supervisors take on the role of Personal Academic Tutor.

Student Advisers, a team of administrative staff who provide comprehensive, full-time student support service on a drop-in basis or by appointment. Advisers are trained to provide advice on matters commonly of concern, including regulatory and other matters; the Adviser will, when necessary, advise the student to seek advice to from other professional services including the university's Centre for Student Affairs or from members of academic staff.

Part B: Programme Structure

Year 1
Full-time students must take 120 credits from the modules in Year 1.

Year 1 Compulsory Modules (Full-time)
Full-time students must take 120 credits from the modules in Compulsory Modules (Full-time).

Module Code	Module Title	Credit
UFMFEG-30-0	Engineering Experimentation 2022-23	30
UFMFBG-30-0	Foundation Mathematics: Algebra and Calculus 2022-23	30
UFCFGK-30-0	Professional and Academic Skills 2022-23	30
UFCEXX-30-0	Program Design and Implementation 2022-23	30

Year 2
Full-time students must take 120 credits from the modules in Year 2.

Year 2 Compulsory Modules (Full-time)
Full-time students must take 120 credits from the modules in Compulsory Modules (Full-time).

Module Code	Module Title	Credit

UFCF93-30-1	Computer and Network Systems 2023-24	30
UFCFP4-30-1	Computer Crime and Digital Evidence 2023-24	30
UFCFC3-30-1	Introduction to OO Systems Development 2023-24	30
UFCFB3-30-1	Web Programming 2023-24	30

Year 3
Full-time students must take 120 credits from the modules in Year 3.

Year 3 Compulsory Modules (Full-time)
Full-time students must take 120 credits from the modules in Compulsory Modules (Full-time).

Module Code	Module Title	Credit
UFCE8B-30-2	Data Science for Cyber Security 2024-25	30
UFCFW5-30-2	Mobile and Embedded Devices 2024-25	30
UFCFLC-30-2	Secure Computer Networks 2024-25	30
UFCFJ6-30-2	Security and Forensic Tools 2024-25	30

Year 4
Full-time students must take 120 credits from the modules in Year 4.

Year 4 Compulsory Modules (Full-time)
Full-time students must take 90 credits from the modules in Compulsory modules (Full-time).

Module Code	Module Title	Credit
UFCFR4-45-3	Computing Project 2025-26	45
UFCF95-15-3	Entrepreneurial Skills 2025-26	15
UFCFC5-15-3	Forensic Computing Practice 2025-26	15

| UFCFRB-15-3 | Security Management in Practice 2025-26 | 15 |

Year 4 Optional Modules (Full-time)

Full-time students take 15 credits form Optional Modules (Full-time) A and 15 credits from Optional Modules (Full-time) B.

Year 4 Optional Modules (Full-time) A

Module Code	Module Title	Credit
UFCFU3-15-3	Advanced Databases 2025-26	15
UFCFT4-15-3	Cryptography 2025-26	15
UFCFM6-15-3	Requirements Engineering 2025-26	15

Year 4 Optional Modules (Full-time) B

Module Code	Module Title	Credit
UFCF7H-15-3	Mobile Applications 2025-26	15
UFCFVJ-15-3	Professional Development 2025-26	15
UFCFD5-15-3	Technical Writing and Editing 2025-26	15

Part C: Higher Education Achievement Record (HEAR) Synopsis

Graduates in this field would be expected to have an excellent understanding of the internal operation of computers and operating and file systems. They would be able to use appropriate tools to investigate computer-based activities, deploy tools and techniques to prevent security breaches and investigate the mis-use of computer systems and other devices. As much of this work is carried out either directly in support of legal processes an understanding of appropriate legal systems and law would be expected.

Part D: External Reference Points and Benchmarks

This programme is consistent with the UWE 2020 strategy in that its focus on the practice of computer security and forensics aligns with our aim of producing practice-oriented graduates. The partnership with GCET helps to ensure that the programme has an inclusive and global reach. The programme adopts the general approach of the department of Computer Science and Creative Technologies in including input from industry in terms both of visiting speakers and placement and work experience opportunities.

The QAA Computing and Law benchmark statements.

The QAA Subject Benchmark Statements for Computing and for Law were published in 2007, and are applicable to this programme.

The programme clearly falls into the cognate area described by the Computing benchmark. Due to the nature of Forensic Computing practice, much of the computing material is of a technical, low-level nature, with relatively little computing theory. Thus, in terms of the benchmark's high level characterisation of Computing, the emphasis of the programme is on software, communication and interaction and practice, developed within the context of the specialised requirements of the programme. From the body of knowledge the following are considered essential to a study of Forensic Computing: Data Mining (in the context of forensic investigations); Computer Based Systems; Computer Networks; Data Structures and Algorithms, with emphasis on data structures; Distributed Computer Systems; Operating Systems; Programming Fundamentals; Security and Privacy; Web-based Computing. The Computing Benchmark Statement also contains (section 5) statements of the standards expected of graduates at both modal and threshold levels. The team is of the view that graduates of the proposed programme will be able to meet the required standards.

The Law benchmark has been considered during the design process at the 'Law as Subsidiary' level of performance, which focuses on the development of legal skills related to some specific area (in this case Forensic Computing). Though the Statement is targeted at programmes with at least 180 credits of legal subjects, its

expectations also apply to programmes such as Forensic Computing, where the legal aspects make up a relatively small, but very important component. No attempt has been made to include all aspects of law or to provide the foundation for a legal career as such – instead the most important points of law and court procedure are covered. The aim of the design team has been to provide sufficient legal knowledge to be aware of the rules and legal system pertaining to Forensic Computing: as suggested in the Benchmark, the relevant law is treated mainly as data from which legal conclusions or opinions can be derived. It is expected that student will be able to assimilate legal information from a variety of sources and apply the knowledge acquired to computer crime investigation and security analysis.

Part E: Regulations

Approved to University Regulations and Procedures.