ITMO 444 SYLLABUS

ITMO 444 Cloud Computing Technologies

Hours: 3 credit hours / 45 contact hours

Instructor: Jeremy Hajek

Textbook, title, author, and year: *The Practice of Cloud System Administration: Designing and Operating Large Distributed Systems, Volume 2,* Thomas A. Limoncelli, Strata R. Chalup and Christina J. Hogan, 2014

Specific course information

a. **Catalog description:** Computing applications hosted on dynamically-scaled virtual resources available as services are considered. Collaborative and non-collaborative "cloud-resident" applications are analyzed with respect to cost, device/location independence, scalability, reliability, security, and sustainability. Commercial and local cloud architectures are examined. A group-based integration of course topics will result in a project employing various cloud computing technologies.
b. **Prerequisite:** ITMD 321

Specific goals for the course

a. **Course Outcomes:** Each successful student will be able to demonstrate building and running cloud-based services on a large scale. They will gain the knowledge of deploying and managing elastic and cloud-based applications on industry standard platforms as well as open-source platforms. Students will be prepared with knowledge of Cloud Based Operations and Application Development.
b. **Course student outcomes:**
    - Explain, document, and implement the fundamental aspects of IaaS, PaaS, SaaS
    - Use and administer industry standard cloud resources
    - Correctly identify cloud native operations and development methodologies
    - Build and deploy elastic scaling applications on a cloud platform
    - Design applications using a cloud native architecture
    - Describe and employ web technologies for software deployment

Topics to be covered

a. Thinking Cloud
b. Designing in a Distributed World
c. Designing for Operations/ Service Platforms
d. AWS Introduction
e. History of Cloud Computing
f. Application Architectures
g. Design Patterns for Scaling
h. Design Patterns for Resiliency
i. Operations in a Distributed World
j. Cloud Concepts w/AWS
k. Design Documents & Monitoring

ITMO 446 SYLLABUS

ITMO 446 Telecommunications over Data Networks

Hours: 3 credit hours / 45 contact hours

Instructor: Carol Davids

Textbook, title, author, and year: *SIP: Understanding the Session Initiation Protocol 3rd Edition,* Alan B. Johnston, 2009

Specific course information

a. **Catalog description:** This course covers a suite of application protocols known as Voice over IP (VoIP). It covers key protocols within that suite, including Session Initiation Protocol (SIP), Real-time Transport Protocol (RTP) and Session Description Protocol (SDP) as well as the architectures of various VoIP installations including on-net to on-net; on-net to PSTN; and inter-domain scenarios. The functions of the Network Elements in these architectures are defined and examples of products that include these network elements are examined. Contrast with circuit-switched and web-based communications systems is provided.
b. **Prerequisites:** ITMO 340.

Specific goals for the course

a. **Course Outcome:** The goal of the course is to provide an understanding of how audio and video communications in real-time can be provided over Internet Protocol networks using protocols, including Session Initiation Protocol (SIP), Real-time Transport Protocol (RTP) and Session Description Protocol (SDP) defined by the Internet Engineering Task Force (IETF.) A further goal of this work is to provide an evolutionary perspective on the SIP-based approach contrasting circuit-switched communications and web-based approaches. This organization of the material is designed to foster innovative thinking and development in the field of real-time communications, based on hands-on work and an understanding of past innovation and development. The successful student will have the necessary knowledge and skills to work in the field of IP-based telecommunications at an entry level.
b. **Course Student Outcomes:**
Upon successful completion of the course the student should be able to:
   - Use protocol analysis tools to analyze the message flows between SIP functional elements.
   - Draw message sequence charts to aid in message flow analysis.
   - Identify the header fields and parameters that may change as the messages traverse the network.
   - Use this message flow analysis to verify correct behavior and to isolate trouble.
   - Identify the media streams and signaling messages associated with a SIP call.
   - Analyze contents of media streams and signaling messages associated with a SIP call.
   - Perform tasks and demonstrate skills necessary to work in the field of IP-based telecommunications at an entry level.

Topics to be covered

a. Protocol (SDP) and Real-time Transport Protocol (RTP)
b. SIP functional elements and architecture
c. SIP message syntax and call flows
d. SIP relationships – transactions, dialogs and sessions
e. Voice payload digitization
f. Codecs
g. Real-time Transport Protocol - RTP and RTCP
h. Session Description protocol (SDP)
i. SIP Methods
j. SIP Feature Creation
k. SIP Architectures
l. Project presentations and demonstrations

ITMO 453 SYLLABUS

ITMO 453 OSS System Administration

Hours: 3 credit hours / 45 contact hours

Instructor: Jeremy Hajek

Textbook, title, author, and year:
The Art of Monitoring, James Turnbull, 2016
Monitoring with Prometheus, James Turnbull, 2018

Specific course information

a. **Catalog description:** Students learn the administration topics and concepts of IT Orchestration, Automation, Monitoring, and Metric Collection. Topics include configuring industry standard automation tooling and using scripting to achieve immutable infrastructure. Students will learn how to monitor and collect and present metrics in regards to the infrastructure they deploy.
b. **Prerequisites: ITMO 340 and ITMO 356**

