UNIVERSITY OF YORK

POSTGRADUATE PROGRAMME SPECIFICATION

This document applies to students who commence the programme(s) in:	September 2017
Awarding institution	**Teaching institution**
University of York	University of York
Department(s)	
Computer Science	
Award(s) and programme title(s)	**Level of qualification**
MSc in Cyber Security PGCert in Cyber Security and Diploma in Cyber Security	Level 7 (Masters)
Award(s) available *only* as interim awards	
Admissions criteria	
In addition to University requirements, we would normally require at least a 2.1 degree in Computer Science, Software Engineering, Information Technology, Electronics, or a related discipline.	

Length and status of the programme(s) and mode(s) of study

Programme	**Length (years) and status (full-time/part-time)**	**Start dates/months** (if applicable – for programmes that have multiple intakes or start dates that differ from the usual academic year)	**Mode**		
			Face-to-face, campus-based	**Distance learning**	**Other**
MSc in Cyber Security	1 year full-time 3 years (part-time)		Yes Yes	No No	N/A N/A
PG Diploma in Cyber Security	1 year full-time 2 Years part-time		Yes Yes	No No	N/A N/A
PG Certificate	20 months part time		Yes	No	N/A

Language of study	English

Programme accreditation by Professional, Statutory or Regulatory Bodies (if applicable)

Certification of programme by GCHQ (from 2014-15 to 2019-2020). Educational requirements are met through MSc course completion. Interim awards (detailed above) are not certified.

Educational aims of the programme(s)

For the Masters, Diploma and Certificate:

The MSc in Cyber Security is a forward looking MSc, available as a full-time one-year intensive programme or else as a three-year part-time programme. It is intended for students either seeking a research career in cybersecurity or else students from industry or Government who seek a technical education in cybersecurity, particularly to inform strategic decision making in this domain.

The programme is NOT a school for hacking. Rather it emphasises important technical material that must be understood in order to make effective cybersecurity decision making. It is targeted at the "high end" of the market, aiming to provide knowledge and understanding of the principles underpinning effective approaches to cyberdefence. This requires understanding of extant threats to current and emerging system types, and understanding and familiarity with a range of technologies that can be brought to bear to reduce risks.

It has been designed for students who already possess a strong computer science, software engineering, or information technology background who want to broaden their knowledge about the specific challenges in cybersecurity and possible solutions to those challenges.

- **The overall goal of the taught (i.e. without ISM) programme is to educate students in the theories, practices, technologies and principles that form the essential knowledge for professionals engaged in the cybersecurity domain.**

Successful graduates of the course will have developed a detailed understanding of fundamental aspects of cybersecurity.

Additionally for the Diploma (if applicable):

They will also have developed research skills and will be well-prepared to enter academic or industrial research, with communicatiosn ability developed to allow engagement with specialists and the general public.

To provide experience of undertaking an individual project, including substantial literature review and the development of a report detailing issues related to the cybersecurity problem addressed.

Additionally for the Masters:

To provide experience of undertaking a significant individual project, including substantial literature review and demonstrating an appropriate lifecycle to consider some aspect of cybersecurity (e.g. engineering lifecycle for the development of a cybersecurity-related system artefact or else demonstrate an appropriate research lifecycle for consideration of an open research question in cybersecurity).

To prepare students for entry into research degrees or to work on research projects.

Intended learning outcomes for the programme – and how the programme enables students to achieve and demonstrate the intended learning outcomes

This programme provides opportunities for students to develop and demonstrate	*The following teaching, learning and assessment methods enable students to achieve and to demonstrate the programme learning outcomes:*

<table>
<tr><td>knowledge and understanding qualities, skills and other attributes in the following areas:</td><td></td></tr>
<tr><td colspan="2">A: Knowledge and understanding</td></tr>
<tr><td rowspan="2">Knowledge and understanding of:

For the Masters, Diploma and Certificate:
1. Up-to-date theory and practice in core areas of cybersecurity. Issues addressed include identity, trust and reputation, cryptography, network security, malware and intrusion detection, risk management, and assurance cases.

Additionally for the Diploma:

2. Individual ISM: students will be able to a) demonstrate that they have acquired specialisation in a particular part of the cybersecurity subject area, including enhanced or new technical skills that build on taught theory and principles; b) can prepare a written report on the work carried out, according to the defined criteria, which should be of a standard acceptable for wider publication.

