



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

ACCREDITATION REPORT

HKCT INSTITUTE OF HIGHER EDUCATION

LEARNING PROGRAMME ACCREDITATION

MASTER OF SCIENCE IN CYBERSECURITY

AUGUST 2025

Table of Contents

	<u>Page</u>
1. TERMS OF REFERENCE.....	1
2. HKCAAVQ'S DETERMINATION	1
3. INTRODUCTION.....	5
4. PANEL'S DELIBERATIONS	6
4.1 <i>Programme Objectives and Learning Outcomes</i>	6
4.2 <i>Learner Admission and Selection</i>	9
4.3 <i>Programme Structure and Content</i>	11
4.4 <i>Learning, Teaching and Assessment</i>	14
4.5 <i>Programme Leadership and Staffing</i>	16
4.6 <i>Learning, Teaching and Enabling Resources/Services</i>	17
4.7 <i>Programme Approval, Review and Quality Assurance</i>	19
5. IMPORTANT INFORMATION REGARDING THIS ACCREDITATION REPORT	20
 Appendix 1 HKCAAVQ Panel Membership	
 Appendix 2 Graduate Profile of Master of Science in Cybersecurity	

1. TERMS OF REFERENCE

1.1 Based on the Service Agreement (No.: AA1066), 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 (AAVQO) (Cap. 592), was commissioned by HKCT Institute of Higher Education (the Operator) to conduct a Learning Programme Accreditation with the following Terms of Reference:

- (a) To conduct an accreditation test as provided for in the AAVQO to determine whether the Master of Science in Cybersecurity of the Operator meets the stated objectives and QF 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

2.1 HKCAAVQ has determined that, subject to the fulfilment of the conditions and compliance with the restrictions set out below, the Master of Science in Cybersecurity meets the stated objectives and QF standard at Level 6. Subject to the approval by the Secretary for Education, the Programme can be offered as an accredited programme with a validity period of 3 years.

2.2 In order for the validity period to take effect, the Operator must be registered as a Post Secondary College under the Post Secondary Colleges Ordinance (Cap. 320) and it must comply with any restrictions stipulated in the Institutional Review (IR) Report. The authority for registration under Cap. 320 rests with the Permanent Secretary for Education who may take into account the outcome of the IR Report and other considerations as deemed necessary.

2.3 Validity Period

2.3.1 The validity period will, provided the Operator fulfils the pre-conditions to the commencement of the validity period as set out in Para. 2.5.1, 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.

2.4 The determinations on the Programme are specified as follows:

Name of Operator(s) 營辦者名稱	HKCT Institute of Higher Education 港專學院
Name of Award Granting Body 資歷頒授者名稱	HKCT Institute of Higher Education 港專學院
Title of Learning Programme 進修課程名稱	Master of Science in Cybersecurity 網絡安全理學碩士
Title of Qualification(s) [Exit Award(s)] 資歷名稱（結業資歷）	Master of Science in Cybersecurity 網絡安全理學碩士
Primary Area of Study and Training 主要學習及培訓範疇	Computer Science and Information Technology
Sub-area (Primary Area of Study and Training) 子範疇（主要學習及培訓範疇）	Computer Science and Information Technology
Other Area of Study and Training 其他學習及培訓範疇	Not applicable
Sub-area (Other Area of Study and Training) 子範疇（其他學習及培訓範疇）	Not applicable
QF Level 資歷架構級別	Level 6
QF Credits 資歷學分	122
Mode(s) of Delivery and Programme Length 授課模式及修讀期	Full-time, 1 year Part-time, 2 years
Start Date of Validity Period 有效期的開始日期	1 September 2026
End Date of Validity Period 有效期的終止日期	31 August 2029
Number of Enrolment(s) 招收學員次數	One enrolment per year (Full-time) One enrolment per year (Part-time)
Maximum Number of New Students 新學員人數上限	To be confirmed upon the fulfilment of the pre-conditions

Specification of Competency Standards-based Programme 「能力標準說明」為本課程	☐ Yes ☒ No
Address of Teaching / Training Venue(s) 授課地址	(1) HKCT Jockey Club Undergraduate Campus 2 On Shing Street, Ma On Shan, Sha Tin, New Territories 港專賽馬會本科校園 新界沙田馬鞍山鞍誠街 2 號 (2) HKCT Jockey Club Ma On Shan Campus Yiu On Estate, 2 Hang Hong Street, Ma On Shan, Sha Tin, New Territories 港專賽馬會馬鞍山校園 新界沙田馬鞍山恆康街 2 號耀安邨

2.5 Conditions

2.5.1 Pre-conditions

- 2.5.1.1 The Operator is to conduct a thorough analysis of its market demand, identify the target student groups, review the projected student intake numbers and take an active approach in its marketing planning and promotions to support the proposed student intake numbers. (Paras. 4.1.5 – 4.1.7)

For the fulfilment of the pre-condition above, the Operator is to submit a report to HKCAAVQ **on or before 31 December 2025** on the analysis of its market demand, a review of its target student groups, proposed student intake numbers, and an overview of its marketing strategy and related plans for student recruitment.

