New College of the Humanities

Cybersecurity Course Descriptor

Course Title	Cybersecurity	Faculty	EDGE Innovation Unit (London)
Course code	NCHMV583	Course Leader	Marta Rodriguez-Martinez
Credit points	15	Teaching Period	6 weeks
FHEQ level	5	Date approved	March 2021
Compulsory/ Optional	Compulsory		
Prerequisites	None		
Co-requisites	None		

COURSE SUMMARY

This course will provide learners with the ability to assess the impact of various cyber security threats that pose a risk to deployed digital systems. The course will also teach the importance of human and social factors that can lead to exploitation events as part of a prolonged and sustained cyber security attack. Learners will be able to use recognised industry standard frameworks for assessing the risks and associated exposures. Finally, learners will be able to critique the available validation approaches and provide evidence-based recommendations for an organisation.

COURSE AIMS

- Train learners to critically review how cybersecurity-related threats impact digital technologies and solutions.
- Train learners to appraise cyber security standards and their relevance to an organisation.
- Enable learners to make recommendations on security policies for an organisation executing a digital transformation.

LEARNING OUTCOMES

On successful completion of the course, learners will be able to:

KNOWLEDGE AND UNDERSTANDING

K2b	Evaluate the threats and vulnerabilities and their impact in the context of cyber security in an organisation.
K2b	Research and analyse common cyber security breaches and attack techniques and propose mitigation plans.

SUBJECT SPECIFIC SKILLS

S1b	Investigate and interpret security incidents, and propose recovery solutions for security failures.
S1b	Deploy industry-standard frameworks to produce an audit of cyber security policies.

TRANSFERABLE AND PROFESSIONAL SKILLS

T1b	Clearly communicate in writing.
T1b	Present persuasive arguments in an oral presentation.
T3b	Evaluate Cybersecurity risks in a business area and identify areas for improvement.

TEACHING AND LEARNING

The course learning and teaching hours will be structured as follows:

- Seminar = 15 hours
- Applied Seminar = 7.5 hours
- Coaching session = 1 hour
- Academic Drop-ins = 4 hours
- Reading and Assessment Prep = 32.5 hours
- Application of learning = 90 hours

Total = 150 hours

ASSESSMENT

FORMATIVE

Learners will be formatively assessed during the course through a range of techniques. During seminars, applied learning seminars and one to one coaching, questioning and quizzing are used as formative assessment. The purpose of the formative assessment is to provide learners with developmental feedback to support their learning.

SUMMATIVE

AE	Assessment Type	Weighting	Online submission	Duration	Length
1	Exam	60%	Yes	1.5 hours	-
2	Oral	40%	No	30 mins +/-10%	-

The summative assessment will be assessed in accordance with the assessment aims set out in the Programme Specification.

FEEDBACK

Learners will receive formal feedback in a variety of ways. For summative assessments, feedback is written and provided within 20 days of submission or presentation. For formative assessment it could include verbal or written feedback. Learners will also have a progress review each quarter with their Multiverse Coach and their Line Manager. These reviews are an opportunity to discuss progress to date both in their role and on the degree programme.

For summative exams, feedback is provided through generic internal examiners' reports, which are posted on the Appli.ed learning platform.

INDICATIVE READING

Note: Comprehensive and current reading lists for courses are produced annually in the Course Syllabus or other documentation provided to learners; the indicative reading list provided below is used as part of the approval/modification process only.

BOOKS

Janca, T., 2020. *Alice and Bob Learn Application Security.* Wiley

Johansen, G., 2017. *Digital Forensics and Incident Response.* Packt Publishing Ltd.

Steinberg, J., 2019. Cybersecurity for Dummies. John Wiley & Sons.

JOURNALS

Jang-Jaccard, J. and Nepal, S., 2014. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), pp.973-993

ELECTRONIC RESOURCES

Learners are encouraged to consult relevant electronic resources on cybersecurity, such as the British Computing Society Code of Conduct: www.bcs.org.uk.

INDICATIVE TOPICS

- Security of computer systems
- Cybersecurity risk management
- Industry and regulatory security standards

Title: NCHMV583 Cybersecurity Course Descriptor **Approved by: Academic Board**					
Version number	Date approved	Date published	Owner	Location	Proposed next review date
1.0	March 2021	March 2021	Marta Rodriguez -Martinez	Multiverse website	March 2026
Modifications (As per AQF4)					
Version number	Date approved	Date published	Modification (including category number)		