Additionally for the Masters:

3. Individual ISM: students will be able to a) demonstrate that they have acquired significant specialisation in a particular part of the cybersecurity subject area, including enhanced or new technical skills that build on taught theory and principles and b) prepare a written report on the work carried out, according to the defined criteria, which should be of a standard acceptable for wider publication. In addition, students will be expected to produce a précis of their report in a specified journal or conference paper format.</td><td>Learning/teaching methods and strategies (relating to numbered outcomes):
• 1, 2: taught using a combination of lectures, seminars, laboratory exercises, practical classes, and individual study.</td></tr>
<tr><td>Types/methods of assessment (relating to numbered outcomes)
• Core taught modules in 1 are examined by open assessment: students submit a report that addresses theoretical aspects and practical realisation appropriate to each taught module.
• An ISM project report and individual presentation is used for 2 and 3.</td></tr>
</table>

<table>
<tr><th colspan="2">B: (i) Skills – discipline related</th></tr>
<tr><td>Able to:
For the Masters, Diploma and Certificate:
1. Understand, interpret and critically evaluate data and arguments from research papers, other available literature, technical manuals and standards specifications.
2. Appreciate how computer science technologies can be brought to bear to help secure systems.
3. Understand, apply and know the limits of current best-practice in aspects of cybersecurity.
4. Understand non-technical aspects of security such as social engineering, effective tradeoffs, and the reality of cyber decision making.

Additionally for the Diploma:

5. Understand the cybersecurity research process, and how work actually gets published.
6. Scope, plan, execute and manage a small cybersecurity research project.

Additionally for the Masters

7. Understand the cybersecurity research process, and how work actually gets published.
8. Scope, plan, execute and manage a significant cybersecurity research project and produce a précis of it in academic paper form.</td><td>Learning/teaching methods and strategies (relating to numbered outcomes):
• Skills are acquired through a combination of lectures (1-4), practical classes (1-4), cybersecurity research skills module (5,7) and individual study (1-8).

Types/methods of assessment (relating to numbered outcomes)
• Taught modules are examined by open assessment: students submit a report that addresses theoretical aspects and practical realisation appropriate to each taught module (1-5,7).
• An ISM project report and presentation for the Diploma and for the Masters (6, 8).</td></tr>
<tr><th colspan="2">B: (ii) Skills - transferable</th></tr>
<tr><td>Able to:
For the Masters, Diploma and Certificate:

1. Engage in independent study.
2. Access and integrate source material from electronic databases and archives and paper-based libraries.</td><td>Learning/teaching methods and strategies (relating to numbered outcomes):
• Self study (1-5).
• Independent project (1-5).
• Presentations and mock radio broadcast (3,5).
• Lectures, practical classes, laboratory exercises and assessments (1-5).</td></tr>
</table>

3. Explain, through oral presentations and written papers to peer specialists and also to more general audiences, complex technical ideas and arguments. 4. Manage competing demands on time, via a significant load of lectures, labs and open assessment. *Additionally for the Diploma and Masters:* 5. Write academic reports.	Types/methods of assessment (relating to numbered outcomes) • 1-4: open assessments (and their scheduling). • 4: not directly assessed. • 5: independent project.
C: Experience and other attributes	
Able to: ***For the Masters, Diploma and Certificate****:* 1. Identify and work towards targets for personal, academic and career development. 2. Develop skills necessary for self-managed life-long learning. ***Additionally for the Diploma and Masters****:* 3. Work on a project involving independent research, development and evaluation. For the Diploma this will be a 40 credit project, for the Masters this will be a substantial 100 credit project.	Learning/teaching methods and strategies (relating to numbered outcomes): • Self study, presentations, lectures and practical classes, laboratory exercises (1-3). • ISM (3). Types/methods of assessment (relating to numbered outcomes) • Not directly assessed.
Relevant Quality Assurance Agency benchmark statement(s) and other relevant external reference points (e.g. National Occupational Standards, or the requirements of Professional, Statutory or Regulatory Bodies)	
GCHQ Certified Education: https://www.ncsc.gov.uk/information/ncsc-certified-degrees	

University award regulations

To be eligible for an award of the University of York a student must undertake an approved programme of study, obtain a specified number of credits (at a specified level(s)), and meet any other requirements of the award as specified in the award requirements and programme regulations, and other University regulations (e.g. payment of fees). Credit will be awarded upon passing a module's assessment(s) but some credit may be awarded where failure has been compensated by achievement in other modules. The University's award and assessment regulations specify the University's marking scheme, and rules governing progression (including rules for compensation), reassessment and award requirements. The award and assessment regulations apply to all programmes: any exceptions that relate to this programme are approved by University Teaching Committee and are recorded at the end of this document.