- 2.5.1.2 The Operator is to strengthen the teaching team by recruiting new staff to ensure that (i) the teaching team as a whole has adequate experience in teaching master's programmes using the selected MOI, and (ii) possess relevant language proficiency to facilitate effective programme management. (Para. 4.5.3)

For the fulfilment of the Pre-condition, the Operator is to

- (i) provide HKCAAVQ **on or before 31 December 2025** a staff recruitment plan outlining the desired qualifications and

experience, timeline, and planned assignments of responsible staff for each course.

- (ii) provide HKCAAVQ **on or before 31 July 2026** CV / profile / evidence of appointment of new teaching staff members detailing their qualifications, experience, language proficiency, demonstrating their track record in teaching master's programmes in the selected MOI of the Programme and relevant language proficiency to facilitate effective programme management.

2.6 Recommendations

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

- 2.6.1 The Operator should provide more comprehensive research training within the Programme to ensure that students are equipped with necessary individual research capabilities for practical research. (Para. 4.1.3)
- 2.6.2 The Operator should develop and keep under review a plan for the arrangement of elective modules, specifying how elective modules will be organised and offered based on enrolment numbers, to ensure that students have available options even if admissions are below expectations. (Para. 4.3.2)
- 2.6.3 The Operator should enhance engagement with stakeholders, including industry partners and professional bodies, by integrating these collaborations into the curriculum to align with industry standards and practices, thereby enriching the learning experience of students. (Para. 4.3.3)
- 2.6.4 The Operator should provide staff a wider range of industry-related development activities to ensure they stay up-to-date with the rapidly evolving industry landscape, as well as provide broader opportunities for the development of pedagogies. (Para.4.5.5)
- 2.6.5 The Operator should provide additional e-resources such as the access to major international journals and libraries specifically for the Programme, beyond those available for the bachelor's degree and higher diploma programmes in cybersecurity and related fields, ensuring that students have extensive support for their learning and research at the master's level. (Para. 4.6.3)

- 2.6.6 The Operator should develop a plan to offer various support, including activities and/or resources, to assist students who may have difficulties with the selected MOI of the Programme and lack foundational knowledge in cybersecurity. (Para. 4.6.4)
- 2.7 HKCAAVQ will subsequently satisfy itself on 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 the fulfilment of any condition and compliance with any restriction stipulated in this Accreditation Report. During the validity period, HKCAAVQ may request the Operator to provide evidence, such as admission related information, to demonstrate that the Operator and the Programme continue to comply with the determinations and meet the relevant accreditation standards.

3. INTRODUCTION

- 3.1 HKCT Institute of Higher Education (HKCTIHE) was officially established in August 2014 upon registration under the Post Secondary Colleges Ordinance (Cap. 320). HKCTIHE is sponsored by HKCT Group Limited which has been incorporated as a registered company under the Companies Ordinance.
- 3.2 As of June 2025, HKCTIHE is operating six accredited programmes, namely Bachelor of Social Sciences (Honours) in Sports Management with Coaching, Bachelor of Social Sciences (Hons) in Social Work, Certificate in Advanced Sports Coaching Theory, Certificate in Foundation Sports Coaching Theory, Higher Diploma in Early Childhood Education (Inclusive Education) and Higher Diploma in Fitness, Coaching and Sports Management.
- 3.3 HKCTIHE commissioned HKCAAVQ to conduct a Learning Programme Accreditation (LPA) exercise for Master of Science in Cybersecurity (the Programme). For this exercise, HKCAAVQ formed an expert Panel (Panel Membership at **Appendix 1**). HKCAAVQ's *Manual for the Four-stage Quality Assurance Process under the Hong Kong Qualifications Framework (Version 1.2, November 2020)* was the guiding document for the Operator and the

Panel in conducting this exercise. The site visit was conducted at HKCT Jockey Club Undergraduate Campus from 29 to 30 May 2025.

- 3.4 In consideration of the track record of the Operator established from previous accreditation exercises, information on the following aspect of the Programme was not required in accordance with HKCAAVQ's Differentiation Approach:

Domain of Competence	Information Not Required
LPA-6 Learning, Teaching and Enabling Resources / Services	Information on student support services (except those specific for this Programme) and physical resources (except those specific for this Programme) is not required.

4. PANEL'S DELIBERATIONS

The following presents the Panel's deliberations on a range of issues pertinent to its major findings. For aspects of the accreditation standards where no observations are made they are considered to be appropriately addressed by the Operator.

4.1 Programme Objectives and Learning Outcomes

The learning programme must have objectives that address community, education and/or industry needs, with learning outcomes that meet the relevant HKQF standards, for all exit qualifications from the programme.

- 4.1.1 The Master of Science in Cybersecurity is hosted by the Department of Cyber Security. The Programme Objectives (POs) and Programme Intended Learning Outcomes (PILOs) are as follows:

Programme Objectives (POs)

1	Enable students to gain advanced technical skills and knowledge in cybersecurity, equipping them to design, implement, and manage secure systems and networks;
2	Develop students' abilities to analyse security threats, assess vulnerabilities, devise robust solutions, and critical thinking to security challenges through hands-on

	experiences and practical applications;
3	Instil a strong sense of ethical responsibility and professional conduct, ensuring that graduates are prepared to navigate the legal and regulatory landscapes of cybersecurity;
4	Prepare graduates to take on leadership roles in the cybersecurity industry or academia, fostering an innovative mindset to drive advancements in security technologies and practices, and contribute to the ongoing development of the field; and
5	Encourage students to develop self-motivation and the ability to conduct independent research, empowering them to continuously explore new areas in cybersecurity, contribute original ideas, and stay updated with the latest advancements in the field.