Specific goals for the course

a. **Course Outcomes:** This course will enable students to be ready to design, build, and implement logging and metrics in monitored applications. Implementing these foundations will allow any system administrator to integrate logging and metric collection to correlate with business objectives.
b. **Course student outcomes:**
At the conclusion of this course, each student should be able to:
   - Explain the difference between push and pull metrics
   - Explain the difference between logging and metrics
   - Describe event streams are and how they are used in monitoring and metric collection
   - Explain the use of logging and metrics in regards to Operating System containers
   - Design, build, and implement logging and metrics in monitored applications

Topics to be covered

a. Intro - Monitoring & Measurement Framework
b. Managing events and Metrics & Graphing
c. Event Routing and Collection
d. Containers and Logs
e. Building an app & Notifications
f. Getting Started & Monitoring Nodes
g. Service Discovery
h. Alerting & Scaling and Reliability
i. Instrumenting Applications & Logging
j. Building Monitored Applications & Notifications

ITMO 454 SYLLABUS

ITMO 454 Operating System Virtualization

Hours: 3 credit hours / 45 contact hours

Instructor: Philip Matuszak

Textbook, title, author, and year: *Virtualization Essentials, Second Edition,* Matthew Portnoy, 2016

Specific course information

a. **Catalog description:** Each successful student in this course will be become familiar with hypervisors, virtualization terms, infrastructure considerations, and appropriate use cases. While designed to give an overview of today's Virtualization technologies and methods, students in the course will gain enough practical knowledge to begin deploying various hypervisors and virtual machine environments using current industry standard platforms.
b. **Prerequisites:** None.

Specific goals for the course

a. **Course Outcomes:** This course exposes students to virtualization in an enterprise setting as a tool for the deployment, configuration, and management of server and desktop resources. Students will experience a variety of virtualization environment and products. Students will work with technical implementations of virtualization and learn to design and manage physical to virtual migration.
b. **Course Student Outcomes:**
Students completing this course will be able to:
- Describe and discuss current trends in Operating System Virtualization by experiencing a variety of applications and software packages.
- Explain what a hypervisor is, what it does, and the various types involved and when each is used.
- Demonstrate technical knowledge and limited proficiency in designing and deploying virtualized environments
- Identify and describe various Virtualization platforms and software such as VMware, XenServer, Hyper-V, Virtual box, and VMware workstation, and open source hypervisors.
- Create a proposal and design for migrating an existing physical environment to a virtual environment.

Topics to be covered

a. Introduction to Virtualization & Hypervisors
b. Type 2 Hypervisors and VMs
c. Hardware, Infrastructure, & Type 1 HV
d. VM Creation and Management
e. CPU, Memory, and Consumables
f. Storage
g. Networking
h. Management
i. Availability
j. Virtual Applications
k. VDI
l. Security
m. Backup and Recovery
n. Open Source / Apple Virtualization

ITMS 418 SYLLABUS

ITMS 418 Coding Security

Hours: 3 credit hours / 45 contact hours

Instructor: Bonnie A. Goins

Textbook, title, author, and year: Online publications from The Open Web Application Security Project (OWASP) at https://owasp.org/

Specific course information

a. **Catalog description:** In-depth examination of topics in application security program development, stakeholder engagement, software assurance maturity measurement, identification and treatment of software vulnerabilities and implementation of a formal vulnerability management program. Homework is required for this course.
b. **Prerequisites:** ITMD 411.
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course outcomes:** Each successful student will demonstrate foundation knowledge of application security concepts and best practices. Students will describe and identify application security vulnerabilities and weaknesses, how to assess for them in an environment, how to treat these vulnerabilities and how to respond to incidents involving coding issues.
b. **Course student outcomes:**
At the conclusion of this course each student should be able to:
   - Explain the concept of application security
   - Identify and describe the OWASP Top Ten application vulnerabilities
   - Recall and describe the secure software/system development lifecycle
   - Create, implement, and maintain a formal Application Security Program
   - Describe how a formal program assists the CISO and other business stakeholders in maintaining a robust security program
   - Describe the application security assessment process
   - Write an appropriate application security report

Topics to be covered

a. Introduction to Application Security
b. Building an Application Security Program – Day 1
c. Building an Application Security Program – Day 2
d. Software Assurance Maturity Model (SAMM) – Intro
e. SAMM – Business Functions
f. SAMM – Security Practices
g. Security Practices
h. SAMM – Security Practices
i. Application Security Assessment
j. Application Vulnerability Management

ITMS 428 SYLLABUS

ITMS 428 Database Security

Hours: 3 credit hours / 45 contact hours

Instructor: Kevin Vaccaro

Textbook, title, author, and year: *Database Security,* Alfred Basta & Melissa Zgola, 2011.

