NEW UNDERGRADUATE PROGRAM PROPOSAL

ILLINOIS INSTITUTE OF TECHNOLOGY

The following information is required by the Undergraduate Studies Committee to approve new programs. After approval by UGSC this form should be routed to Faculty Council for approval and then the Provost's office.

College(s): School of Applied Technology

Department(s): Information Technology and Management

Date: 9/25/17
(Updated 11/17/17 as the Program Title was amended by the Undergraduate Studies Committee)

Approvals Required

(1) Academic Unit Head(s): Chair, Department of Information Technology and Management

(2) Dean(s): Dean, School of Applied Technology

(3) Other: Undergraduate Studies Committee / University Faculty Council

GENERAL INFORMATION

Program Title: Bachelor of Science in Applied Cybersecurity and Information Technology

Program Scheduling: Spring 2018

Total Program Credit Hours: 129

Program Description: *Provide a brief narrative of the program content (use as much space as needed).*
The Bachelor of Science in Applied Cybersecurity and Information Technology (BSCIT) lays down a solid base of 36 hours of required courses in information technology as a foundation for the 21 hours of dedicated courses in cybersecurity, along with a 3 hour capstone course. It includes a mathematics track culminating in a calculus-based probability and statistics course, properly equipping students for advanced study and research in the field. The Bulletin pages for the program follow this form and provide more complete details. This program prepares students to enter the workforce in cybersecurity roles, particularly entry-level security analyst positions, or to continue on to advanced studies and research in the field. It requires students to demonstrate knowledge and proficiency in these areas:

- Information technology basics including hardware and operating systems
- Application development and programming
- Human-computer interaction
- Databases and data management
- Networking and communications
- Websystems
- Cybersecurity
- System Integration
- Professionalism
- Information Security
- Software Security
- System Security
- Human Security
- Organizational Security
- Societal Security

Program Purpose/Program Benefits: *Provide details on the intent of the program and its relation to other programs. State the impact of the program for students and for IIT.*
Cybersecurity is one of the fastest growing fields in the world. "ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cyber-security related roles, according to cyber security data tool CyberSeek." (*Forbes*, "The Fast-Growing Job With A Huge Skills Gap: Cyber Security" by Jeff Kauflin, March 16, 2017) According to the U.S. Bureau of Labor Statistics, between 2012 and 2022, the rate of growth for information security analysts is expected to be 36.5 percent. With this huge gap in supply and demand, there is a clear need for educated cybersecurity professionals in the job market, and an even bigger need for researchers in the field. ABET is expected to begin accrediting programs in cybersecurity possibly as early as 2018. Additional workforce demand details can be seen at the National Initiative for Cybersecurity Education (NICE) website at https://www.nist.gov/sites/default/files/documents/2017/01/30/nice_workforce_demand.pdf

This degree encompasses existing requirements for the Bachelor of Information Technology and Management as a foundation and builds on this base to develop cybersecurity knowledge, skills, and abilities. When ABET finalizes the Program Criteria for Cybersecurity and Similarly Named Computing programs, this program as drafted will meet requirements for accreditation in both Information Technology and Cybersecurity.

It will increase enrollment in the Department of Applied Mathematics because students will be required to complete a sequence of math courses leading to completion of a calculus-based course in probability and statistics to properly equip them to pursue further research in the field.

It will have the same admission requirements, mathematics requirements, and expectations as other Illinois Tech Bachelor of Science degrees in engineering and science.

It will feed graduate programs in cybersecurity in our department. One of these programs is a research degree also being proposed, the Master of Science in Applied Cybersecurity and Digital Forensics. The increased visibility brought about by this research-focused degree path will attract more students and ideally will eventually lead to designation of the university by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense Research.

Significant Federal scholarship opportunities are open to students in this curriculum including the CyberCorps® Scholarship for Service Scholarships, Department of Defense Information Assurance Scholarships, and the State Department Foreign Affairs Information Technology (IT) Fellowship Program. These programs not only cover two to three years of fully funded study, but also award stipends to students ranging from $22,000 to $37,500 per year. In addition more limited scholarships are available non-government organizations such as the Cybersecurity Scholarships from the International Information System Security Certification Consortium's Center for Cyber Safety and Education. These opportunities already exist due to our designation by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense Education.

There is a draft Model Curriculum for this degree jointly prepared by the Joint Task Force on Cybersecurity Education which includes ACM, IEEE-CS, and AIS SIGSEC at https://docs.wixstatic.com/ugd/895bd2_331dd0a4e2cf41a1b17f394e3e62a955.pdf.
In addition, the ABET accreditation Program Criteria for Cybersecurity and Similarly Named Computing programs has just been placed in the public review and comment phase; the most current iteration of these criteria can be seen at https://www.surveymonkey.com/r/cybersecuritycriteria.

Classification of Instructional Programs (CIP) Code **1** **1** . **1** **0** **0** **3**
(Computer and Information Systems Security/Information Assurance.)

PROGRAM VIABILITY

Competitive Programs: *Indicate other similar programs locally and nationally detail their success.*

Serious competitors:	Drexel University, Philadelphia, PA *
	Kennesaw State University, Kennesaw, GA *
	Pennsylvania State University, multiple locations, PA *
	Rochester Institute of Technology, Rochester, NY *
	Southern Methodist University, Dallas, TX *
	Stevens Institute of Technology, Hoboken, NJ *
	United States Air Force Academy, Colorado Springs, CO *
	United States Naval Academy, Annapolis, MD *
	University of Texas at San Antonio, San Antonio TX *
Minor competitors:	Bellevue University, Bellevue NE *
(Illinois in blue)	Capitol Technology University, Laurel, MD *
	Charleston Southern University, Charleston, SC
	City University of Seattle, Seattle, WA *
	DePaul University, Chicago, IL *
	East Stroudsburg University, East Stroudsburg, PA
	Fairleigh Dickinson University, Teaneck NJ *
	Illinois State University, Normal, IL (starting Fall 2017) *
	Immaculata University, Immaculata, PA *
	Lewis University, Romeoville, IL *
	National University, San Diego, CA *
	University of Central Missouri, Warrensburg, MO
	University of Illinois Springfield, Springfield, IL *
	University of Nebraska Omaha, Omaha, NE *

* National Center of Academic Excellence in Cyber Defense Education
Online only degrees are not listed; there are a great number of those.
Most degrees in this field are Master's degrees.

Market Analysis for Recruiting Students: *Detail what work has been done with UG Admissions to identify and recruit potential students.*

We are very aware of the market for graduates of the program, and have seen that awareness of the opportunities in this field have reached the secondary school level. Our ability to recruit students is significantly enhanced by our designation by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense Education. Admissions will target much of the same population historically attracted by other computing and engineering degrees at the university.

Market Analysis for Graduates: *Detail what work has been done with the Career Services Center to identify potential employment opportunities for graduates.*

By virtue of our cooperation and involvement with the National Security Agency, the National Initiative for Cybersecurity Education, the Women in Cybersecurity Conference, and the Mayor Emmanuel's Cybersecurity Roundtable, we are very aware of the market for graduates of the program. We are actively involved with and in contact with employers seeking students with these skills. In our weekly student newsletter we already regularly feature internship and employment opportunities in the field. Since we currently offer a professional master's degree in cybersecurity, Career Services is already actively engaged in cultivating industry connections. Employability of our graduate is enhanced by our designation by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Cyber Defense Education.

ACADEMIC INFORMATION

Enrollment Estimates: *Are there enrollment estimates for this program, and if so, what are they and what are they based on? What is the minimum number of students necessary in the program to make the program viable (i.e.to offer classes unique to the program often enough)?*
Enrollment estimates are initially 20 to 25 first-year students per year. This is extrapolated from current enrollment in the Bachelor of Information Technology and Management degree coupled with known interest and demand in industry. There is not a minimum number of students necessary for the new program to succeed because only one completely new course is required and all new courses are coupled with existing or new graduate courses.

Advising Strategy: *Since quality advising is a key component of good retention, graduation and career placement, how will students be advised and mentored? Specifically for interdisciplinary programs, how will advising responsibilities be shared? What student professional organizations will be formed? How will the department work with the Career Services Center to develop industry connections?*
Students will be advised and mentored by existing advisers who are cybersecurity faculty members. No new advisers will be required for this program.

We have had initial formation of a student chapter of the High Technology Crime Investigation Association (HTCIA), and we will also investigate interest in forming a chapter of the National Cybersecurity Student Association. We are the host of the NSF-funded national 2018 Women in Cybersecurity Conference and will continue our association with that conference beyond this event.

Since we currently offer a professional master's degree in cybersecurity, Career Services is already actively engaged in cultivating industry connections. In addition, scholarships currently or expected to be offered to students in the curriculum come with significant connections to government employment including access to national career fairs and travel funding for attendance.