Programme Intended Learning Outcomes (PILOs)

Upon completion of the Programme, graduates should be able to:

1	Master technical skills in designing, implementing, and managing secure systems and networks, utilising common security tools and technologies;
2	Apply analytical abilities to critically assess security threats and vulnerabilities, and develop practical, effective solutions to cybersecurity challenges;
3	Exhibit a thorough understanding of ethical, legal, and regulatory standards in cybersecurity, and will conduct themselves with integrity and professionalism in all aspects of their work;
4	Demonstrate leadership by leading cybersecurity teams and projects while collaborating as a team member;
5	Conduct independent research, and demonstrate self-motivation to contribute new knowledge and solutions to the field of cybersecurity; and
6	Communicate, using appropriate methods, to a range of stakeholders and audiences including peers.

4.1.2 To demonstrate the PILOs meet the QF standard at Level 6, the Programme Team provided the following information to the Panel for review:

- (a) Mapping of the POs and PILOs;
- (b) Mapping of Modules with PILOs;

- (c) Mapping of Modules with the Generic Level Descriptors (GLDs) at QF Level 6;
- (d) Mapping between Module Intended Learning Outcomes (MILOs) and PILOs;
- (e) Module Descriptions for core and elective modules with QF credits, contact hours and self-study hours, Module Objectives (MOs), MILOs, module contents, teaching and learning activities, assessment, list of texts and references;
- (f) Samples of learning and teaching materials, for three core modules and two elective modules, to demonstrate the academic and exit standards of the Programme; how the intended learning outcomes will be achieved through the teaching and learning materials/activities; and how the latest trend and development in the disciplines are incorporated;
- (g) Mapping between PILOs and Graduate Attributes; and
- (h) Mapping between the mission of the Institute and the POs

4.1.3 Upon reviewing the information above, the Panel enquired about how the Programme can equip the students with the ability to conduct independent research as outlined in PO5 and PILO 5 and questioned how the research components and directions of the modules align with HKQF Level 6 standards. In the Operator's response to initial comments and during the site visit, the Operator indicated that two project-based modules are designed to enhance students' research capabilities, including *Applied Research Methods for Cybersecurity (Core Module)* and *Technology Innovation Project (Elective Module)*. Additionally, other modules also incorporate group project elements to further develop students' research skills. The Panel emphasised that a more comprehensive approach to research training is necessary to better equip students for independent research and to ensure the achievement of the POs and PILOs. Therefore, the Panel **recommended** the Operator provide more comprehensive research training within the Programme to ensure that students are equipped with necessary individual research capabilities for practical research.

4.1.4 The Operator indicated in the accreditation documents and during the site visit that the demand for cybersecurity professionals is increasing. External stakeholders, including potential employers, also highlighted the industry's need for more talents and expressed their support for the Programme during the site visit.

4.1.5 While recognising the need for cybersecurity professionals in the industry, the Panel raised concerns about the specific market demand for this Programme. The Operator emphasised that the

Programme's practical approach is its key strength and uniqueness. Despite the availability of similar programmes in the market, the Operator remains optimistic about the proposed student intake of 40 full-time and 20 part-time students in AY2026/27, with plans to gradually increase this to 80 full-time and 40 part-time students by AY2030/31. However, the Panel expressed concerns about whether the Programme could admit the relatively large proposed intake of local students.

- 4.1.6 During the site visit, the Operator provided data on first-year intakes of different local bachelor's programmes in cybersecurity and related fields, along with a survey of employers on the demand for cybersecurity professionals, to demonstrate sufficient demand for the Programme. The Panel also noted that the Programme Development Team had identified both local and non-local students as target groups. However, at the time the report is issued, the Operator is not eligible to admit students from MMT into Bachelor's and Master's programmes.
- 4.1.7 After considering the information outlined in Paras 4.1.5 and 4.1.6, as well as reviewing the details provided by the Operator and the responses during the site visit, the Panel considered that the Operator should conduct a thorough analysis of the market demand for the Programme, review the projected student intake, and develop a detailed marketing plan to attract both local and non-local applicants. Therefore, the Panel stipulated the following pre-condition:

Pre-Condition

The Operator is to conduct a thorough analysis of its market demand, identify the target student groups, review the projected student intake numbers and take an active approach in its marketing planning and promotions to support the proposed student intake numbers.

For the fulfilment of the pre-condition above, the Operator is to submit a report to HKCAAVQ **on or before 31 December 2025** on the analysis of its market demand, a review of its target student groups, proposed student intake numbers, and an overview of its marketing strategy and related plans for student recruitment.

4.2 Learner Admission and Selection

The minimum admission requirements of the learning programme

must be clearly outlined for staff and prospective learners. These requirements and the learner selection processes must be effective for recruitment of learners with the necessary skills and knowledge to undertake the programme.

