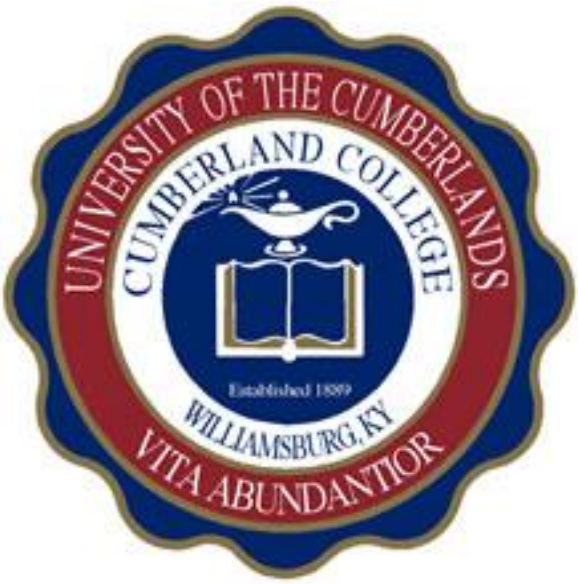
University of the Cumberlands

School of Computer and Information Sciences



Graduate Catalog

2017 - 2019

Accreditation

University of the Cumberlands is accredited by the Southern Association of Colleges and Schools Commission on Colleges to award associate, baccalaureate, masters, education specialist, and doctorate degrees. Contact the Commission on Colleges at 1866 Southern Lane, Decatur, Georgia 30033-4097 or call 404-679-4500 for questions about the accreditation of University of the Cumberlands.

Center of Academic Excellence

University of the Cumberlands (UC) was recently named a National Center of Academic Excellence in Cyber Defense (CAE-CD) by the National Security Agency (NSA) and the Department of Homeland Security (DHS). According to the NSA website, the overall objective of CAE-CD designations is to reduce national vulnerability by "promoting higher education and research in cyber defense" and by producing professionals with cyber expertise.

Non-Discrimination Policy

The University does not illegally discriminate in its programs and activities on the basis of race, color, national or ethnic origin, sex, disability, age, religion, genetic information, veteran or military status, or any other basis on which the University is prohibited from discrimination under local, state, or federal law. As a non-profit Christian institute of higher learning, the University exercises its rights under state and federal law to use religion as a factor in making employment decisions. The University has been granted exemption from certain regulations promulgated under Title IX of the Education Amendments of 1972 which conflict with the University's religious tenets.

The University has grievance procedures to provide students, employees, or applicants an opportunity to file a complaint of illegal discrimination of any kind. In order to file a grievance, see the grievance procedures published below or contact the appropriate person:

The following person has been designated to handle inquiries or complaints regarding the disability non-discrimination policy, including compliance with Section 504 of the Rehabilitation Act of 1973:

Mr. Nate Clouse
Student Success Coordinator
Boswell Campus Center, Student Services Office Suite
(606) 539-3561, nate.clouse@ucumberlands.edu

The following person has been designated as the University's Title IX Coordinator to handle inquiries or complaints regarding the sex non-discrimination policy and compliance with Title IX of the Education Amendments of 1972:

Mr. Steve Allen
Human Resources Director and Title IX Coordinator

Gatliff Administration Office 001
(606) 539-4211, steve.allen@ucumberlands.edu

Dr. Emily Coleman
Vice President for Student Services and Deputy Title IX Coordinator
Boswell Campus Center, Student Services Office Suite
(606) 539-4171, emily.coleman@ucumberlands.edu

The following person has been designated to handle inquiries or complaints regarding all other portions of the nondiscrimination policy:

Mr. Quentin Young
Director of Business Services
Gatliff Administration Office 116
(606) 539-4597, quentin.young@ucumberlands.edu

MEMBER
American Council on Education
College Entrance Examination Board
Association of Independent Kentucky Colleges and Universities
Kentucky Independent College Fund
International Association of Baptist Colleges and Universities
Council of Independent Colleges

The word “student” in any official University of the Cumberlands publication is defined to be all persons enrolled full or part time in any course or program.

Failure to read this bulletin does not excuse students from the requirements and regulations described herein.

The University reserves the right to make necessary changes without further notice.

TABLE OF CONTENTS

School of Computer and Information Science
Graduate Catalog

University of the Cumberlands

School of Computer and Information Science

Department Chair

Dr. Donald Grimes
Professor
104 Maple Street
Williamsburg, KY 40769
606-539-4154

University of the Cumberlands Mission Statement

University of the Cumberlands has historically served students primarily, but not exclusively, from the beautiful mountain regions of Kentucky, Tennessee, West Virginia, Virginia, Georgia, North Carolina, South Carolina, Ohio and Alabama which have traditionally been described as Appalachia. The University's impact can be seen in the achievements of its graduates who have assumed roles of leadership in this region and throughout the nation. While located in the resort like area of Appalachia, with emphasis primarily on serving the beautiful mountain area, the University now reaches into every state and around the world through its student body and alumni. UC continues to offer promising students of all backgrounds a broad-based liberal arts program enriched with Christian values. The University strives for excellence in all of its endeavors and expects from students a similar dedication to this pursuit. Its commitment to a strong academic program is joined with a commitment to a strong work ethic. UC encourages students to think critically and creatively so that they may better prepare themselves for lives of responsible service and leadership. This focus of its undergraduate programs is extended and extrapolated into its graduate programs. These programs prepare professionals to be servant-leaders in their disciplines and communities, linking research with practice and knowledge with ethical decision-making in the pursuit of the life-more-abundant for both the individual and society.

Mission

The School of Computer and Information Sciences strives for excellence in creating, applying, and imparting knowledge in information technology through comprehensive educational programs, research in collaboration with industry and government, dissemination through scholarly publications, and service to professional societies, the community, the state, and the nation.

Vision

Graduates of the School of Computer and Information Sciences will be recognized as innovative leaders in the field of information technology by their work in a myriad of application areas, and through their work in advanced study and research. The faculty will continue to be known for their passion for teaching these students and for their knowledge, expertise, and innovation in advancing the frontiers of knowledge in information technology.

Policies and Procedures
School of Computer and Information Science

Admission Requirements

Master's Programs
Admission to the master's programs will be based on evidence that the applicant has demonstrated academic proficiency and the capability for success at the graduate level. Documentation for the following items must be received before an admission decision will be made:

- Completed graduate application form with application fee.
- Official transcripts for all undergraduate and graduate work from accredited colleges or universities.
- A cumulative grade point average (GPA) of 2.5 or above on a 4.0 scale.
    - If coursework has been completed outside of the US transcripts must be evaluated by one of the following evaluating agencies: WES, ECE, or IES.
- Documentation of language fluency for non-native speakers of English, such as a score report from the Test of English as a Foreign Language (TOEFL) or the International English Language Testing System (IELTS). The minimum acceptable TOEFL or IELTS scores for admission are
    - Paper-based TOEFL (PBT) – 550
    - Internet-based TOEFL (IBT) – 79
    - IELTS – 6

PhD Program
Admission to the doctoral program will be based on evidence that the applicant has demonstrated academic proficiency and the capability for success at the graduate level. Documentation for the following items must be received before an admission decision will be made:

- Completed graduate application form with application fee.
- Official transcripts for all undergraduate and graduate work from accredited colleges or universities.
- Completed master's degree or higher from an accredited college or university.
- A cumulative grade point average (GPA) of 3.0 or above on a 4.0 scale in accredited master's degree or higher.
    - If coursework has been completed outside of the US transcripts must be evaluated by one of the following evaluating agencies: WES, ECE, or IES.
- Interview
- Documentation of language fluency for non-native speakers of English, such as a score report from the Test of English as a Foreign Language (TOEFL) or the

International English Language Testing System (IELTS). The minimum acceptable TOEFL or IELTS scores for admission are

- Paper-based TOEFL (PBT) – 550
- Internet-based TOEFL (IBT) – 79
- IELTS – 6

Conditional Admission

Students having one of the above criteria for regular admission waived may be admitted on a conditional or provisional basis. Students granted conditional admission will be required to satisfy specific conditions in order to continue enrollment in the program. These conditions include maintaining a cumulative GPA of at least 3.5 during a probationary period in which the student is allowed to earn 12 hours of program credit. Other conditions may include additional enrollment or re-enrollment in administrative courses deemed prerequisites to the program. Some students entering the program under provisional or conditional admissions status may be required to successfully participate in the program's tutoring program while concurrently enrolled in first year classes.