Course Requirements: *Detail the courses needed for the program including courses currently offered, new courses to be developed (including syllabi), and dependence on courses from other academic units with their commitments to provide these courses on a long-range basis. Include descriptions of laboratories that will need to be developed along with equipment and facilities requirements.*
All courses needed for the program are currently offered except for three new courses which are:
ITMS 418 Coding Security
ITMS 438 Digital Forensics
ITMS 483 Digital Evidence

ITMS 418 and ITMS 438 already exist at the graduate level as ITMS 518 and ITMS 538, so they are not in fact new courses but are adaptions of existing courses suitable for undergraduates, and will be taught in common lecture sections with ITMS 518 and ITMS 543. ITMS 483 Digital Evidence is a new course. A syllabus for each of these courses is attached.

The program will add to student loading in MATH 151, 152, 230, 251, and 474, all of which are regularly offered in support of their own majors or other programs within the university. Draft accreditation criteria require completion of discrete mathematics and statistics.

We already have an existing laboratory structure for our current cybersecurity degree, which has just been augmented by a $299,000 grant from the National Security Agency, so no new equipment or laboratory facilities will be required for this degree.

Sample Curriculum/Program Requirements: *Provide a sample semester by semester curriculum and the program requirements, as they would appear in the IIT Undergraduate Programs bulletin.*

Applicable pages providing a sample semester by semester curriculum and the program requirements, as they would appear in the IIT Undergraduate Bulletin, are attached.

Attached Program Outcomes and Assessment Process: *Provide the program learning goals and assessment plan (for more information contact the Assessment Office within Academic Affairs). Also see* https://sites.google.com/a/iit.edu/student-learning-assessment/

Program Educational Objectives:

The Bachelor of Science in Applied Cybersecurity and Information Technology degree produces graduates who are able to:

1. Problem solve, create, and effectively communicate 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. Design and implement an enterprise security program using both policy and technology to implement technical, operational, and managerial controls, which will technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
4. Investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.
5. Apply current technical and mathematical concepts and practices in the core information technologies and recognize the need to engage in continuing professional development.

Student Outcomes/Learning Goals:

Students completing the Bachelor of Science in Applied Cybersecurity and Information Technology will be able to:

(a) Analyze a problem and identify and define the computing requirements appropriate to its solution.
(b) Design, implement, and evaluate a computer-based solution to meet a given set of computing requirements.
(c) Communicate effectively with a range of audiences about technical information.
(d) Make informed judgments in computing practice based on legal and ethical principles.
(e) Function effectively on teams to establish goals, plan tasks, meet deadlines, manage risk, and produce deliverables.
(f) Identify and analyze user needs and to take them into account in the selection, integration, evaluation, and administration of computer-based systems. [IT]
(g) Apply security principles and practices to the environment, hardware, software, and human aspects of a system. [Cybersecurity]
(h) Analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats. [Cybersecurity]

(These learning goals are based on the newly-approved ABET Criteria 3 Student Outcomes for Information Technology and the proposed ABET Criteria 3 Student Outcomes for Cybersecurity.)

See the attached Assessment Plan for full details.

INFORMATION TECHNOLOGY AND MANAGEMENT

10 W. 33rd St.
Perlstein Hall Room 223
Chicago IL 60616
312.567.5290
appliedtech.iit.edu/information-technology-and-management

Daniel F. and Ada L. Rice Campus
201 E. Loop Rd.
Wheaton, IL 60189
630.982.6000

Dean and Chair
C. Robert Carlson

Associate Chair and Director of Undergraduate Advising
Ray Trygstad

Faculty with Research Interests
For information regarding faculty visit the Department of Information Technology and Management website.

The objective of bachelors' degrees offered by the Department of Information Technology and Management is to produce graduates prepared for a career in the information technology field, while equipping them with the critical thinking skills necessary to cope with the emergence of new technologies and with management principles needed to advance in their careers. While the Bachelor of Information Technology and Management degree was originally designed for students who have achieved an associate's degree and would like to complete a bachelor's degree, students may also enter the program as first-year students. Bachelor of Science degrees give students the mathematical grounding necessary to prepare them for further research-focused graduate studies.

Government studies such as Free and Aspray: ***The Supply of Information Technology Workers in the United States***, show that technology positions will be the fastest growing segment in the United States for the next 30 years. Organizations of all kinds have become dependent on networked computing infrastructure as the key element to enabling modern business processes, and our graduates are prepared to select, manage, and maintain that infrastructure, ensuring that it meets organizational needs. Information technology professionals assume responsibility for selecting hardware and software products appropriate for an organization, integrating those products with organizational needs and infrastructure, and installing, customizing, and maintaining those applications for the organization's computer users. Planning and managing an organization's technology infrastructure is a difficult and complex job that requires a solid foundation in applied computing as well as management and people skills. Professionals in this discipline require special skills, such as understanding how networked systems are composed and structured and what their strengths and weaknesses are, and being prepared to deal with important software systems concerns such as reliability, security, usability, and effectiveness and efficiency for their intended purpose. These topics are difficult and intellectually demanding.

The Bachelor of Information Technology and Management degree produces graduates who are able to:

- Problem solve, create, and effectively communicate innovative answers to provide technology solutions for the problems of business, industry, government, non-profit organizations, and individuals.
- 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.
- Apply current technical and mathematical concepts and practices in the core information technologies and recognize the need to engage in continuing professional development.

To meet these goals, graduates must demonstrate knowledge and proficiency in these areas:

- Information technology basics including hardware and operating systems
- Application development and programming
- Human-computer interaction
- Databases and data management
- Networking and communications
- Websystems
- Cybersecurity
- Professionalism

Bachelor of Information Technology and Management students are required to complete a minor. The minor may be in a field which will complement information technology such as business or professional and technical communication, or may be chosen from a field very different such as history or sociology to provide a more widely rounded educational experience.

The Bachelor of Science in Applied Cybersecurity and Information Technology degree produces graduates who are able to:

- Problem solve, create, and effectively communicate innovative answers to provide technology solutions for the problems of business, industry, government, non-profit organizations, and individuals.
- 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.
- Design and implement an enterprise security program using both policy and technology to implement technical, operational, and managerial controls, which will technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.
- Investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.
- Apply current technical and mathematical concepts and practices in the core information technologies and recognize the need to engage in continuing professional development.

To meet these goals, in addition to the knowledge and proficiency expected of graduates in Information Technology and Management, Cybersecurity graduates must complete 45 hours of coursework in computing and cybersecurity that must cover application of the crosscutting concepts of confidentiality, integrity, availability, risk, and adversarial thinking, as well as fundamental topics from the following areas:

- Information Security
- Software Security
- System Security
- Human Security
- Organizational Security
- Societal Security

Admission for transfer students is based on a review of college transcripts and documentation of work experience. Applicants must submit an application for admission as a degree-seeking student. Transfer applicants must hold an associate's degree (A.A.) from an accredited college or the equivalent (completion of at least 55 credit hours). Only courses in which the student has earned a grade of "C" or better may be accepted for transfer. Supporting documentation to be included with the application includes official transcripts of all college-level work.

IIT/College of DuPage and IIT/Joliet Junior College Dual Admissions Programs

Students who meet the requirements of the Dual Admissions Program (DAP) may enroll simultaneously at the College of DuPage (COD) or Joliet Junior College (JJC) and Illinois Institute of Technology. Students accepted into the DAP will have access to advising and other services from both institutions. Students who successfully complete the institutional course requirements of both institutions under the DAP will be awarded an associate's degree from COD or JJC and a Bachelor of Information Technology and Management from Illinois Institute of Technology.

Eligibility for the Program

Students applying to the DAP must be enrolled in one of the following programs:

At COD: Associate of Applied Science in Computer Information Systems or Associate of Applied Science in Computer Internetworking Technologies

At JJC: Associate of Applied Science in Computer Information Systems; Network Specialist, Programming, or Web Design and Administration options

Students must have and maintain a cumulative GPA of at least 3.00 at COD or JJC to be eligible for admission to IIT. Students must make satisfactory academic progress at COD, as defined by COD, or at JJC, as defined by JJC.

Application Process

Applicants must complete a Statement of Intent Form, which permits the exchange of academic admission and advising information between IIT and COD or JJC. Applicants must also complete the application process at both COD or JJC and IIT in order to be admitted to both institutions. The IIT application may be submitted only for a Bachelor in Information Technology and Management. Admission to other IIT programs may have additional requirements that are outside the scope of the program.

Academic Program Requirements

Students must follow each institution's policies regarding admission, course enrollment, transfer hours, probation, dismissal, and reinstatement. Transcripts must be sent to the IIT Office of Undergraduate Academic Affairs each semester for each student attending COD or JJC and enrolled in the DAP. IIT will provide COD and JJC with major and course updates, course prerequisites, and program requirements for the information technology and management bachelor's degree completion program.

Graduation Requirements

Students enrolled in the DAP must follow the COD or JJC catalog to satisfy requirements for the associate's degree and the requirements set out in the IIT Undergraduate Bulletin in effect at the time of admission into the DAP for the bachelor's degree.

