香港學術及職業資歷評審局
Hong Kong Council for Accreditation of
Academic & Vocational Qualifications

SUMMARY ACCREDITATION REPORT

SCHOOL FOR HIGHER AND PROFESSIONAL EDUCATION, VOCATIONAL TRAINING COUNCIL

AND

COVENTRY UNIVERSITY

LEARNING PROGRAMME ACCREDITATION

BSc (HONS) ETHICAL HACKING AND CYBERSECURITY

JUNE 2020

1. Terms of Reference

1.1 Based on the Service Agreement (No.: AA620), the Hong Kong Council for Accreditation of Academic and Vocational Qualifications (HKCAAVQ), in the capacity of the Accreditation Authority as provided for under the Accreditation of Academic and Vocational Qualifications Ordinance (Cap. 592), was commissioned by the School for Higher and Professional Education, Vocational Training Council and Coventry University (jointly as the Operator) to conduct a learning programme accreditation exercise with the following Terms of Reference:

(a) To conduct an accreditation test as provided for in the AAVQO to determine whether the BSc (Hons) Ethical Hacking and Cybersecurity programme of the School for Higher and Professional Education, Vocational Training Council (SHAPE) and Coventry University (CU) meets the stated objectives and HKQF standards and can be offered as an accredited programme; and

(b) To issue to the Operator an accreditation report setting out the results of the determination in relation to (a) by HKCAAVQ.

2. HKCAAVQ'S Determination

Learning Programme Accreditation

2.1 HKCAAVQ has determined that, subject to the fulfilment of the condition, the BSc (Hons) Ethical Hacking and Cybersecurity (the programme) meets the stated objectives and HKQF standards at Level 5 and can be offered as an accredited programme with a validity period of four years from 1 September 2020 to 31 August 2024.

2.2 Validity Period

2.2.1 The validity period will commence on the date specified below. Operators may apply to HKCAAVQ to vary the commencement date of the validity period. Applications will be considered on a case-by-case basis.

2.3 The determinations on the programme are specified as follows:

Name of Local Operator	School for Higher and Professional Education, Vocational Training Council 職業訓練局 才晉高等教育學院
Name of Non- local Operator	Coventry University
Name of Award Granting Body	Coventry University
Title of Learning Programme	BSc (Hons) Ethical Hacking and Cybersecurity
Title of Qualification(s) [Exit Award(s)]	BSc (Hons) Ethical Hacking and Cybersecurity
Primary Area of Study and Training	Computer Science and Information Technology
Sub-area (Primary Area of Study and Training)	Computer Science and Information Technology
Other Area of Study and Training	Not applicable
Sub-area (Other Area of Study and Training)	Not applicable
HKQF Level	Level 5
HKQF Credits	160 HKQF Credits
Mode(s) of Delivery and Programme Length	Full-time, 12 months Part-time, 16 months
Start Date of Validity Period	1 September 2020
End Date of Validity Period	31 August 2024
Number of Enrolment(s)	One enrolment per year

Maximum Number of New Students	Full-time: 60 per year (from the 2020/21 to 2023/24 academic years) Part-time: 60 per year (from the 2021/22 to 2023/24 academic years)
Address of Teaching / Training Venue(s)	1. 30 Shing Tai Road, Chai Wan, Hong Kong 2. 6 Oi Kwan Road, Wan Chai, Hong Kong 3. 25 Hiu Ming Street, Kwun Tong, Kowloon 4. 702 Lai Chi Kok Road, Cheung Sha Wan, Kowloon 5. 3 King Ling Road, Tseung Kwan O, New Territories 6. 20 Tsing Yi Road, Tsing Yi Island, New Territories 7. 18 Tsing Wun Road, Tuen Mun, New Territories 8. 21 Yuen Wo Road, Sha Tin, New Territories 9. 20 Hing Shing Road, Kwai Chung, New Territories

2.4 **Recommendations**

HKCAAVQ also offers the following recommendations for continuous improvement of the programme.

2.4.1 The Operator should monitor the usage levels of the cybersecurity centre when the number of students increases.

2.4.2 The Operator should establish mechanisms for both CU and SHAPE staff to formally engage with industry experts in Hong Kong in the process of programme development and review.

2.5 HKCAAVQ will subsequently satisfy itself whether the Operator remains competent to achieve the relevant objectives and the Programme continues to meet the standard to achieve the relevant objectives as claimed by the Operator by reference to, amongst other things, the Operator's fulfilment of any conditions and compliance with any restrictions stipulated in this Accreditation Report. For the

avoidance of doubt, maintenance of accreditation status is subject to fulfilment of any condition and compliance with any restriction stipulated in this Accreditation Report.