Provisions for Reapplying to the Doctoral Program

A candidate whose initial application was denied admissions may reapply to the program after one full semester or 16 weeks. A person committed to being accepted into the program should work toward developing and strengthening writing, critical thinking, and computational skills. It is also essential to recognize that potential dissertation topics must be compatible with the academic interests and expertise of the program's full-time faculty. Based upon an assessment of all information provided by prospective candidates, admission will be granted to the limited number of places available in a given cohort.

Course Restrictions

Courses numbered 500 or above may be counted as credit toward a master's degree, provided they are approved as part of the candidate's planned program. Some 500-level courses are open to both graduates and undergraduates, whereas 600-level courses are open only to qualified graduate candidates. Courses cannot be counted toward both the undergraduate and graduate programs. A senior can take six (6) hours approved of 500-level courses.

Transfer of Credit Policy

For Master's programs a maximum of nine (9) semester hours of credit may be transferred from an accredited graduate institution. For a Doctoral program a maximum of thirty (30) semester hours earned beyond the master's degree used for admissions purposes may be accepted. In all cases, transfer credits must be in courses equivalent to courses in the program.

All transfer credits must be approved by the Program Director and the Registrar. Grades for any transfer credits accepted into the program do not count in the program GPA. Transfer courses must be transcripted with letter grades (A, B, or C). Transfer courses with P or S grades will not be accepted because those grades are not compatible with UC's grading policy.

Transfer Credit Related to Military Service

Credit carried by all United States military veterans and personnel may be acceptable for application to a University of the Cumberlands transcript. Some credits may not be applicable if the university does not offer comparable coursework. Credit may vary with regard to application to general education, major/minor requirements or general electives. Final determination of credit awarded for course requirements and general electives will be determined by the office of the Registrar while major/minor requirements will be determined by collaboration with the appropriate department Chair and the Registrar.

Requirements for the acceptance of Military Credit:

1. An official copy of a JST (Joint Services Transcript) delivered to the Registrar's Office directly from the Joint Services Transcript Office.

2. A student must request that JST credit be considered for General Education and/or general electives through the Registrar's Office.

3. A student must request that JST credit be considered for a major or minor through the appropriate department Chair or program Director.

Determination of the type and amount of credit to be awarded will be assessed using ACE (American Council on Education, http://www2.acenet.edu/militaryguide/CourseSearch.cfm) recommendations according to the specifications mentioned above.

Credit for Prior Learning

The School of Computer and Information Sciences will accept the following certifications as replacement for the corresponding course(s).

Course#	Course Name	Certification
ISOL 633 **ISOL 699** **Or**	Legal Regulations, Compliance, and Investigation Information Security Project Or	(ISC)2 CISSP

MSDF 630 **MSDF 699**	Legal Regulations, Compliance, and Investigation Digital Forensics Project	
ISOL 633 **ISOL 699**	Legal Regulations, Compliance, and Investigation Information Security Project	ISACA CISM
ISOL 633 **ISOL 699**	Legal Regulations, Compliance, and Investigation Information Security Project	GIAC Information Security Professional (GISP)
MSDF 530 **MSDF 533**	Investigation and Triage Digital Forensics Tools and Techniques	GIAC Certified Forensic Examiner or GIAC Certified Forensic Analyst
MSDF 630 **MSDF 631** **MSDF 699**	Legal, Regulations, Investigations, and Compliance Digital Forensics Evidence Digital Forensics Project	Conferred Juris Doctorate Degree

Department Policies

Required Courses
Consult the planned programs (curriculum contracts) of various programs for required courses in each area of study.

Grading
The graduate programs uses the following grades and quality points:

A Superior performance, four quality points are earned for each semester hour with a grade of “A”
B Performance distinctly above average, three quality points are earned for each semester hour with a grade of “B”
C Average performance, two quality points are earned for each semester with a grade of “C”
F Failure, given for unsatisfactory work, no quality points.
W Withdrawn from class without punitive grade.

I Incomplete, assigned only in instances where a small unit of work is not complete because of verifiable, extenuating circumstances. An "I" contract is submitted to the Registrar's Office with each "I" grade assigned.

The grade point average is computed on all graduate course work with the exception of "W." The grade of "I" is computed as an "F" in determining qualifications for candidacy. If the grade point average is below 3.0 (B), the candidacy application is held until the incomplete is cleared and the grade earned is then considered in determining the grade point average. Courses with a grade of "F" cannot be used toward degree or non-degree programs but will be used toward computing GPA. Candidates for a graduate degree are required to have a combined cumulative grade point average of "B" in all courses. A "W" grade has no bearing on the grade point average. Students wishing to withdraw prior to completing the semester should complete an official withdrawal form from the Office of Academic Affairs.

The grade of incomplete is awarded only when legitimate circumstances warrant. The grade of "I" will be recorded on the graduate student's transcript and will remain until the faculty member awarding this grade makes the appropriate change or until the time specified on the "I" contract expires. The maximum length of time an "I" may remain on a transcript is one calendar year. At the end of a one calendar year period, the incomplete will change to the grade of "F" if the student has not completed the course requirement as specified by the instructor. Each submitted incomplete must be accompanied by a valid contract for this grade. This contract will indicate all of the necessary steps to be taken by the student to satisfactorily change the grade of "I".

Academic Status

The following standards will determine a student's academic status:

1. Students must maintain a GPA of 3.0 to complete the program successfully.
2. A student whose GPA drops below 3.0 will be placed on academic probation. The student then has two semesters to improve the GPA to a 3.0 or higher. If the student fails to do so, the student will normally not be allowed to continue in the program.
3. A student must pass a course that is a prerequisite for another course with a "B" or better before taking the following course.

Being placed on probation is a warning to the student that academic performance is below the minimum requirements of the Program. During the probation period, a student has the opportunity to raise the GPA or correct other specifically identified problems. If these deficiencies are not remediated, a student may be dismissed from the Program. Probationary status is determined and monitored by the Program Director in consultation with the Academic Coordinator and the Registrar. The minimum length of probation is one semester.

Full-Time Enrollment
Registration for six or more graduate credit hours during any semester entitles a graduate candidate to full-time status.

When evaluating which courses were taken in seat vs. on line, the following guidance can be applied to the graduate, executive programs highlighted in this academic catalog. Courses identified as "MAIN" are considered in seat courses, and include residency weekend attendance requirements. Courses identified as "IG" or "IIG" are considered on line courses. The exception to this classification are courses with the INTR prefix. INTR courses are courses with an internship requirement and require direct work experience with the approved internship employer/supervisor.

Degree Time Limit
Master's program students must complete all program requirements within four years.

A doctoral candidate should be able to complete the PhD program in approximately five years. If a candidate has not completed the degree after seven years in the program, an application for additional time must be filed in the program office. This application will be reviewed and acted upon by the Program Director with the assistance of the PhD faculty. Candidates may not remain in the program beyond seven years unless an additional application for a time extension has been approved. Such an approval may include the need for additional course work to remain current in the field, as well as other conditions.