4.2.1 As stated in the accreditation documents provided by the Operator, the Panel noted that the minimum admission requirements of the Programme are as follows:

- (a) Holders of recognised bachelor's degree in science, engineering or a related discipline; OR
- (b) Holders of recognised bachelor's degree in other disciplines with at least one year of working experience in the related fields (such as cybersecurity, information technology, computer science, artificial intelligence, etc.); OR
- (c) Holders of other qualifications (such as Certified Information Systems Security Professional (CISSP), Certified Information Security Professional (CISP), Certified Information Security Professional - Penetration Testing Engineer (CISP-PTE), etc.) with relevant working experience will be considered on a case-by-case basis; OR
- (d) Other equivalent qualifications; AND
- (e) Pass in the admission interview.

In addition to the above requirements, if the applicant's bachelor's degree was obtained from a university/tertiary institute where English is not the medium of instruction, the following English language proficiency should be attained:

- (a) Overall score of IELTS 6.0 or above (academic version); OR
- (b) Grade C or above in IGCSE English; OR
- (c) TOEFL score of 60 or above (internet-based test); OR
- (d) Band 6 in the Mainland China's College English Test (CET) with a total score of 430 or above and the test result should be valid within two years; OR
- (e) Other equivalent qualifications.

4.2.2 The Panel noted that the Programme would accept students not only from cybersecurity backgrounds but also from various other disciplines, including information technology, computer science, and artificial intelligence. While students would be required to pass an admission interview assessing their basic knowledge of cybersecurity and their language proficiency in the selected MOI of the Programme, the Panel considered that the interview might only evaluate their speaking skills without thoroughly assessing their

overall language and technical abilities. Given that students' foundational knowledge of cybersecurity may vary significantly, potentially impacting their academic performance, the Panel **advised** the Operator to consider incorporating writing tests under supervision into the admission interview to assess applicant's language proficiency in the selected MOI and their foundational knowledge relevant to the discipline of the Programme, in order to identify those who may need additional support and to ensure all students are well-prepared for the Programme.

- 4.2.3 A pre-condition is stipulated in Para. 4.1.7 regarding the market demand and target student groups of the Programme, which are key factors influencing the target student demographic. Therefore, the maximum number of new students per year of the Programme is to be confirmed upon the fulfilment of the pre-condition.
- 4.2.4 In line with the Government's policy on the yearly quota of non-standard admission for programmes accredited under the Qualifications Framework, for local degree programmes operating in the 2023/24 academic year and onwards, the maximum number of non-standard admission (including mature students) should be capped at a maximum of 15% on a programme basis and 10% on an institutional basis of the actual number of new students of the year. The cap is applied in line with the general expectation on self-financed degree-awarding institutions in safeguarding teaching and learning quality and thereby upholding the credibility and recognition of the qualifications. The percentages are based on the sum of new student numbers across all years of study.
- 4.2.5 In light of the recent incidents regarding fraudulent qualifications, the Panel noted from the response to initial comments that the Operator has established procedures to verify the applicants' qualifications prior to enrolment.
- 4.2.6 In consideration of the information above, the Panel considered that the minimum admission requirements and the student selection process are appropriate.

4.3 **Programme Structure and Content**

The structure and content of the learning programme must be up-to-date, coherent, balanced and integrated to facilitate progression in order to enable learners to achieve the stated learning outcomes and to meet the programme objectives.

- 4.3.1 The Programme is a one-year full-time and two-year part-time Programme. To optimise resource utilisation, the Operator has revised the programme structure in the response to initial comments, rearranging all core modules to be offered in Year 1 for both Full-time and Part-time mode students. The updated structure is as follows:

Programme Structure of the Programme (1-year Full-Time Mode)

Module Title	QF Level	Core/ Elective	Generic/ Specialised	(Contact + Self-study) Notional Learning Hours	QF Credit
Year 1 Term 1					
1. The Foundation of Cybersecurity	6	Core	Specialised	135	13.5
2. Applied Research Methods for Cybersecurity	6	Core	Specialised	135	13.5
3. Elective 01#	6	Elective	Specialised	135	13.5
4. Elective 02#	6	Elective	Specialised	135	13.5
5. Elective 03#	6	Elective	Specialised	135	13.5
Sub-total				675	67.5
Year 1 Term 2					
6. Advanced Cybersecurity Governance and Risk Management	6	Core	Specialised	135	13.5
7. Human and Ethical Factors in Information Technology	6	Core	Specialised	135	13.5
8. Elective 04#	6	Elective	Specialised	135	13.5
9. Elective 05#	6	Elective	Specialised	135	13.5
Sub-total				540	54
Total				1215	121.5

5 elective modules are selected out of the total of 8 elective modules offered

Programme Structure of the Programme (2-year Part-Time Mode)

Module Title	QF Level	Core/ Elective	Generic/ Specialised	(Contact + Self-study) Notional Learning Hours	QF Credit
Year 1 Term 1					
1. The Foundation of Cybersecurity	6	Core	Specialised	135	13.5

2. Applied Research Methods for Cybersecurity	6	Core	Specialised	135	13.5
Sub-total				270	27
Year 1 Term 2					
3. Advanced Cybersecurity Governance and Risk Management	6	Core	Specialised	135	13.5
4. Human and Ethical Factors in Information Technology	6	Core	Specialised	135	13.5
Sub-total				270	27
Year 2 Term 1					
5. Elective 01#	6	Elective	Specialised	135	13.5
6. Elective 02#	6	Elective	Specialised	135	13.5
7. Elective 03#	6	Elective	Specialised	135	13.5
Sub-total				405	40.5
Year 2 Term 2					
8. Elective 04#	6	Elective	Specialised	135	13.5
9. Elective 05#	6	Elective	Specialised	135	13.5
Sub-total				270	27
Total				1215	121.5

