Title	Cybersecurity Law and Regulations
Long Title	Cybersecurity Law and Regulations
Credits	**6**
NFQ Level	9
Module Author	Lubna Lumxi

Module Description:

The aim of the module is to enable students to be aware of Security Standards and associated laws and regulations for Information Technology (IT) convergence. This module was developed under the CyberSkills HCI Pillar 3 Project. Please refer to the consortium agreement for ownership.

Learning Outcomes

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

LO1	Appraise the laws, regulations, policies and ethics as they relate to cyber security and privacy.
LO2	Assess manage and apply the reporting standards relevant to Cyber Security Technologies .
LO3	Demonstrate an understanding of the ethical issues associated with computing.
LO4	Evaluate the threat landscape associated with Information Technology (IT) integration of systems
LO5	Value and accept the importance of laws, standards and ethics related to cyber security in computing

Indicative Content

Landscape

- Multi-level governance and regulatory system i.e. International standards, EU rules, Domestic Rules.

Legal, ethics and cybersecurity

- The meaning of 'Ethics'. The relationship between Law and Morality. Ethical issues in Computing. Ethical and common law duties. Contractual and regulatory duties to protect information. Cyber Ethics Case Studies (e.g. Ethical hacking principles and techniques (NIST) OR Certified Ethical Hacker – EC Council, the Cyber Culture OR Professional Responsibility in Cybersecurity Research and Industry), Policy measures and Cyber Insurance.

Laws, Regulations & Standard

- Ireland and EU: EU Cybersecurity Act, Personally Identifiable Information (PII), GDPR/Statutory Data Audit, NIS. Criminal Justice (Offences Relating to Information Systems) Act 2017. USA:CFA Act, CSA Act, ECPA, GLB Act, SOX, DMCA, CCPA. Personal Health Information (PHI)Health Insurance Portability and Accountability Act of 1996 (HIPAA). ENISA Threat Landscape.

Standards, Compliance & Violation

- Reporting standards. NIST. SSAE-16. AT-101. Federal Risk and Authorization Management Program (FedRAMP) compliance. ISO compliance. Regulatory Compliance. Reputational damage. Gambling Commission, Auditing. Skill in implementing and testing network infrastructure contingency and recovery plans.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written	This report will assess the student's theoretical knowledge of cybersecurity laws, regulations, ethics and standards and the application of these in mitigating various threats.	1, 2, 3	40%	Week 6
Project	Learners must select the appropriate compliance, legal and governance mechanisms to implement and adhere to in a defined ambiguous scenario. Learners must document their research and decision making in a detailed report and create a presentation capable of clearly expressing a summary of their findings to their peers and experts in the field.	3, 4, 5	60%	Week 12

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Tutorial	Tutorial to support student learning – online support	1.0	Every Week	1.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	5.0	Every Week	5.0
		Total Hours		10.0
		Total Weekly Learner Workload		10.0
		Total Weekly Contact Hours		4.0

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Tutorial	Tutorial to support student learning – online support	1.0	Every Week	1.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	5.0	Every Week	5.0
		Total Hours		10.0
		Total Weekly Learner Workload		10.0
		Total Weekly Contact Hours		4.0

Recommended Web Resources

- **Complete guide to GDPR Compliance https://gdpr.eu/**
- **ENISA.Cybersecurity Standards and Certification https://www.enisa.europa.eu/topics/standards**
- **The EU cybersecurity certification framework https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework**
- **ETSI. ETSI - Cyber Security. Cyber Security Standards. Cyber Security Technology https://www.etsi.org/technologies/cyber-security**

Recommended Book Resources

- **Joseph Lee, Aline Darbellay. 2022, Data Governance in AI, FinTech and LegalTech - Law and Regulation in the Financial Sector. [ISBN13: 9781800379947]**
- **Schreider, T. 2020, Cybersecurity Law, Standards and Regulations, 2nd Ed. [ISBN: 978-194448056]**
- **Jelena Madir. 2021, FinTech - Law and Regulation, Second Edition. [ISBN13 9781800375949]**

Case Studies

- **ICS Cyber Attack**
- **University Students Records Stolen Data Breach**
- **Fashion Industry – PII Data Breach**
- **5 Star Hotel Chain Ransomware Data Breach**
- **Customer Credit Card – Online platform vulnerabilities Data breach**
- **Fintech – Impact of hack that leaked personal data of over 1 million customers.**