Academic Appeals
A student wishing to appeal a grade must appeal first to the professor of the course. If the situation remains unresolved, the student may then appeal to the Program Director. Following the ruling of the Program Director, either the professor or the student may file a complaint with the Academic Appeals Committee of the University. This formal written appeal must be filed by the end of the 4th week of classes in the next regular term following the term in which the course in question was taken. The Academic Appeals Committee then gathers information from the student, the professor, and any other relevant parties. The Committee will deliver its recommendation on the complaint to the Vice President for Academic Affairs. After reviewing this recommendation and concurring with or amending it, the Vice President for Academic Affairs will inform the student and professor of the disposition of the complaint no later than the last day of classes of the regular term in which the complaint was filed.

An appeal of any application of program policy made by the Program Director may also be filed with the Vice President for Academic Affairs, who will make the final determination in the matter.

Leave of Absence
A leave of absence from the School of Computer and Information Sciences programs may be granted by the Program Director for medical or personal reasons. Requests for

leaves of absence must be made in writing to the Program Director. A student on a leave of absence may be permitted to resume course work upon receipt of documentation that satisfactory resolution has occurred of the problem necessitating the leave of absence. Repetition of course work satisfactorily completed prior to the leave of absence will not be required provided resumption in training occurs within one academic year from the date the leave of absence begins.

Withdrawal

Students may voluntarily withdraw from the School of Computer and Information Sciences programs in accordance with the University's general policies and procedures. Written notice of intent to withdraw must be provided to the Program Director prior to initiating the formal withdrawal process.

A student desiring to withdraw from University of the Cumberlands within any semester must complete required paperwork and receive permission from the Vice President for Academic Affairs. The following policies and procedures govern withdrawal from the University for the current term.

1. The permanent record of a student who withdraws from University of the Cumberlands up until the last day to drop a class published on the Academic Calendar for that semester or bi-term will list a mark of "W" for all courses for which another grade (such as an "F") has not been previously posted. A "W" carries no grade point penalty.
2. Students withdrawing after the last day to drop a course for the semester or bi-term will receive a of "F."
3. No student who withdraws from University of the Cumberlands is entitled to a grade report or transcript of credits until the student's account is cleared by the Bursar's Office.
4. The official date of withdrawal will be used by the Bursar's Office and the Office of Financial Planning to determine any adjustments involving financial aid and financial charges.

Medical / Emergency Withdrawal Students who must withdraw from classes for medical reasons or because of dire personal circumstances may submit a written request to the Academic Affairs Office as soon as the student intends to stop attending classes. This request must be supported by a letter from a medical professional or other source supporting the student's request with specific information on the student's diagnosis, current condition, and continuing treatment requirements, or on the student's personal emergency that necessitates the withdrawal request. If the medical / emergency withdrawal is granted, the student will receive grade of a "W" in all current classes. NOTE: Normally, partial medical / emergency withdrawals are not permitted (that is, withdrawal from one or two courses while the student continues in others).

Administrative Withdrawal A student may be withdrawn from all classes by administrative action based upon:

1. Disciplinary action against a student confirmed by the Vice President for Academic Affairs, the Vice President for Student Services, or other university officer;

2. Failure of the student to confirm enrollment during the enrollment confirmation period at the beginning of a term.

3. Non-Participation in classes resulting in an active schedule of less than 1 credit hour and the posting of an F, W in other classes.

Readmission
Any individual who has previously matriculated and failed to complete the entire program of study within the required time period will be required to initiate a new application for admission. Likewise, applicants who have been previously offered admission into the Program but failed to matriculate in the designated class will also be required to initiate a new application for admission.

Executive Format Policies

Residency Requirement
Residency weekend sessions are mandatory. A student must attend all three-days (3) to receive credit and fulfill immigration in-seat class component to retain F-1 Status. Should a student not attend any part of a full session, the student will be counted absent for the entire residence weekend. As such, requests to arrive late or leave early will not be approved. Absolutely no exceptions allowed. For details visit http://www.ucumberlands.edu/residency

Attendance Policy
Attendance to each residency class session is mandatory. Students may make-up no more than one (1) residency session throughout the duration of their academic program. Missing a second residency results in student being dismissed from the academic program and for F1 students, SEVIS record (I-20) terminated. No exceptions. For details visit http://www.ucumberlands.edu/residency

Physical Attendance Records
As referenced in prior policy statements, any student enrolled in the Executive Residency Weekend program must attend their assigned Residency Weekend as a component of their course enrollment. Due to course structure in the Executive program, a student cannot be successful in their residency courses without full physical attendance at the entire assigned residence weekend each term. Please use the catalog

attendance statements, course syllabus, and personal travel receipts for any documentation needed regarding physical attendance at assigned residence weekends.

For international students gathering “Request for Evidence” (RFE) documentation regarding Physical Attendance Records, please use the policy statements above, university transcripts demonstrating successful course completion, course syllabi, and personal travel receipts to verify physical course attendance. The aforementioned university specific documentation represents what the university can provide related to physical attendance records.

Student Privacy

Student Privacy and Informed Consent
Students pursuing School of Computer and Information Sciences programs are granted privacy through the Family Educational Rights and Privacy Act of 1974 (FERPA) enacted to protect the privacy associated with educational records, to establish the rights of students to inspect and review their educational records, and to provide guidelines for the correction of inaccurate or misleading data through informal and formal hearings.

Privacy Rights of Students
The University is subject to the provision of the Family Educational Rights and Privacy Act (FERPA). This federal law affords students certain rights with respect to the student's education records. These rights are:

1. **The right to inspect and review the student's education records within 45 days of the day the University receives a request for access.** Students should submit to the Office of the Registrar written requests that identify the record(s) they wish to inspect. The Registrar will make arrangements for access and notify the student of the time and place the records may be inspected.

2. **The right to request the amendment of the student's education records that the student believes are inaccurate.** Students may ask the University to amend a record that they believe is inaccurate. They should write the Registrar, clearly identify the part of the record they want changed, and specify why it is inaccurate. If the Registrar decides not to amend as requested, the Registrar will notify the student of the decision and advise the student of his or her right to a hearing regarding the request and will provide the student with additional information regarding the hearing procedures.

3. **The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent**. One exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. A

school official is a person employed by the University in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Upon request, the University discloses education records without consent to officials of another school in which a student seeks or intends to enroll.

The University may also disclose without the student's consent "directory information" unless the student has advised the Registrar in writing at least five days following registration that the student does not wish part or all of the directory information to be made public. Once filed, this instruction becomes a permanent part of the student's record until the student instructs the University, in writing, to have the request removed. The primary purpose of directory information is to allow the University to include this type of information in certain University publications, the media, and outside organizations. The University has designated the following as examples of directory information: The student's name, addresses including electronic mail address, telephone numbers, date and place of birth, major field of study, degree sought, attained class level, expected date of completion of degree requirements and graduation, degrees and awards received, picture, dates of attendance, full or part-time enrollment status, the previous educational agency or institution attended, class rosters, participation in officially recognized activities and sports, weight and height of athletic team members and denominational preference. The University may disclose education records in certain other circumstances, but shall do so only upon the authorization of the Registrar.

4. **The right to file a complaint with the U.S. Department of Education concerning alleged failures by the University to comply with the requirements of FERPA.** The name and address of the office which administers FERPA and to which complaints are to be sent is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC, 20202-8520.

Office of Financial Planning
To learn more about financial aid options, please contact the Office of Financial Planning by calling 606-539-4220.

Tuition and Expenses
Students will be assessed a per-hour tuition fee as well as a per term technology fee. The latest costs for tuition and expenses can be found at the University Website www.ucumberlands.edu

Refund Schedule

Courses Fifteen Weeks or Greater in Length

Official Date of Withdrawal	Charge	Refund
Last day to Register	0%	100%
Week 2 of classes	20%	80%
Week 3 of classes	40%	60%
Week 4 of classes	60%	40%
Week 5 of classes	80%	20%
After 5th week of classes	100%	0%

Courses Greater than Six Weeks but Less than Fifteen Weeks in Length

Official Date of Withdrawal	Charge	Refund
Last day to Register	0%	100%
Week 2 of classes	50%	50%
After 2nd week of classes	100%	0%

Courses Six Weeks or Less in Length

Official Date of Withdrawal	Charge	Refund
Last day to Register	0%	100%
After 1st week of classes	100%	0%

If a student officially withdraws after the posted cancellation deadline and on or before the first day of the term, they will be charged a **non-cancellation fee of $150 for tuition and $150 for room and board** for the fall and spring term. There is no non-cancellation fee for the summer term(s).

