Module Definition Form (MDF)

Module code: MOD007360	**Version:** 3 **Date Amended:** 27/Nov/2025

1. Module Title
Software Security

2a. Module Leader
Charles Marrow

2b. School
School of Computing and Information Sciences

2c. Faculty
Faculty of Science and Engineering

3a. Level
6

3b. Module Type
Standard (fine graded)

4a. Credits
15

4b. Study Hours
150

5. Restrictions

Type	Module Code	Module Name	Condition
Pre-requisites:	None		
Co-requisites:	None		
Exclusions:	None		
Courses to which this module is restricted:	BSc (Hons) Cyber Security BSc (Hons) Cyber Security and Digital Forensics		

LEARNING, TEACHING AND ASSESSMENT INFORMATION

6a. Module Description

The software development industry is rapidly evolving. Generative AI now contributes an estimated 20–30% of new code, rising even higher in some organisations. While this accelerates the design-to-production cycle, it also introduces new security challenges. This module introduces the principles of DevSecOps, the Software Development Life Cycle (SDLC), and the integration of security practices into both AI-generated and existing legacy applications.

You'll develop knowledge and hands-on skills in secure coding techniques, web application security, vulnerability assessment, and security testing. Key concepts such as input validation, cross-site scripting, data leakage, and web-service vulnerabilities will be explored. The importance of effective security management is emphasised through the design and implementation of custom security policies. You'll have the opportunity to build applications, test them for vulnerabilities, recommend mitigations, and integrate secure coding practices into AI-generated or other code.

6b. Outline Content

- SDLC
- Web Application Security
- Application testing
- Agile Frameworks
- DevSecOps Maturity Model
- AI Generated Code
- Vulnerability assessment and Mitigation

6c. Key Texts/Literature

The reading list to support this module is available at: https://readinglists.aru.ac.uk/

6d. Specialist Learning Resources

Computer labs with admin rights and the ability to use virtualisation via a tool such as VMware Workstation.

A mixture of current Linux and Windows web server environments for application testing with a programming language such as Python installed.

Access to AI generative tools for coding and programming

Access to NETLAB facilities

7. Learning Outcomes (threshold standards)		
No.	**Type**	**On successful completion of this module the student will be expected to be able to:**
1	Knowledge and Understanding	Discover and analyse security vulnerabilities in software applications.
2	Knowledge and Understanding	Demonstrate in-depth knowledge of secure software requirements.
3	Intellectual, practical, affective and transferrable skills	Illustrate how to exploit the code of a vulnerable application.
4	Intellectual, practical, affective and transferrable skills	Justify and critically appraise the use of chosen mitigations methods of software vulnerabilities in applications.

8a. Module Occurrence to which this MDF Refers				
Year	**Occurrence**	**Period**	**Location**	**Mode of Delivery**
2025/6	ZZF	Template For Face To Face Learning Delivery		Face to Face

8b. Learning Activities for the above Module Occurrence			
Learning Activities	**Hours**	**Learning Outcomes**	**Details of Duration, frequency and other comments**
Lectures	12	1-4	12x1Hr(s) Lecture
Other teacher managed learning	24	1-4	12x2Hr(s) Practical
Student managed learning	114	1-4	Self-directed study
TOTAL:	150		

9. Assessment for the above Module Occurrence					
Assessment No.	**Assessment Method**	**Learning Outcomes**	**Weighting (%)**	**Fine Grade or Pass/Fail**	**Qualifying Mark (%)**
010	Coursework	1-4	100 (%)	Fine Grade	30 (%)
Course Work Equivalent to 3000 Words					

In order to pass this module, students are required to achieve an overall mark of 40% (for modules at levels 3, 4, 5 and 6) or 50% (for modules at level 7*).

In addition, students are required to:
(a) achieve the qualifying mark for each element of fine graded assessment as specified above
(b) pass any pass/fail elements

[* the pass mark of 50% applies for all module occurrences from the academic year 2024/25 – see Section 3a of this MDF to check the level of the module and Section 8a of this MDF to check the academic year]