Specific course information

a. **Catalog description:** Students will engage in an in-depth examination of topics in data security, including security considerations in applications and systems development, encryption methods, Cryptography and security architecture models, policy, testing, and auditing.
b. **Prerequisites:** ITMD 321.

Specific goals for the course

a. **Course Outcomes:** Each student will learn the fundamentals of database security as well as concepts and technologies such as encapsulation (information hiding) and using relational database security management techniques. They will be conversant with database hardening on a variety of platforms, defense against the most common threats and attacks, and the legal and regulatory environment affecting database security.
b. **Course student outcomes:**
At the conclusion of this course, each successful student will able to:
   - Recall and describe concepts of information security
   - Describe and explain security architectures for protection of database resources
   - Secure and harden database deployments using leading industry-standard database management systems
   - Recall and describe access control approaches, including authentication, authorization, privileges and roles
   - Discuss cryptography and encryption
   - Identify elements of a cryptographic system
   - Describe how crypto can be used, strengths and weaknesses, modes, and issues that must be addressed in an implementation
   - Describe the technical details of SQL injection attacks
   - Explain how to protect against SQL injection attacks
   - Discuss issues and recall techniques and best practices in the protection of Big Data and data in the cloud
   - Describe and discuss the processes of auditing and testing database security
   - Describe and understand NoSQL and different types of NoSQL

Topics to be covered

a. Security and Information Technology Security and Information Technology Operating System Best Practices and Review / Virtual Machines Database Review
b. Database Hardening: MySQL Database Hardening: SQL Server
c. Database Hardening: PostgreSQL
d. Cloud Databases / NoSQL / Other DB Types
e. SQL Injection – Identification and Procedure
f. Passwords, Profiles, Privileges, and Roles Encryption Policy, Documents, and Education Database Security Auditing
g. Security and System Testing

ITMS 438 SYLLABUS

ITMS 438 Cyber Forensics

Hours: 3 credit hours / 45 contact hours

Instructor: William Lidinsky

Textbook, title, author, and year:

Guide to Computer Forensics and Investigations, B. Nelson, A. Phillips, C. Steuart, 2019

File System Forensic Analysis, B. Carrier,2005

Specific course information

a. **Catalog description:** This course will address methods to properly conduct a computer and/or network forensics investigation including digital evidence collection and evaluation and legal issues involved in network forensics. Technical issues in acquiring court admissible chains-of-evidence using various forensic tools that reconstruct criminally liable actions at the physical and logical levels are also addressed. Technical topics covered include detailed analysis of hard disks, files systems (including FAT, NTFS and EXT) and removable storage media; mechanisms for hiding and detecting hidden information; and the hands-on use of powerful forensic analysis tools.

b. **Prerequisites:** ITMS 448 and ITMO 356

c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. Course Outcomes:

- Demonstrate knowledge of cyber forensic analysis at levels ranging from professional to executive levels including applicable legal issues.
- Apply this knowledge to planning and executing specific cyber forensic analyses. This includes the use of cyber forensic tools.
- Demonstrate knowledge of steganography and steganalysis and apply it to determination of existence of covert information.

c. Course student outcomes:

At the conclusion of this course, each student should be able to:

- Demonstrate knowledge of cyber forensic procedures, planning of analyses and the use of common tools for analysis
- Describe several file systems including FAT, EXT, YAFFS and NTFS.
- Describe several common booting procedures.
- Describe how to find file system objects that have been deleted or obfuscated.
- Describe how to track past computer and Internet activity and to establish time lines for this activity.
- Describe techniques for inserting covert information in various text, document and image carrier files.
- Demonstrate the ability to use tools such as WinHex, EnCase, SleuthKit and Autopsy. Also, several forensic imaging, carving and discovery tools.

Topics to be covered

a. Course Introduction. ForSec Lab Discussion. Introduction to Network & Computer Forensics.
b. Computer Investigations. Forensic Tools and Tool systems
c. Certification: Investigators and Laboratories.
d. Data Acquisition & Image Creation. Proc. Crimes & Incidents.
e. Mass storage. Solid state (flash) and rotating magnetic drives.
f. Volumes & Partitions.
g. MBR Partitions. GPT Partitions.
h. FAT File system. NTFS File system.
i. Linux Boot & Disk & Partition. EXT File Systems. Sleuthkit
j. File Carving. File carving analysis & lab
k. ADS. ADS lab.
l. Memory (RAM) forensics.
m. Virtual machine forensics.

