H7SFD: Security Fundamentals and Development

Module Code:	H7SFD
Long Title	Security Fundamentals and Development APPROVED
Title	Security Fundamentals and Development
Module Level:	LEVEL 7
EQF Level:	6
EHEA Level:	First Cycle
Credits:	10
Module Coordinator:	
Module Author:	Alex Courtney
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	Master's degree/PhD in Computing or cognate discipline.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
#	**Learning Outcome Description**
LO1	Identify a range of security threats and examine technologies, regulations, standards, and practices to protect individuals and organisations from cyber-attacks.
LO2	Identify threats and formulate responses to mitigate risk through the application of appropriate tools and technologies.
LO3	Describe a range of roles, responsibilities and procedures across the information security management sector.
LO4	Demonstrate an in-depth knowledge of cryptographic mechanisms and the ability of applying these mechanisms to the achievement of security services.
LO5	Demonstrate an understanding of business continuation and disaster recovery response procedures.

Dependencies
Module Recommendations
No recommendations listed
Co-requisite Modules
No Co-requisite modules listed

Entry requirements	Learners should have attained the knowledge, skills and competence gained from stage 2 of the BSc (Hons) in Computing.

H7SFD: Security Fundamentals and Development

Module Content & Assessment

Indicative Content
Introduction to Information Security & Information security fundamentals Introduction to information security & security fundamentals with a high-level overview of security models, IS standards and attack overviews
Cybersecurity Common Threats Introduction to a range of cybersecurity threats – Malware, spyware , phishing, Cyber Extortion, activism, social engineering DDOS and advance persistent threats
CIA Triad and Cybersecurity Roles Overview of the CIA Triad and an examination of governance as it relates to cybersecurity. Identification of organisational roles pertaining to cybersecurity and information management.
Security Frameworks and Policies A high-level overview of security frameworks and their application in a data driven organisation. . An introduction to Information classification and ISO 27001
Risk management, Threat modelling & training for awareness An introduction to and high-level view of threat modelling, risk management and how security training & awareness benefits an organisation.
Network Security Architecture A high-level overview of network vulnerabilities and how network architecture must be given careful consideration. This should include Access control, patch management and logging and monitoring. Wireless network security should be included here.
Incident management & Data loss management Vulnerabilities of data management and an introduction to data loss prevention tools.
Business continuity Key stakeholders and legal regulatory, and organisational compliance.
Disaster Recovery A high-level introduction to a project plan and the impact of an attack as it relates to disaster recovery. This should identify the technical impact in such a situation
Software Development Lifecycle A demonstration of how security procedures should apply to all aspects of the SDL
Cryptography Symmetric, Asymmetric cryptography, PKI & digital signatures

Assessment Breakdown	%
Coursework	50.00%
End of Module Assessment	50.00%

Assessments

Full Time

Coursework

Assessment Type:	Formative Assessment	**% of total:**	Non-Marked
Assessment Date:	n/a	**Outcome addressed:**	1,2,3,4,5
Non-Marked:	Yes		

Assessment Description:
Formative assessment will be provided on the in-class individual or group activities.

Assessment Type:	Project	**% of total:**	50
Assessment Date:	n/a	**Outcome addressed:**	1,2,4
Non-Marked:	No		

Assessment Description:
Learners in a group must participate in a case study project which will rationalise a series of risk remediation factors and execute a high-level demonstration of techniques to integrate these remediation's. The project will demonstrate Cryptography Programming

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	50
Assessment Date:	End-of-Semester	**Outcome addressed:**	1,2,3,5
Non-Marked:	No		

Assessment Description:
Terminal Exam Covering All Learning Outcomes and All Content Delivered Throughout The Module

No Workplace Assessment

Reassessment Requirement

Repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

Reassessment Description
Repeat examination Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

H7SFD: Security Fundamentals and Development

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom & Demonstrations (hours)	24	Every Week	24.00
Tutorial	Other hours (Practical/Tutorial)	24	Every Week	24.00
Independent Learning	Independent learning (hours)	202	Every Week	202.00
			Total Weekly Contact Hours	48.00

Module Resources

Recommended Book Resources

Trim P. & Lee Y. ,. (2016), ,Cybersecurity Management, Risk and Compliance Framework ,CRC Press.

Kohnke A. ,. (2016), ,The Complete Guide to Cybersecurity Risks and Controls (Internal Audit and IT Audit).

Supplementary Book Resources

Stallings W. ,. (2011), ,Cryptography and Network Security: Principles and Practice ,Pearsons.

(2018), ,(ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide ,ISC Official Study Guides.

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note:	