5 elective modules are selected out of the total of 8 elective modules offered

Elective Modules (students need to select 5 out of 8 modules)

Module Title	QF Level	Core/ Elective	Generic/ Specialised	(Contact + Self-study) Notional Learning Hours	QF Credit
Cybersecurity Engineering and Operations	6	Elective	Specialised	135	13.5
Advanced Cybersecurity Practice	6	Elective	Specialised	135	13.5
Mobile Application Security Analysis	6	Elective	Specialised	135	13.5
Cutting-Edge Cybersecurity and Emerging Technologies	6	Elective	Specialised	135	13.5
Information System and Environment Development	6	Elective	Specialised	135	13.5

Comprehensive Cybersecurity Frameworks for Organisations	6	Elective	Specialised	135	13.5
Defense Mechanisms for Enterprises	6	Elective	Specialised	135	13.5
Technology Innovation Project	6	Elective	Specialised	135	13.5

- 4.3.2 The Panel noted that students are required to complete five elective modules from a selection of eight offered. The Panel enquired about the arrangement of elective modules if the number of students choosing a module falls short of expectations. In the event of low enrolment, there may be insufficient elective modules for students to choose from, which could result in them having very little elective choice. During the site visit, the Operator explained that surveys would be conducted before the start of Term 1 to assess student interest in the elective modules, with the intention of providing a variety of choices. However, it was also indicated that a minimum of 13 students is required for an elective module to be offered, while the breakeven and minimum enrollment number for the Programme is only 12 students. The Panel considered that this discrepancy raises concerns about students' choices of elective modules if enrolment falls slightly below expectations. In this regard, the Panel **recommended** the Operator develop and keep under review a plan for the arrangement of elective modules, specifying how elective modules will be organised and offered based on enrolment numbers, to ensure that students have available options even if admissions are below expectations.
- 4.3.3 The Panel noted that the Operator has made efforts to establish a collaborative network with industry partners. However, considering the rapidly evolving nature of the industry and the practicality of the Programme, collaborations with professional body such as Hong Kong Computer Society, ISACA can also be strengthened. Therefore, the Panel **recommended** the Operator enhance engagement with stakeholders, including industry partners and professional bodies, by integrating these collaborations into the curriculum to align with industry standards and practices, thereby enriching the learning experience of students.
- 4.3.4 Notwithstanding the recommendations above, the Panel considered that the structure and contents of the Programme are appropriate and would enable students to achieve the stated learning outcomes and meet the Programme Objectives.

4.4 Learning, Teaching and Assessment

The learning, teaching and assessment activities designed for the learning programme must be effective in delivering the programme content and assessing the attainment of the intended learning outcomes.

- 4.4.1 The Programme employs a range of learning and teaching methods according to the nature of the modules, including lectures, project-based learning, tutorials, laboratory practice, seminars and workshops. The Operator provided the Panel with Module Descriptions for each module, which include MOs, MILOs, module contents, learning and teaching activities, module assessment in alignment with MILOs, and reading lists. The MOI of the Programme is English.
- 4.4.2 In terms of assessments, a range of methods are adopted in the Programme, including in-class exercise, laboratory exercise, assignments, quizzes, examinations, group projects and presentations.
- 4.4.3 The Operator provided the Panel with samples of learning and teaching materials, assessment tasks and associated assessment criteria/rubrics for the modules such as The Foundation of Cybersecurity, Applied Research Methods for Cybersecurity, Human and Ethical Factors in Information Technology, Mobile Application Security Analysis, and Information System and Environment Development. The Panel considered the content and level of the learning and teaching materials appropriate for the Programme.
- 4.4.4 To be eligible for graduation, students must:
 - (a) Pass all required modules of the Programme unless otherwise exempted; and
 - (b) Obtain an overall GPA of 1.7 for meeting the requirements of graduation.

Students may be allowed to graduate if they have been granted the provision of condonement in the final term at the discretion of the Board of Examiners (BoE).

- 4.4.5 In consideration of the information above, the Panel formed the view that the learning, teaching and assessment activities designed for the Programme were appropriate in delivering the Programme

content and assessing students' attainment of the intended learning outcomes.

4.5 Programme Leadership and Staffing

The Operator must have adequate programme leader(s), teaching/training and support staff with the qualities, competence, qualifications and experience necessary for effective programme management, i.e. planning, development, delivery and monitoring of the programme. There must be an adequate staff development scheme and activities to ensure that staff are kept updated for the quality delivery of the programme.

4.5.1 The Operator provided the following information to the Panel to demonstrate the academic leadership and staffing for the Programme:

- (a) Profile of Academic Staff
- (b) CV of Academic Staff
- (c) Appointment Criteria for Academic Staff
- (d) Staff Development Record for AY2023-24 and AY2024-25
- (e) Staff Handbook
- (f) Lecturer's Handbook
- (g) Staff Performance Appraisal Form
- (h) 5-year Staff Development Plan

4.5.2 According to the accreditation documents, the projected Staff-Student Ratio (SSR) for the Programme, following the institutional policy, is set at 1:25. The Programme team currently consists of seven staff members. Based on the teaching staff requirement plan outlined in the accreditation documents for the next five academic years, the team indicated that they have adequate staff to deliver the Programme.