Departmental policies on assessment and feedback

Detailed information on assessment (including grade descriptors, marking procedures, word counts etc.) is available in the written statement of assessment which applies to this programme and the relevant module descriptions. These are available in the student handbook and on the Department's website:

Written statement of assessment: http://www.cs.york.ac.uk/student/assessment/policies/

Module Descriptions: http://www.cs.york.ac.uk/modules/

Projects Website: http://www.cs.york.ac.uk/projects

Postgraduate Taught Student Handbook: http://www.cs.york.ac.uk/student/handbook/

Information about Academic Misconduct is available:

Postgraduate Taught Student Handbook: http://www.cs.york.ac.uk/student/handbook/

Written statement of assessment: http://www.cs.york.ac.uk/student/assessment/policies/

University Regulations: https://www.york.ac.uk/about/organisation/governance/corporate-publications/ordinances-and-regulations/regulation-5/#5.7

Information on formative and summative feedback to students on their work is available in the written statement on feedback to students which applies to this programmes and the relevant module descriptions. These are available in the student handbook and on the Department's website:

Written statement of assessment: http://www.cs.york.ac.uk/student/assessment/policies/

Module Descriptions: http://www.cs.york.ac.uk/modules/

Postgraduate Taught Student Handbook: http://www.cs.york.ac.uk/student/handbook/

Diagrammatic representation of the programme structure, showing the distribution and credit value of core and option modules

Masters (180 credits)

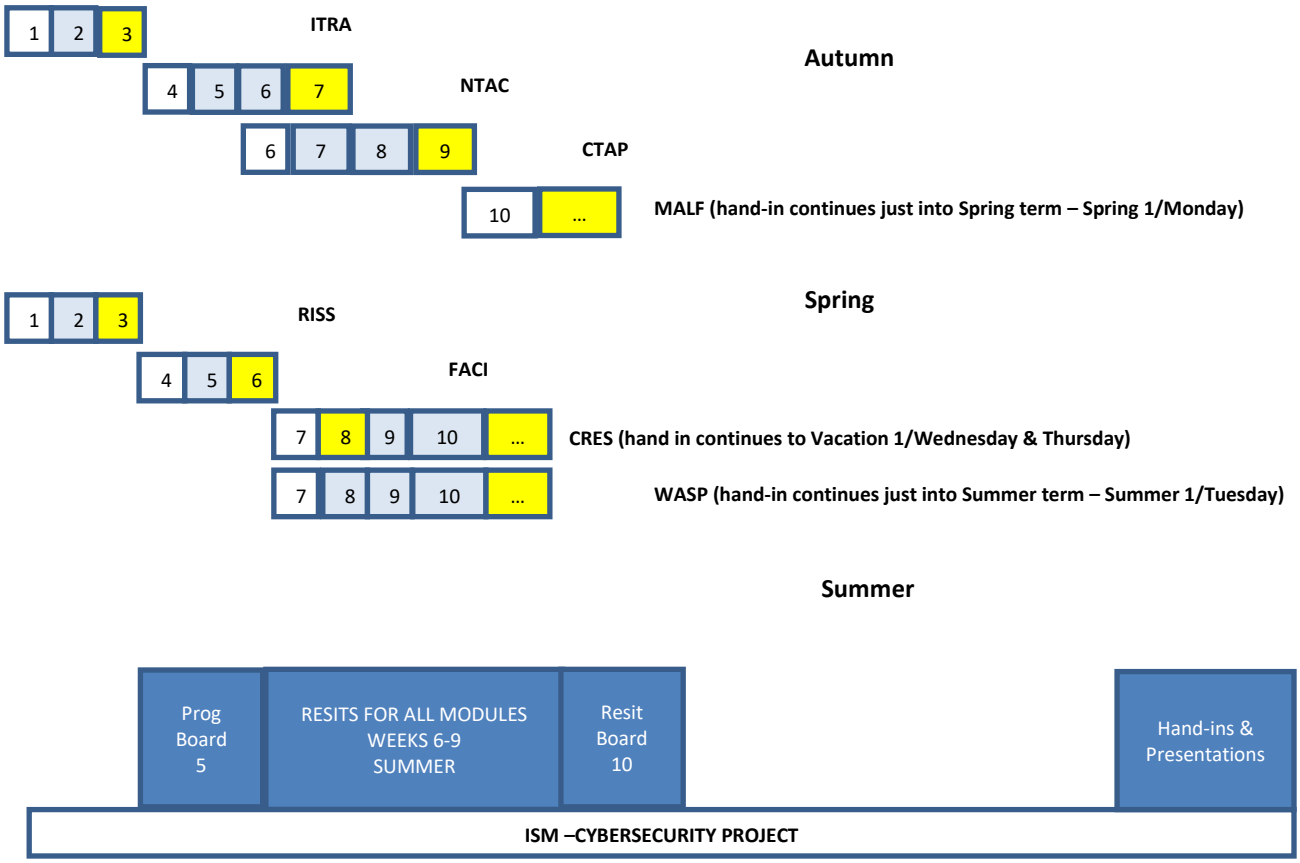
All modules except the Diploma 40 credit "project" and the MSc 100 credit project (ISM) are 10 credits. Teaching for each 10 credit module takes place in a one week intensive block, and open assessment then takes place over 4 weeks. Students take 80 credits of core modules, with the ISM accounting for 100 credits.