If a student officially withdraws after the first day of classes, they will be charged an **administrative withdrawal fee of $100 for the fall and spring terms and $50 fee for the summer and bi-terms**.

A student is **not eligible for any financial aid prior to the first day of class** attendance.

Treatment of Title IV Aid When A Student Withdraws

The law specifies how your school must determine the amount of Title IV program assistance that you earn if you withdraw from school. The title IV programs that are covered by this law are: Federal Pell Grants, Academic Competitiveness Grants, National SMART grants, TEACH Grants, Stafford Loans, PLUS Loans, Federal Supplemental Educational Opportunity Grants (FSEOGs), and Federal Perkins Loans.

When you withdraw during your payment period or period of enrollment (your school can define these for you and tell you which one applies) the amount of Title IV program assistance that you have earned up to that point is determined by a specific formula. If you received (or your school or parent received on your behalf) less assistance than the

amount that you earned, you may be able to receive those additional funds. If you received more assistance than you earned, the excess funds must be returned by the school and/or you.

The amount of assistance that you have earned is determined on a prorated basis. For example, if you completed 30% of your payment period or period of enrollment, you earn 30% of the assistance you are originally scheduled to receive. Once you have completed more than 60% of the payment period or period of enrollment, you earn all the assistance that you were scheduled to receive for that period. If you did not receive all of the funds that you earned, you may be due a post-withdrawal disbursement. If your post-withdrawal disbursement includes loan funds, your school must get your permission before it can disburse them. You may choose to decline some or all of the loan funds so that you don't incur additional debt.

Your school may automatically use all or a portion of your post-withdrawal disbursement of grant funds for tuition, fees, and room and board charges (as contracted with the school). The school needs your permission to use the post-withdrawal grant disbursement for all other school charges. If you do not give your permission (some schools ask for this when you enroll), you will be offered the funds. However, it may be in your best interest to allow the school to keep the funds to reduce your debt at the school.

If you receive (or your school or parents receive on your behalf) excess Title IV program funds that must be returned, your school must return a portion of the excess equal to the lesser of: 1. Your institutional charges multiplied by the unearned percentage of your funds, or 2. The entire amount of excess funds.

The school must return this amount even if it didn't keep this amount of your Title IV program funds. If your school is not required to return all of the excess funds, you must return the remaining amount. Any loan funds that you must return, you (or your parent for a PLUS loan) repay in accordance with the terms of the promissory note. That is, you make scheduled payments to the holder of the loan over a period of time.

Any amount of unearned grant funds that you must return is called an overpayment. The maximum amount of a grant overpayment that you must repay is half of the grant funds you received or were scheduled to receive. You must make arrangements with your school or the Department of Education to return the unearned grant funds.

The requirements for Title IV program funds when you withdraw are separate from any refunds policy that your school may have. Therefore, you may still owe funds to the school to cover unpaid institutional charges. Your school may also charge you for any Title IV program funds that the school was required to return. If you don't already know what your school's refund policy is, you can ask your school for a copy. Your school can

also provide you with the requirements and procedures for officially withdrawing from school.

If you have questions about your Title IV program funds, you can call the Federal Student Aid Information Center at 1-800-4-fedaid (1-800-433-3243). TTY users may call 1-800-730-8913. Information is also available on Student Aid on the Web at www.studentaid.ed.gov.

Disability Accommodations

University of the Cumberlands accepts students with certified disabilities and provides reasonable accommodations for their certified needs in the classroom, in housing, in food service or in other areas. (Please see the University's Non-Discrimination Policy on page 2.) Students with disabilities may incur additional costs for services not provided by the University. The University's obligation to reasonably accommodate any student's disability ends where the accommodation would pose an undue hardship on the University or where accommodation in question would fundamentally alter the academic program.

For accommodations to be awarded, a student must submit a completed Accommodations Application form and provide documentation of the disability to the Disability Services Coordinator, Dr. Tom Fish Library 021, (606) 539-4216. Documentation may include copies of accommodation records from a high school or previously attended educational institution, testing results and evaluation by a licensed psychometrician, and/or statements from a physician describing the disability and the necessary restrictions. When all paperwork is on file, a meeting between the student and the Coordinator will be arranged to discuss possible accommodations before accommodations are formally approved. Students must then meet with the Coordinator at the beginning of each semester before any academic accommodations can be certified for that term. Certifications for other accommodations are normally reviewed annually. All accommodations may be reviewed at any time at the request of the student or the Disabilities Coordinator.

Master of Science
Information Security Systems
(MSISS)

31 hours

All courses are three (3) credit hours unless otherwise noted.

Program Description

The Master of Science in Information Security at University of the Cumberlands focuses on information security challenges relating to mitigating the risk of loss or disclosure of data. With the combination of the ubiquitous nature of electronic information and the associated security risks, the field of information security has become a critical need for every organization.

Program of Study

The Master of Science in Information Systems Security is comprised of the following thirty-one (31) required credit hours:

ISOL 531 – Access Control
ISOL 532 – Telecommunications and Network Security
ISOL 533 – Information Security and Risk Management
ISOL 534 – Application Security
ISOL 535 – Cryptography
ISOL 536 – Security Architecture and Design
ISOL 631 – Operations Security
ISOL 632 – Business Continuity Planning and Disaster Recovery Planning
ISOL 633 – Legal Regulations, Compliance, and Investigation
ISOL 634 – Physical Security
ISOL 699 – Information Security Project (1hr)

With the approval of the Program Director, ISOL 690 Special Topics may substitute for one required course in the program.

Master of Science
Digital Forensics
(MSDF)

31 hours

All courses are three (3) credit hours unless otherwise noted.

Program Description

The Master of Science in Digital Forensics program at University of the Cumberlands prepares candidates for the advanced practice role of recovering and investigating data lost to computer crime, fraud, abuse, or other illegal activities. In addition to nurturing the skills necessary for digital forensics, the program offers a curriculum based upon need within the industry.

Program of Study

The Master of Science in Digital Forensics is comprised of the following twenty-eight (28) required credit hours of core required credit hours and three (3) hours in an approved elective course:

MSDF 530 – Investigation and Triage
MSDF 531 – Windows Digital Forensics
MSDF 532 – Windows Registry Forensics
MSDF 533 – Digital Forensics Tools and Techniques
MSDF 630 – Digital Forensics Evidence
MSDF 631 – Malware Analysis and Mitigation
MSDF 632 – INFOSEC Leadership and Communications
MSDF 633 – Laws, Regulations, Investigations, and Compliance
MSDF 634 – Web Browser Forensics
MSDF 699 – Digital Forensics Capstone (1hr)

Students are required to complete three (3) credit hours from the following approved courses:

ISOL 532 – Telecommunications and Network Security
ISOL 534 – Application Security
ISOL 535 – Cryptography
ISOL 631 – Operations Security
ITS 530 – Analyzing and Visualizing Data
ITS 632 – Introduction to Data Mining

With the approval of the Program Director, ISOL 690 Special Topics may substitute for one required course in the program.

Master of Science
Information Technology
(MSIT)

31 hours

All courses are three (3) credit hours unless otherwise noted.

Program Description

The Master of Science in Information Technology at University of the Cumberlands focuses on the advanced practice role of the use of predictive analytics to identify cyber threats, employ big data analytics to improving healthcare, and empower smart cities in making data-driven policy changes critical for societal well-being. This program is designed to meet the aggressive demand for qualified data scientists in virtually every sector of the economy, with classes in computer science, data intelligence, analytics, security.