The Center for Cyber Security and Forensics Education

The Center for Cyber Security and Forensics Education (C2SAFE) is a multi-disciplinary center within the School of Applied Technology. The objectives of the Center for Cyber Security and Forensics Education are to:

- Develop, promote, and support education and research in cybersecurity technologies and management, information assurance, and digital forensics across all academic disciplines at Illinois Institute of Technology.
- Engage with business and industry, government, professional associations, and community colleges to enhance knowledge, awareness, and education in cybersecurity and digital forensics and improve practices in information assurance.
- Coordinate the designation of Illinois Institute of Technology as a National Center of Academic Excellence in Cyber Defense Education.
- Maintain resources for education and research in cybersecurity and digital forensics, publish student and faculty research in the field, and sponsor, organize, and conduct conferences and other events to promote and advance cyber security and forensics education.
- Support the university's academic departments in the delivery of the highest caliber of cyber security and digital forensics education.

The center plans, organizes, and conducts the annual ForenSecure conference in the spring of each year, as well as additional activities and student competitions that advance the mission of the center.

The center actively cooperates and coordinates activities with agencies of the federal government and with professional organizations and programs such as the Information Systems Security Association (ISSA), the Information Systems Audit and Control Association (ISACA), the Association of Information Technology Professionals (AITP), the Association for Computing Machinery (ACM), the Institute of Electrical and Electronic Engineers (IEEE), UNIFORUM, CompTIA, Infragard, and others. The center makes every effort to engage in joint activities with these organizations and to encourage them to engage with the center whenever possible.

Illinois Institute of Technology has been designated as a National Center of Academic Excellence in Cyber Defense Education by the National Security Agency and the U.S. Department of Homeland Security. This designation results from meeting stringent Center of Academic Excellence criteria and mapping of information technology and management curricula to a core set of cyber defense knowledge units. Students attending Center of Academic Excellence in Cyber Defense Education institutions are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. This designation reflects Illinois Institute of Technology's commitment to producing professionals with cyber defense expertise for the nation.

Resources for education and research as well as published student and faculty research in the form of technical reports and white papers are available on the center's website (appliedtech.iit.edu/c2safe).

Degree Programs

- Bachelor of Information Technology and Management
- Bachelor of Information Technology and Management: Transfer Program
- Bachelor of Science in Applied Cybersecurity and Information Technology

Co-Terminal Options

The Department of Information Technology and Management also offers the following co-terminal degrees, which enables a student to simultaneously complete both an undergraduate and graduate degree in as few as five years:

- Bachelor of Information Technology and Management/Master of Cyber Forensics and Security
- Bachelor of Information Technology and Management/Master of Information Technology and Management
- Bachelor of Information Technology and Management/Master of Science in Cybersecurity and Digital Forensics
- Bachelor of Science in Cybersecurity and Information Technology /Master of Science in Cybersecurity and Digital Forensics

These co-terminal degrees allow students to gain greater knowledge in specialized areas while, in most cases, completing a smaller number of credit hours with increased scheduling flexibility. For more information, please visit the Department of Information Technology and Management website (appliedtech.iit.edu/information-technology-and-management).

Course Descriptions

ITM 100
Introduction to Information Technology as a Profession
Introduces students to the profession of information technology, beginning with concepts of systems, systems theory and modeling, information systems, and system integration. Examines the steps necessary to analyze a business problem and identify and define the computing and information requirements appropriate to its solution, with a focus on how to design, implement, and evaluate a technology-based system to meet desired needs. Students learn to analyze the local and global impact of computing on individuals, organizations, and society. Leads students to recognize of the need for continuing professional development, and imparts an understanding of professional, ethical, legal, security and social issues and responsibilities in information technology. Students write and present, building their ability to communicate effectively with a range of audiences, and using standard planning methodologies design an information system to meet the information needs of a small business.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITM 300
Communication in the Workplace
Review, analyze and practice verbal and written communication formats found in the workplace. Emphasis on developing skills in technical writing and oral presentations using electronic and traditional media. Credit not granted for both ITM 300 and COM 421. INTM 301 may be substituted for this course.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITM 301
Introduction to Contemporary Operating Systems and Hardware I Students study the basics of computer architecture and learn to use a contemporary operating system. Hardware requirements, hardware components, software compatibility, and system installation topics are covered along with post-installation, storage, security and system diagnosis, and repair. Topics also include discussion of current and future technology industry trends.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITM 311
Introduction to Software Development
A broad introduction to object-oriented programming and the related knowledge necessary to program in a contemporary programming language. This would include coverage of an Application Development Kit, a standard integrated Development environment, and the use of GUI components.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITM 312
Introduction to Systems Software Programming
Introduces basic concepts of systems programming. Students learn to apply basic programming concepts toward solving problems, create source files and implement header files, work with and effectively use basic data types, abstract data types, control structures, code modularization and arrays. Students will be introduced to object paradigm including, classes, inheritance, and polymorphism applications.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITM 497
Independent Study
Special projects.
Credit: Variable

ITM 498
Undergraduate Research Immersion: Team
This course provides a faculty-mentored immersive research experience as a part of a student team. Research topics are determined by faculty mentor's area of research.
Lecture: 0 **Lab:** 0 **Credits:** 3

ITMD 361
Fundamentals of Web Development
This course will cover the creation of Web pages and sites using HTML, CSS, Javascript, jQuery, and graphical applications as well as the client and server architecture of the Internet and related web technologies. The creation and deployment of modern, standards- compliant web pages are addressed. Students create and deploy a Web site with multiple pages and cross-linked structures.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 362
Human-Computer Interaction and Web Design
Students in this course will learn the importance of human-computer interaction design and the effectiveness of user-centered design. The course will cover a survey of methods frequently used by the HCI profession, such as usability testing and prototyping, as well as general design principles and how to use design guidelines. A particular emphasis will be placed on usability for Web site engineering, and students will apply knowledge from the field in the design and construction of user-centered Web sites.
Prerequisite(s): [(ITMD 361)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 411
Intermediate Software Development
This course covers a broad spectrum of object-oriented programming concepts and application programming interfaces. The student considers the details of object-orientated development in topics of multi-threading, data structure collections, stream I/O and client interfaces. Software engineering topics of packaging and deployment are covered as well. Hands-on exercises reinforce concepts taught throughout the course.
Prerequisite(s): [(ITM 311 and ITM 312)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 412
Advanced Structured and Systems Programming
Structured programming continues with advanced concepts including strings, arrays, pointers, data structures, file manipulation, and dynamic memory management. Students create more complex applications that work with user input, manipulate user supplied text or text obtained from a file, apply standard library routines for working with literal text, use pointers to store complex structures within arrays, and read and write data from files, the console, and the terminal. The object-oriented programming (OOP) paradigm is covered in depth including the philosophy of OOP, classes and objects, inheritance, template classes, and making use of class libraries.
Prerequisite(s): [(ITM 312)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 413
Open Source Programming
Contemporary open-source programming languages and frameworks are presented. The student considers design and development topics in system, graphical user interface, network, and web programming. Dynamic scripting languages are covered using object-oriented, concurrent, and functional programming paradigms. Concepts gained throughout the course are reinforced with numerous exercises which will culminate in an open-source programming project.
Prerequisite(s): [(ITMD 411)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 415
Advanced Software Development
This course considers Web container application development for enterprise systems. The primary focus is on database connectivity (JDBC) integration with Web application programming using an enterprise-level application framework. A Web application term project considers the design and implementation of a database instance that serves as the information tier in a contemporary 3-tier enterprise solution.
Prerequisite(s): [(ITMD 411)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 419
Topics in Software Development
This course will cover a particular topic in software development, 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 ITMD 419/519 credit may be applied to a degree. **Credit:** Variable

ITMD 421
Data Modeling and Applications
Basic data modeling concepts are introduced. Hands-on database design, implementation, and administration of single-user and shared multi-user database applications using a contemporary relational database management system.
Lecture: 2 **Lab:** 2 **Credits:** 3

iTMD 422
Advanced Database Management
Advanced topics in database management and programming including client server application development are introduced. Expands knowledge of data modeling concepts and introduces object-oriented data modeling techniques. Students will learn the use of Structured Query Language in a variety of application and operating system environments.
Prerequisite(s): [(ITMD 421)]
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMD 453
Enterprise Intelligent Device Applications
Intelligent device application development is covered with proprietary enterprise and open-source technologies on media device, mobile, and robotic platforms. Utilizing contemporary toolkits, the student considers design and development on simulated and real "smart" devices including smart phones, tablets, sensors, actuators, drones, and robots. Numerous exercises reinforce concepts gained throughout the course. A term project will integrate course topics into a comprehensive intelligent device application.
Prerequisite(s): [(ITM 311)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 454
Mass-Market Intelligent Device Applications
Intelligent device application development is covered with leading mass-market and open-source technologies on media device, mobile, and robotic platforms. Utilizing contemporary toolkits, the student considers design and development on simulated and real "smart" devices including smart phones, tablets, sensors, actuators, drones, and robots. Numerous exercises reinforce concepts gained throughout the course. A term project will integrate course topics into a comprehensive intelligent device application.
Prerequisite(s): [(ITM 312)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 455
Open-Source Intelligent Device Applications
Intelligent device application development is covered with various technologies on mobile and robotic platforms. Utilizing contemporary toolkits, the student considers design and development on emulated and real "smart" devices including smart phones, personal digital assistants, sensors, actuators, and robots. Numerous exercises reinforce concepts gained throughout the course. A term project will integrate course topics into a comprehensive intelligent device application.
Prerequisite(s): [(ITM 311)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 460
Fundamentals of Multimedia
Students are introduced to computer-based multimedia theory, concepts, and applications. Topics include desktop publishing, hypermedia, presentation graphics, graphic images, animation, sound, video, multimedia on the World Wide Web and integrated multimedia authoring techniques.
Lecture: 2 **Lab:** 2 **Credits:** 3
Satisfies: Communications (C)