6 modules are core to all three programmes (Masters, Diploma and Certificate). These have a solid yellow background below. Cybersecurity Research Skills (CRES) and Wider Aspects of Cybersecurity (WASP) are common and mandatory for Masters and Diploma (solid yellow, grey horizontal cross-hatching, shown below).

The MSc has a mandatory ISM worth 100 credits. (This is the MSc specific project. It is shown in solid blue below.)

Autumn term	Spring term	Summer term	Summer vacation
Identity, Trust, Reputation and their Applications (ITRA)	Rigour in Secure System Development and Assessment (RISS)	Independent Study Module: Cyber-security Individual Project (PCYB)	Independent Study Module: Cyber-security Individual Project (PCYB) continues
Networks and Communications Security: Threats, Attacks and Countermeasures (NTAC)	Forensic Analysis of Cyber Incidents (FACI)		
Cryptography Theory and Applications (CTAP)	Cyber-security Research Skills (CRES)		
Malware and Other Malfeasance (MALF)	Wider Aspects of Cybersecurity (WASP)		

Diagrammatic representation of the delivery of all modules including teaching week (white background) to assessment hand in (yellow background)



The diagram above envisions the teaching and assessment schedule together with progression meetings. The final Exam Board is in November. Top set is Autumn, middle is Spring, lower set is rest of year (with Summer weeks shown for progression and resit boards).

Teaching is typically 1 week intensive followed by 2-3 weeks to complete assignment (minor adjustments will be made to cross Christmas vacation into Spring term as shown). Module delivery may overlap with assessment of other modules as shown.

ISMs start in Spring 12 and go throughout summer term and vac as shown.

Diploma (120 Credits)

All modules are 10 credits. Teaching is intensive and a week long. Open assessment then follows**. Students take 80 credits of core taught modules and the ISM (40 credit project).**

Autumn term	Spring term	Summer term	Summer vacation
Identity, Trust, Reputation and their Applications (ITRA)	Rigour in Secure System Development and Assessment (RISS)	Cybersecurity Diploma Individual Project (PCYD)	Cybersecurity Diploma Individual Project (PCYD) continues
Networks and Communications Security: Threats, Attacks and Countermeasures (NTAC)	Forensic Analysis of Cyber Incidents (FACI)		
Cryptography Theory and Applications (CTAP)	Cyber-security Research Skills (CRES)		
Malware and Other Malfeasance (MALF)	Wider Aspects of Cybersecurity (WASP)		

Postgraduate Certificate

All modules are 10 credits. Teaching is intensive and a week long. Open assessment then follows**. Students take 60 credits of core modules**. **There are no options.**

Autumn term	Spring term	Summer term	Summer vacation
Identity, Trust, Reputation and their Applications (ITRA)	Rigour in Secure System Development and Assessment (RISS)		
Networks and Communications Security: Threats, Attacks and Countermeasures (NTAC)	Forensic Analysis of Cyber Incidents (FACI)		
Cryptography Theory and Applications (CTAP)			
Malware and Other Malfeasance (MALF)			

Diagrammatic representation of the timing of module assessments and reassessments, and the timing of departmental examination/progression boards

