QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

CERTIFICATE OF VALIDATION

Provider name	National College of Ireland
Date of validation	20-07-2016

	First Intake	**Last Intake**
Enrolment interval	September 2016	September 2020

	Code	**Title**	**Award**	**Duration**
Principal programme	PG22518	MSc in CyberSecurity	Master in Sceience (9M20282)	1 calendar year full-time, 2 calendar years part-time
Embedded programme	PG22519	Postgraduate Diploma in Science in CyberSecurity	Postgraduate Diploma in Science (9M20283)	1 academic year full-time, 2 academic years part-time
Embedded programme				

	Name	**Maximum number of learners**	**Minimum number of learners**
Approved centre	National College of Ireland	As per the validated programmes	As per the validated programmes

Target learner groups	As per the validated programmes
Approved countries for provision	Ireland
The teaching and learning modalities	As per the validated programmes
Brief synopsis of the programme (e.g. who it is for, what is it for, what is involved for learners, what it leads to.)	As per the validated programmes
Specifications for teaching staff	As per the validated programmes
Specifications for the ratio of learners to teaching-staff	As per the validated programmes

Programmes being replaced		
Code	**Title**	**Comment**
		N/A

Conditions of validation

The statutory (section 45(3) of the 2012 Act) conditions of validation are that the provider of the programme shall:

a) co-operate with and assist QQI in the performance of QQI's functions in so far as those functions relate to the functions of the provider,
b) establish procedures which are fair and consistent for the assessment of enrolled learners to ensure the standards of knowledge, skill or competence determined by QQI under section 49 (1) are acquired, and where appropriate, demonstrated, by enrolled learners,
c) continue to comply with section 65 of the 2012 Act in respect of arrangements for the protection of enrolled learners, if applicable, and
d) provide to QQI such information as QQI may from time to time require for the purposes of the performance of its functions, including information in respect of completion rates.

Conditions from HET Core Validation Policy and Criteria 2010, Revised 2013

The provider of the programme shall (for each programme):

1. Maintain the status of the programme(s) recognition;
2. Establish, having regard to existing quality assurance procedures, procedures for quality assurance for the purpose of further improving and maintaining the quality of education and training which is provided, organised or procured by that provider as part of the programme(s) concerned, and agree those procedures with QQI;
3. Operate quality assurance procedures agreed with QQI;
4. Implement procedures for the assessment of learners which are consistent with Assessment and Standards, Revised 2013;
5. Implement the procedures described in the document Policies, Actions and Procedures for Access, Transfer and Progression for Learners;
6. Implement any special conditions of validation attached to the relevant awards standards.

Other conditions from HET Core Validation Policy and Criteria 2010, Revised 2013

7. Notify QQI of any change in circumstances affecting the provider which could affect or be perceived to affect the provision of the programme(s). This includes significant changes in corporate or academic governance, ownership, legal status, profile of teaching staff, profile of learners, numbers enrolled, facilities, or resources;
8. Maintain learner data records (personal identification, progression, module marks, stage classification etc.) in order to assist QQI in the performance of its functions;
9. Provide the information required by QQI's award making and monitoring functions, including information in respect of completion rates;
10. Implement the programme in accordance with the **approved programme schedule(s)** (appended) and current assessment strategies;
11. Subject to Section 4.6.1 of *HET Core Validation Policy and Criteria 2010*, Revised 2013, obtain QQI's approval prior to substantially amending the programme's minimum intended learning outcomes, save in the case of incremental enhancements arising from the implementation of findings of the provider's agreed quality assurance procedures;
12. Notify QQI of any information concerning the programme(s), or circumstances that may reasonably be expected to give QQI cause to consider reviewing the programme. Explicitly this includes where another awarding body withdraws or seeks to withdraw validation from the programme(s) and /or any alterations to accreditations (additions or withdrawals) by a professional or regulatory body;
13. Implement the programme(s) as agreed with the resources indicated;
14. Adhere to, and implement the Provider Lifecycle of Engagements.

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

Approved Programme Schedule(s)

Name of Provider	National College of Ireland
Programme Title (i.e. named award)	MSc in Cyber Security
Award Title (QQI named award)	MSc in Cyber Security
Stage Exit Award Title	Postgraduate Diploma in Science in Cyber Security
Modes of Delivery (FT/PT/ACCS/BLENDED/OC etc.)	FT, Blended, Block, ACCS

Award Class	Award NQF Level	Award EQF Level	Stage	Stage NQF Level	Stage EQF Level	Stage Credit (ECTS)	Date Effective	ISCED Subject Code
Major	9		Award	9		90	September 2016	481

