COURSE SPECIFICATION DOCUMENT

Academic School / Department: School of Liberal Arts

Programme: Computer Science

***FHEQ* Level:** 5

Course Title: Cyber Security

Course Code: DGT 5120

Total Hours: 120 (standard 3- credit BA course)

Timetabled Hours: 45
Guided Learning Hours: 0
Independent Learning Hours: 75

Semester: Fall, Spring, Summer

Credits: 12 UK CATS credits
6 ECTS credits
3 US credits

Course Description:
This course considers online security and protection. Students will learn how to identify threats and take steps to reduce vulnerabilities. The course will frame digital safety in the context of the Web, introducing concepts like malware, viruses, Trojans, network security, cryptography, identity theft and risk management, and will outline contemporary security strategies being developed. It is highly recommended that students have access to the use of a laptop and a smartphone for the duration of the course.

Prerequisites:
DGT 4100 or DGT 4101

Aims and Objectives:
The primary aim of this course is to familiarise students with online security terminology and protection strategies for business or home. It will focus on understanding and using cryptography terminology and its applications. Students will be able to understand the range of malware types for example Adware, Spyware, Trojan horse, Ransom ware and

learn the skills to for preventing malware attacks. They will have guidance in contextualising this through appropriate examples and Case studies. Alongside using a range of software, students will be required to maintain a reflective technical journal that can act as a reference point for problem solving and protection from online threats in the future.

Programme Outcomes:

Computer Science: A3, A6, B1, B2, B4, C1, C4

The learning outcomes satisfy the program outcomes of the Digital Minor: 5Ai, 5Bi, 5Ci

Programme Outcomes Digital Minor
Level 5

- Demonstrate a detailed understanding of different digital environments and their respective digital languages. (5Ai)
- Demonstrate the ability use digital software to produce high quality relevant outcomes and critically reflect on the results. (5Bi)
- Appreciate the connections between theories and their applications in specific digital environments and to be able to critically evaluate these. (5Ci)

A detailed list of the programme outcomes is found in the Programme Specification. This is maintained by Registry and located at: https://www.richmond.ac.uk/programme-and-course-specifications/

Learning Outcomes:
By the end of this course, successful students should be able to:

- Demonstrate an ability to identify, analyse and evaluate a range of cyber security strategy and digital information assets.
- Demonstrate an ability to identify main malware types, cryptography terminology and be aware of alternate authentication methods.
- Demonstrate understanding of firewalls, networks and recoveries from security failures
- Engage in self-directed research to problem solve technical issues to produce innovative solutions.

Indicative Content:

- Threats: Terminology, Ransom Threats, Spyware Threats, Staying Updated.
- Authentication: passwords, two-factor authentication
- Malware: types of malware, preventing infection

- Networking: communications, security challenges
- Cryptography: symmetric and asymmetric cryptography, applications
- Network security: firewalls, intrusion detection and prevention
- Security failures: cyber security laws, recovering from attacks
- Managing security risks: risk analysis and management

Assessment:
This course conforms to the University Assessment Norms approved at Academic Board and found at https://www.richmond.ac.uk/university-policies

Teaching Methodology:
- Lecture presentations with the key concepts
- Group discussions on journal articles and online resources.
- Lecture demonstration with the key applications and software.
- Teamwork solving technical problems.
- Individual research on online sites related to coding and the use of digital media
- Videos and On-line demonstrations.
- Intra-net access to lecture notes, links to applications and online tutorials and reading material.

Indicative Text(s):
- **Introduction to Computer Networks and Cybersecurity Hardcover – 1 Mar 2013** by Chwan-Hwa (John) Wu (Author), J. David Irwin (Author)
- Young C (2019) *The Cybersecurity Playbook: Practical Steps for Every Leader and Employee--To Make Your Organization More Secure* John Wiley & Sons
- Reuvid J (2016) *Managing Cybersecurity Risk: How Directors and Corporate Officers Can Protect their Businesses* Legend Business publishing.
- Shrobe H, Shrier D, Pentland A (2018) *New Solutions for Cybersecurity* MIT Press

WEB LINKS
- **https://www.ncsc.gov.uk/**
- **https://www.reuters.com/news/archive/cybersecurity**
- **https://www.wired.com/tag/cybersecurity/**

- **https://www.digitalhealth.net/2019/02/cyber-security-news-round-up-5/**

See syllabus for complete reading list

Change Log for this CSD:

Nature of Change	Date Approved & Approval Body (School or AB)	Change Actioned by Registry Services
Changes to pre-requisite	Dec 2023	
Course description updated	Dec 2023	
Total Hours Updated	April 2024	