|  |  |  |
| --- | --- | --- |
| **Course Code:** ICT-5315 | **Year: MSc** | **Term: Optional** |
| **Course Title:** Applied Cyber Security | | |

**Course Status:** Optional **Credit:** 3.0 **Prerequisite(s):** None

**Rationale**

This course covers cyber security threats, technologies, and management practices in the public and private sectors, as well as the importance of governing principles in cyber security, the theory and practice of technology risks and countermeasures, and the role of security management in the overall perspective of cyber security.

|  |  |  |
| --- | --- | --- |
| **Course Contents** | | **CLOs** |
| **1.** | **Introduction to Information Security Fundamentals:** Protecting Your Computer and its Contents.  Securing Computer Networks–Basics of Networking; Compromised Computers; Secure Communications and Information Security Best Practices; Privacy  Guidelines; Safe Internet Usage. | 1 |
| **2.** | **Ethics in Cybersecurity & Cyber Law:** Privacy; Intellectual Property; Professional Ethics; Freedom of Speech; Fair User and Ethical Hacking;  Trademarks; Internet Fraud; Electronic Evidence; Cybercrimes. | 2 |
| **3.** | **Forensics:** Forensic Technologies; Digital Evidence Collection; Evidentiary  Reporting; Network Assurance: Layered Defense; Surveillance and Reconnaissance; Outsider Thread Protection. | 3 |
| **4.** | **Secure Software & Browser Security:** Software Construction; Software Design and Architecture; Software Testing; Methodologies; The New Universal Client;  The Web Model; Cookies and Browser Storage; HTML5 Security; | 4 |
| **5.** | **Business Information Continuity:** Managing a Business Information Continuity Plan; Vulnerabilities and Controls; The Law and Business Information Continuity Plan.  **Information Risk Management:** Asset Evaluation and Business Impact Analysis; Risk Identiﬁcation; Risk Quantiﬁcation; Risk Response Development  and Control; Security Policy, Compliance, and Business Continuity. | 5 |
| **6.** | **Cyber Incident Analysis and Response:** Incident Preparation; Incident Detection and Analysis; Containment, Eradication, and Recovery; Proactive and  Post-Incident Cyber Services. | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Upon completion of this course the students will be able to: | | **Mapping** |
|  | **with PLOs** |
|  |  | Understand cyber security threats, technologies, and |  |
| **Course** | CLO1 | management practices within public and private | 1,2 |
| **Learning** |  | sectors. |  |
| **Outcomes** |  | Understand key terms and concepts in cyber law, |  |
| **(CLOs)** | CLO2 | intellectual property and cybercrimes, trademarks, and | 2,4 |
|  |  | domain theft. |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | CLO3 | Analyze digital evidence collection, and evidentiary reporting in forensic acquisition. | 3,6 |
| CL04 | Apply approaches to secure networks, ﬁrewalls, intrusion detection systems, and intrusion prevention systems. | 6, 7 |
| CLO5 | Incorporate approaches for risk management and response for cyber incident. | 3, 6,7,8 |

**Mapping CLOs with the Teaching-Learning and Assessment Strategy**

|  |  |  |
| --- | --- | --- |
| **CLOs** | **Teaching-Learning Strategy** | **Assessment Strategy** |
| CLO1 | Interactive lectures, Discussions | Class Tests, Assignments, Final Examination |
| CLO2 | Interactive lecturing, Discussions | Class Tests, Assignments, Final Examination |
| CLO3 | Interactive lecturing, Discussions | Class Tests, Assignments, Final Examination |
| CLO4 | Interactive lecturing, Discussions | Class Tests, Assignments, Final Examination |
| CLO5 | Interactive lecturing, Discussions | Class Tests, Assignments, Final Examination |

**Distribution (Planning) of the Course Contents:**

**Module 1: Introduction to Cyber Security (Weeks 1-2)**

1. **Introduction to Information Security** – Importance, principles, and goals of cybersecurity.
2. **Fundamentals of Computer & Network Security** – Networking basics, firewalls, encryption.
3. **Common Cyber Threats & Attack Vectors** – Malware, phishing, DoS, insider threats.

**TUTORIAL** -**1**

**Module 2: Ethics & Cyber Laws (Weeks 3-4)**

1. **Cybersecurity Ethics –** Ethical Hacking: Hacking Techniques, Tools and Incident Handling Penetration Planning, Ethical Hacking and Network Defense.
2. **Attack Techniques and Testing:** Vulnerability Analysis, External and Internal Network Penetration Testing, Information System Incident Handling and Response.
3. **Cyber Laws & Regulations –** Privacy laws, GDPR, CCPA, Intellectual property.

**Module 3: Cyber Attack Techniques & Countermeasures (Weeks 5-6)**

1. **Network Attacks & Defense Mechanisms** – Intrusion detection, firewalls.
2. **Social Engineering & Insider Threats** – Phishing, pretexting, mitigation.
3. **Advanced Persistent Threats (APTs)** – Understanding nation-state attacks.

**TUTORIAL-2**

**Module 4: Digital Forensics & Investigations (Weeks 7-8)**

1. **Introduction to Digital Forensics** – Role, process, and legal considerations.
2. **Forensic Technologies & Digital Evidence** – Data recovery, logging, chain of custody.

**Module 6: Cyber Incident Handling & Response (Weeks 9-10)**

1. **Incident Detection & Analysis** – SIEM, logs, anomaly detection.
2. **Incident Response & Recovery** – Containment, eradication, forensic analysis.
3. **Post-Incident Security Measures** – Lessons learned, improving security posture.

**TUTORIAL 3**

**Module 4: Secure Software & Web Security (Weeks 10-11)**

1. **Secure Software Development** – Secure coding principles, vulnerabilities.
2. **Web Security & Browser Attacks** – HTML5 security, cookies, cross-site scripting.

**Module 5: Business Information Continuity & Risk Management (Weeks 12-13)**

1. **Business Continuity Planning (BCP)** – Disaster recovery, backup strategies.
2. **Risk Management Frameworks** – Risk identification, mitigation, response.
3. **Security Compliance & Policies** – ISO 27001, NIST, compliance measures.

**Recommended Textbook**

**Learning Materials**

1. Cybersecurity and Cyberwar: What Everyone Needs to Know by Allan Friedman and P. W. Singer.
2. Hacking Exposed: Network Security Secrets & Solutions by Joel Scambray.
3. Cybersecurity incident management masters guide: Volume 1 - Preparation, Threat Response, & Post-Incident Activity(2020) by Colby A Clark , Ireland J Clark.