CYBERSECURITY AND INFORMATION TECHNOLOGY (CIT)

CIT 310. Enterprise System Administration
Credits: 3
Prerequisite: CIS 216.
Typically Offered: ONDEMAND
This class focuses on performing systems administration in an enterprise environment. Server and client security policy, imaging, remote administration, terminal services, and fault tolerance are among the topics covered.

CIT 314. Implementing a Microsoft Windows Active Directory Infrastructure
Credits: 3
Prerequisite: CIT 216 or instructor approval
Typically Offered: FALL
This course provides students with the knowledge and skills necessary to install, configure, and administer Microsoft Windows Active Directory services. The course also focuses on implementing Group Policy and performing the Group Policy related tasks that are required to centrally manage users and computers. Active Directory tools, techniques, and security will be analyzed. Students will also learn modern Active Directory administration using cloud and data center based tools.

CIT 315. Human Factors in Cybersecurity
Credits: 3
Typically Offered: FALL
This course explores the psychological, social, and organizational factors that influence security practices and vulnerabilities in various settings. Students will examine topics such as user behavior, risk perception, and decision-making processes in the context of cybersecurity threats.

CIT 320. Disaster Recovery & Incident Response
Credits: 3
Typically Offered: SPRING
This course provides students with the knowledge and skills necessary to develop and implement robust disaster recovery plans and incident response strategies. Topics include Risk Assessment, Business Impact Analysis, Continuity Planning, and other pertinent issues in the DR and IR fields.

CIT 326. Linux Network and Security Administration
Credits: 3
Prerequisite: CIS 223 or instructor approval.
Typically Offered: FALL
This course provides experience installing, configuring, securing, and administering Linux network services. Topics include name servers, web servers, reverse proxies, network file sharing, secure administration, application of encryption, and other common network security technologies.

CIT 330. Data Center Virtualization Fundamentals
Credits: 3
Typically Offered: SPRING
In this course, students use hands-on technologies to learn about the implementation, support, and maintenance of a virtualized data center infrastructure. Topics include machine virtualization, virtual machine storage and storage area network technologies, as well as virtual networking.

CIT 331. Digital Forensics Fundamentals
Credits: 3
Typically Offered: SPRING
This course introduces students to digital forensics. Topics covered include the investigative process, preservation of evidence, examination of Windows and other systems, mobile and cloud forensics issues, as well as providing experience using digital forensics software. Students will gain an understanding of the underlying technologies examined in todays investigations, as well as using tools to examine them.

CIT 340. IT Policies and Procedures
Credits: 3
Typically Offered: FALL
This course introduces the writing of information security policies and procedures. Their contents and organization will be examined in detail. Students will learn to write effective documents for the governance of IT and cybersecurity operations.

CIT 341. Mobile Forensics Fundamentals
Credits: 3
Prerequisite: CIT 331 or instructor approval.
Typically Offered: FALL
This course introduces students to the application of digital forensics methods for mobile devices, as well as additional tools and techniques specific to forensics of mobile devices.

CIT 342. Memory Forensics Fundamentals
Credits: 3
Prerequisite: CIT 331 or instructor approval.
Typically Offered: FALL
This course introduces students to the application of digital forensics methods to retrieving memory artifacts from devices, as well as additional tools and techniques specific to forensics of device memory.

CIT 345. Cybersecurity Governance
Credits: 3
Typically Offered: SPRING
This course explores the frameworks used to provide oversight and accountability for information technology and cybersecurity programs.

CIT 350. Software Security
Credits: 3
Prerequisite: CSCI 174 or instructor approval.
Typically Offered: FALL
This course examines how hackers exploit poorly designed code for their benefit. It also shows students how to secure their code from these attacks.

CIT 355. Software Reverse Engineering
Credits: 3
Prerequisite: CSCI 250 or instructor approval.
Typically Offered: FALL
This course examines executable software code to understand how it works and what it does.

CIT 364. Network Defenses
Credits: 3
Prerequisite: CIS 267 or instructor approval.
Typically Offered: FALL
In this course, students learn to design and configure a secure network environment using Virtual Private Networks, Intrusion Detection Systems, firewalls, and other network security technologies.

CIT 367. Cybersecurity Infrastructure Configuration
Credits: 3
Prerequisite: CIS 165 or instructor approval.
Typically Offered: ONDEMAND
This course provides students an understanding of how to install, configure, and manage firewalls for defense of enterprise network architectures. Students will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies. In addition to gaining practical Next Generation Firewall experience, this course helps to prepare students for the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification exam.