Program of Study

The Master of Science in Information Technology is comprised of the following eighteen (18) hours of core required credit hours and twelve (12) hours in department elective courses:

Core Courses:
ITS 530 – Analyzing and Visualizing Data
ITS 531 – Business Intelligence
ITS 532 – Cloud Computing
ITS 630 – Organization Leadership and Decision Making
ITS 631 – Operational Excellence
ITS 631 – Introduction to Data Mining
ITS 699 – Information Security Project (1hr)

With the approval of the Program Director, ISOL 690 Special Topics may substitute for one required course in the program.

Doctorate of Philosophy
Information Technology
(PhD IT)

60 hours

All courses are three (3) credit hours unless otherwise noted.

Program Description

The Doctorate of Philosophy in Information Technology at University of the Cumberlands focuses on the advanced practice role of the use of predictive analytics to identify cyber threats, employ big data analytics to improving healthcare, and empower smart cities in making data-driven policy changes critical for societal well-being. This program is designed to meet the aggressive demand for qualified data scientists in virtually every sector of the economy, with classes in computer science, data intelligence, analytics, security, strategic planning, governance and global economy.

Program of Study

The Doctorate of Philosophy in Information Technology is comprised of the following eighteen (18) hours of core required credit hours, at least eighteen (18) hours of professional research courses, and twenty-four (24) hours in a content specialty.

Core Courses:
ITS 831 – Information Technology Importance in Strategic Planning
ITS 832 – Information Technology in a Global Economy
ITS 833 – Information Governance
ITS 834 – Emerging Threats and Countermeasures
ITS 835 – Enterprise Risk Management
ITS 836 – Data Science and Big Data Analytics

Professional Research:
LEAR 734 / ITS 734 – Inferential Statistics
LEAR 736 / ITS 736 – Dissertation Seminar
LEAR 839 / ITS 839 – Advanced Research Methods
LEAR 930 / ITS 930 – Dissertation
LEAR 931 / ITS 931 – Dissertation
*LEAS 730, LEAS 830, LEAC 836 or approved elective

Content Specialty Area: A content specialty area of at least twenty-four hours must be earned in one of these disciplines: Cybersecurity, Information Technology, Digital Forensics, Computer Information Systems, Computer Science, or other related discipline at the discretion of the Dean of the School.

PhD IT Program Requirements

Research Students will formally identify a dissertation topic and write the review of the literature in fulfillment of the requirements for ITS736/LEAR736-Dissertation Seminar. The remaining sections of the first three chapters of the dissertation will be written while enrolled in ITS839/LEAR 839- Advanced Educational Research. Candidates will carry out their research to complete the dissertation.

Comprehensive Exam Candidates sit for the Comprehensive Examination prior to enrolling in ITS930/LEAR930. The specific content, structure, and scheduling of this examination is determined by the Program Director. Tailored to each student's program of study, questions on the Comprehensive Examination are generated by the program's four content-related goals:

Goal 1: Expand information sciences through advanced study.

Goal 2: Promote critical thinking and problem-solving skills to include leadership at the organizational and system level and the ability to evaluate and improve the quality and safety of Information Sciences.

Goal 3. Afford structured and supervised research experiences so that students develop the technical, conceptual and communication skills that are required to conduct high-quality, independent research.

Goal 4: Provide training in basic and advanced information systems theory and practice so that students master the technical and conceptual tools needed for conducting high-quality research.

Goal 5: Instill ethical leadership, service, and values

The Comprehensive Examination is normally completed in one four-hour session scheduled during the operating hours of the department. It is graded by contributing members of program faculty, with passing marks required on all sections of the examination before a candidate can graduate. A student failing any or all parts of the Comprehensive Examination has one opportunity to retake these sections within one month of the original testing date. A student who fails the exam or a portion of it a second time must sit out for 16 weeks before taking it a third time. Students failing the exam a third time must retake relevant courses. Once the student has successfully retaken relevant courses, the cycle of testing begins anew.

The Dissertation

The dissertation is the capstone experience in the PhD program of Information Technology. A dissertation is a research-based project that may use a wide-range of statistical, quantitative, and qualitative methods. However, in the University's practitioner-focused program, the dissertation is conceived as a reality-based project in which the candidate engages in authentic professional problem-solving to extend best

practices in the field. Specific details on dissertation requirements are included in the "PhD IT Dissertation Handbook."

All program features highlighted above combine to make the doctoral program at the University of the Cumberlands a rigorous academic experience focused on strengthening the skills of information technology professionals.

School of Computer and Information Science
Course Descriptions

ISOL 531 – Access Control. The course provides an in depth study of the three main security principles: availability, integrity and confidentiality. The course examines mechanisms used to control what resources an entity can access, and the extent of the entity's capabilities to interact with the resource. The course also examines approaches to auditing how the entity interacts with the resource.

Upon completion of the course, students will be able to

- Identify the types of access control technologies used in a networking environment.
- Implement knowledge-based and biometric authentication
- Identify knowledge-based and characteristics-based authentication technologies.
- Recognize how single sign-on systems (SSOs), one-time passwords (OTPs), and smart cards are used for authentication.
- Determine the appropriate type of authentication to implement in a given enterprise scenario.
- Recognize ways of securing passwords and identify different types of attack against passwords and password files.
- Select the appropriate access control model for a scenario.
- Determine the most appropriate access control model to implement in a given situation.
- Recognize how different types of access control techniques operate.
- Distinguish between centralized and decentralized access control administration mechanisms.
- Identify information detection system (IDS) mechanisms and implementation methods, and recognize various intrusion detection and prevention techniques.

ISOL 532 – Telecommunications and Network Security. The course provides fundamental concepts of networking including: examination of public and private communication systems, networking topologies, devices, protocols, and remote access. It additionally explores strategies on identifying areas for security vulnerabilities on networks.

Upon completion of the course, students will be able to

- Identify security issues associated with e-mail, facsimile, and PBX systems.
- Identify the characteristics and functionality of the different technologies used to protect an organization at the network's edge.
- Identify the characteristics of TCP and IP.
- Distinguish between the layers of the OSI reference model and their associated functionality and technologies.
- Distinguish between types of data topology and physical media, and recognize the functionality of different LAN technologies.

- Recognize the network topologies, media access methods, data transmission types, and devices used by LANs and WANs.
- Identify the characteristics of the switching, remote access, and authentication methods used by LANs and WANs.
- Recognize the characteristics of the various network communications mechanisms and technologies used in an enterprise environment, and identify the protocols used by VPNs.
- Recognize the characteristics and functionality of the protocols used to secure data in transit in an enterprise environment.
- Distinguish the various wireless technologies.

ISOL 533 – Information Security and Risk Management. The course provides a methodology to identify an institution's information technology assets, the proper way to determine the necessary level of protection required, and techniques for developing budgets for security implementations.

Upon completion of the course, students will be able to

- Recognize the goals of security management and change control.
- Identify the change control mechanisms used to secure the operational environment.
- Recognize the objectives and criteria associated with data classification, and distinguish between information classification roles.
- Distinguish between policies, standards, baselines, and guidelines.
- Recognize best practices and procedures for dealing with different aspects of employee relations.
- Determine the appropriate security procedures for hiring a new employee in a given scenario.
- Identify the principles of risk management, distinguish between planning types, and recognize what's involved in the analysis of different threats and vulnerabilities.
- Calculate the potential loss expectancy and the cost of countermeasures used for risk reduction in a given scenario.
- Calculate the loss expectancy associated with an information asset, perform a cost-benefit analysis, and determine how to handle the risk depending on the outcome of the countermeasure.
- Identify the security-related responsibilities associated with different roles within an organization.

ISOL 534 – Application Security. This course discusses methods to increase the security of application development and thwart attacker attempts to manipulate code. It also explores the software lifecycle and change control to reduce the probability of poorly written applications that allows an attacker to exploit coding errors. Database development models will be introduced focusing on choosing the best model to increase security.

Upon completion of the course, students will be able to

- Match issues related to applications development with corresponding ways in which they create security vulnerabilities.