4.5.3 During the site visit, the Operator indicated that it would be preferable for academic staff teaching the master's degree programmes to hold a doctoral degree in the relevant discipline, along with relevant experience and a proven track record in industrial training or tertiary-level teaching. However, upon reviewing the profile and CVs of the teaching staff assigned to the Programme, the Panel expressed concerns that most of the teaching staff lack experience in delivering master's programmes in the selected medium of instruction (MOI) for the Programme, and much of their experience in such programmes has been limited to roles as tutors or teaching assistants rather than

in full teaching capacities. The Panel considered that the teaching team may not possess the necessary experience to effectively deliver the Programme at QF level 6. The Panel, therefore, stipulated the following pre-condition:

Pre-Condition

The Operator is to strengthen the teaching team by recruiting new staff to ensure that (i) the teaching team as a whole has adequate experience in teaching master's programmes using the selected MOI, and (ii) possess relevant language proficiency to facilitate effective programme management.

For the fulfilment of the Pre-condition, the Operator is to

- (i) provide HKCAAVQ **on or before 31 December 2025** a staff recruitment plan outlining the desired qualifications and experience, timeline, and planned assignments of responsible staff for each course.
- (ii) provide HKCAAVQ **on or before 31 July 2026** CV / profile / evidence of appointment of new teaching staff members detailing their qualifications, experience, language proficiency, demonstrating their track record in teaching master's programmes in the selected MOI of the Programme and relevant language proficiency to facilitate effective programme management.

4.5.4 The Panel also **advised** the Operator to keep under review and ensure effective programme management and the quality of programme delivery using the selected MOI.

4.5.5 In terms of staff development, the Panel was provided with the staff development record for AY2023-24 and 2024-25. After reviewing the activities and discussing with various stakeholders, the Panel noted that there is a need to enhance staff development efforts, especially in industry-related areas. Considering the fast-paced changes in the cybersecurity field, it is essential to ensure that both staff and the Programme remain current with the latest trends. The Panel, therefore, **recommended** the Operator provide staff a wider range of industry-related development activities to ensure they stay up-to-date with the rapidly evolving industry landscape, as well as provide broader opportunities for the development of pedagogies.

4.6 Learning, Teaching and Enabling Resources/Services

The Operator must be able to provide learning, teaching and enabling resources/services that are appropriate and sufficient for the learning, teaching and assessment activities of the learning programme, regardless of location and mode of delivery.

4.6.1 The Programme will be offered at the Campuses of the Institute located at Ma On Shan, including the HKCT Jockey Club Undergraduate Campus (MUC) and the HKCT Jockey Club Ma On Shan Campus (MOS). The Operator provided the Panel with the following information for review in the accreditation documents and during the site visit:

- (a) Physical Resources in the two Campuses
- (b) Programme-specific library resources, e-database and e-resources
- (c) Cyber Range Utilisation Analysis

4.6.2 The Panel noted that in addition to the general facilities identified as physical resources on the campuses, there are several programme-specific facilities, including the Security Operations Centre and the Cyber Range & Practice Centre. These facilities support a variety of learning and teaching activities, such as scene simulation, competitions, research, testing, drills, and exercises. Students in these Centres can interact with the virtual and cyber world in real-time for experiments and training. A campus tour covering these facilities was arranged for the Panel to assess the available resources.

4.6.3 During the site visit, the Panel was given to understand that there are library resources and e-resources specifically for the cybersecurity discipline. However, it was noted that these resources are shared among the higher diploma and bachelor's degree programmes in cybersecurity, with no additional offerings available for the master's programme. Therefore, the Panel **recommended** the Operator provide additional e-resources such as the access to major international journals and libraries specifically for the Programme, beyond those available for the bachelor's degree and higher diploma programmes in cybersecurity and related fields, ensuring that students have extensive support for their learning and research at the master's level.

4.6.4 In terms of student support, the Panel noted in the accreditation documents that there are institute-wide language and student

support services available. However, as highlighted in Para 4.2.2, the Panel is concerned about the diverse backgrounds of the students, particularly those who may lack foundational knowledge in cybersecurity and have varying levels of language proficiency in the MOI of the Programme. In this regard, the Panel **recommended** the Operator develop a plan to offer various support, including activities and/or resources, to assist students who may have difficulties with the selected MOI of the Programme and lack foundational knowledge in cybersecurity.

- 4.6.5 Notwithstanding the recommendations above, the Panel considered that the Operator was able to provide learning, teaching and enabling resources that were appropriate and sufficient for the delivery of the Programme.

4.7 Programme Approval, Review and Quality Assurance

The Operator must monitor and review the development and performance of the learning programme on an on-going basis to ensure that the programme remains current and valid and that the learning outcomes, learning and teaching activities and learner assessments are effective to meet the programme objectives.