CIT 368. Cybersecurity Prevention & Countermeasures
Credits: 3
Prerequisite: CIT 367 or Instructor approval.
Typically Offered: ONDEMAND
This course provides students with advanced information in installing, configuring, and managing firewalls for defense of enterprise network architecture. Students will learn the theory and extended configuration features necessary to set up traffic handling, advanced content/user identification, quality of service, global protect, monitoring/reporting and high availability of next generation firewall technologies. In addition to gaining practical next generation firewall experience, this course helps to prepare students for the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification exam.

CIT 380. Network Forensics
Credits: 3
Prerequisite: CIS 274 or instructor approval.
Typically Offered: SPRING
This course introduces the tools and techniques used to investigate and locate evidence of network attacks.

CIT 381. IT Project Management
Credits: 3
Typically Offered: SPRING
An investigation of the project management techniques and appropriate software used to effectively manage projects. This course covers the knowledge areas and other topics as defined by the Project Management Body of Knowledge (PMBOK).

CIT 410. Wireless Networking and Mobile Security
Credits: 3
Prerequisite: CIS 165 or instructor approval.
Typically Offered: ONDEMAND
This course examines the role wireless communication plays in business communications. It also explores enterprise management of wireless and mobile devices.

CIT 415. Insider Threat Analysis
Credits: 3
This course explores various types of insider threats, malicious actors, negligent insiders, and collusion while delving into psychological and sociological factors that contribute to these behaviors. The course will cover methodologies for threat detection, risk assessment, and the implementation of preventive measures, including employee training, monitoring systems, and incident response protocols.

CIT 430. Cloud Computing Fundamentals
Credits: 3
Typically Offered: FALL
This course introduces the use and administration of cloud computing platforms, as well as their security. Students gain experience using common cloud providers, such as Amazon Web Services and Azure.

CIT 440. Cybersecurity Program Fundamentals
Credits: 3
Typically Offered: SPRING
This course examines the topics used to successfully build an organizations cybersecurity program. Students will learn about a wide range of security concepts, tools, and techniques. This course provides foundational knowledge required for the Certified Information Systems Security Professional (CISSP) certification.

CIT 445. Information Assurance and Risk Management
Credits: 3
Typically Offered: SPRING
This course provides a comprehensive examination of the principles, practices, and technologies essential for safeguarding information assets and managing associated risks.

CIT 450. Database and Web Application Security
Credits: 3
Prerequisites: CIS 204 and one of CSCI 160, CIS 253, CIS 264 or instructor approval.
Typically Offered: FALL
This course explores the vulnerabilities found in database servers and web applications. It also provides techniques for securing them.

CIT 455. Malware Analysis
Credits: 3
Prerequisite: CIT 355 or instructor approval.
Typically Offered: SPRING
This course examines the behavior of malicious software, providing insight into how it is written and how to protect against it.

CIT 460. Operating System Concepts
Credits: 3
Typically Offered: ONDEMAND
This course provides an overview of various operating system concepts. Topics covered include processes, interrupts, interprocess communication, virtual memory management, CPU scheduling and deadlocks.

CIT 469. Cybersecurity & Information Technology Capstone
Credits: 3
Typically Offered: ONDEMAND
A capstone course for the Cybersecurity and Information Technology BAS program. In this class students will complete a security based final project that reflects upon what they've learned in the program. Students will be asked to present their final project upon completion to the class. The final projects will be examined by their fellow classmates who will try to determine if the project is secure or not.

CIT 470. Penetration Testing Fundamentals
Credits: 3
Prerequisite: CIS 282 or instructor approval.
Typically Offered: SPRING
This course provides theoretical and practical aspects of network and web application penetration testing. The course uses a hands-on approach to the different phases of penetration testing. Students will learn tools and methodologies typically used to exploit vulnerabilities.

CIT 475. Emerging Threats and Defenses
Credits: 3
Prerequisites: CIS 282 and CIT 450 or instructor approval.
Typically Offered: SPRING
In this course, students learn to implement a variety of tools, strategies, and techniques to defend and administer an IT infrastructure. Role based scenarios and challenges will be presented, allowing students to practice and apply their cybersecurity defense skills. Trending topics in cybersecurity will also be examined.

CIT 480. Cyber Threat Hunting
Credits: 3
Prerequisite: CIT 380 or instructor approval.
Typically Offered: FALL
This course introduces the terminology, tools, and techniques to search for evidence of threat actor activities in networked devices.

CIT 485. Social Engineering Fundamentals
Credits: 3
Typically Offered: SPRING
This course examines various forms of social engineering, including phishing, pretexting, baiting, and tailgating, with an emphasis on understanding the motivations and behaviors of both attackers and victims.