Programme Specification

Cyber Security and Digital Forensics [Jan][FT][NepalBrit][3yrs]

Version: 2021-22, v1.0, 05 Nov 2021

Contents

Section 1: Key Programme Details

Part A: Programme Information

Programme title: Cyber Security and Digital Forensics [Jan][FT][NepalBrit][3yrs]

Highest award: BSc (Hons) Cyber Security and Digital Forensics

Interim award: BSc Cyber Security and Digital Forensics

Interim award: DipHE Cyber Security and Digital Forensics

Interim award: CertHE Cyber Security and Digital Forensics

Awarding institution: UWE Bristol

Affiliated institutions: The British College Nepal

Teaching institutions: The British College Nepal

Study abroad: No

Year abroad: No

Sandwich year: Yes

Credit recognition: No

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

Contributing departments: Not applicable

Professional, statutory or regulatory bodies: Not applicable

Apprenticeship: Not applicable

Mode of delivery: Full-time

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

For implementation from: 01 January 2022

Programme code: G4HJ-JAN-FT-NE-G4H4

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

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

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 be able to communicate with legal personnel at an appropriate level

C3. Be able to 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

Part B: Programme Structure

Year 1

The student must take 120 credits from the modules in Year 1.

Year 1 Compulsory Modules

The student must take 120 credits from the modules in Compulsory Modules.

Module Code	Module Title	Credit

UFCF93-30-1	Computer and Network Systems 2021-22	30
UFCFP4-30-1	Computer Crime and Digital Evidence 2021-22	30
UFCFTK-30-1	Introduction to Databases 2021-22	30
UFCFGL-30-1	Programming in C++ 2021-22	30

Year 2

The student must take 120 credits from the modules in Year 2.

Year 2 Compulsory Modules

The student must take 105 credits from the modules in Compulsory Modules.

Module Code	Module Title	Credit
UJUUKM-30-2	Law, Experts and Justice 2022-23	30
UFCFWK-15-2	Operating Systems 2022-23	15
UFCFLC-30-2	Secure Computer Networks 2022-23	30
UFCFJ6-30-2	Security and Forensic Tools 2022-23	30

Year 2 Optional Modules

The student must take 15 credits from the modules in Optional Modules.

Module Code	Module Title	Credit
UFCFVK-15-2	Internet of Things 2022-23	15
UFCFDL-15-2	Secure Embedded Systems 2022-23	15

Year 3

The student must take 120 credits from the modules in Year 3.

Year 3 Compulsory Modules

The student must take 30 credits from the modules in Compulsory Modules.

Module Code	Module Title	Credit

UFCFC5-15-3	Forensic Computing Practice 2023-24	15
UFCFRB-15-3	Security Management in Practice 2023-24	15

Year 3 Optional Modules A

The student must take 30 credits from the modules in Optional Modules A.

Module Code	Module Title	Credit
UFCFXK-30-3	Digital Systems Project 2023-24	30
UFCFM5-30-3	Information Systems Dissertation 2023-24	30

Year 3 Optional Modules B

The student must take 45 credits from the modules in Optional Modules B.

Module Code	Module Title	Credit
UFCFU3-15-3	Advanced Databases 2023-24	15
UFCFT4-15-3	Cryptography 2023-24	15
UFCF95-15-3	Entrepreneurial Skills 2023-24	15
UFCFA5-15-3	Information, Networks and Society 2023-24	15
UFCFM6-15-3	Requirements Engineering 2023-24	15
UFCFEL-15-3	Security Data Analytics and Visualisation 2023-24	15

Year 3 Optional Modules C

The student must take 15 credits from the modules in Optional Modules C.

Module Code	Module Title	Credit
UFCFB5-15-3	Ethical and Professional Issues in Computing and Digital Media 2023-24	15
UFCFVJ-15-3	Professional Development 2023-24	15

Part C: Higher Education Achievement Record (HEAR) Synopsis

Graduates in the field of Computer Security and Computer Forensics 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 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 Digital Forensic 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 Digital Forensics: 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 Digital Forensics). Though the Statement is targeted at programmes with at least 180 credits of legal subjects, its expectations also apply to programmes such as Digital Forensics, 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 Digital Forensics: 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.

https://www1.uwe.ac.uk/about/departmentsandservices/professionalservices/studentandacademicservices/regulationspoliciesquality/regulationsandprocedures.aspx