H9SFND: Security Fundamentals

Module Code:	H9SFND
Long Title	Security Fundamentals APPROVED
Title	Security Fundamentals
Module Level:	LEVEL 9
EQF Level:	7
EHEA Level:	Second Cycle
Credits:	10
Module Coordinator:	Vanessa Ayala-Rivera
Module Author:	Margarete Silva
Departments:	School of Computing
Specifications of the qualifications and experience required of staff	PhD/Master's degree in a computing or cognate discipline. May have industry experience also.

Learning Outcomes

On successful completion of this module the learner will be able to:

#	Learning Outcome Description
LO1	Compare and contrast new threats and technologies with respect to regulations, standards, and practices in order to protect businesses from cyber-attacks.
LO2	Research, evaluate and apply security management methodologies and best practices.
LO3	Compare and contrast security solutions for wired and wireless network
LO4	Devise and develop business continuity and disaster recovery plans.
LO5	Analyse and assemble responses from various Security Monitoring Systems.

Dependencies

Module Recommendations

No recommendations listed

Co-requisite Modules

No Co-requisite modules listed

Entry requirements	Programme entry requirements must be satisfied.

H9SFND: Security Fundamentals

Module Content & Assessment

Indicative Content
Cybersecurity Landscape Open Cloud Manifesto; Cloud Computing: services, Deployment models, characteristics; Future trends in Devices, services, etc
Introduction into Cybersecurity Concepts Definitions of various cybersecurity related terms; CIA Triad, Data Breaches; Types of Cyber Crime Primary Security concepts: Prevention, Detection, and Recovery; Access Control Process; Understanding Assets, Threats, Vulnerabilities, Control; User Security Management Techniques
Introduction into Information Security History and evolution of information Security; Information Security terms and concepts; Characteristics of Information; Components of Information System
Information Security Management Information Security Models; Security Systems Development Life Cycle (SecSDLC); Information Security roles and responsibilities
Common Threats Introduction & Terminology; Employee and Ex-Employee Threats; Malware; Hackers and Attacks; Competitor Threats; Cyberwar and Cyberterrorism
Networking Network Topologies, Firewalls, Routers and Switches, Proxy Servers
Security Networks Importance of Securing the Network; (DoS) attack; ARP poisoning; access controls; Securing Ethernet networks; WLAN access and security standards; Examples of network attacks
Security Monitoring Systems Intrusion Detection Systems and Intrusion Prevention Systems: objectives, classification, monitoring approaches, data sources; Honeypot
Securing Wireless Network Wireless footprint; Various security protocols; MAC filtering; SSID; VPN
Security Frameworks Policies, Standards, Procedures and Guidelines; Information Classification; Security Policy Development Live Cycle; Security; Information Security Management System; Business continuity and disaster recovery plans; Examples of Framework and Standards e.g., ISO 27001. COBIT, NIST, SETA, etc.
Risk and Compliance Sensitive Data an Assets; Risk and Compliance; Data Protection and Prevention of Data Leakage; General Data Protection Regulation (GDPR)
Introduction to Cryptography History of Cryptography, Cryptography in the Modern World; Types of Cryptography; Application of Cryptography

Assessment Breakdown	%
Coursework	40.00%
End of Module Assessment	60.00%

Assessments

Full Time

Coursework

Assessment Type:	Continuous Assessment	**% of total:**	40
Assessment Date:	n/a	**Outcome addressed:**	1,2
Non-Marked:	No		

Assessment Description:
The assessment requires research work and critical analysis on current threats, high-profile attacks/exploits related to selected threat, as well as security management methodologies.

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

Assessment Description:
Informal assessment will be provided a in-class individual tasks or group activities. Feedback will be provided in written or oral format, or on-line through Moodle. In addition, in class discussions will be undertaken as part of the practical approach to learning.

End of Module Assessment

Assessment Type:	Terminal Exam	**% of total:**	60
Assessment Date:	End-of-Semester	**Outcome addressed:**	3,4,5
Non-Marked:	No		

Assessment Description:
The examination will be of two hours duration and may include a mix of: theoretical, applied and critical analysis questions.

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
The reassessment strategy for this module will consist of a terminal examination that will assess all learning outcomes.

H9SFND: Security Fundamentals

Module Workload

Module Target Workload Hours 0 Hours

Workload: Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	214	Per Semester	17.83
			Total Weekly Contact Hours	3.00

Workload: Blended

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	12	Per Semester	1.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Directed Learning	Directed e-learning	12	Per Semester	1.00
Independent Learning	Independent learning	214	Per Semester	17.83
			Total Weekly Contact Hours	3.00

Workload: Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Classroom and demonstrations	24	Per Semester	2.00
Tutorial	Mentoring and small-group tutoring	12	Per Semester	1.00
Independent Learning	Independent learning	214	Per Semester	17.83
			Total Weekly Contact Hours	3.00

Module Resources

Recommended Book Resources

Tim Rains. (2020), Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks, Packt Publishing, [ISBN: 978-1800206014].

Andy Taylor,David Alexander,Amanda Finch,David Sutton. (2020), Information Security Management Principles. BCS, The Chartered Institute for IT, 3rd Ed. BCS, The Chartered Institute for IT, p.224, [ISBN: 978-1780175188].

Supplementary Book Resources

Umesha Nayak,Umesh Hodeghatta Rao. (2014), The InfoSec Handbook: An Introduction to Information Security, 1st Ed. Apress, p.392, [ISBN: 978-1430263821].

Corey Schou,Steven Hernandez. (2014), Information Assurance Handbook: Effective Computer Security and Risk Management Strategies, McGraw-Hill Education, p.480, [ISBN: 978-0071821650].

This module does not have any article/paper resources

This module does not have any other resources

Discussion Note:	