ITMS 443 SYLLABUS

ITMS 443 Vulnerability Analysis and Control

Hours: 3 credit hours / 45 contact hours

Instructor: Kevin Vaccaro

Textbook, title, author, and year: *Mastering Kali Linux for Advanced Penetration Testing*, Vijay Kumar Velu, 2017

Specific course information

a. **Catalog description:** This course addresses hands-on ethical hacking, penetration testing, and detection of malicious probes and their prevention. It provides students with in-depth theoretical and practical knowledge of the vulnerabilities of networks of computers including the networks themselves, operating systems, and important applications. Integrated with the lectures are laboratories focusing on the use of open source and freeware tools; students will learn in a closed environment to probe, penetrate, and hack other networks. It is recommended, but not required, that students also take ITMS 448 prior to or in parallel with this course.
b. **Prerequisites:** None
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each student will be able to explain the professional hacker's methodology for attacking a network and differentiate between different methods of attacks and countermeasures.
b. **Course student outcomes:**
At the conclusion of this course, each student should be able to:
- Explain the professional hacker's methodology for attacking a network.
- Explain the script kiddie's methodology for attacking network.
- Explain Network Security vulnerabilities.
- Explain Hackers, hacker techniques, tools and methodologies
- Describe hacker motivation, perform network reconnaissance and network scanning methods
- Describe and perform covering tracks after gaining access to a network.
- Describe the general symptoms of a virus attack
- Define and describe the two basic approaches to antivirus software.
- Describe how to defend against a worm and virus attack.
- Describe the steps in planning for a computer incident.
- Identify the difficulty is establishing who has jurisdiction over a computer crime.
- Understand the legal issues with regard to preserving digital evidence.
- Identify and describe the incident response goals and priorities.
- Describe the factors involved in identifying a computer incident.
- Describe and use the various tools associated with identifying an intruder.
- Describe how to handle and evaluate a computer incident.
- Recognize the role of law enforcement and rule of particularity in executing a search warrant.
- Describe the role the network security specialist would play in assisting the law enforcement and prosecution effort.
- Describe the difficulties in prosecuting a computer crime incident.
- Differentiate between competitive intelligence, economic intelligence, and industrial espionage

Topics to be covered

a. Goal Based Penetration Testing
b. Kali / Using Linux /Basic Scripting
c. Open Source Intelligence and Passive Reconnaissance
d. Active Reconnaissance of External and Internal Networks
e. Vulnerability Assessment
f. Physical Security and Social Engineering
g. Reconnaissance and Exploitation of Web-Based Applications
h. Attacking Remote Access
i. Client-Side-Exploitation
j. Bypassing Security Controls
k. Exploitation
l. Action on Objective
m. Privilege Escalation
n. Command and Control

ITMS 448 SYLLABUS

ITMS 448 Cyber Security Technologies

Hours: 3 credit hours / 45 contact hours

Instructor: Maurice Dawson

Textbook, title, author, and year: *Official (ISC) 2 Guide to the CISSP CBK.* CRC Press. Gordon, A. (Ed.). 2015

Specific course information

a. **Catalog description:** Prepares students for a role as a network security analyst and administrator. Topics include viruses, worms, and other attack mechanisms, vulnerabilities, and countermeasures; network security protocols, encryption, identity and authentication, scanning, firewalls, security tools, and organizations addressing security. A component of this course is a self-contained team project that, if the student wishes, can be extended into a fully operational security system in a subsequent course.
b. **Prerequisites:** ITMO 440
c. **Required.**

Specific goals for the course

a. Program Educational Objective
2. Perform requirements analysis, design and administration of computer and network-based systems conforming to policy and best practices, and monitor and support continuing development of relevant policy and best practices as appropriate.
b. Course Outcomes:
Each successful student will gain an in-depth understanding of various important network and computer security concepts and practices. Students, through their course exams, labs, and homework will demonstrate the ability to apply information assurance and security concepts, specifically on the topics of malware analysis, attack vectors, mitigation/deterrents, cryptography, steganography, computer forensics, firewalls, IDS/IPS, internet security protocols, authentication, and wireless network security.
c. Course student outcomes:
- Recall and describe various careers in cybersecurity
- Describe Access Control and Bash Scripting
- Describe use of the NIST SP 800 Series Publications
- Describe Security Architecture and Design, DIACAP IA Controls, Virtualization
- Recall and describe key concepts of Physical and Environmental Security
- Recall and describe key concepts of Telecommunications and Network Security
- Recall and describe key concepts of Cryptography and Cryptographic Applications
- Describe the need for and function of Business Continuity and Disaster Recovery
- Recall applicable Laws, Regulations, Compliance, and Investigations and describe their application
- Demonstrate knowledge of Application Security
- Demonstrate knowledge of Operations Security
- Recall and describe special topics in cybersecurity
- Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions **(ABET Computing Criterion 3.1)**
- Communicate effectively in a variety of professional contexts **(ABET Computing Criterion 3.3)**
- Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline **(ABET Computing Criterion 3.5)**
- Assist in the creation of an effective project plan

Topics to be covered

a. Careers in Cyber Security, Security Trends, Information Security and Risk Management, Introduction to Linux
b. Access Control, Bash Scripting, Introduction to NIST SP 800 Series
c. Security Architecture and Design, DIACAP IA Controls, Virtualization
d. Physical and Environmental Security
e. Telecommunications and Network Security
f. Cryptography and Cryptographic Applications
g. Business Continuity and Disaster Recovery
h. Legal, Regulations, Compliance, and Investigations
i. Application Security
j. Operations Security
k. Special Topics: Cyber Terrorism, Destructive Coding Practices, Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signatures Intelligence (MASINT), Open Source Intelligence (OSINT), Offensive Security, Defensive Security, Certification and Accreditation (DIACAP, NIST SP 800 Series, Common Criteria, NSA Rainbow Series, Directive of Central Intelligence Directives), Reverse Engineering