3. Introduction

3.1 The School for Higher and Professional Education (SHAPE) was established in September 2003 as a member institution of the Vocational Training Council (VTC). Through collaboration with 12 overseas universities, it offers 51 top-up degree programmes as of January 2020.

3.2 Coventry University (CU) was established under the Education Reform Act 1988 and granted degree awarding powers in accordance with the United Kingdom Further and Higher Education Act 1992. CU is also granted the authority to approve programmes conducted at an external institution.

3.3 CU and SHAPE jointly as the Operator commissioned HKCAAVQ to conduct a Learning Programme Accreditation (LPA) of the BSc (Hons) Ethical Hacking and Cybersecurity Programme. HKCAAVQ formed an expert Panel. Due to the outbreak of the novel coronavirus infection, the Panel held meetings with the Operator via video conferencing from 8 to 9 April 2020.

4. Programmes Details

The following programme information is provided by the operator.

4.1 Programme Aims

The Programme Aims (PAs) shown in the Programme Specification are as follows:

<u>Programme Aims (PAs)</u>

Successful graduates of the programme will:

- Have a clearly targeted and developed sets of skills in computer science with special emphasis on security;
- Be able to identify and analyse the threats posed to modern information structures and will be able to apply defences against such threats;

- Be able to devise methods of testing a system's security and possess the skills needed to break into systems that have vulnerabilities; and
- Be able to advise a company on how to set up secure systems.

The skills base of this programme generally resides within the body of knowledge defined by the UK Quality Assurance Agency for Higher Education (QAA) Computing benchmark statement. As well as the technical foci, the modules all contain content that prepares students in social, ethical, legal and professional aspects of a cooperative human environment such as the workplace.

4.2 Programme Intended Learning Outcomes (PILOs)

Knowledge and Understanding
On successful completion of the programme, a student should be able to demonstrate knowledge and understanding and depth relevant to the level of study of:

KU1	The underlying technology, design methods and programming languages required to practice in the domain Cybersecurity.
KU2	The cultural, commercial, ethical and professional issues connected with Ethical Hacking, Digital Forensics and Ethical Hacking and professional practice within them.
KU3	The requirements and/or the relevant background information required for the development of product in a domain appropriate to their programme of study.
KU4	The means of production of a product of a nature relevant to their domain of study to meet a set of agreed requirements.
KU5	Knowledge of emergent technologies appropriate to their domain of study.

Cognitive Skills (CS)
On successful completion of the programme, a student should be able to:

CS1	Apply appropriate design and problem-solving techniques to computing, ethical hacking, cyber security and digital forensics requirements or issues.
CS2	Research the concept, design and development of a product relevant to their domain of study.

CS3	Conduct an in-depth investigation relating to the requirements and/or relevant background information for the development of a product in a domain appropriate to Ethical Hacking and Cybersecurity.
CS4	Research relevant and useful conclusions in the evaluation of the implementation of a product in a domain appropriate to Ethical Hacking and Cybersecurity.

Practical Skills (PS)

On successful completion of the programme, a student should be able to:

PS1	Use design, production and programming tools relevant to cyber security, in exploit development and associated areas.
PS2	Apply UI and HCI design techniques in the context of a product relevant to cyber security.
PS3	Structure and write reports on various aspects of their domain of study.
PS4	Structure and write an in depth report detailing the concept, design and development of a product relevant to their domain of study.

Transferable Skills (TS)

On successful completion of the programme, a student should be able to:

TS1	Demonstrate professional and ethical practice in cyber security and digital forensics.
TS2	Demonstrate personal and time management skills appropriate to professional conduct in their field of study.
TS3	Communicate effectively using an appropriate media and style.
TS4	Demonstrate an ability to work effectively as part of a group.
TS5	Demonstrate an ability to learn independently, reflect on one's learning needs and achievements and to develop a plan for learning development.
TS6	Demonstrate problem solving skills and reflect on the process of development of a product appropriate to their field of study and report and communicate findings effectively.

4.3 Programme Structure

In the UK, the three-year programme at CU requires the completion of 360 credits. In Hong Kong, the programme is a 12-month full-time and 16-month part-time top-up degree programme. It comprises eight modules which are listed below:

	Modules	**Generic/ Specialised**	**Contact hours**	**Non-contact hours**	**Notional learning hours**	**QF Credits**
1	Digital Forensics Fundamentals	Specialised	44	156	200	20
2	Intermediate Digital Forensics	Specialised	44	156	200	20
3	Academic Writing 3: Writing Skills for Dissert and Res Prj	Generic	22	78	100	10
4	Advanced Network Management and Design	Specialised	44	156	200	20
5	Ethical Hacking 2	Specialised	44	156	200	20
6	Systems Security	Specialised	44	156	200	20
7	Data Recovery and Advanced Digital Forensic Analysis	Specialised	44	156	200	20
8	Individual Project	Specialised	23	277	300	30
		Total	**309**	**1,291**	**1,600**	**160**

4.4 Graduation Requirements

The graduation requirement is an achievement of 160 credits and a pass in all the modules of the programme.

