CYBERSECURITY (CYS)

CYS 1101 Practices in Security Management (3 Credits)
This course offers in depth coverage of the current risks and threats to an organization's data as well as the strategies for safeguarding critical electronic assets. The course provides a foundation for those responsible for protecting network services, devices, traffic, and data. Additionally, Fundamentals of Network Security prepares students for further study in more specialized security fields. The course provides a foundation for those preparing for the Computing Technology Industry Association's (CompTIA) Security+ Certification exam.
Previous: Legacy Equivalent(s): CST*248, CST*273

CYS 2111 Network Security (3 Credits)
Broad introduction to the field of cybersecurity. Information assurance terminology and issues in context of the rules and guidelines that control them. Methodologies and technologies for assurance. Security policies and laws related to cyber defense.
Prerequisites: CST 1221 or instructor permission The former course, CST 1121 Networking I -3 credits , also fulfills this pre-requisite.
Previous: Legacy Equivalent(s): CST* 246, CST* 269, CST* 270, CST* 274, CST* 275, CST* 277, CST* 280

CYS 2121 Information Assurance and Risk Management (3 Credits)
This course is designed to introduce students to information assurance and risk mitigation principles as applied to information management. Topics covered in the course include asset identification, vulnerabilities assessment, risk management, threat identification, and physical safeguards of mission critical data. Students will also learn how to conduct a security gap analysis, create a risk management plan, and select an appropriate risk control.
Prerequisites: CYS 2111
Previous: Legacy Equivalent(s): CST*247, CJS*234

CYS 2131 Computer Forensics and Network Intrusions (3 Credits)
This course exposes students to a broad range of forensic methods and techniques used to detect, trace, and stop network intrusions and perform network forensic investigations after an intrusion has occurred. Students will learn how to identify network intrusion paths and points of entry and how to bag-and-tag digital evidence, examine evidence, and document a chain of custody throughout a forensic investigation.
Prerequisites: CYS 2111
Previous: Legacy Equivalent(s): CJS* 235, CST* 156

CYS 2141 Cyber Crimes (3 Credits)
This course provides an overview of the different types of computer crimes including hacking, fraud, social engineering, ransomware; their impact on the laws and regulations at the state, federal, and international level, and the guidance provided by the National Institute of Standards and Technology (NIST) to protect against cybercrime. Topics include types of cybercrimes, cybercrime laws and regulations, protection against cybercrime, impact of cybercrime in the economy.
Prerequisites: CYS 2111
Previous: Legacy Equivalent(s): CST*135, CJS*224

CYS 2151 Ethical Hacking and Pen Testing I (3 Credits)
Introduces students to ethical hacking and penetration testing using the latest open source software, techniques, and methodologies used by hackers and security professionals to lawfully hack an organization. Ethical hackers are employed by corporations for the purpose of testing their networks for weaknesses. Topics include stages of ethical hacking, foot printing and reconnaissance, scanning networks, enumeration, and vulnerability analysis. Emphasis will be given to the legal and ethical issues related to hacking. This course is the first of two Ethical Hacking courses, and covers the first part of the CEH exam content requirements.
Prerequisites: CYS 2111
Previous: Legacy Equivalent(s): CST*267, CST*284, CST*285

CYS 2152 Ethical Hacking and Pen Testing II (3 Credits)
This course covers advanced ethical hacking and penetration testing techniques using the latest software, techniques, and methodologies used by hackers and security professionals to lawfully hack an organization. Topics include session hijacking, hacking of web applications and servers, as well as social engineering and denial of services hacking techniques. This course is the second of two Ethical Hacking courses and covers the second part of the CEH exam content requirements.
Prerequisites: CYS 2151
Previous: Legacy Equivalent(s): CST* 288

CYS 2161 Cryptography Fundamentals (3 Credits)
This course will cover where and how cryptography is used, Topics will include the role of keys, cryptographic algorithms, and protocols as they relate to security (attacks and defenses) in complex real-life systems.
Prerequisites: CYS 2111
Previous: Legacy Equivalent(s): CST* 287

CYS 2171 Cybersecurity Operations (3 Credits)
Students will learn the foundational knowledge and skills required for a career in cybersecurity operations, including managing a Security Operation Center (SOC). The course introduces students to cybersecurity technologies, including network intrusion detection, network traffic monitoring, packet analysis, and Computer Security Incident Response Team (CSIRT).
Prerequisites: CYS 2111