ITMS 458 SYLLABUS

ITMS 458 Operating System Security

Hours: 3 credit hours / 60 contact hours

Instructor: Sean Hughes-Durkin

Textbook, title, author, and year: Online materials will be assigned for reading

Specific course information

a. **Catalog description:** This course will address theoretical concepts of operating system security, security architectures of current operating systems, and details of security implementation using best practices to configure operating systems to industry security standards. Server configuration, system-level firewalls, file system security, logging, anti-virus and anti-spyware measures and other operating system security strategies will be examined.
b. **Prerequisites: ITMO 356.**
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will be able to describe the different types of malicious threats targeted to an operating system. The student will be able to explain ways to mitigate these threats, correct vulnerable configurations, and use best practices to harden systems. This course and the concepts described in the class cover topics included on the Certified Information Systems Security Professional (CISSP). The GIAC Security Essentials (GSEC) certification is another recognized security certification that covers the concepts the student will learn throughout this course.
b. **Course student outcomes:**
   Students completing this course will be able to:
   - Describe potential system attacks and the actors that might perform them
   - Describe appropriate measures to be taken should a system compromise occur
   - Describe characteristics of malware and identify different malware
   - Apply tools and techniques for identifying vulnerabilities
   - Describe, for a given OS, the steps necessary for hardening the OS with respect to various applications
   - Securely install a given OS, remove or shut down unnecessary components and services, close unnecessary ports, ensure that all patches and updates are applied
   - Identify the major concepts in modern operating systems and the basic security issues in OS design and implementation (how the first principles of security apply to operating systems)

Topics to be covered

a. Malicious Software/Attacks (2 parts)
b. Incident Handling
c. User Authentication & Access Control Cryptographic Tool
d. Host Firewalls
e. Host Based Intrusion Detection (2 parts)
f. General OS Hardening
g. Linux Hardening
h. Windows Hardening
i. Post OS Hardening Testing

ITMS 478 SYLLABUS

ITMS 478 Cyber Security Management

Hours: 3 credit hours / 45 contact hours

Instructor: Ray Trygstad

Textbook, title, author, and year: *Management of Information Security, Sixth Edition,* Michael E. Whitman & Herbert J. Mattord, 2018

Specific course information

a. **Catalog description:** In-depth examination of topics in the management of information technology security including access control systems & methodology, business continuity & disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.
b. **Prerequisites:** None.
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will demonstrate foundation knowledge and application of cybersecurity concepts as they to apply the management of information system security in a large organizational environment. Students will describe and identify policy frameworks, legal and moral implications, and best practices in information security management. Students will be able assist in the conduct of a security audit of an organization and report on the results with appropriate suggestions for amelioration of problem areas identified.
b. **Course student outcomes:**
Upon completion of this course, each student should be able to:
    - Discuss the history of computer security and how it evolved into information security
    - Identify and define key terms and critical concepts of information security
    - Describe the business need for information security
    - Differentiate between laws and ethics, describe the role of ethics in professional practice in information security, and identify major national laws that relate to the practice of information security
    - Define risk management and its role in the Security Systems Development Life Cycle
    - Assist in the preparation and conduct of a cybersecurity audit of an existing business, government agency or organization and prepare a complete audit report with appropriate suggestions for amelioration of problem areas identified
    - Describe management's role in the development, maintenance, and enforcement of information security policy, standards, practices, procedures, and guidelines
    - Assist in the design and implementation of a comprehensive enterprise security program using policy and standards to implement technical, operational, and managerial controls
    - Recall and describe recommended security management models
    - Explain what contingency planning is and how incident response planning, disaster recovery planning, and business continuity plans are related to contingency planning.
    - Describe common technical security controls, implementations in an enterprise setting, and how they are driven by policy and standards

Topics to be covered

a. Introduction to Information Security
b. Compliance, Legal, Ethical/Professional Issues Governance and Planning for Security
c. Security Policy
d. Developing Security Programs
e. Risk Management I
f. Risk Management II
g. The Information Security Audit
h. Security Management Models
i. Security Management Practices
j. Contingency Planning: Disasters/Business Continuity
k. Security Maintenance and Digital Forensics Protection Mechanisms
l. HIPAA

ITMS 479 SYLLABUS

ITMS 479 Topics in Information Security

Hours: Variable, but normally 3 credit hours / 45 contact hours

Instructor: TBD

Textbook, title, author, and year: Will vary based on specific course content.

Specific course information

a. **Catalog description:** This course will cover a particular topic in Information Security, varying from semester to semester, in which there is particular student or staff interest. This course may be taken more than once but only 9 hours of ITMS 479/579 credit may be applied to a degree.
b. **Prerequisites:** Will vary based on course content.