- Recognize types of attacks used in the enterprise environment.
- Determine the appropriate methods to counteract a given attack.
- Match types of computer attacks to their corresponding countermeasures.
- Match types of malicious code to their corresponding descriptions.
- Recognize the purpose of software forensics.
- Recognize characteristics of knowledge-based systems.
- Determine the appropriate development model to use for a given software development project
- Distinguish between various database models and technologies

ISOL 535 – Cryptography. The course examines methods and techniques for concealing data for security purposes. Topics covered will include cryptographic techniques, approaches and technologies.

Upon completion of the course, students will be able to

- Define key cryptographic terms.
- Identify the characteristics of quantum cryptography.
- Match symmetric key algorithms to their corresponding descriptions.
- Distinguish between types of asymmetric algorithms.
- Determine the appropriate use for a given message format.
- Recognize types of ciphers.
- Match types of cryptanalytic attack with their corresponding descriptions.
- Determine the appropriate hash algorithm to use in a given scenario.
- Recognize characteristics of message authentication codes.
- Identify the characteristics of digital signatures.
- Identify guidelines for key management and distribution.
- Identify characteristics of the XKMS.
- Recognize the appropriate application of the split knowledge method of key management.
- Recognize methods of key distribution.

ISOL 536 – Security Architecture and Design. The course focuses on the concepts and standards for designing and implementing secure software systems.

Upon completion of the course, students will be able to

- Recognize the components of the basic information system architecture and their functionality, and differentiate between hardware, software, and firmware.
- Differentiate between machine types and recognize the functions of network protocols and the resource manager.
- Distinguish between types of storage devices and how they are used.
- Determine which system resources can be found at the different protection rings and how the rings control subject access to objects.
- Differentiate between key security concepts, recognize the roles of TCB, reference monitor, and security kernel in protecting the operating system.

- Differentiate between the various criteria and standards used to evaluate security in a networking environment.
- Specify the security level that should be assigned to various objects and determine how to implement the standard.
- Recognize the logistics of various security models used to enforce rules and protection mechanisms. .

ISOL 631 – Operations Security. The course examines controls over personnel, hardware, software, and systems. It also covers possible abuse channels and proper countermeasures.

Upon completion of the course, students will be able to

- Recognize the activities involved in securing the operations of an enterprise and identify the technologies used to maintain network and resource availability.
- Identify the effects of various hardware and software violations on the system, and recognize how different types of operational and life-cycle assurance are used to secure operations.
- Determine the effects of different attacks on the network and identify the consequences of those effects.
- Recognize how different auditing and monitoring techniques are used to identify and protect against system and network attacks.
- Recognize the need for resource protection, distinguish between e-mail protocols, and identify different types of e-mail vulnerability.
- Identify basic mechanisms and security issues associated with the Web, and recognize different technologies for transferring and sharing files over the Internet.
- Recognize key reconnaissance attack methods and identify different types of administrative management and media storage control.
- Identify the appropriate security measures and controls for creating a more secure workspace.

ISOL 632 – Business Continuity Planning and Disaster Recovery Planning. The course examines the preservation of business activities when faced with disruptions or disasters. It involves the processes that are used to create a business continuity and disaster recovery plan and strategies for critical resource recovery.

Upon completion of the course, students will be able to

- Identify activities that occur during the project initiation phase of business continuity planning.
- Recognize considerations for business continuity and disaster recovery planning.
- Perform a business impact analysis on given business functions.
- Recognize key considerations when conducting a business impact analysis.
- Recognize the considerations that are weighed when determining an appropriate recovery strategy.
- Match recovery strategies for business operations to corresponding descriptions.
- Match recovery strategies for technology environments to corresponding descriptions.

- Recognize the components of a business continuity and disaster recovery plan.
- Identify the various test types for the plan.

ISOL 633/MSDF 633– Legal Regulations, Compliance, and Investigation. The course examines computer crimes, laws and regulations. It includes techniques for investigating a crime, and gathering evidence. It also covers techniques for creating incident reports.

Upon completion of the course, students will be able to

- Distinguish between the major categories of computer crime and recognize examples of each.
- Recognize the characteristics of various computer-related crimes.
- Identify the type of intellectual property law that applies in a given scenario.
- Identify laws related to information security and privacy.
- Distinguish between the laws that have been created to deal with different types of computer crime.
- Understand the principles of due care and due diligence, and identify the phases and types of evidence involved in computer crime.
- Determine the appropriate process for controlling evidence when investigating a computer-related crime in a given scenario.
- Recognize the investigative and ethical considerations involved in dealing with computer crime.

ISOL 634 – Physical Security. The course examines risks, threats, and countermeasures to secure data, personnel and hardware. This involves facility creation and selection concerns, facility access control methods, and safety issues.

Upon completion of the course, students will be able to

- Recognize basic threats to an organization's physical security and identify the security mechanisms used in securing an enterprise environment.
- Identify the security mechanisms and strategies used to protect the perimeter of a facility.
- Identify the appropriate physical security mechanisms to implement in a given scenario.
- Identify the appropriate mechanisms and controls for securing the inside of a building or facility.
- Select the most appropriate intrusion detection technology for a scenario.
- Select the appropriate strategy for securing compartmentalized areas in a given scenario.

ISOL 690 – Special Topics. The course presents special topics of interest in the domain of information security and information governance. Topic areas might include business continuity planning, legal and regulatory compliance issues and operations security

Upon completion of the course, students will be able to

- Demonstrate an understanding of one of the core domains of information security.
- Demonstrate knowledge of current research in one of the core domains of information security.
- Demonstrate the ability to integrate their knowledge and skills to solve problems from a core domain of information security.

ISOL 699 – Information Security Project.* All students are required to demonstrate the ability to clearly evaluate a particular information security need, identify potential solutions, evaluate the alternatives, and implement the best solution.

Upon completion of the course, students will be able to

- Demonstrate the ability to clearly evaluate a particular need related to information technology.
- Demonstrate the ability to discern the best method to address a particular need related to information security.
- Demonstrate the ability to integrate their knowledge and skills base into a workable plan to address a particular need in information security.

*Successful completion of INTR 599/799 will replace ISOL699

ITS 530 – Analyzing and Visualizing Data This course is intended to introduce students to modern programs and technologies that are useful for organizing, manipulating, analyzing, and visualizing data. We start with an overview of the R language, which will become the foundation for your work in this class. Then we'll move on to other useful tools, including working with regular expressions, basic UNIX tools, XML, and SQL.

Upon completion of the course, students will be able to

- Become a contributor on a data science team
- Deploy a structured lifecycle approach to data analytics problems
- Apply appropriate analytic techniques and tools to analyzing big data
- Learn how to tell a compelling story with data to drive business action.

ITS 531 – Business Intelligence This course covers theories and applications of business analytics. The focus is on extracting business intelligence from firms' business data for various applications, including (but not limited to) customer segmentation, customer relationship management (CRM), personalization, online recommendation systems, web mining, and product assortment. The emphasis is placed on the 'know-how' -- knowing how to extract and apply business analytics to improve business decision-making.

Upon completion of the course, students will be able to

- Perform business reporting and visual analytics
- Understand management support system technologies
- Understand foundations and technologies for decision making
- Understand techniques for predictive modeling
- Understand emerging trends and future impacts

ITS 532 – Cloud Computing This course is designed as a primer for cloud computing which many believe is the third major wave of computing, after mainframe and client-server computing. The course examines this technology from a business perspective. The course is designed to deliver a holistic and balanced view of business model, technological infrastructure, and security issues of cloud computing useful for the technology student to understand the business challenges and the business student to understand the technology challenges.

