CYBERSECURITY (CY)

CY 2020 Cybersecurity Fundamentals (4)
Provides foundation for understanding key issues of protecting digital information, identifying threats, and determining protection levels, response to security incidents, examination of pre- and post-incident procedures, and designing consistent, reasonable cyber security system, with appropriate intrusion detection and reporting features. Includes technical and managerial responses and an overview of cyber security governance, policy, ethics, and planning. Springs.

CY 3010 Ethical Hacking & Pentesting (4)
Introduces ethical hacking and penetration testing on securing modern information systems. Students will explore reconnaissance techniques, system hacking phases, network and web vulnerabilities, wireless and mobile hacking, and cryptographic attacks. Hands-on labs emphasize practical skills in applying penetration testing techniques and analyzing vulnerabilities, with a focus on ethical and legal considerations. Springs.
Prerequisite(s): CY 2020 , CS 3240

CY 3020 Network Security (4)
Provides thorough exploration of network security, covering both theoretical foundations and practical applications. Students will examine the design and analysis of network security protocols in different layers and their role in real-world systems, including but not limited to HTTPS, DNSSEC, IPSec, and wireless communication protocols. Hands-on labs will include network and host-based intrusion detection and prevention, evasion techniques, and attacks. Falls.
Prerequisite(s): CY 2020 , CS 3240

CY 3030 Digital Forensics & Incident Response (4)
Provides a comprehensive introduction to Digital Forensics and Incident Response. Focusses on integration of forensic concepts with real-world incident handling. Explore topics such as disk, memory and network forensics, file carving, and Security Information and Event Management (SIEM). Through hands-on labs, students will learn to acquire, analyze, and interpret digital evidence, apply policy frameworks, and utilize industry-standard tools. Falls.
Prerequisite(s): CY 2020, CS 3240

CY 3040 Cloud Security and Privacy (4)
A practical introduction to cloud security and privacy, focusing on protecting cloud environments through effective technical and administrative measures. Key concepts include cloud architectures, service models (SaaS/PaaS/IaaS) and deployment types (public/private/hybrid). Identifying and responding to cloud threats and applying legal, governance, risk, and compliance strategies. Emphasizes hands-on activities in identity management, security monitoring, and safeguarding infrastructure, data and applications. Springs.
Prerequisite(s): CY 2020

CY 3100 Red Team/Blue Team Capstone (4)
Provides a team-based environment where students explore and implement offensive (Red Team) and defensive (Blue Team) cybersecurity strategies to simulate real-world scenarios. Through hands-on labs, simulations, and collaborative exercises, students will develop expertise in pentesting, incident response, threat analysis, and securing networks. Post-event debriefs will provide opportunities to analyze actions, identify successes, and pinpoint areas for improvement.
Prerequisite(s): CY 3010, CY 3020 and CY 3030