ITMD 462
Web Site Application Development
Programming the Common Gateway Interface (CGI) for Web pages is introduced with emphasis on creation of interfaces to handle HTML form data. CGI programming is taught in multiple languages. Security of Web sites is covered with an emphasis on controlled access sites. Setup, administration and customization of content management systems including blog and portal sites is introduced. Students design and create a Web site including basic CGI programs with Web interfaces and process data flows from online forms with basic database structures.
Prerequisite(s): [(ITMD 361)]
Lecture: 2 **Lab:** 2 **Credits:** 3
Satisfies: Communications (C)

ITMD 463
Intermediate Web Application Development
In-depth examination of the concepts involved in the development of Internet applications. Students will learn the differences and similarities between Internet applications and traditional client/ server applications. A discussion of the technologies involved
in creating these Internet applications is included, and students will learn to use these technologies to create robust server-side applications.
Prerequisite(s): [(ITMD 361)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 464
Advanced Web Application Development
Strategies for management of electronic commerce allow students to learn to re-engineer established business processes to increase enterprise competitive advantage, provide better customer service, reduce operating costs, and achieve a better return on investment. Students will learn to evaluate, use, and deploy state-of-the-art tools and techniques needed to develop a reliable e-commerce offering on the Web. The course will cover state-of-the-art programming and development tools. This class will provide students with hands-on exposure needed to design and build a fully functional e-commerce Web site.
Prerequisite(s): [(ITMD 463)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 465
Rich Internet Applications
Students learn to create interactive rich internet applications using web development frameworks, applications, and techniques that primarily operate on the client-side. These applications often exhibit the same characteristics as desktop applications and are typically delivered through a standards-based web browser via a browser plug-in or independently via sandboxes or virtual machines. Current software frameworks used to download, update, verify, and execute these applications are addressed as well as writing applications for deployment in these frameworks.
Prerequisite(s): [(ITMD 361)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 466
Service-Oriented Architecture
This course covers IT enterprise systems employing web services technologies in SOA and ESB architectural patterns. The student considers SOA which defines and provisions IT infrastructure and allows for a loosely-coupled data exchange over disparate applications participating in business processes. The simplification of integration and flexible reuse of business components within SOA is greatly furthered by ESB. Lab exercises using contemporary tool- kits are utilized to reinforce platform-agnostic course topics.
Prerequisite(s): [(ITMD 361 and ITMD 411)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 467
Web Systems Integration
In this project-based course, student teams will build an enterprise- grade website and web infrastructure integrating server-side applications, databases, and client-side rich internet applications as a solution to a defined business problem.
Prerequisite(s): [(ITMD 462 and ITMD 465)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMD 469
Topics in Application Development
This course will cover a particular topic in application development, 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 ITMD 469/569 credit may be applied to a degree. **Credit:** Variable

ITMM 464
Social Media Marketing
Class participants will explore the tactics, tools, and strategies of incorporating new media channels to successfully grow a business and/or to maximize the goals of other types of organizations.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMM 470
Fundamentals of Management for Technology Professionals
This course explores fundamentals of management for professionals in high-technology fields. It addresses the challenges of the following: managing technical professionals and technology assets; human resource management; budgeting and managerial accounting; management of services, infrastructure, outsourcing, and vendor relationships; technology governance and strategy; and resource planning.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMM 471
Project Management for Information Technology and Management Basic principles of project management are taught with a particular focus on project planning for information technology hardware, software and networking project implementation. Management of application development and major Web development projects will also be addressed.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMM 481
Information Technology Entrepreneurship
This course prepares students to become leaders in information technology and to build ITM companies. Students design and develop a prototype ITM product and prepare a business plan and venture proposal presentation.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMM 482
Business Innovation
This course is designed to teach innovative thinking through theory, methods, and practice of innovation. The course incorporates Einstein's thinking, and Edison's method to establish the innovation process that can be applied in current business environment. Current economic conditions and global sourcing requires that innovation becomes a leading tool for developing a competitive edge. Innovation has been considered a competency of educated, design engineering, and a selected few employees that has become insufficient today. Corporations and organizations need innovation to develop customer-specific solutions in almost real time.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMM 485
Legal and Ethical Issues in Information Technology
Current legal issues in information technology are addressed including elements of contracting, payment systems and digital signatures, privacy concerns, intellectual property, business torts, and criminal liability including hacking, computer trespass and fraud. Examination of ethical issues including privacy, system abuse, and ethical practices in information technology equip students to make sound ethical choices and resolve legal and moral issues that arise in information technology.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMO 417
Shell Scripting for System Administration
Focuses on preparation of shell scripts to enhance and streamline system administration tasks in all contemporary server operating systems. Scripting will be taught in both native and portable environments. The course will address shell programming, regular expressions, common and system-specific shell utilities and built-in commands, user defined and shell variables, flow control structures, shell functions, and the creation and execution of shell scripts.
Homework and hands-on exercises will provide practical experience in contemporary server environments. Same as ITMO 517.
Prerequisite(s): [(ITMO 456)]
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMO 433
Enterprise Server Administration
Students learn to set up, maintain, and administer X86-based servers and associated networks using a contemporary industry-standard proprietary operating system. Topics include hardware requirements; software compatibility; system installation, configuration and options, and post-installation topics; administrative and technical practices required for system security; process management; performance monitoring and tuning; storage management; back-up and restoration of data; and disaster recovery and prevention. Also addressed is configuration and administration of common network and server services such as DNS, DHCP, remote access, email, basic virtualization, web and web services, and more.
Prerequisite(s): [(ITM 301 and ITMO 440)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 440
Introduction to Data Networks and the Internet
This course covers current and evolving data network technologies, protocols, network components, and the networks that use them, focusing on the Internet and related LANs. The state of worldwide networking and its evolution will be discussed. This course covers the Internet architecture, organization, and protocols including Ethernet, 802.11, routing, the TCP/UDP/IP suite, DNS, SNMP, DHCP, and more. Students will be presented with Internet-specific networking tools for searching, testing, debugging, and configuring networks and network-connected host computers. There will be opportunities for network configuration and hands-on use of tools. **Lecture:** 3 **Lab:** 0 **Credits:** 3

ITMO 441
Network Administration and Operations
Students learn the details, use, and configuration of network applications. Currently protocols and application technologies considered include SNMP, SMTP, IMAP, POP, MIME, BOOTP, DHCP, SAMBA, NFS, AFS, X, HTTP, DNS, NetBIOS, and CIFS/SMB. Windows workgroups and domains: file and printer sharing, remote access, and Windows networking are addressed. A research paper in the above topic areas is required.
Prerequisite(s): [(ITMO 440) OR (ITMO 540 with min. grade of C)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 444
Cloud Computing Technologies
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.
Prerequisite(s): [(ITMD 411 and ITMO 456)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 450
Enterprise End-User System Administration
Students learn to set up, configure, and maintain end-user desktop and portable computers and devices in an enterprise environment using a contemporary proprietary operating system, including the actual installation of the operating system in a networked client- server environment. User account management, security, printing, disk configuration, and backup procedures are addressed with particular attention to coverage of networked applications. System installation, configuration, and administration issues as well as network file systems, network access, and compatibility with other operating systems are also addressed.
Administration of central server resources associated with management and provisioning of end-user systems in workgroups, domains, or forests is also addressed.
Prerequisite(s): [(ITM 301)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 453
Open Source Server Administration
Students learn to set up, configure, and administer an industry-standard open source server operating system including integration with client systems using a variety of operating systems in a mixed environment. Topics include hardware requirements; software compatibility; administrative and technical practices required for system security; process management; performance monitoring and tuning; storage management; back-up and restoration of data; and disaster recovery and prevention. Also addressed are configuration and administration of common network and server services such as DNS, DHCP, firewall, proxy, remote access, file and printer sharing, email, web, and web services as well as support issues for open source software.
Prerequisite(s): [(ITMO 440 and ITMO 456)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 454
Operating System Virtualization
This course will cover technologies allowing multiple instances of operating systems to be run on a single physical system. Concepts addressed will include hypervisors, virtual machines, paravirtualization and virtual appliances. Both server and desktop virtualization will be examined in detail, with brief coverage of storage virtualization and application virtualization. Business benefits, business cases and security implications of virtualization will be discussed. Extensive hands-on assignments and a group project will allow students to gain first-hand experience of this technology.
Prerequisite(s): [(ITM 301) OR (ITMO 456)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMO 456
Introduction to Open Source Operating Systems
Students learn to set up and configure an industry-standard open source operating system including system installation and basic system administration; system architecture; package management; command-line commands; devices, filesystems, and the filesystem hierarchy standard. Also addressed are applications, shells, scripting and data management; user interfaces and desktops; administrative tasks; essential system services; networking fundamentals; and security, as well as support issues for open source software.
Multiple distributions are covered with emphasis on the two leading major distribution forks.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 418
Coding Security
This course examines security architecture elements within modern object-oriented programming languages that create the framework for secure programming. Analysis of components and services with their inherent strength and weaknesses give rise to common coding security challenges. An exploration of identity management, encryption services and common hacking techniques will enable the student's ability to develop secure code. Homework assignments and projects will reinforce theories taught.
Prerequisite(s): [(ITMD 411)]
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 428
Database Security
Students will engage in an in-depth examination of topics in data security including security considerations in applications and systems development, encryption methods, cryptography law and security architecture and models.
Prerequisite(s): [(ITMD 421)]
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 438
Digital Forensics
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.
Prerequisite(s): [(ITMO 456) and (ITMS 448) OR (ITMS 548)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 443
Vulnerability Analysis and Control
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.
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 448
Cyber Security Technologies
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.
Prerequisite(s): [(ITMO 440) OR (ITMO 540)]
Lecture: 2 **Lab:** 2 **Credits:** 3
Satisfies: Communications (C)