Upon completion of the course, students will be able to

- Understand basic concepts and terminology relating to cloud computing
- Understand cloud delivery models such as IaaS, PaaS, and SaaS
- Understand virtualization technology
- Understand fundamental cloud security
- Understand cloud management and security mechanisms

ITS 630 – Organization Leadership and Decision Making One of the most important skills a business leader needs to have concerning technology involves effective decision making and governance. This class will consist of a case study approach presenting different scenarios that require decisions to be made on technology issues that are relevant to today's business environment. Students will develop the skills for understanding the components and elements of these technology decisions, and assess associated risks. This course will draw upon a cross section of technology, finance, security, project management, leadership, and other aspects of effective decision making.

Upon completion of the course, students will be able to:

- Develop IT strategy for business value
- Understand business metrics
- Understand how to communicate with business managers
- Understand the management of IT-based risk
- Create and evolve a technology roadmap

ITS 631 – Operational Excellence This course focuses on the skills and knowledge to guide an organization in its best use of technology to achieve its business goals and objectives. Although technical knowledge and skills are essential for technology professionals, this course focuses on the development of more general leadership skills. The ability to communicate with a broad set of stakeholders is essential and this course will offer exercises in skills such as negotiation, persuasion, agility, coaching and facilitation through case studies, role playing and simulation. Technology leaders must also understand the elements of developing and implementing an overall IT Strategy for the organization. This course will review the various levels of strategy and how strategy is implemented through tactical and operational plans.

Upon completion of the course, students will be able to:

- Develop program strategy, objectives, activities, processes, and systems fully aligned with the business/mission strategy and objectives

- Understand the six D's of operational excellence
- Identify and prioritize improvement opportunities
- Understand measures of performance
- Understand performance assessments.

ITS 632 –Introduction to Data Mining The goal of the course is to introduce students to the current theories, practices, tools and techniques in data mining. Because many topics and concepts in data mining are learned most efficiently through hands-on work with data sets, we will spend time with software analyzing and mining data. The goal is to gain a better understanding of how data mining is applied and what is involved in data mining projects.

Upon completion of the course, students will be able to:

- Explain how businesses can gain competitive advantage through the mining of data.
- Describe when and how various data mining techniques should be applied.
- Understand the basic process and mechanics of data mining.
- Be able to make strategic recommendations based on data mining results.

ITS 699 – Information Technology Project* All students are required to demonstrate the ability to clearly evaluate a particular information technology need, identify potential solutions, evaluate the alternatives, and implement the best solution.

Upon completion of the course, students will be able to

- Demonstrate the ability to clearly evaluate a particular need related to information technology.
- Demonstrate the ability to discern the best method to address a particular need related to information technology.
- Demonstrate the ability to integrate their knowledge and skills base into a workable plan to address a particular need in information technology.

*Successful completion of INTR 599/799 will replace ITS699

ITS 831 – Information Technology Importance in Strategic Planning This course focuses on the information technology leader's collaborative roles working with an organization's senior leadership, including aligning business strategy with IT strategy, acting as an equal contributor to the formation of organizational strategy, and integrating ethical policies and practices into an organization. Learners evaluate multidisciplinary research and practices related to leadership, organizational structures, and culture. Through the lens of complexity/chaos and change theories, learners analyze information technology's role in contributing to organizational resiliency.

Upon completion of the course, students will be able to:

- Be proactive with risk management practices.
- Understand IT business management.
- Understand the economics of cloud computing.
- Understand the benefits of eco-efficient technology adoption
- Understand how to balance customer and shareholder value.

- Understand how emerging technologies effect strategic planning.

ITS 832 – Information Technology in a Global Economy This course covers theory, development and impacts of national and international policy on IT. It explores how frequent shifts in public policy require IT businesses to adjust rapidly to adhere to regulations. Students will develop sophisticated strategies to be able to adapt to the changing environment including new technologies, global transfer and analysis.

Upon completion of the course, students will be able to:

- Develop an understanding of public policy and how it impacts IT from a business and development standpoint.
- Demonstrate the ability to perform analyses related to trade policy, standards, domestic and international regulatory policy, and the impacts of changes in policy on the IT structure of a business.
- Describe an example of: (1) a public policy that had a positive impact on IT, and (2) a public policy that had a negative impact on IT.
- Discuss the current trends in the global IT arena ranging from technology, hardware, policy, software, and available services including out-sourcing.
- Define the activities and tools required to develop a sophisticated national and international strategy for IT.
- List and describe available tools to assist business organizations in the development of a competitive strategy.
- Understand how international and developing markets play an ever-changing role in IT; and integrate that understanding into an existing strategy to develop reasonable estimates of the effect of new products, services and vendors.
- Describe an example of the effect of an emerging market on global IT competition.

ITS 833 – Information Governance This course presents key issues related to the discipline of information governance and how it is being applied to electronic document and records management, email, social media, cloud computing, mobile computing, and, in fact, the management and output of information organization-wide. IG leverages information technologies to enforce policies, procedures and controls to manage information risk in compliance with legal and litigation demands, external regulatory requirements, and internal governance objectives. Information Governance: Concepts, Strategies, and Best Practices reveals how, and why, to utilize IG and leverage information technologies to control, monitor, and enforce information access and security policies.

Upon completion of the course, students will be able to:

- Compare and contrast information governance, IT governance and data governance.
- Understand information governance principles.
- Understand strategic planning and best practices for information governance.
- Understand information governance policy development.

ITS 834 – Emerging Threats and Countermeasures Covers security issues and current best practices in several applicative domains, ranging from the enterprise to the military. Discusses emerging security threats and available countermeasures with respect to the most recent

network and computing technologies, including wireless networks, computer-controlled physical systems, and social networks. Concludes by presenting current trends and open problems.

Upon completion of the course, students will be able to:

- Define and structure metrics to manage cybersecurity engineering.
- Identify and evaluate existing capabilities for cybersecurity engineering.
- Identify competency and capability gaps for cybersecurity engineering.
- Define and prioritize cybersecurity engineering needs.
- Exploring the options for addressing cybersecurity engineering needs.
- Summarize and plan for improvements in cybersecurity engineering performance

ITS 835 – Enterprise Risk Management This course goes beyond looking at risk management from the confines of quantitative topics to cover the full spectrum of risks that may emerge in enterprises. It covers a more holistic approach that includes the decisions and actions of employees in an active enterprise. It uses case studies to demonstrate the issues and challenges in total risk management. Finally, the course explore techniques for balancing enterprise risk and reward to enable performance optimization.

Upon completion of the course, students will be able to:

- Design and implement an appropriate ERM framework and risk governance structure customized to any type of organization.
- Conduct qualitative risk assessments to identify/prioritize key risks from among all risk sources.
- Quantify all types of risks, including strategic, operational, financial, and insurance.
- Develop a clear definition of risk appetite (the aggregate enterprise-level risk limit).
- Enhance strategic planning, increasing the likelihood of achieving strategic plan goals.
- Provide a rigorous business case for both business and mitigation risk-reward decision-making.
- Assure the board of directors that key risks are well understood and managed.
- Understand and satisfy ERM requirements from rating agencies, regulators, and shareholders.

ITS 836 – Data Science and Big Data Analytics In this course the students explore key data analysis and management techniques, which applied to massive datasets are the cornerstone that enables real-time decision making in distributed environments, business intelligence in the Web, and scientific discovery at large scale. In particular, students examine the map-reduce parallel computing paradigm and associated technologies such as distributed file systems, no-sql databases, and stream computing engines. This highly interactive course is based on the problem-based learning philosophy. Students are expected to make use of technologies to design highly scalable systems that can process and analyze Big Data for a variety of scientific, social, and environmental challenges.

Upon completion of the course, students will be able to:

- Identify fundamental concepts of Big Data management and analytics.

- will become competent in recognizing challenges faced by applications dealing with very large volumes of data as well as in proposing scalable solutions for them.
- will be able to understand how Big Data impacts business intelligence, scientific discovery, and our day-to-day life.