Autumn term	Spring term	Summer term	Summer vacation	Date of final award board
(open assessments)				November
	(open assessments)	Progression board sum/5	ISM	
	ISM SpT/12	*Reassessment for Open Assessments SuT/6-9* Resit progression board suT/10	ISM presentation Vac/12	

Overview of modules

Core module table

Module title	Module code	Credit level[1]	Credit value[2]	Prerequisites	Assessment rules[3]	Timing (term and week) and format of main assessment[4]	Independent Study Module?[5]
Identity, Trust, Reputation and their Applications (ITRA)	COM00094M	7/M	10	None		Open: AuT/1-3	No
Networks and Communications Security: Threats, Attacks and Countermeasures (NTAC)	COM00091M	7/M	10	None		Open: AuT/4-7	No
Cryptography Theory and Applications (CTAP)	COM00093M	7/M	10	None		Open: AuT/6-9	No
Malware and Other Malfeasance (MALF)	COM00095M	7/M	10	None		Open: AuT/10 – SpT/1	No
Rigour in Secure System Development and Assessment (RISS)	COM00116M	7/M	10	None		Open: SpT/1-3	No
Forensic Analysis of Cyber Incidents (FACI)	COM00115M	7/M	10	None		Open: SpT/4-6	No
Wider Aspects of Cybersecurity (WASP)	COM00113M	7/M	10	None		Open: SpT/7-12 Open: SpT/7 – SuT/1	No

[1] The **credit level** is an indication of the module's relative intellectual demand, complexity and depth of learning and of learner autonomy. Most modules in postgraduate programmes will be at Level 7/Masters. Some modules are permitted to be at Level 6/Honours but must be marked on a pass/fail basis. See University Teaching Committee guidance for the limits on Level 6/Honours credit.
[2] The **credit value** gives the notional workload for the module, where 1 credit corresponds to a notional workload of 10 hours (including contact hours, private study and assessment)
[3] **Special assessment rules** (requiring University Teaching Committee approval)
P/F – the module is marked on a pass/fail basis (NB pass/fail modules cannot be compensated)
NC – the module cannot be compensated
NR – there is no reassessment opportunity for this module. It must be passed at the first attempt
[4] AuT – Autumn Term, SpT – Spring Term, SuT – Summer Term, SuVac – Summer vacation
[5] **Independent Study Modules** (ISMs) are assessed by a dissertation or substantial project report. They cannot be compensated (NC) and are subject to reassessment rules which differ from 'taught modules'. Masters programmes should include an ISM(s) of between 60 and 100 credits. This is usually one module but may be more.

Module title	Module code	Credit level[1]	Credit value[2]	Prerequisites	Assessment rules[3]	Timing (term and week) and format of main assessment[4]	Independent Study Module?[5]
Cyber-security Research Skills (CRES)	COM00097M	7/M	10	None		Open (50%): SpT/7-8 Open (50%): SpT/7-11	No
Independent Study Module: Cyber-security Individual Project (PCYB)	COM00098M	7/M	100	All taught modules	NC	Vac	Yes (for MSc students)
Cyber Security Individual Diploma Project (PCDP)	COM00099M	7/M	40	All taught modules	NC	Vac	Yes (for Diploma students)

Option modules
N/A

Transfers out of or into the programme
None

Exceptions to University Award Regulations approved by University Teaching Committee	
Exception	**Date approved**

Quality and Standards

The University has a framework in place to ensure that the standards of its programmes are maintained, and the quality of the learning experience is enhanced.

Quality assurance and enhancement processes include:

- The academic oversight of programmes within departments by a Board of Studies, which includes student representation
- The oversight of programmes by external examiners, who ensure that standards at the University of York are comparable with those elsewhere in the sector
- Annual monitoring and periodic review of programmes
- The acquisition of feedback from students by departments.

More information can be obtained from the Academic Support Office:
http://www.york.ac.uk/about/departments/support-and-admin/academic-support/

Date on which this programme information was updated:	August 2017
Departmental web page:	http://www.cs.york.ac.uk

Please note

The information above provides a concise summary of the main features of the programme and learning outcomes that a typical student might reasonably be expected to achieve and demonstrate if he/she takes full advantage of the leaning opportunities that are provided.

Detailed information on learning outcomes, content, delivery and assessment of modules can be found in module descriptions.

The University reserves the right to modify this overview in unforeseen circumstances, or where processes of academic development, based on feedback from staff, students, external examiners or professional bodies, requires a change to be made. Students will be notified of any substantive changes at the first available opportunity.