ITMS 458
Operating System Security
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.
Prerequisite(s): [(ITMO 456)]
Lecture: 2 **Lab:** 2 **Credits:** 3

ITMS 478
Cyber Security Management
In-depth examination of topics in the management of information technology security including access control systems and methodology, business continuity and disaster recovery planning, legal issues in information system security, ethics, computer operations security, physical security and security architecture & models using current standards and models.
Lecture: 3 **Lab:** 0 **Credits:** 3
Satisfies: Communications (C)

ITMS 479
Topics in Information Security
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.
Credit: Variable

ITMS 483
Digital Evidence
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, e-mail investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding.
Prerequisite(s): [(ITMS 438)]
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMS 484
Governance, Risk, and Compliance
This course is an in-depth examination of topics in information technology/information security governance, risk, and compliance including information assurance policies, standards, and compliance as well as the examination of security risk analysis and the performance of systems certification and accreditation.
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMT 430
System Integration
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 requirements using business process models and will learn and apply key systems 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.
Prerequisite(s): [(ITMD 411, ITMD 421, ITMD 434, ITMD 461, ITMM 471, ITMO 440, and ITMO 456)]
Lecture: 2 **Lab:** 2 **Credits:** 3
Satisfies: Ethics (E)

ITMT 491
Undergraduate Research
Undergraduate research. Written consent of instructor is required.
Credit: Variable

ITMT 492
Embedded Systems and Reconfigurable Logic Design
This course covers reconfigurable intelligent devices programmed with modern high level languages focusing on design and integration to modern environments. The course will also cover 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.
Prerequisite(s): [(ITM 311) OR (ITM 312)]
Lecture: 3 **Lab:** 0 **Credits:** 3

ITMT 495
Topics in Information Technology
This course will cover a particular topic varying from semester to semester in which there is particular student or staff interest.
Credit: Variable

TECH 497
Special Projects
Independent study and projects in applied technology that are multi/ cross-disciplinary not tied to a specific department.
Credit: Variable

BACHELOR OF SCIENCE IN APPLIED CYBERSECURITY AND INFORMATION TECHNOLOGY

All students must complete a minimum of 36 credit hours of courses with a significant written and oral communication component, identified with a (C) in the bulletin; 12 credit hours of (C)-coded courses must be taken in the major.

A maximum of 9 credit hours of ITM graduate courses taken as an undergraduate may be applied to a Master's degree offered by the Department of Information Technology and Management, and any graduate courses taken to fulfill undergraduate degree requirements may not also be applied to a graduate degree unless the student is enrolled in a co-terminal master's degree program.

Required Courses

Information Technology Core Requirements		(33)
ITM 100	Introduction to Information Technology as a Profession	3
ITM 301	Introduction to Contemporary Operating Systems and Hardware	3
ITM 311	Introduction to Software Development	3
ITM 312	Introduction to Systems Software Programming	3
ITMD 361	Fundamentals of Web Development	3
ITMD 362	Human-Computer Interaction and Web Design	3
ITMD 411	Intermediate Software Development	3
ITMD 421	Data Modeling and Applications	3
ITMM 471	Project Management for Information Technology and Management	3
ITMO 440	Introduction to Data Networks and the Internet	3
ITMO 456	Introduction to Open Source Operating Systems	3
Cybersecurity Core Requirements		(27)
ITMM 485	Legal and Ethical Issues in Information Technology	3
ITMS 418	Coding Security	3
ITMS 438	Digital Forensics	3
ITMS 443	Vulnerability Analysis and Control	3
ITMS 448	Cyber Security Technologies	3
ITMS 458	Operating System Security	3
ITMS 478	Cyber Security Management	3
ITMS 483	Digital Evidence	3
ITMT 430	System Integration	3
Cybersecurity and Information Technology Electives		(6)
Select 6 credit hours from ITMD, ITMM, ITMO, ITMS, ITMT, or TECH		6
Mathematics Requirements		(20)
MATH 151	Calculus I	5
MATH 152	Calculus II	5
MATH 230	Introduction to Discrete Math	3
MATH 251	Multivariate and Vector Calculus	4
MATH 474	Probability and Statistics	3
Natural Science and Engineering Requirements		(10)
EG 225 and PHYS 200 are recommended		
See IIT Core Curriculum, section D		10
Humanities and Social Sciences Requirements		(21)
PSYC 301 is recommended		
See IIT Core Curriculum, sections B and C		21
Interprofessional Projects (IPRO)		(6)
See IIT Core Curriculum, section E		6
Free Electives		(6)
Select 6 credit hours		6
Total Credit Hours		129

Bachelor of Science in Applied Cybersecurity and Information Technology Curriculum

Students should be aware that students not completing 30 credit hours of study in their first year will still be classified as a first-year student in the first semester of their second year of study, which may adversely impact some financial aid. Students with issues or questions about this should discuss it with a financial aid counselor.

			Year 1
Semester 1	**Credit Hours**	**Semester 2**	**Credit Hours**
ITM 301	3	ITM 311	3
ITMD 421	3	ITMO 440	3
MATH 151	5	MATH 152	5
Humanities 200-level Elective	3	Social Sciences Elective	3
		Natural Science or Engineering Elective	3
	14		17

			Year 2
Semester 1	**Credit Hours**	**Semester 2**	**Credit Hours**
ITM 100	3	ITMD 362	3
ITM 312	3	ITMD 411	3
ITMD 361	3	ITMO 456	3
MATH 251	4	ITMS 478	3
Natural Science or Engineering Elective	4	MATH 230	3
		Natural Science or Engineering Elective	3
	17		18

			Year 3
Semester 1	**Credit Hours**	**Semester 2**	**Credit Hours**
ITMM 471	3	ITMS 438	3
ITMS 418	3	ITMS 443	3
ITMS 448	3	ITMS 458	3
Humanities Elective (300+)	3	IPRO Elective I	3
Social Sciences Elective (300+)	3	MATH 474	3
Free Elective	3		
	18		15

			Year 4
Semester 1	**Credit Hours**	**Semester 2**	**Credit Hours**
ITMM 485	3	ITMT 430	3
ITMS 483	3	Cybersecurity Elective	3
Cybersecurity Elective	3	Social Sciences Elective (300+)	3
Humanities Elective (300+)	3	IPRO Elective II	3
Free Elective	3	Humanities or Social Sciences Elective	3
	15		15

Total Credit Hours: 129

ITMS 418 Coding Security
Fall 2018

Professor Bonnie A. Goins

Professor: **Bonnie A. Goins**
Address: Department of Information Technology & Management, 10 W. 33rd St., Chicago, IL 60616
Telephone: 630-387-9496
Email: bgoins@iit.edu
Office: Perlstein Hall Suite 225, 10 W. 33rd St.
Office Hours: By appointment.

Course Catalog Description: This course examines security architecture elements within modern object-oriented programming languages that create the framework for secure programming. Analysis of components and services with their inherent strength and weaknesses give rise to common coding security challenges. An exploration of identity management, encryption services and common hacking techniques will enable the student's ability to develop secure code. Homework assignments and projects will reinforce theories taught.. **Prerequisites:** ITMD 411 **Credit:** 3-0-3 Semester Hours

Lecture Day, Time & Place: Day TBD, 6:25pm-9:05pm, room TBD, or online via IIT Online.

Course Objectives: 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.

