Semester : III	Internal Marks:25		External Marks:75	
COURSE CODE	**COURSE TITLE**	**CATEGORY**	**HRS/WEEK**	**CREDITS**
22PGCS3CCC2A	**CYBER SECURITY**	**CORE CHOICE**	**3(T) + 2(P)**	**4**

Course Objective

- To develop skills in students that can help them plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
- To expose students to governance, regulatory, legal, economic, environmental, social, and ethical contexts of cyber security.
- To expose students to the responsible use of online social media networks.
- To systematically educate the necessity to understand the impact of cyber-crimes and threats with solutions in a global and societal context.
- To select suitable ethical principles, commit to professional responsibilities and human values, and contribute value and wealth for the benefit of society

Prerequisites

Basic Knowledge of Cyber Security

Course Outcome and Cognitive Level Mapping

CO Number	CO Statement	Cognitive Level
CO1	Understand the cyber security threat landscape	K1,K2
CO2	Develop a deeper understanding and familiarity with various types, cyber crimes, vulnerabilities, and remedies thereto.	K2, K3
CO3	Analyse and evaluate existing legal frameworks and laws on cyber security.	K4, k5
CO4	Analyse and evaluate the digital payment system security and remedial measures.	K4, K5
CO5	Analyse and evaluate the cyber security risks, plan suitable security controls	K4, k5

Mapping of CO with PO and PSO

COs	PSO 1	PSO 2	PSO 3	PSO 4	PSO 5	P0 1	PO 2	PO 3	PO 4	PO 5
CO1	3	3	3	3	3	3	3	3	3	3
CO2	3	3	3	3	3	3	3	3	3	3
CO3	3	3	3	3	2	3	3	3	3	2
CO4	3	3	3	3	2	3	3	3	3	2
CO5	3	3	3	3	2	3	3	3	3	2

“1” – Slight (Low) Correlation “2” – Moderate (Medium) Correlation
“3” – Substantial (High) Correlation “-” indicates there is no correlation

SyllabusTheory:

UNIT	CONTENT	HOURS	COs	COGNITIVE LEVEL
I	Overview of Cyber Security: Cyber security increasing threat landscape, -Cyberspace, attack, attack vector, attack surface, threat, risk, vulnerability, exploit, exploitation, hacker., Non-state actors, Cyber terrorism, Protection of end user machine, Critical IT and National Critical Infrastructure, Cyber warfare, Case Studies.	9	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
II	Cyber Crimes: Cyber Crimes targeting Computer systems and Mobiles- data diddling attacks, spyware, logic bombs, DoS, DDoS, APTs, virus, Trojans, ransomware, data breach., Online scams and frauds- email scams, Phishing, Vishing, Smishing, Online job fraud, Online sextortion, Debit/credit card fraud, Online payment fraud, Cyberbullying, website defacement, Cyber-squatting, Pharming, Cyber espionage, Cryptojacking, Darknet-illegal trades, drug trafficking, human trafficking., Social Media Scams & Frauds- impersonation, identity theft, job scams, misinformation, fake news cyber crime against persons –cyber grooming, child pornography, cyber stalking., Social Engineering attacks, Cyber Police stations, Crime reporting procedure, Case studies.	9	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
III	Cyber Law: Cyber Crime and legal landscape around the world, IT Act, 2000 and its amendments. Limitations of IT Act, 2000. Cyber Crime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies-AI/ML, IoT, Blockchain, Darknet and Social media, Cyber Laws of other countries, Case Studies.	9	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
IV	Data Privacy and Data Security: Defining data, meta-data, big data, non-personal data. Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries- General Data Protection Regulations(GDPR),2016 Personal Information Protection and Electronic Documents Act (PIPEDA). Social media-data privacy and security issues.	9	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
V	Cyber security Management, Compliance and Governance: Cyber security Plan-cyber security policy, cyber crises management plan., Business continuity, Risk assessment, Types of security controls and their goals, Cyber security audit and compliance, National cyber security policy and strategy.	9	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5

VI	**Self Study for Enrichment** **(Not included for End Semester Examinations)** **Case Studies**: Largest Cyber Attacks : Yahoo Data Breach, Equifax Data Breach, WannaCry Malware Attack, Simple Locker.	-	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5

Reference Books

1. Vivek Sood, (2017). *Cyber Law Simplified*. McGraw Hill Education
2. Sumit Belapure and Nina Godbole, (2011). *Computer Forensics and Legal Perspectives*. Wiley India Pvt. Ltd.
3. Dorothy F. Denning, (1998). *Information Warfare and Security*. Addison Wesley.
4. Henry A. Oliver, (2015). *Security in the Digital Age: Social Media Security Threats and Vulnerabilities*.Create Space Independent Publishing Platform.
5. Natraj Venkataramanan and Ashwin Shriram, (2016). *Data Privacy Principles and Practice*. 1st Edition, CRC Press.
6. W.Krag Brothy, (2008). *Information Security Governance, Guidance for Information Security Managers*. 1st Edition, Wiley Publication.
7. Martin Weiss, Michael G.Solomon, (2015). *Auditing IT Infrastructures for Compliance*. 2nd Edition, Jones & Bartlett Learning.

Web References

1. https://www.tutorialspoint.com/principles-of-information-system-security
2. https://www.geeksforgeeks.org/principle-or-information-system-secutiry/
3. https://www.techtarget.com/searchsecurity/definition/cybersecurity
4. https://www.ukessays.com/essays/computer-science/analysis-of-the-yahoo-data-breaches.php
5. https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
6. https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware
7. https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/

Practicals:

List of Exercises: (Not included for End Semester Examinations)

1. Platforms for reporting cyber crimes.
2. Checklist for reporting cyber crimes online
3. Setting privacy settings on social media platforms.
4. Do’s and Don’ts for posting content on Social media platforms.
5. Registering complaints on a Social media platform.
6. Prepare password policy for computer and mobile device.
7. List out security controls for computer and implement technical security controls in the personal computer.
8. List out security controls for mobile phone and implement technical security controls in the personal mobile phone.
9. Log into computer system as an administrator and check the security policies in the system.

Web References

1. https://cybercrime.gov.in/
2. https://cybercrime.gov.in/webform/crime_onlinesafetytips.aspx
3. https://www.digitalvidya.com/blog/social-media-dos-and-donts/
4. https://www.medianama.com/2023/02/223-platform-grievance-appellate-committees-social-media/
5. https://www.ibm.com/topics/security-controls
6. https://docs.oracle.com/cd/E19683-01/817-0365/concept-2/index.html

Pedagogy

Chalk and Talk, Group discussion, Seminar & Assignment.

Course Designer

From UGC SYLLABUS