MSDF 530 – Investigation and Triage The student becomes familiar with the practical methodologies of digital forensics in this course. We discuss real world cases in the exciting, burgeoning field, such as digital forensics triage, investigations, and the prominent techniques and tools deployed in the profession.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Understand the challenges inherent to digital forensics in interconnected environments.
- Perform imaging and triage-based acquisition and extraction, and prioritize the resulting evidence.
- Build a practical toolkit, and deploy relevant techniques.

MSDF 531 – Windows Digital Forensics This example-driven course instructs the student to build a skillset in order to perform digital forensics examinations in the Windows environment. The core skills necessary to perform forensic analysis of digital data will be covered. We will learn how to acquire and analyze data from a Windows system. Many digital forensics tools and techniques will be used in this course.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Properly assemble different types of Windows-based evidence.
- Perform live analysis, and analyze volatile and nonvolatile data in the Windows environment.
- Triage Windows hard drives using forensics tools on the Windows Registry and systems logs.

MSDF 532 – Windows Registry Forensics In this course the student is guided through advanced forensic investigations of the Windows Registry system. From the Registry's background to its basic topics—*e.g.*, hive files, information in keys and values—to discovering the trove of available data, the learner will be prepared to prove that a specific user performed specific actions in a Windows platform.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Understand the structure of registry hive files, as well as information stored within keys and values that can have a significant impact on forensic investigations.

- Determine which files and folders a user accessed via recent docs keys and open/save keys in the Registry.
- Profile a computer system and its user activities using evidence found in the Registry.

MSDF 533 – Digital Forensics Tools and Techniques Learn about up-to-date free and open-source digital forensics tools. In this course, the learner not only gains experience using digital forensics tools but also will understand the "why" behind the "how" when analyzing a Windows system. The course includes lessons about data acquisition and analysis of USB devices, a key topic in digital forensics especially useful in workplace cases of the bring-your-own-device ("BYOD") nature that are on the rise.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Analyze Windows systems and processes using free and open-source tools.
- Track USB and BYOD devices that were connected to the system via the Registry and file system.
- Perform live response, file analysis, malware detection, and timeline construction.

MSDF 630 – Digital Forensics Evidence This engaging course introduces the learner to critical legal knowledge as designed, written, and taught by legal practitioners. When a civil or criminal case may end up in court, all of the digital forensics skills that IT professionals bear are at risk unless chain-of-custody is maintained and the rules of evidence are followed. Understanding evidence law, therefore, prepares the information security professional to put into full force her or his digital forensics analyses and effectively serve the corporate, private, or governmental client with utmost professionalism. MSDF 640 *Laws, Regulations, Investigations, and Compliance* and this course complement each other to place the learner at a great competitive advantage over peers who tend to leave the law to the lawyers.

Upon completion of the course, students will be able to:

- Understand the legal challenges inherent to admissibility of evidence derived from digital forensics.
- Perform cursory legal research about digital evidence
- Discern between admissible evidence in civil cases, criminal cases, and "evidence" applicable to internal investigations.
- Intelligently discuss and digital evidence and e-discovery concepts with legal counsel and law enforcement; and, potentially serve as a witness.

MSDF 631 – Malware Analysis and Mitigation This course focuses on malware in Windows environments. The student will understand the various techniques used to analyze different types of malware programs such as Trojan horses, botnets, and rootkits. As other MSDF courses do, so too does MSDF 660 provide the student with useful tools to perform digital forensics, here focused on analyzing and mitigating malware.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Use forensic software to recover and analyze deleted objects, and attendant meta data, from e-mail archives.
- Understand the dark side of the Internet known as malware and how it infects Windows systems via email attachments and Windows artifacts.

MSDF 632 – INFOSEC Leadership and Communications Without effective and efficient leadership in the security domain, both informational and physical, all of the analyses may be for naught. In this unique course offering among otherwise hard skills instruction in the MSDF program, the student will gain an advantage among professional peers by becoming an excellent communicator, and developing leadership skills. Technology professionals require both technological toolkits and "soft skills" abilities in order to inform and support law enforcement, executives, and similar lay-stakeholders. The ability to translate jargon into concise, actionable business actions results in added value.

Upon completion of the course, students will be able to:

- Effectively and efficiently communicate security concepts to all levels of an organization.
- Demonstrate core leadership skills in all facets of a security program.
- Provide useful approaches to organization design by applying the converged security model thereby positively impacting the business.

MSDF 634 – Web Browser Forensics In this unique course, the student will be provided with the knowledge, skills, and abilities to comprehensively understand web browser vulnerabilities. The approach taken includes becoming aware of browser-based risk by embracing tutorials designed by experienced browser hackers. Through this perspective, you will learn how hackers target Internet Explorer, Chrome, and Firefox web browsers, and therefore how to fight back against such attacks.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Track a user's activity in browser history and cache files and identify local file access.
- Exploit web browsers and their ecosystems including plugins and extensions while identifying anti-forensics activities and finding private browsing session data.

MSDF 699 – Digital Forensics Project* The proverbial rubber hits the road in this practical course where the student applies the knowledge and tools attained and obtained through successful completion of at least seven MSDF courses. While the student will likely be concurrently taking up to two other MSDF courses he or she will work with an assigned faculty member(s) to design a cybersecurity incident, draft and implement a response plan, acquire and analyze relevant data, and report the results in a mock attorney meeting with the goal of having the case picked up for prosecution.

Upon completion of the course, students will be able to:

- Prepare for the Global Information Assurance Certification's Certified Forensic Examiner certification exam.
- Utilize the tools and techniques discussed throughout the MSDF program's curriculum in order to identify potential evidence.
- Report about the most critical pieces of evidence discovered, what facts they tend to prove, and why their admissibility at trial is likely or not.
- Present the report's findings in a court brief meant to uphold the admissibility of the discovered evidence.

*Successful completion of INTR 599/799 will replace MSDF699

Curricular Practical Training

The School of Computer and Information Sciences, has graduate (masters and doctorate) programs in Digital Forensics, Information Security Systems, and Information Technology. These programs all have a curricular practical training component (internship/practicum (CPT)) that is an integral (essential) part of the established curriculum. These programs all require the student take part in an internship that is offered by the sponsoring employer through a cooperative agreement with the school. Additionally, due to the advanced nature of the**se** programs, students are often required to participate immediately in an internship.

"An F-1 student may be authorized by the DSO to participate in a curricular practical training program that is an integral part of an established curriculum. Curricular practical training is defined to be alternative work/study, internship, cooperative education, or any other type of required internship or practicum that is offered by sponsoring employers through cooperative agreements with the school."

Source: 2002 Final SEVIS Rule: 67 Fed. Reg. 76256 (December 11, 2002), amending 8 CFR 214.2(f)(10)(i)

Students who have received one year or more of full time curricular practical training are ineligible for post-completion academic training. Exceptions to the one academic year requirement are provided for students enrolled in graduate studies that require immediate participation in curricular practical training. A request for authorization for curricular practical training must be made to the DSO. A student may begin curricular practical training only after receiving his or her Form I–20 with the DSO endorsement

INTR 599/799 – Applied Learning Practicum (1 credit hour)*

This course provides students enrolled in an eligible master's program to participate in a Curricular Practical Training program that is an integral part of an established curriculum. This allows for the opportunity to apply essential professional applications to their respective academic coursework.

The Applied Learning Practicum can be either an alternative work/study, internship, cooperative education, or any other type of required internship or practicum in an area directly related to

the student's course of study, or project conducted in collaboration with program faculty applying coursework to a professional setting.

Through this course the University will have a Collaborative/Cooperative Agreement with any practicum or internship site prior to course enrollment. Department approval will be received prior to enrolling. The course can be repeated and would also fulfill CPT requirements for students on an F1 Visa. Offered as needed.

* For international students, within in the US for the first time on an F1 student visa and/or have not completed a year-long residency on an F1 student visa in the US, the INTR 599 is a required course for applied learning opportunities and success in this highly challenging program necessitates/requires immediate participation.

This course may be repeated.

Failure to complete this course will result in violation of USCIS CPT Regulation.