Module Specification

Information Security

Version: 2026-27, v2.0, Approved

Contents

Part 1: Information

Module title: Information Security

Module code: UFCFHJ-15-M

Level: Level 7

For implementation from: 2026-27

UWE credit rating: 15

ECTS credit rating: 7.5

College: College of Arts, Technology and Environment

School: CATE School of Computing and Creative Technologies

Partner institutions: None

Field: Computer Science and Creative Technologies

Module type: Module

Pre-requisites: None

Excluded combinations: None

Co-requisites: None

Continuing professional development: No

Professional, statutory or regulatory body requirements: None

Part 2: Description

Overview: Information Security develops a critical understanding of how organisations protect information assets across technical and managerial domains. Students study core principles and risk management within legal, ethical and societal contexts, and examine governance frameworks, policy development and secure software practice. By combining theory with applied analysis and standards-aligned policy work, the module prepares students to design, assess and justify security strategies for professional practice and senior management audiences.

Features: Not applicable

Educational aims: The module aims to give students a critical appreciation of the principles, risks, and governance practices that shape modern information security. It develops the ability to evaluate threats and vulnerabilities, interpret legal and regulatory requirements, and appraise the ethical and societal implications of security decisions.

Students will strengthen their capacity to research and synthesise current issues, to assess the suitability of technical and managerial controls, and to articulate well-reasoned, standards-aligned security policies for senior management audiences. The knowledge and analytical skills gained provide a solid foundation for further study or professional roles in information security management, compliance, and governance.

Outline syllabus: The module provides a structured exploration of the concepts, controls, and management practices that underpin contemporary information security. Indicative topics include the following:

Foundational principles: confidentiality, integrity, availability, risk assessment, threat modelling, and vulnerability analysis

Legal and ethical context: regulation and compliance requirements, privacy and data protection, civil liberties, intellectual property, and cybercrime

Security governance and management: security policies and frameworks, organisational ethics, incident response planning, disaster recovery, and business continuity

Technical controls: authentication and authorisation mechanisms, data protection and encryption, network and computer security, secure application development, and physical and environmental safeguards

Emerging trends: security governance developments, identity and access management, and other evolving issues in the information-security landscape

This outline signals the breadth of material while allowing for the inclusion of current developments and sector-specific case studies each year.

Part 3: Teaching and learning methods

Teaching and learning methods: The module is delivered through a weekly lecture that combines presentation of core concepts with interactive elements such as short discussions, problem-based questions, and case-study analysis. These sessions introduce key principles, explore current issues, and highlight emerging trends in information security, providing the foundation for independent study and assessment work.

Independent learning remains essential. Students are expected to undertake directed reading, critically review contemporary literature, and collaborate in their groups to research and develop the assessed management report. Formative feedback is provided through lecture interactions, scheduled guidance opportunities, and informal consultation, enabling students to refine their analysis and written work.

This approach ensures that students engage critically with theoretical and practical aspects of information security and acquire the analytical and professional communication skills required to meet the module learning outcomes.

Module Learning outcomes: On successful completion of this module students will achieve the following learning outcomes.

MO1 Synthesise and evaluate the key information security principles, risks, threats and vulnerabilities by organisations.

MO2 Analyse information security issues related to privacy, civil liberties and intellectual property, reporting to senior level.

MO3 Create and justify an information security strategy, presenting well-reasoned technical and managerial controls in line with professional and regulatory standards.

Hours to be allocated: 150

Contact hours:

Independent study/self-guided study = 126 hours

Face-to-face learning = 24 hours

Reading list: The reading list for this module can be accessed at readinglists.uwe.ac.uk via the following link https://uwe.rl.talis.com/modules/ufcfhj-15-m.html

Part 4: Assessment

Assessment strategy: The module is assessed through a single summative component: an individual written report in which students create and justify an Information Security Strategy for a given organisational scenario. The report requires students to evaluate threats, risks, vulnerabilities, and propose well-reasoned technical and managerial controls aligned with professional and regulatory standards.

Formative guidance and feedback will be provided during scheduled teaching sessions to help students refine their analysis, structure, and written work.

The resit assessment will follow the same format and requirements as the main assessment, ensuring consistency in expectations and marking.

Assessment tasks:

Report (First Sit)
Description: Information security report based on a scenario.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Report (Resit)
Description: Information security report based on a scenario.
Weighting: 100 %
Final assessment: Yes
Group work: No
Learning outcomes tested: MO1, MO2, MO3

Part 5: Contributes towards

This module contributes towards the following programmes of study:

Information Technology [Frenchay] MSc 2025-26

Information Technology [Frenchay] MSc 2026-27

Information Technology [Frenchay] MSc 2026-27

Information Technology [Frenchay] MSc 2026-27

Information Technology [Villa] MSc 2026-27

Information Technology [Villa] MSc 2026-27