Schedule of Topics/Readings: ***You should do all readings prior to class.***

Session	Week of	General Topic	Reading
1	August 20	Introduction to Application Security	
2	August 27	OWASP Top Ten	OWASP
3	September 3	OWASP Top Ten Triage	OWASP
4	September 10	OWASP Top Ten Triage	OWASP
5	September 17	Secure SDLC	Microsoft SDL
6	September 24	Application Security Testing	NSA IEM
7	October 1	Application Security Testing	NSA IEM
8	October 8	Application Security Testing	NSA, multiple
9	October 15	Working with the CWE list	mitre.org
10	October 22	Working with CVSS scoring	mitre.org, websites
11	October 29	Writing an Application Security Report	Multiple sources
12	November 5	Responding to Application Security Incidents	NIST, CERT
13	November 12	Responding to Application Security Incidents	NIST, CERT
14	November 19	NO CLASS: THANKGIVING BREAK	
15	November 26	Wrap –Up and ***Final Exam Review***	
Exam	December 3	***Take home final due at 9:05 p.m. December 7***	

Course Outcomes: When you complete this course, you should be able to:

- Describe basic concepts of application security
- Identify and describe the OWASP Top Ten application vulnerabilities
- Describe how the Top Ten vulnerabilities manifest in code and how to successfully treat them
- Recall the concepts involved in the secure software/system development lifecycle
- Work with authoritative sources, such as MITRE's lists and scoring systems, for application security weaknesses and exposures
- Describe the application security assessment process
- Write an appropriate application security report
- Respond to application security vulnerabilities.

Course Materials: Slide decks and/or readings will be assigned by the instructor and posted to Blackboard for students to download.

Readings: Readings are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings are assigned by topic above. Online resources will be linked from Blackboard or will be posted on Blackboard.

ITMS 418 Coding Security
Fall 2018 Professor Bonnie A. Goins

Course Notes: Copies of any course lecture materials/slides decks will be available on Blackboard.

Course Web Site: http://blackboard.iit.edu/ Additional websites may be added as the course progresses. These links will be added to Blackboard.

Blackboard: The course will make intensive use of Blackboard (http://blackboard.iit.edu/)

Attendance: If you are in a live section of the class (-01) and will not be able to attend class, please notify me via email prior to class time. Live section students who miss a class should always watch the lecture online.

Assignments: There will be homework required for this class. Homework will be assigned after each major topic, at instructor's discretion, through the Grade Center section of Blackboard. Homework must be turned in one week after assignment for the full grade; 10% of the homework value (based on the full point value possible for the assignment) will be deducted for each day the homework is submitted after the due date, up to one week. ***Homework will NOT be accepted for credit if submitted later than one week after the original due date; NO EXCEPTIONS.*** Students will have AT MOST two (2) attempts to submit each homework assignment; resubmissions will only be accepted for two week after the initial due date. ***No additional rework will be accepted for grading after the second attempt; NO EXCEPTIONS.*** Homework must be satisfactorily completed in order for students to pass this course and will count for 50% of your grade.

Examinations: The final examination will consist of a take-home exam. The exam will be posted on Blackboard for you to download; students will have one week to complete the exam and may use any reference materials, with the exception of other students or professors, to complete the exams. Because the exam is administered as an open book exam, grading will be more rigorous for this final. This exam will count for 50% of your grade. The final exam must be satisfactorily completed in order for students to pass this course. ***The exam MUST be submitted by the stated deadline, December 7 at 9:05 pm. Late exams will NOT be accepted; NO EXCEPTIONS.***

Extensions: Extensions ("I") can be granted to students not turning in required materials by the due date with a sufficient reason for the request, such as workload at a job or due to serious illness. ***Requests for Incompletes must be requested to the instructor no later than two weeks prior to the end of class, with a valid reason submitted; NO EXCEPTIONS.***

Academic Honesty: All work you submit in this course **must be your own.**

Plagiarism: You must fully attribute **all** material directly quoted in assignments and exams and you must document all sources used in the preparation using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. If you submit plagiarized material you **WILL** receive a grade of **ZERO** for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. **There is no excuse for not understanding this policy** and if you do not understand it please let me know and I will be happy to discuss it with you until you do.

Collaboration: Students may only collaborate on assignments or projects that are explicitly designated as group assignments or projects. Students submitting work that is identical or in some cases even substantively the same will be asked to discuss the assignment with me. If one student admits to having copied the work, or if there is clear evidence who is guilty, the guilty student will be assigned a grade of zero. If no one admits to the offense or a reasonable determination of guilt cannot be made, each student involved will be assigned a grade of zero. In either case, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies.

Grading: Grading criteria for ITMS 483 students will be as follows:

A	*Outstanding work reflecting substantial effort*	90-100%
B	*Excellent work reflecting good effort*	80-89.99%
C	*Satisfactory work meeting minimum expectations*	70-79.99%
D	*Substandard work not meeting expectations*	60-69.99%
E	*Unsatisfactory work*	0-59.99%

The final grade for the class will be calculated as follows:

Assignments	**50%**
Final Exam	**50%**

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312 567.5744 or disabilities@iit.edu.

ITMS 438 Digital Forensics
Spring 2018

Professor Bill Lidinsky

Professor: **Bill Lidinsky**
Address: ITM Department, 201 E Loop Rd., Wheaton, IL 60189
Telephone: 630-682-6028
Fax: 630-682-6010
Email: lidinsky@iit.edu
Office: Room 225 at IIT's Rice campus
Office Hours: Mondays & Wednesdays, 3:30pm-4:30pm. Other times by appointment.

Course 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.
Prerequisites: ITMO 456 and ITMS 448 **Credit:** 2-2-3 Semester Hours

Lecture Day, Time & Place: Day TBD, 5:50pm-9:05pm, room 250 Rice Campus. Lectures and labs will be conducted in an integrated fashion.

Course Objectives: Objectives and outcomes should be considered close to but not exhaustive. Because of rapidly changing technology, a modest amount of material will likely be added or modified. Each successful student in this course will be able to demonstrate knowledge of cyber forensic analysis at a professional level including applicable legal issues, apply this knowledge to planning and executing specific cyber forensic analyses—this includes the use of cyber forensic tools—and will demonstrate knowledge of steganography and steganalysis and apply it to determination of existence of covert information. Students satisfactorily completing this course will have the knowledge, ability and tools to perform cyber forensic analysis.

Schedule of Topics:

Session	Week of	General Topic
1	January 8	Course Introduction. ForSec Lab Discussion. Introduction to Network & Computer Forensics
2	January 15	Computer Investigations. Forensic Tools and Tool systems
3	January 22	Certification: Investigator and Laboratory. Data Acquisition & Image Creation
4	January 29	Q&A: Proc. Crimes & Incidents. 04aLab: Do a crime forensic analysis
5	February 5	Volumes & Partitions
6	February 12	Q&A: Hard Disks, Volumes, Partitions Lec: MBR Partitions.
7	February 19	Lec: GPT Partitions. FAT File system.
8	February 26	Lec: NTFS File system. Review for midterm exam
9	March 4	**Midterm Exam** (2 parts). 1. Timed exam taken in class. 2. Hands on forensic examination of flash drive (take home) Lec: Flash File systems
10	March 12	**NO CLASS: Spring Break**
11	March 19	Linux Boot & Disk & Partition. Linux File Systems
12	March 22	Web Forensics. Internet Forensics
13	April 2	File formats: Image. audio, video, document. Steganography & steganalysis.
14	April 9	RAM forensics
15	April 16	Data carving
16	April 23	Class replaced by required attendance at ForenSecure18. The final exam will include questions derived from the ForenSecure18 conference. Final Exam review provided on line.
Exam	Week of April 30	Final Examination as per IIT Final Exam Schedule

ITMS 438 Digital Forensics
Spring 2018

Professor Bill Lidinsky

Textbook: The textbooks for this course are **mandatory.** Previous editions are not acceptable.

B. Nelson, A. Phillips, C. Steuart, *Guide to Computer Forensics and Investigations, 5th edition* Course Technology, Cengage Learning ISBN-13: 978-1-285-06003-3. Includes 1 DVDROM. Publication date: 2016

B. Carrier, *File System Forensic Analysis,* Addison Wesley ISBN-13: 978-0321268174; ISBN10: 0-32-126817-2 Publication date: 2005

Readings: Readings for the class will be assigned from the textbook as well as in the form of handouts or online reading. It is essential that you do all readings before coming to class on the assigned date. Readings are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings will be assigned in Blackboard. Online resources will be linked from Blackboard or will be posted on Blackboard.

Course Outcomes: When you complete this course, you 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, as well as several forensic imaging, carving and discovery tools.

Course Web Site: http://blackboard.iit.edu/

Blackboard: The course will make use of Blackboard (http://blackboard.iit.edu/) for communications, assignment submissions, group project coordination, providing online resources and administering examinations.

Guest Speakers: Guest speakers may be featured as part of course topics. When a guest speaker is expected you should make an extra effort to be seated and ready prior to class time. A question & answer/discussion period will be held at the end of each speaker's presentation.

Attendance: If you will not be able to attend class, please notify me via email prior to class time.

Assignments: Assignments will be made on a week-by-week basis. All assignments will be submitted via Blackboard in pdf format. Also, unless otherwise specified, assignments will be due on or before 11:55 pm on the 2nd Sunday following the date that they were assigned. This should accommodate most extenuating circumstances that students may encounter. Assignments will generally correspond to the lecture topics, which in turn will correspond to the texts, modified by rapidly evolving technology. The evolving nature of operating systems, data networks and Digital Forensics requires continual upgrading of labs and assignments.