- 4.7.1 The Operator provided to the Panel with the following information to demonstrate that the Programme is monitored and reviewed on an on-going basis:

- (a) Quality Assurance Manual
- (b) Approval Records of Faculty Board, Academic Planning and Development Committee (APDC) and Quality Assurance Committee (QAC)
- (c) Meeting minutes and extracts of APDC and QAC
- (d) Meeting minutes and extracts of departmental level meetings
- (e) Programme Validation Panel Report (9 January 2025) and the corresponding response
- (f) Templates of Student Feedback Questionnaire, Module Review Report and Annual Programme Review Report
- (g) Sample meeting minutes of Staff-Student Consultative Meeting
- (h) Staff and Student Handbook
- (i) Profile of External Advisor and External Examiner

- 4.7.2 Having reviewed the above documents and discussed with the internal and external stakeholders, the Panel noted that the Operator has an established Quality Assurance System and the Programme

is subject to on-going monitoring and periodic review. The Panel noted the Operator adopts a systematic approach in collecting feedback from stakeholders, planning actions to follow up with the feedback, and reporting back the actions taken.

- 4.7.3 During the site visit meetings with the external stakeholders of the Programme, the Panel was given to understand their previous and upcoming engagement in the Programme in various roles, such as external advisor, external examiner and potential employer of the Programme. The Panel reviewed how the Institute has received and responded to stakeholder feedback, as well as their views on the Programme's relevance to industry needs, and acknowledged that the Programme team has established a strong network with industry partners. As stated in the recommendation in Para. 4.3.3, the Panel highlighted the necessity for timely updates to curriculum content due to the rapid evolution of the technology sector. Additionally, the Panel emphasised the importance of conducting regular programme reviews to incorporate current industry trends. In this regard, the Panel **advised** the Operator to continue to leverage strong industry connections and actively incorporate industry insights into the programme review process for continuous improvement of the Programme.
- 4.7.4 In consideration of the information above, the Panel formed the view that the Operator has a comprehensive quality assurance system to monitor and review the development and performance of the Programme on an on-going basis.

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 (<https://www.elegislation.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 QF website at <https://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 <https://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 QF.

Ref: 51/37/01

8 August 2025

JoH/CQ/SiC/jof

HKCT Institute of Higher Education

**Learning Programme Accreditation for
Master of Science in Cybersecurity**

29 – 30 May 2025

Panel Membership

Panel Chair

Professor VAN ERNST Barbara
Consultant and Emeritus Professor
Swinburne University
AUSTRALIA

*** Panel Secretary**

Ms Shita CHEUNG
Registrar
Academic Accreditation and Assessment
Hong Kong Council for Accreditation of
Academic and Vocational Qualifications
HONG KONG

Panel Members

Professor NG Kee Yin Joseph
Professor Emeritus
Department of Computer Science
Hong Kong Baptist University
HONG KONG

Dr ZHENG Yuanqing
Associate Professor
Department of Computing
The Hong Kong Polytechnic University
HONG KONG

Mr SUN Kin Kwok
Head of Information Technology
Hong Kong Housing Society
HONG KONG

* The Panel Secretary is also a member of the Accreditation Panel.

Appendix 2

Graduate Profile of Master of Science in Cybersecurity

Qualification Title	Master of Science in Cybersecurity 網絡安全理學碩士
Qualification Type	Master's Degree
QF Level	Level 6
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
Programme Objectives	The objectives of the Programme are to: 1. Enable students to gain advanced technical skills and knowledge in cybersecurity, equipping them to design, implement, and manage secure systems and networks; 2. Develop students' abilities to analyse security threats, assess vulnerabilities, devise robust solutions, and critical thinking to security challenges through hands-on experiences and practical applications; 3. Instil a strong sense of ethical responsibility and professional conduct, ensuring that graduates are prepared to navigate the legal and regulatory landscapes of cybersecurity; 4. Prepare graduates to take on leadership roles in the cybersecurity industry or academia, fostering an innovative mindset to drive advancements in security technologies and practices, and contribute to the ongoing development of the field; and 5. Encourage students to develop self-motivation and the ability to conduct independent research, empowering them to continuously explore new areas in cybersecurity, contribute original ideas, and stay updated with the latest advancements in the field.