Specific goals for the course

a. **Course Outcomes:** Will vary based on specific course content.
b. **Course Student Outcomes:** Will vary based on specific course content.

Topics to be covered: Will vary based on specific course content.

ITMS 483 SYLLABUS

ITMS 483 Digital Evidence

Hours: 3 credit hours / 45 contact hours

Instructor: Shawn Davis

Textbook, title, author, and year: *E-discovery: An Introduction to Digital Evidence*, Phillips, Amelia; Godfrey, Ronald; Steuart, Christopher; Brown, Christine, 2014

Specific course information

a. **Catalog description:** In this course, students learn the fundamental principles and concepts in the conduct of investigations in the digital realm. Students will learn the process and methods of obtaining, preserving and presenting digital information for use as evidence in civil, criminal, or administrative cases. Topics include legal concepts and terminology, ethics, computer crime, investigative procedures, chain of custody, digital evidence controls, processing crime and incident scenes, data acquisition, email investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding.
b. **Prerequisites:** ITMS 438
c. **Required for Applied Cybersecurity and Information Technology.**

Specific goals for the course

a. **Course Outcomes:** Each successful student will demonstrate foundation knowledge and application of digital evidence and e discovery concepts as they apply to the investigation of computer crimes and cyber security incidents in a large organizational environment. Students will describe and identify policy frameworks, legal and moral implications, and best practices in the collection, processing and presentation of digital evidence. Students will be able to conduct digital investigations in full compliance with applicable law, policy, and regulations, and present the investigative results as an expert witness.
b. **Course student outcomes:**
    - Acquire, process, preserve, evaluate, and present digital evidence in a forensically and legally sound manner.
    - Recall and describe law, theories, techniques, and practices that apply to digital forensic investigations.
    - Identify and describe types of computer and Internet crimes.
    - Preserve and process a crime scene involving digital evidence.
    - Explain the legal procedures and standards in the collection and analysis of digital evidence.
    - Prepare a report of a digital investigation for appropriate stakeholders and defend your findings.
    - Present an analysis of digital evidence in a legal or administrative proceeding as an expert witness.

Topics to be covered

a. Introduction to Legal Concepts and Terminology
b. Introduction to Digital Evidence
c. History and Ethics of E-discovery and Digital Evidence
d. Planning and Tools
e. Experts in Digital Evidence and E Discovery
f. Digital Evidence Case Flow
g. Case Study: From Beginning to Trial
h. Information Governance and Litigation Preparedness
i. Presenting Digital Evidence in Court
j. Digital Evidence Case Law
k. The Future of Digital Evidence

ITMS 484 SYLLABUS

ITMS 484 Governance, Risk and Compliance

Hours: 3 credit hours / 45 contact hours

Instructor: Bonnie A. Goins

Textbook, title, author, and year: Online resources including COBIT, NIST, and other sources

Specific course information

a. **Catalog description:** In-depth examination of topics in governance, risk and compliance, including security program development; development and implementation of policies, standards and procedures; risk management and assessment methodologies, practices and outcomes; compliance standards, methods, processes and practices.
b. **Prerequisites:** None.

Specific goals for the course

a. **Course student outcomes:**
Each successful student will demonstrate foundation knowledge of governance, risk and (GRC) concepts, practice and outcomes as they apply to an organization. Students will be able to describe and identify policy frameworks and best practices for GRC.
b. **Course student outcomes:**
At the conclusion of this course, each student should be able to:
    - Describe governance, risk and compliance frameworks.
    - Describe governance, risk and compliance methodologies.
    - Identify and detail program components for governance, risk management and compliance programs
    - Apply GRC concepts in the build of a Data Governance model and corresponding deliverables.
    - Evaluate and categorize risk 1) with respect to technology; 2) with respect to individuals, and 3) in the enterprise, and recommend appropriate responses.
    - Compare advantages and disadvantages of various risk assessment methodologies.
    - Select the optimal methodology based on needs, advantages and disadvantages.
    - Describe the impact of legal/regulatory standards on a given system.
    - Describe how audits are conducted using the SOC 2.
    - Describe the difference between auditing and assessment.

Topics to be covered

a. Introduction to GRC
b. Governance Introduction and Methodology
c. Governance Implementation-Data Governance
d. Governance Design
e. Risk Management Introduction and Framework
f. Risk Assessment Method
g. Risk Assessment Threat and Vulnerability Considerations
h. Risk Assessment Outcomes
i. Compliance Introduction
j. Compliance Audit and Assurance

ITMT 430 Syllabus

ITMT 430 Systems Integration (Senior Capstone Course)

Hours: 3 credit hours / 60 contact hours; 30 hours lecture, 30 hours lab

Instructor: Jeremy Hajek

3. Textbook, title, author, and year:
   a. *DevOps Handbook - How to Create World-Class Agility, Reliability, & Security in Technology Organizations*, Gene K., Patrick D., John W., Jez H., 2016.
   b. *Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations*, Nicole F., Jez H., Gene Kim, 2018.