Quizzes: I may give quizzes at my discretion and may use them for verification that you have completed assigned reading. As they are discretionary, the weight of quizzes in grading is also left to my discretion and will be included in your class participation grade.

Examinations: The course will include a 2-part midterm examination and a final examination.

Class and Lab Resources: The take home lab assignments will make use of RADISH (Remotely Accessible Distributed Internet for Students to Hack). RADISH allows students to do many hands-on labs remotely. (RADISH was developed by forensic and security students at IIT.)

Arrangements have been made with several cyber forensic vendors for the use of expensive forensic analysis tools and software in the ForSec Lab. While these tools and software are limited to ForSec Lab use, RADISH allows many of them to be used remotely.

You will need very good Internet access in order to be able to access RADISH.

Other Class Resources: Online readings and other class resources may be found at on Blackboard.

ITMS 438 Digital Forensics
Spring 2018 Professor Bill Lidinsky

Academic Honesty: All work you submit in this course **must be your own.**

Plagiarism: You must fully attribute **all** material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. If you submit plagiarized material you **WILL** receive a grade of **ZERO** for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. **There is no excuse for not understanding this policy** and if you do not understand it please let me know and I will be happy to discuss it with you until you do.

Collaboration: Students may only collaborate on assignments or projects that are explicitly designated as group assignments or projects. Students submitting work that is identical or in some cases even substantively the same will be asked to discuss the assignment with me. If one student admits to having copied the work, or if there is clear evidence who is guilty, the guilty student will be assigned a grade of zero. If no one admits to the offense or a reasonable determination of guilt cannot be made, each student involved will be assigned a grade of zero. In either case, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies.

Grading: Grading criteria for ITMS 438 students will be as follows:

A	*Outstanding work reflecting substantial effort*	90-100%
B	*Excellent work reflecting good effort*	80-89.99%
C	*Satisfactory work meeting minimum expectations*	70-79.99%
D	*Substandard work not meeting expectations*	60-69.99%
E	*Unsatisfactory work*	0-59.99%

The final grade for the class will be calculated as follows:

Assignments	**35%**
Mid-Term Exam	**30%**
Final Exam	**30%**
Quizzes/Class Participation	**5%**

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312 567.5744 or disabilities@iit.edu.

ITMS 483 Digital Evidence
Spring 2018

Professor Shawn Davis

Professor: **Shawn Davis**
Address: Department of Information Technology & Management, 10 W. 33rd St., Chicago, IL 60616
Telephone: 312.248.3454
Email: sdavis17@iit.edu
Office: Perlstein Hall Suite 225, 10 W. 33rd St.
Office Hours: By appointment in person, or online via *GoogleHangout* (username *sdavis17@iit.edu*) or by telephone to 312.248.3454

Course 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, e-mail investigations, applicable case law, and appearance as an expert witness in a judicial or administrative proceeding. **Prerequisites:** ITMS 438 Cyber Forensics **Credit:** 3-0-3 Semester Hours

Lecture Day, Time & Place: Day TBD, 6:25pm-9:05pm, room TBD, or online via IIT Online.

Course Objectives: 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 support digital investigations in full compliance with applicable law, policy, and regulations, and present the investigative results as an expert witness.

Schedule of Topics/Readings: ***You should do all readings prior to class.***

Session	Week of	General Topic	Reading
1	January 8	Introduction to Legal Concepts and Terminology	Online
2	January 15	Introduction to Digital Evidence	Chapter 1
3	January 22	History and Ethics of E-discovery and Digital Evidence	Chapter 2
4	January 29	Planning and Tools	Chapter 3
5	February 5	Experts in Digital Evidence and E-Discovery	Chapter 4
6	February 12	Cybercrime, Evidence, and the Law *Research paper 1 due*	Online
7	February 19	Digital Evidence Case Flow	Chapter 5
8	February 26	Technical Evidence Collection Procedures and Dos & Don'ts	Online
9	March 4	Case Study: From Beginning to Trial	Chapter 6
10	March 12	**NO CLASS: Spring Break**	
11	March 19	Information Governance and Litigation Preparedness	Chapter 7
12	March 22	Project Definition and Parameters	Online
13	April 2	Presenting Digital Evidence in Court	Online
14	April 9	Digital Evidence Case Law *Research paper 2 due*	Chapter 8
15	April 16	The Future of Digital Evidence/Exam Review	Chapter 9
16	April 23	Project Class Presentations	
Exam	Week of April 30	Final Examination as per IIT Final Exam Schedule	

Textbook: The textbook for this course is **mandatory.** Previous editions are not acceptable.
Phillips, Amelia; Godfrey, Ronald; Steuart, Christopher; Brown, Christine: *E-discovery: An Introduction to Digital Evidence*, Course Technology Incorporated, 2014, ISBN 9781111310646; an eBook version is available at https://www.vitalsource.com/referral?term=9781285961286

Readings: Readings for the class will be assigned from the textbook as well as in the form of handouts or online reading. It is essential that you do all readings before coming to class on the assigned date. Readings are a necessary and integral part of the class and will form the basis for any class discussions on the topic. Specific readings are assigned by topic above. Online resources will be linked from Blackboard or will be posted on Blackboard.

ITMS 483 Digital Evidence
Spring 2018 Professor Shawn Davis

Course Outcomes: When you complete this course, you should be able to:

- 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.
- Recall and identify types of computer and Internet crimes.
- Preserve and process a crime scene involving digital evidence.
- Describe the legal procedures and standards in the collection and analysis of digital evidence.
- Assist in the preparation of 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.

Course Notes: Copies of the course lecture notes in the form of a PDF of the PowerPoint presentation accompanying each lecture will be provided for each student on Blackboard. This should be useful if you must miss a class. You should be aware that note taking is encouraged and should help your understanding of the material.

Course Web Site: http://blackboard.iit.edu/

Blackboard: The course will make intensive use of Blackboard (http://blackboard.iit.edu/) for communications, assignment submissions, group project coordination, providing online resources and administering examinations. All remote students will view the course lectures online via Blackboard, and online readings will be found on Blackboard.

Guest Speakers: Guest speakers may be featured as part of course topics. When a guest speaker is expected you should make an extra effort to be seated and ready prior to class time. A question & answer/discussion period will be held at the end of each speaker's presentation.

Attendance: If you are in a live section of the class (-01) and will not be able to attend class, please notify me via email or by text message to 312.248.3454 prior to class time. Live section students who miss a class should always watch the lecture online.

Assignments: There will be two assignments for this class.

Assignment 1: Two short research papers addressing topics in digital evidence and e-discovery. The papers can be a solution to a problem in digital evidence, a discussion of an e-discovery strategy or a case study. The papers will be five to seven pages long, double-spaced. Instructions for submission of the papers will be included with the assignment on Blackboard. You must fully attribute all material directly quoted and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. *Failure to format your bibliography entries in APA style will result in an automatic reduction of one letter grade for this assignment.* No more than thirty-three percent of material included in any paper may be direct quotes. No more than sixty percent of the resources cited may be from online. However, online ebooks that have a corresponding print version and PDF files located online count as—and should be cited as—print sources. *Wikipedia* may not be cited. The papers will be due the weeks of February 12 and April 9.

Note for Assignment 1: I will not provide topics for research papers. Topic selection is an important part of the research process. There is an enormous and expansive variety of topics in this field and with a little work on your part arriving at a topic should not be difficult at all. Topics should be very specific as you will be covering it in a relatively short amount of writing and you want to reflect an in-depth coverage of your topic which you can not do with a very broad topic.
TL;DR: Pick your own research paper topic. Broad topic = <u>bad</u>; specific, narrow topic = <u>good</u>.

Assignment 2: A digital evidence project conducted in teams, to be defined and assigned via a Blackboard entry. The project will be due the week of April 23.

Quizzes: I may give quizzes at my discretion and may use them for verification that you have completed assigned reading. As they are discretionary, the weight of quizzes in grading is also left to my discretion and will be included in your class participation grade. Quizzes will be online via Blackboard.

Examinations: The final examination will consist of a take-home essay section and an in-class multiple choice examination measuring course outcomes as discussed above. Internet students will arrange for examination proctoring through IIT Online.

Academic Honesty: All work you submit in this course **must be your own.**

Plagiarism: You must fully attribute **all** material directly quoted in papers and you must document all sources used in the preparation of the paper using complete, APA-style bibliographic entries. Including directly quoted material in an assignment without attribution is always plagiarism and will always be treated as such by me. No more than thirty-three percent of material included in any paper may be direct quotes. If you submit plagiarized material you **WILL** receive a grade of **ZERO** for the assignment, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies. **There is no excuse for not understanding this policy** and if you do not understand it please let me know and I will be happy to discuss it with you until you do.

Collaboration: Students may only collaborate on assignments or projects that are explicitly designated as group assignments or projects. Students submitting work that is identical or in some cases even substantively the same will be asked to discuss the assignment with me. If one student admits to having copied the work, or if there is clear evidence who is guilty, the guilty student will be assigned a grade of zero. If no one admits to the offense or a reasonable determination of guilt cannot be made, each student involved will be assigned a grade of zero. In either case, an Academic Honesty Violation Report will be filed, and it may result in your expulsion from the course with a failing grade as per the IIT and ITM academic honesty policies.