Programme Intended Learning Outcomes	Upon completion of the Programme, students should be able to: 1. Master technical skills in designing, implementing, and managing secure systems and networks, utilising common security tools and technologies; 2. Apply analytical abilities to critically assess security threats and vulnerabilities, and develop practical effective solutions to cybersecurity challenges; 3. Exhibit a thorough understanding of ethical, legal, and regulatory standards in cybersecurity, and will conduct themselves with integrity and professionalism in all aspects of their work; 4. Demonstrate leadership by leading cybersecurity teams and projects while collaborating as a team member; 5. Conduct independent research, and demonstrate self-motivation to contribute new knowledge and solutions to the field of cybersecurity; and 6. Communicate, using appropriate methods, to a range of stakeholders and audiences including peers.																		
Education Pathways	Graduates of MSc in Cybersecurity can choose to pursue a local/non-local postgraduate qualification, either on a full-time or part-time basis. Some examples of postgraduate degrees for programme articulation in Hong Kong are as follows: <table><tr><th>Operator</th><th>Programme</th><th>QF Level</th></tr><tr><td>The University of Hong Kong</td><td>PhD in Information Security</td><td>7</td></tr><tr><td>The Chinese University of Hong Kong</td><td>PhD in Computer Science and Engineering</td><td>7</td></tr><tr><td>The Hong Kong University of Science and Technology</td><td>PhD in Computer Science and Engineering</td><td>7</td></tr><tr><td>City University of Hong Kong</td><td>PhD in Computer Science</td><td>7</td></tr><tr><td>Kong Baptist University</td><td>PhD in Computer Science</td><td>7</td></tr></table>	Operator	Programme	QF Level	The University of Hong Kong	PhD in Information Security	7	The Chinese University of Hong Kong	PhD in Computer Science and Engineering	7	The Hong Kong University of Science and Technology	PhD in Computer Science and Engineering	7	City University of Hong Kong	PhD in Computer Science	7	Kong Baptist University	PhD in Computer Science	7
Operator	Programme	QF Level																	
The University of Hong Kong	PhD in Information Security	7																	
The Chinese University of Hong Kong	PhD in Computer Science and Engineering	7																	
The Hong Kong University of Science and Technology	PhD in Computer Science and Engineering	7																	
City University of Hong Kong	PhD in Computer Science	7																	
Kong Baptist University	PhD in Computer Science	7																	
Employment Pathways	The career paths open to the graduates include: 1. <u>The Cybersecurity field</u> - Graduates can initially start with an entry level or junior position in the areas of penetration testing, system hardening, personnel training, services and product sales. They should																		

	also be capable of assisting the verification of cybersecurity threshold standards and requirements set by industries/ organisations/ companies, either in the capacity of an employee, or as a technical staff of a third-party entity offering related certification services. 2. <u>The Computer Science field</u> -- They should also be capable to perform tasks in other computer science areas including system and network administration and maintenance, IT technical supports, application or web development according to their interests. Graduates can initially start with an entry level or junior position in various cybersecurity roles across Hong Kong and Mainland China. Some examples are as follows: <table border="1" data-bbox="641 824 1444 1375"> <thead> <tr> <th>Hong Kong</th><th>Mainland China</th></tr> </thead> <tbody> <tr> <td>Information Security Specialist</td><td>Cybersecurity Researcher 網絡安全研究員</td></tr> <tr> <td>Information Security Officer</td><td>Safety Emergency Engineer 安全應急工程師</td></tr> <tr> <td>Information Technology Manager</td><td>Penetration Test Engineer 滲透測試工程師</td></tr> <tr> <td>Penetration Tester</td><td>Cybersecurity Consultant 網絡安全顧問</td></tr> <tr> <td>Network Administrator</td><td>Information Security Lecturer 資訊安全類講師</td></tr> <tr> <td>Network and System Security Engineer</td><td>Research Assistant in Cybersecurity 網絡安全研究員</td></tr> <tr> <td>Information System Auditor</td><td></td></tr> </tbody> </table>	Hong Kong	Mainland China	Information Security Specialist	Cybersecurity Researcher 網絡安全研究員	Information Security Officer	Safety Emergency Engineer 安全應急工程師	Information Technology Manager	Penetration Test Engineer 滲透測試工程師	Penetration Tester	Cybersecurity Consultant 網絡安全顧問	Network Administrator	Information Security Lecturer 資訊安全類講師	Network and System Security Engineer	Research Assistant in Cybersecurity 網絡安全研究員	Information System Auditor	
Hong Kong	Mainland China																
Information Security Specialist	Cybersecurity Researcher 網絡安全研究員																
Information Security Officer	Safety Emergency Engineer 安全應急工程師																
Information Technology Manager	Penetration Test Engineer 滲透測試工程師																
Penetration Tester	Cybersecurity Consultant 網絡安全顧問																
Network Administrator	Information Security Lecturer 資訊安全類講師																
Network and System Security Engineer	Research Assistant in Cybersecurity 網絡安全研究員																
Information System Auditor																	
Minimum Admission Requirements	(a) Holders of recognised bachelor's degree in science, engineering or a related discipline; OR (b) Holders of recognised bachelor's degree in other disciplines with at least one year of working experience in the related fields (such as cybersecurity, information technology, computer science, artificial intelligence, etc.); OR (c) Holders of other qualifications (such as Certified Information Systems Security Professional (CISSP), Certified Information Security Professional (CISP), Certified Information Security Professional - Penetration Testing Engineer (CISP-PTE), etc.) with relevant working experience will be considered on a case-by-case basis; OR (d) Other equivalent qualifications; AND (e) Pass in the admission interview.																

	In addition to the above requirements, if the applicant's bachelor's degree was obtained from a university/tertiary institute where English is not the medium of instruction, the following English language proficiency should be attained: (a) Overall score of IELTS 6.0 or above (academic version); OR (b) Grade C or above in IGCSE English; OR (c) TOEFL score of 60 or above (internet-based test); OR (d) Band 6 in the Mainland China's College English Test (CET) with a total score of 430 or above and the test result should be valid within two years; OR (e) Other equivalent qualifications.
Graduation Requirements	The MSc in Cybersecurity adheres to the Academic Regulations by which a student must pass all required modules of the Programme unless otherwise exempted and obtain an overall GPA of 1.7 for meeting the requirements of graduation. Students may be allowed to graduate if they have been granted the provision of condonement in the final term at the discretion of the Board of Examiners (BoE).
Operator	HKCT Institute of Higher Education 港專學院