4.5 Admission Requirements

Target Students	Graduates from relevant VTC's Higher Diploma (HD) programmes or equivalent.
Minimum Admission Requirements	1. Graduates of VTC HD in Information and Network Security *# 2. Mathematics Entry Requirement ▪ All candidates must be able to demonstrate competence equivalent to an HKCEE Grade E or HKDSE Level 2 in Mathematics. Applicants from the approved VTC feeder programme are considered to have met this requirement. 3. English language requirements: ▪ Holders of VTC HD taught and assessed in English.
Non-Feeder Programmes / Special / Alternative Admission Requirements and Arrangements	1. Non-feeder applicants holding equivalent qualifications will be considered on a case-by-case basis. 2. Applicants who are not from the approved VTC feeder programmes should have successfully completed a HD or Associate Degree taught and assessed in English from a recognised institution in Hong Kong or equivalent, or alternatively they should have attained a minimum overall IELTS score of 6.5 or equivalent.

* HD programmes using HKDSE results or equivalent as general admission requirements.

\# HD programmes using HKCEE / HKALE results or equivalent as general admission requirements.

4.6 Teaching and Learning Activities

The programme employs a range of teaching and learning activities, such as lectures, seminars, workshops and guided project supervision.

5. Important Information Regarding this Accreditation Report

5.1 Variation and withdrawal of this Accreditation Report

5.1.1 This Accreditation Report is issued pursuant to section 5 of the AAVQO, and contains HKCAAVQ's substantive determination regarding the accreditation, including the validity period as well as any conditions and restrictions subject to which the determination is to have effect.

5.1.2 HKCAAVQ may subsequently decide to vary or withdraw this Accreditation Report if it is satisfied that any of the grounds set out in section 5 (2) of the AAVQO apply. This includes where HKCAAVQ is satisfied that the Operator is no longer competent to achieve the relevant objectives and/or the Programme no longer meets the standard to achieve the relevant objectives as claimed by the Operator (whether by reference to the Operator's failure to fulfil any conditions and/or comply with any restrictions stipulated in this Accreditation Report or otherwise) or where at any time during the validity period there has/have been substantial change(s) introduced by the Operator after HKCAAVQ has issued the accreditation report(s) to the Operator and which has/have not been approved by HKCAAVQ. Please refer to the '*Guidance Notes on Substantial Change to Accreditation Status*' in seeking approval for proposed changes. These Guidance Notes can be downloaded from the HKCAAVQ website.

5.1.3 If HKCAAVQ decides to vary or withdraw this Accreditation Report, it will give the Operator notice of such variation or withdrawal pursuant to section 5(4) of the AAVQO.

5.1.4 The accreditation status of Operator and/or Programme will lapse immediately upon the expiry of the validity period or upon the issuance of a notice of withdrawal of this Accreditation Report.

5.2 Appeals

5.2.1 If the Operator is aggrieved by the determination made in this Accreditation Report, then pursuant to Part 3 of the AAVQO the Operator has a right of appeal to the Appeal Board. Any appeal must be lodged within 30 days of the receipt of this Accreditation Report.

5.2.2 If the Operator is aggrieved by a decision to vary or withdraw this Accreditation Report, then pursuant to Part 3 of the AAVQO the

Operator has a right of appeal to the Appeal Board. Any appeal must be lodged within 30 days of the receipt of the Notice of Withdrawal.

5.2.3 The Operator should be aware that a notice of variation or withdrawal of this Accreditation Report is not itself an accreditation report and the right to appeal against HKCAAVQ's substantive determination regarding accreditation arises only from this Accreditation Report.

5.2.4 Please refer to Cap. 592A (http://www.legislation.gov.hk) for the appeal rules. Details of the appeal procedure are contained in section 13 of the AAVQO and can be accessed from the HKQF website at http://www.hkqf.gov.hk.

5.3 Qualifications Register

5.3.1 Qualifications accredited by HKCAAVQ are eligible for entry into the Qualifications Register ("QR") at http://www.hkqr.gov.hk for recognition under the QF. The Operator should apply separately to have their quality-assured qualifications entered into the QR.

5.3.2 Only learners who commence the study of the named accredited learning programme during the validity period and who have graduated with the named qualification listed in the QR will be considered to have acquired a qualification recognised under the HKQF.

Report No.: 20/66
File Reference: 100/19/11