Grading: Grading criteria for ITMS 483 students will be as follows:

A	*Outstanding work reflecting substantial effort*	90-100%
B	*Excellent work reflecting good effort*	80-89.99%
C	*Satisfactory work meeting minimum expectations*	70-79.99%
D	*Substandard work not meeting expectations*	60-69.99%
E	*Unsatisfactory work*	0-59.99%

The final grade for the class will be calculated as follows:

Assignment 1	**30%**
Assignment 2	**30%**
Final Exam	**30%**
Quizzes/Class Participation	**10%**

Other Class Resources: Online readings and other class resources may be found at on Blackboard.

Our Contract: This syllabus is my contract with you as to what I will deliver and what I expect from you. If I change the syllabus, I will issue a revised version of the syllabus; the latest version will always be available on Blackboard. Revisions to readings and assignments will be communicated via Blackboard.

Disabilities: Reasonable accommodations will be made for students with documented disabilities. In order to receive accommodations, students must obtain a letter of accommodation from the Center for Disability Resources and make an appointment to speak with me as soon as possible. My office hours are listed on the first page of the syllabus. The Center for Disability Resources (CDR) is located in 3424 S. State St., room 1C3-2 (on the first floor), telephone 312 567.5744 or disabilities@iit.edu.

Bachelor of Science in Applied Cybersecurity and Information Technology Assessment Plan, 2018-2019

Assessment plans for 2018-2019 will adhere to the rubric as defined by the IIT Assessment Report Evaluation Rubric. One or two program educational objectives and four to five student outcomes will be assessed each term, and all objectives and outcomes will be assessed at least once in each three-year cycle. The full list of objectives and outcomes follows beginning on page 2 below. In addition to the objectives and outcomes listed below, course objectives for each course will be assessed.

Fall 2018:
Program Educational Objectives Assessed: 3, 4
Student Outcomes Assessed: (c), (d), (g), (h)
Student Artifacts: Survey / November 2018 / Evaluation by ITM Curriculum Committee
Assignments / December 2018 / Evaluators: TBD
Courses assessed:

Curricular Area	***Course***
Digital Investigation	ITMS 483 Digital Evidence
System Security	ITMS 448 Cyber Security Technologies
Management	ITMS 478 Cyber Security Management

Spring 2019:
Program Educational Objectives Assessed: 1, 2
Student Outcomes Assessed: (a), (b), (c), (f)
Student Artifacts: Survey / April 2019 / Evaluation by ITM Curriculum Committee
Assignments / May 2019 / Evaluators: TBD
Courses assessed:

Curricular Area	***Course***
Web Design and HCI	ITMD 362 Human Computer Interaction & Web Design
Software Development	ITMD 411 Intermediate Software Development
Systems	ITMT 430 System Integration

The following program education objectives will be evaluated for HLC and ABET accreditation purposes.

The Bachelor of Science in Applied Cybersecurity and Information Technology degree produces graduates who are able to:

Program Educational Objective	Required Courses Supporting the Objective
1. Problem solve and create innovative answers to provide technology solutions for the problems of business, industry, government, non-profit organizations, and individuals.	ITMD 411 Intermediate Software Development ITMD 421 Data Modeling & Applications ITMT 430 Systems Integration IPRO 3/497 Interprofessional Project (Not assessed by the department)
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.	ITM 311 Introduction to Software Development ITMD 362 Human-Computer Interaction and Web Design ITMO 440 Introduction to Data Networking & the Internet ITMO 456 Introduction to Open Source Operating Systems (Not included in assessment cycle as role is very narrow) ITMS 448 Cyber Security Technologies ITMT 430 Systems Integration
3. Design and implement an enterprise security program using both policy and technology to implement technical, operational, and managerial controls, which will technically secure enterprise information assets and resources to deter, detect, and prevent the success of attacks and intrusions.	ITMS 443 Vulnerability Analysis and Control ITMS 448 Cyber Security Technologies ITMS 478 Cyber Security Management
4. Investigate information security incidents and violation of law using computer resources in a manner such that all evidence is admissible in a court of law.	ITMS 438 Digital Forensics ITMS 483 Digital Evidence
5. Apply current technical and mathematical concepts and practices in the core information technologies and recognize the need to engage in continuing professional development.	ITM 100 Introduction to Information Technology as a Profession ITMD 411 Intermediate Software Development ITMD 421 Data Modeling & Applications ITMM 471 Project Management for ITM ITMO 440 Introduction to Data Networking & the Internet ITMT 430 Systems Integration

The following student outcomes will be evaluated for ABET accreditation purposes:

Students completing the Bachelor of Science in Applied Cybersecurity and Information Technology will be able to:

Student Outcomes	Required Courses Supporting the Outcome
(a) Analyze a problem, and identify and define the computing requirements appropriate to its solution	ITM 311 Introduction to Software Development ITM 312 Introduction to Systems Software Programming| ITMD 361 Fundamentals of Web Development ITMD 362 Human-Computer Interaction and Web Design ITMD 411 Intermediate Software Development ITMD 421 Data Modeling & Applications ITMO 440 Introduction to Data Networking & the Internet\ ITMS 448 Cyber Security Technologies ITMT 430 Systems Integration
(b) Design, implement, and evaluate a computer-based solution to meet a given set of computing requirements	ITM 301 Intro to Contemp Operating Systems & Hardware I ITM 311 Introduction to Software Development ITM 312 Introduction to Systems Software Programming ITMD 361 Fundamentals of Web Development ITMD 362 Human-Computer Interaction and Web Design ITMD 411 Intermediate Software Development ITMD 421 Data Modeling & Applications ITMO 440 Introduction to Data Networking & the Internet ITMO 456 Introduction to Open Source Operating Systems ITMS 448 Cyber Security Technologies ITMT 430 Systems Integration
(c) Communicate effectively with a range of audiences about technical information	ITMD 361 Fundamentals of Web Development ITMD 362 Human-Computer Interaction and Web Design ITMM 471 Project Management for ITM ITMS 448 Cyber Security Technologies IPRO 397/497 Interprofessional Project
(d) Make informed judgments in computing practice based on legal and ethical principles	ITM 100 Introduction to Information Technology as a Profession ITM 311 Intro to Contemp Operating Systems & Hardware I ITMM 471 Project Management for ITM ITMM 485 Legal and Ethical Issues in Information Technology ITMS 438 Digital Evidence ITMT 430 Systems Integration
(e) Function effectively on teams to establish goals, plan tasks, meet deadlines, manage risk, and produce deliverables	ITM 100 Introduction to Information Technology as a Profession ITMM 471 Project Management for ITM ITMS 448 Cyber Security Technologies ITMT 430 Systems Integration
(f) Identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems [IT]	ITM 311 Introduction to Software Development ITMD 362 Human-Computer Interaction and Web Design ITMD 411 Intermediate Software Development ITMD 421 Data Modeling & Applications ITMM 471 Project Management for ITM ITMO 440 Introduction to Data Networking & the Internet ITMO 456 Introduction to Open Source Operating Systems ITMT 430 Systems Integration
(g) Apply security principles and practices to the environmental, hardware, software, and human components of a system. [Cybersecurity]	ITMS 443 Vulnerability Analysis and Control ITMS 448 Cyber Security Technologies ITMS 478 Cyber Security Management ITMT 430 Systems Integration
(h) Analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats. [Cybersecurity]	ITMO 456 Introduction to Open Source Operating Systems ITMS 418 Coding Security ITMS 448 Cyber Security Technologies ITMS 458 Operating System Security ITMT 430 Systems Integration

Survey drafting and data collection staff:

Amber Chattalier, ITM Department Manager
Angela Jarka, ITM Assistant Department Coordinator

Assessment Evaluators:

ITM Curriculum Committee

The Curriculum Committee evaluates Survey Artifacts and makes recommendations based on evaluations of all assessment artifacts. All full-time faculty members are voting members of the committee should they elect to participate.

Chair: Ray Trygstad, ITM Associate Chair and Industry Professor
Members: Jeremy Hajek, Industry Associate Professor
Louis F. McHugh IV, SAT Computer Systems Manager and Adjunct Industry Associate Professor
Thomas "T.J." Johnson, Adjunct Industry Professor
Sheik "Sam" Shamsuddin, Adjunct Industry Professor; College of DuPage Professor and Computer Information System Program Coordinator
Faculty: C. Robert Carlson, ITM Chair and Professor
Karl Stolley, Associate Professor (joint appointment)
Adarsh Arora, Coleman Entrepreneur-in-Residence and Industry Professor
William Lidinsky, Interim Director, Center for Cyber Security and Forensics Education and Industry Professor
James Pappademas, Industry Professor
Yong Zheng, Senior Lecturer

All full-time faculty members may be appointed as assessment evaluators for Assignment Artifacts. Appointments will be made at the beginning of each term in which assignments will be assessed, and the Assessment Plan will be updated to reflect these appointments.