Ref	Module Title	Semester	Module		ECTS Credit Number	Total Student Effort			Allocation of Marks			
			Status (M/E)	NQF Level		Total Hours	Contact Hours	Independent Learning	CA %	Project %	Exam %	Total %
	Security Fundamentals	1	M	9	10	250	48	202	40	0	60	100
	Secure Programming for Web	1	M	9	10	250	60	190	60	40	0	100
	IT Law and Ethics	1	M	9	5	125	24	101	40	0	60	100
	Network Security and Penetration Testing	1	M	9	5	125	24	101	40	0	60	100
	Research in Computing	2	M	9	5	125	24	101	20	80	0	100
	Secure Programming for Application Development	2	M	9	5	125	36	89	60	40	0	100
	Cryptography	2	M	9	5	125	24	101	40	0	60	100
	Malware Analysis	2	GE1A, GE2A	9	5	125	24	101	60	40	0	100
	Domain Context	2	GE1B, GE2B	9	5	125	24	101	100	0	0	100
	Incident Response and Analytics	2	GE1	9	5	125	24	101	40	0	60	100
	Forensics and eDiscovery	2	GE1	9	5	125	24	101	40	0	60	100
	Cloud Security	2	GE2	9	10	250	48	202	0	40	60	100
	Research Methods	3	M	9	5	125	24	101	60	40	0	100
	Internship	3	M	9	25	600	10	490	0	100	0	100

Special Regulations:

Note 1: A student must pass Research in Computing and not repeat more than 10 ECTS credits to be eligible to register for the Internship

Note 2: Learners must complete and pass Internship.

Note 3: **Students must choose ONE Group Elective**

Group Elective 1 – Forensics (Modules: Incident Response and Analytics, Forensics and eDiscovery, Cryptography ,and Malware Analysis or Domain Context

Group Elective 2 – Cloud Security (Modules: Cloud Security, Cryptography and Malware Analysis or Domain Context

Note 4: Students from each group elective must to select a 5 credits module from a set of elective modules such as: Malware Analysis or Domain Context.

Note 5: Domain Context module may have a number of instances within the same semester it runs. For example, a different module instance for each specialisation.

QQI
Quality and Qualifications Ireland
Dearbhú Cáilíochta agus Cáilíochtaí Éireann

Name of Provider			National College of Ireland										
Programme Title (i.e. named award)			Postgraduate Diploma in Cyber Security										
Award Title (QQI named award)			Postgraduate Diploma in Cyber Security										
Stage Exit Award Title			Postgraduate Diploma in Science in Cyber Security										
Modes of Delivery (FT/PT/ACCS/BLENDED/OC etc.)			FT, Blended, Block, ACCS										
Award Class	Award NQF Level	Award EQF Level	Stage	Stage NQF Level	Stage EQF Level	Stage Credit (ECTS)	Date Effective	ISCED Subject Code					
Major	9		Award	9		90	September 2016	481					
Ref	Module Title	Semester	Module		ECTS Credit Number	Total Student Effort			Allocation of Marks				
			Status (M/E)	NQF Level		Total Hours	Contact Hours	Independent Learning	CA %	Project %	Exam %	Total %	
	Security Fundamentals	1	M	9	10	250	48	202	40	0	60	100	
	Secure Programming for Web	1	M	9	10	250	60	190	60	40	0	100	
	IT Law and Ethics	1	M	9	5	125	24	101	40	0	60	100	
	Network Security and Penetration Testing	1	M	9	5	125	24	101	40	0	60	100	
	Research in Computing	2	M	9	5	125	24	101	20	80	0	100	
	Secure Programming for Application Development	2	M	9	5	125	36	89	60	40	0	100	
	Cryptography	2	M	9	5	125	24	101	40	0	60	100	
	Malware Analysis	2	GE1A, GE2A	9	5	125	24	101	60	40	0	100	
	Domain Context	2	GE1B, GE2B	9	5	125	24	101	100	0	0	100	
	Incident Response and Analytics	2	GE1	9	5	125	24	101	40	0	60	100	
	Forensics and eDiscovery	2	GE1	9	5	125	24	101	40	0	60	100	
	Cloud Security	2	GE2	9	10	250	48	202	0	40	60	100	

Special Regulations:

Note 1: **Students must choose ONE Group Elective**

Group Elective 1 – Forensics (Modules: Incident Response and Analytics, Forensics and eDiscovery, Cryptography ,and Malware Analysis or Domain Context

Group Elective 2 – Cloud Security (Modules: Cloud Security, Cryptography and Malware Analysis or Domain Context

Note 2: Students from each group elective must to select a 5 credits module from a set of elective modules such as: Malware Analysis or Domain Context.

Note 3: Domain Context module may have a number of instances within the same semester it runs. For example, a different module instance for each specialisation.