University of the Cumberlands

Master of Science in Information Security

Academic Handbook

and

Course Catalog

2016-2018

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.

Non-Discrimination Policy

University of the Cumberlands does not illegally discriminate on the basis of race, color, national or ethnic origin, sex, disability, age, religion, genetic information, veteran status, because a person is a smoker or nonsmoker, or any other basis on which the University is prohibited from discrimination under local, state, or federal law, in its employment or in the provision of its services, including but not limited to its programs and activities, admissions, educational policies, scholarship and loan programs, and athletic and other University -administered programs. In order to fulfill its purpose, the University may legally discriminate on the basis of religion in employment, and the University has sought and 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 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: Dr. Tom Fish, Dean of Undergraduate Studies, Retention, and Assessment, Library Office 021, (606) 539-4216. Tom.fish@ucumberlands.edu

The following person has been designated to handle employee inquiries or complaints regarding the sex nondiscrimination policy including compliance with Title IX of the Education Amendments of 1972: Ms. Pearl Baker, Human Resources Director and Title IX Coordinator, Gatliff Administration Office 116, (606) 539-4211. Pearl.baker@ucumberlands.edu

The following person has been designated to handle student inquiries or complaints regarding the sex nondiscrimination policy including compliance with Title IX of the Education Amendments of 1972: Dr. Emily Coleman, Student Success Coordinator and Deputy Title IX Coordinator, Gatliff Administration Office 103, (606) 539-4171. Emily.coleman@ucumberlands.edu

The following person has been designated to handle inquiries or complaints regarding all other portions of the non-discrimination policy: Mr. Steve Morris, Vice President for Business Services, Gatliff Administration Office 001, (606) 539-4597.

TABLE OF CONTENTS

Master of Science in Information Security
Academic Handbook and Course Catalog

University of the Cumberlands

Master of Science in Information Security

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.

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.

Admission Requirements

Admission to the master's 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.
- 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

Transfer of Credit Policy

A maximum of nine semester hours of credit may be transferred from an accredited graduate institution. 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 and have been earned within the last five years. Grades for any transfer credits accepted into the program do not count in the program GPA.

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 General Education 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**	Legal Regulations, Compliance, and Investigation Information Security Project	(ISC)2 CISSP
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)

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 program's Website (http://gradweb.ucumberlands.edu/information-technology-degree-program/overview).

Program of Study

The Master of Science in Information Systems Security is comprised of the following thirty-one (31) required credit hours: (ISOL 699 is one (1) semester hour; otherwise, each course is three (3) semester 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

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

Course Descriptions

Below are concise descriptions of each course in the Master of Science in Information Security program;

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 – 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.

Curricular Practice Training

INTR 599 – Applied Learning Practicum (1 credit hour)* This course provides students enrolled in a master's program an opportunity to apply professional applications to their respective academic coursework. The Applied Learning Practicum can be either a practicum or internship in an area directly related to the student's course of study, or a project conducted in collaboration with program faculty applying coursework to a professional setting. The University must have a Collaborative Agreement with any practicum or internship site prior to course enrollment. Department approval must 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 who are 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 799 is a required course for applied learning opportunities.

Policies and Procedures

Grading

The Information Security program 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. Students may have a maximum of two grades (six credit hours) of "C" on their transcript that count toward the degree. Students may retake a course once to raise a “C” grade."
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.
4. Students must complete all program requirements within four years of matriculation.

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.

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 instructor, 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 instructor of the disposition of the complaint no later than the last day of classes of the 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 M.S. in Information Security program 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 M.S. in Information Security program in accordance following 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 "aF") 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).

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.

Student Privacy and Informed Consent

Students pursuing a Master of Science in Information Security 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, 20202-4605.

Office of Financial Planning

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

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.