Specific course information

a. Catalog description: In this capstone course, students will identify, gather, analyze, and write requirements based on user needs and will then design, construct, integrate, and implement an information system as a solution to a business problem. Students will document integration architecture, methodologies, and technologies using industry best practices. User needs and user centered design will be applied in the selection, creation, evaluation, and administration of the resulting system. The system design process will take into account professional, ethical, legal, security, and social issues and responsibilities and stress the local and global impact of computing on individuals, organizations, and society. Discussion will also cover the need to engage in continuing professional development.
b. Prerequisites: ITMD 321, ITMD 411, ITMD 362, ITM 100, ITMM 471, ITMO 340, and ITMO 356
c. Required

Specific goals for the course

a. Program Educational Objectives:
   1. Problem solve and create innovative answers to provide technology solutions for the problems of business, industry, government, non-profit organizations, and individuals.
   2. Perform requirements analysis, design and administration of computer and network-based systems conforming to policy and best practices, and monitor and support continuing development of relevant policy and best practices as appropriate.
   3. Apply current technical and mathematical concepts and practices in the core information technologies and recognize the need to engage in continuing professional development.
b. Course Outcomes:
   At the completion of this course you will have experienced software application development in a team setting. You will understand the roles of the project manager, a software developer, security analyst, IT operations, and UI/UX developer. You will have produced artifacts consistent with the nature of each job and applied the techniques and concepts learned in all of your pre-requisite courses. The final measurable outcome will be a full deployment of a working application from scratch. You will be familiar with DevOps terminology and development practices. You will have integrated hardware and software into a complete information system to meet identified user needs as a solution to a defined business problem and demonstrated ethics, and an understanding of legal, security, and social issues and responsibilities of information systems. You will have integrated hardware and software into a complete information system to meet identified user needs as a solution to a defined business problem. You will have demonstrated building world class reliable, agile, and secure cloud native applications.
c. Course student outcomes:
   At the conclusion of this course, each successful student will able to:
   - Identify, gather, analyze, and write information system requirements based on user needs.
   - Document integration requirements using business process models.
   - Design, construct, integrate, and implement an information system as a solution to a business problem.
   - Apply key systems integration architecture, methodologies, and technologies in the construction of an information system using industry best practices.
   - Based on identified user needs, demonstrate the use of user centered design in the selection, creation, evaluation, and administration of an information system.
   - Recall and explain professional, ethical, legal, security, and social issues and responsibilities in information systems.
   - Describe the local and global impact of computing on individuals, organizations, and society
   - Describe the need to engage in continuing professional development and explain how this may be achieved.
   - Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions **(ABET Computing Criterion 3.1)**
   - Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline **(ABET Computing Criterion 3.2)**
   - Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline **(ABET Computing Criteria 3.5)**
   - Identify and analyze user needs and take them into account in the selection, creation, evaluation, and administration of computer-based systems **(ABET IT Criterion 3.6)**
   - Assist in the creation of an effective project plan

Topics to be covered

a. Course Introduction
b. Introduction to Tooling, Project Management, & Communication
c. The Three Ways and Where to Start
d. Technical Practices of Flow
e. Technical Practices of Feedback
f. Technical Practices of Learning
g. Technical Practices of Information Security
h. Measuring Performance; Measuring & Changing Culture
i. Technical Practices of Architecture
j. Information Security and Management Practices
k. Product Development; Making Work Sustainable
l. Leading & Managing; Data

ITMT 491 SYLLABUS

ITMT 491 Undergraduate Research

Hours: Variable, but normally 1-3 credit hours / 15-45 contact hours

Instructor: TBD

Textbook, title, author, and year: Will vary based on specific course content.

Specific course information

a. **Undergraduate research.** Written consent of instructor is required.
b. **Prerequisites:** Will vary based on course content.

Specific goals for the course

a. **Course Outcomes:** Will be defined by student research proposal or prospectus.
b. **Course Student Outcomes:** Will be defined by student research proposal or prospectus.

Topics to be covered: Will be defined by student research proposal or prospectus.

ITMT 492 SYLLABUS

ITMT 492 Introduction to Smart Technologies

Hours: 3 credit hours / 45 contact hours

Instructor: Jeremy Hajek

Textbook, title, author, and year: Online resources will be assigned in Blackboard.

Specific course information

a. **Catalog description:** This course covers reconfigurable intelligent devices programmed with modern high-level languages focusing on design and integration to modern environments. This course also covers the topic and deployment of wireless sensor networks and the use of rapid prototyping for commercial application. Students will discover hardware, software and firmware design trade-offs as well as best practices in current embedded systems development. A final project will integrate course topics into a system using an embeddable single-board microcontroller.
b. **Prerequisites:** ITM 311 or ITM 312 or ITM 313.

