CYBERSECURITY (CYS)

CYS 100 (1 credit hours)
Cybersecurity Orientation
Provides an orientation to the field of cybersecurity and outlines expectations of the Cybersecurity AAS degree. Lecture: 1 credit (15 contact hours).
Attributes: Technical
Components: LEC: Lecture

CYS 101 (3 credit hours)
Cybersecurity Foundations
Provides students with an overview of the cybersecurity field and its related concepts. Includes an introduction to cybersecurity terminology, best practices and ethics, principles and standards, and planning and managing cybersecurity functions and assets. Presents a foundation for understanding common threats and attacks and the methods and tools to defend and protect against the same. Includes an overview of human, organizational, social and legal issues related to cybersecurity. Presents concepts which meet national standards in cybersecurity. Lecture: 3 credits (45 contact hours).
Attributes: Technical
Components: LEC: Lecture

CYS 130 (3 credit hours)
Introduction to Cyber Forensics
Provides an overview of cybersecurity forensics. Includes an overview of data acquisition, processing crime and incident scenes, working with different platforms (Windows, Linux, Mac OS X, mobile, cloud), current forensics tools, report writing and ethical considerations in the digital forensics arena. Lecture: 3 credits (45 contact hours).
Pre- or co-requisite: CYS 101 or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 140 (3 credit hours)
Data Security
Provides a foundation for designing, creating, maintaining and secure databases. Emphasizes security for all topics presented. Introduces various database models and common security concerns including SQL injections. Presents database security models and concerns including inference, injections, hashing and encryption, data corruption, and access controls (DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC, (Role Based Access Control) and Clark). Requires students to design and deploy a simple secure database for a specified application. Lecture: 3 credits (45 contact hours).
Pre-requisite: College Readiness in Math or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 145 (3 credit hours)
Foundations of Cyber Systems
Provides students with an understanding of the components in an information technology system and their roles in system operations. Includes a theoretical understanding of the roles of an operating system, its basic functions, services, and security issues. Presents concepts related to common computer hardware and basic networking. Lecture: 3 credits (45 contact hours).
Pre-requisite: MAT 150 OR Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 150 (3 credit hours)
Secure Software Development I
Introduces secure software development using an easy-to-learn programming language appropriate for a first semester of secure coding. Covers secure coding principles and practices while focusing on developing software that is free from security vulnerabilities. Presents foundational programming concepts (data types; sequence, selection, and repetition control structures; single and two-dimensional arrays; and classes and objects) from a security perspective. Compares the strengths, weaknesses, and optimal applications for several scripting and programming languages, but focuses on writing secure code in a selected language, such as Python. Presents concepts which meet national standards in secure software development. Lecture: 3 credits (45 contact hours).
Pre-requisite: MAT 150 or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 202 (3 credit hours)
Human, Organizational, and Societal Security
Provides students with an overview of human, organizational, and societal security. Covers trends in human behavior and resulting risks to individuals, organizations, and society. Covers techniques to encourage personal compliance with cybersecurity rules, policies, and norms. Provides an overview of personal, local, national, and international cybersecurity policies and legislation. Introduces cybersecurity ethics, theories, and related impact on individuals and society. Lecture: 3 credits (45 contact hours).
Pre-requisite: ENG 101 or consent of instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 231 (3 credit hours)
Internet of Things Security and Forensics
Presents an overview of the Internet of Things (IoT) ecosystem and how to secure IoT devices and the data they contain. Covers IoT standards, guidelines and tools, including NIST (National Institute of Standards and Technology) standards and recommendations. Provides an overview of common IoT devices, applications and related security. Lecture: 3 credits (45 contact hours).
Pre-requisite: CYS 145 or consent of instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 234 (3 credit hours)
Computer Operating Systems Forensics
Provides an overview of digital forensics for computer operating systems (Linux, Windows, and macOS systems). Includes an in-depth study of registry/preference/configuration files, file systems, memory forensics, data and file recovery, web browsing, tracking artifacts, log files, executable programs, email and other related topics. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 130 and CYS 145) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 245 (3 credit hours)
Advanced Cyber Systems
Provides an advanced exploration of cyber systems including threats, attacks and vulnerabilities on an organization's information assets (hardware, software, data, and networks) and defense tools and techniques against threats, attacks, and vulnerabilities. Covers network protocols, logical and physical security measures, encryption and decryption techniques, disaster recovery, and incident response. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 145 and MAT 150) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 247 (3 credit hours)
Linux Security
Focuses on security aspects related to installation and administration and implementation of the Linux operating system. Lecture: 3 credits (45 contact hours).
Pre-requisite: CYS 245 or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 248 (3 credit hours)
Network Security and Authentication
Explores various communication protocols with a concentration on TCP/IP. Explores communication protocols from the point of view of the hacker to highlight protocol weaknesses. Encompasses internet architecture, routing, addressing, topology, fragmentation and protocol analysis and the use of various utilities to explore TCP/IP (Transmission Control Protocol/Internet Protocol). Lecture: 3 credits (45 contact hours).
Pre-requisite: CYS 245 or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 249 (3 credit hours)
Ethical Hacking
Covers an in-depth exploration of methods for attacking and defending various types of networks. Explores network security concepts from a hacker's viewpoint including attack methodologies. Lecture: 3 credits (45 contact hours).
Pre-requisite: CYS 245 or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 250 (3 credit hours)
Secure Software Development II
Provides a comprehensive study of secure software development using an object-oriented language appropriate for a second semester of programming (in a language different from CYS 150 to allow for a broader study of security across programming languages). Includes a syntax and security review of data types, control structures, and arrays for the language used in the course. Covers classes, objects, inheritance, polymorphism, sorting and searching algorithms, streams and files, exception handling, recursion, efficiency of algorithms, and standard libraries. Compares the strengths, weaknesses and optimal uses of several object-oriented programming languages but focuses on a single language such as Java or C/C++/C#. Covers syntax and logic concepts through a security perspective. Presents concepts which meet national standards in secure software development. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 150 and MAT 150) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 251 (3 credit hours)
Secure Software Development Bridge
Provides an introduction to secure software development for students who have transfer courses for the first and second semester of software development (another college/university or KCTCS CIT courses). Presents an in-depth study of secure coding principles and practices typically covered in the first and second semester of secure software development courses. Presents concepts which meet national standards in secure software development. Lecture: 3 credits (45 contact hours).
Pre-requisite: ((CIT 149 and CIT 249) or (CS 115 and CS 215) or (INF 120 and INF 260) or (CIT 142 and CIT 242) or (CIT 143 and CIT 243)) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 255 (3 credit hours)
Secure Software Development III
Provides an overview of data structures and related security issues. Presents an in-depth study of arrays, lists, linked lists, stacks, queues, trees, hash tables, heaps, and graphs. Provides on overview of several object-oriented languages and how they support and implement data structures. Presents concepts which meet national standards in secure software development. Lecture: 3 credits (45 contact hours).
Pre-requisite: (MAT 150 and (CYS 250 or CYS 251)) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 258 (3 credit hours)
Survey of Programming Languages
Provides an overview of modern programming languages (scripting, query, and object-oriented) and highlights the strengths, weaknesses, and security implications of each. Presents scenarios and applications for each language (when to use and when not to use). Covers techniques for overcoming security vulnerabilities of the languages. Lecture: 3 credits (45 contact hours).
Pre-requisite: CYS 101.
Attributes: Technical
Components: LEC: Lecture

CYS 265 (3 credit hours)
Network and Cloud Forensics
Provides an overview of network and cloud forensics. Includes a review of the investigation methodology in the context of network and cloud evidence. Includes an in-depth study of network and cloud forensics including deep packet inspection, statistical flow analysis, tunneling and encryption, malware, network intrusions and footprints, and various tools to assist with network and cloud forensics. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 130 and CYS 245) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 266 (3 credit hours)
Mobile Device Forensics
Provides an overview of cyber forensics for mobile devices including but not limited to smartphones, tablets, IoT (Internet of Things) devices, and embedded systems (i.e. GPS (global positioning system), game consoles, smart TVs, drones, medical equipment, automotive equipment). Investigates common mobile operating systems (i.e. iOS, Android, Windows, and others). Includes a review of the investigation methodology in the context of mobile devices and evidence. Provides hands-on experience with open source and commercial (when possible) mobile device forensic tools. Covers how to create simple SQLite queries and/or scripts for mobile file interrogations. Covers how to write forensic reports that that meet judicial and defense scrutiny. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 130 and CYS 245) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 270 (3 credit hours)
Secure Web Applications
Provides an introduction to secure web application development. Includes an overview of PHP (Hypertext Preprocessor), SQL (Structure Query Language), HTML (Hypertext Markup Language), and JavaScript and how each is used in developing secure web applications. Covers common security vulnerabilities found in web applications and how to mitigate them. Lecture: 3 credits (45 contact hours).
Pre-requisite: (CYS 140 and CYS 150) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 285 (3 credit hours)
Cryptography
Provides students with an overview of cryptography and its role in cybersecurity. Introduces a variety of encryption algorithms and cryptographic protocols, tools, techniques, and standards. Includes a review of basic mathematical concepts which students will use to construct and break classical and modern ciphers. Lecture: 3 credits (45 contact hours).
Pre-requisite: (MAT 150 and CYS 101) or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture

CYS 299 (3 credit hours)
Cybersecurity Capstone
Prepares students for experiences and challenges that may be met while applying, interviewing, and working in a cybersecurity workplace. Includes three primary objectives of teamwork, experience, and employability. Includes an assessment of core cybersecurity curriculum competencies. Lecture: 3 credits (45 contact hours).
Pre-requisite: Completion of 18 hours of CYS core or Consent of Instructor.
Attributes: Technical
Components: LEC: Lecture