Specific goals for the course

a. **Course Outcomes:** The student will be exposed to a wide array of tools and services that support smart technology. They will be able to solve problems that involve the concepts of data collection, data transmission, and data presentation by using the technologies learned in the course. This survey of Smart Technologies covering wireless protocols, AR devices, voice assistants, solar powered and battery back sensor networks and cloud storage will give students a sufficient ability to create innovative solutions to problems they encounter.
b. **Student course outcomes:**
At the conclusion of the course, the student should be able to:
    - Describe and apply principles of electricity and electronics that support smart tech.
    - Read and use schematics, diagrams, and electronic symbols.
    - Explain concepts of Data Collection, Data Transmission, and Data presentation using small computers and sensor networks
    - Recall the fundamentals and use of wireless communication standards: Bluetooth, NFC, xBee (802.15), Wi-Fi
    - Describe concepts of solar panels and LiPo batteries
        - Deploy solar panels and LiPo batteries
    - Describe the use of cloud data storage for smart technology
    - Recall the basics of Augmented Reality devices
    - Describe the principles and use of Voice Assistants
        - Demonstrate a basic working knowledge of Voice Assistants

Topics to be covered

a. Data Transmission: wireless tech Wi-Fi
b. Adafruit IoT Portal
c. AWS/Azure IoT Portals
d. Intro to Voice Assistants
e. Final Project

ITMT 495 SYLLABUS

ITMT 495 Topics in Information Technology

Hours: Variable, but normally 3 credit hours / 45 contact hours

Instructor: TBD

Textbook, title, author, and year: Will vary based on specific course content.

Specific course information

a. **Catalog description:** This course will cover a particular topic varying from semester to semester in which there is particular student or staff interest.
b. **Prerequisites:** Will vary based on course content.

Specific goals for the course

a. **Course Outcomes:** Will vary based on specific course content.
b. **Course Student Outcomes:** Will vary based on specific course content.

Topics to be covered: Will vary based on specific course content.

TECH 465 SYLLABUS

TECH 465 Introduction to Social Commerce

Hours: 3 credit hours / 45 contact hours

Instructor: TBD

Textbook, title, author, and year: None assigned. Excerpts from books, web sites and articles will be used.

Specific course information

a. **Catalog description:** Provides an introduction and basic knowledge of social commerce to help students develop a practical understanding of the design, construction, market readiness and synergistic integration of a business mobile application. The course will provide a practitioner focus that will benefit students in a start-up or company/corporate setting.
b. **Prerequisites:** None .

Specific goals for the course

a. **Course Outcomes:** Understand and apply the basic concepts of social commerce: definition and structure; design which meets customer needs; technology factors to make a winning mobile application; understanding and application of basic algorithms and data analytics; integration with partner and customer applications, systems and rewards; working as part of a team-design, develop and prepare proposal for an actual social commerce mobile application and how to win in the market place with the application.
b. **Course Student Outcomes:**
Upon completion of this course, students should be able to:
   - Recall basic concepts and components of social commerce
   - Explain how to meet customer needs and the role of research and analysis
   - Describe market research for social commerce
   - Identify and employ algorithms for customer experiences, partner experiences, and rewards
   - Describe the use of data analytics and data mining in social commerce
   - Explain integration with partner and customer applications, systems and rewards
   - Recall and describe the principles and concepts of mobile application development
   - Develop and prepare a proposal for a social commerce mobile application
   - Explain how to win in the marketplace with the proposed application

Topics to be covered:

a. Syllabus; Intro: Definition, Structure, Scope, Business future
b. Components of Social Commerce: Needs, Configuration, Design
c. Customer needs research and analysis
d. Customer factors and Ideation
e. Competitive Advantage-Competition research
f. Market Research-Proof of Idea
g. Risks and Options-Market for Idea
h. Final design of Idea-Lean Canvas
i. Algorithms for Customer experiences
j. Algorithms for Partner experiences
k. Algorithms for Rewards
l. Data Analytics
m. Data Mining
n. Big data mining integration, synergies and rewards
o. System flow of Idea include: DBs, files, structure
p. Mobile application basics
q. Mobile application designs, data handling/transmission
r. Mobile application final design for Idea
s. Mobile application security
t. Mobile application process-order
u. Mobile application process-payment
v. Mobile application data base design and uses
w. Mobile application final design bench test
x. Mobile application integration with other apps, systems, etc.
y. Idea application programming requirements
z. Idea application testing requirements
aa. Go to market-pricing and channels of distribution
bb. Roll-out and Feedback loop
cc. Business Model and Plan Bus Group Paper
dd. Group Presentation

TECH 497 SYLLABUS

TECH 497 Independent Study

Hours: Variable, but normally 1-3 credit hours / 15-45 contact hours

Instructor: TBD

Textbook, title, author, and year: Will vary based on specific course content.

Specific course information

a. **Catalog description:** Independent study and projects in applied technology that are multi/cross-disciplinary not tied to a specific department.
b. **Prerequisites:** Will vary based on course content.

Specific goals for the course

a. **Course Outcomes:** Will vary based on course content or will be defined by student course proposal or prospectus.
b. **Course Student Outcomes:** Will vary based on course content or will be defined by student course proposal or prospectus.

Topics to be covered: Will vary based on course content or will be defined by student course proposal or prospectus.