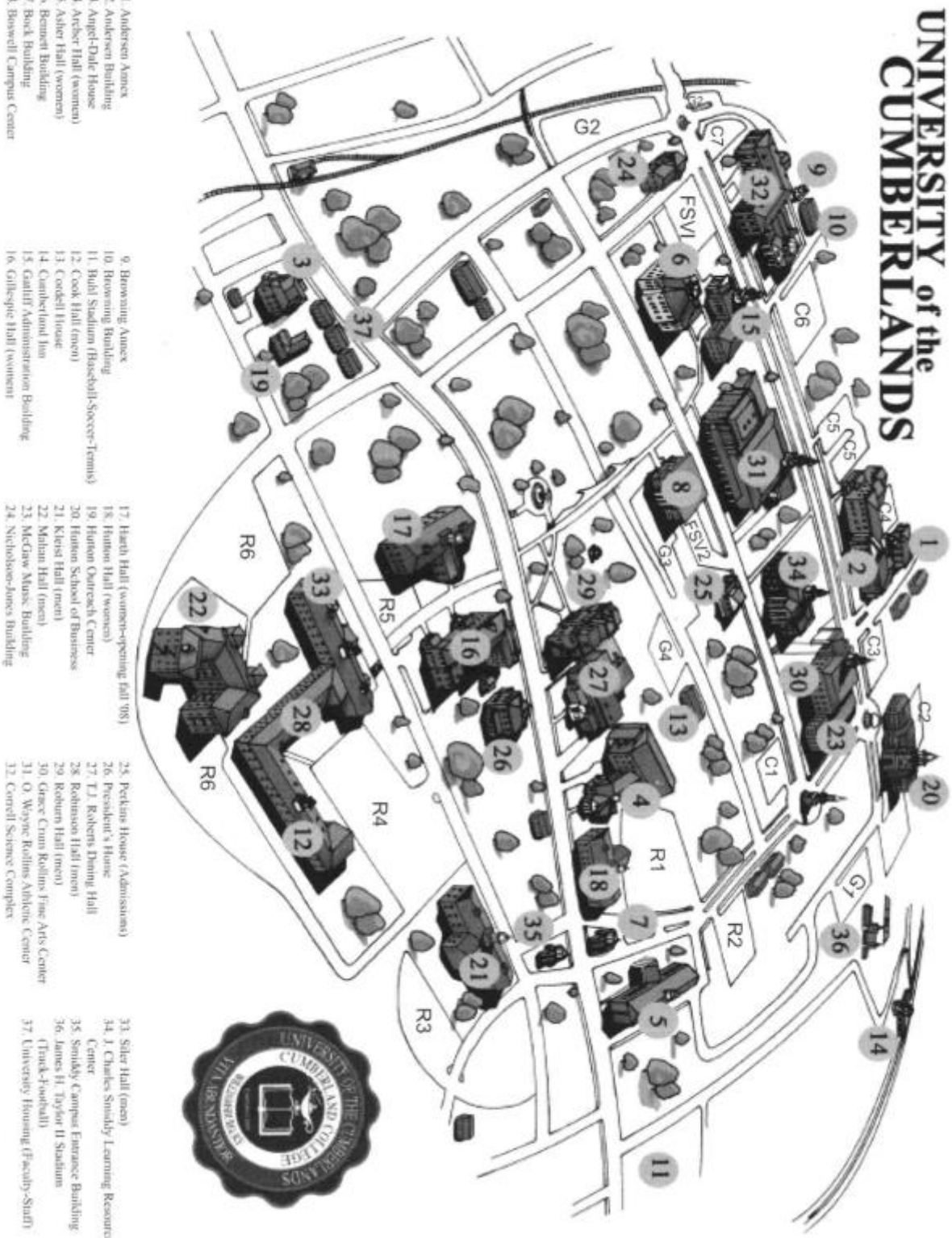
If you have questions about your Title IV program funds, you can call the Federal Student Aid Information Center at 1-800-4-fedaid (1-800-433-3243). TTY users may call 1-800-730-8913. Information is also available on Student Aid on the Web at www.studentaid.ed.gov.

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.

Campus Map


UNIVERSITY of the CUMBERLANDS
1. Andersen Annex
2. Andersen Building
3. Angel-Dale House
4. Archer Hall (women)
5. Asher Hall (women)
6. Bennett Building
7. Bock Building
8. Boswell Campus Center
9. Browning Annex
10. Browning Building
11. Bull Stadium (Baseball-Soccer-Tennis)
12. Cook Hall (men)
13. Cordell House
14. Cumberland Inn
15. Gaither Administration Building
16. Gillespie Hall (women)
17. Hareb Hall (women-opening fall '08)
18. Hutton Hall (women)
19. Hutton Outreach Center
20. Hutton School of Business
21. Kiest Hall (men)
22. Mahan Hall (men)
23. McGaw Music Building
24. Nicholson-James Building
25. Perkins House (Admissions)
26. President's House
27. T.J. Roberts Dining Hall
28. Robinson Hall (men)
29. Reburn Hall (men)
30. Grace Crum Rollins Fine Arts Center
31. O. Wayne Rollins Athletic Center
32. Cornell Science Complex
33. Siler Hall (men)
34. J. Charles Smiddy Learning Resource Center
35. Smiddy Campus Entrance Building
36. James H. Taylor II Stadium (Track-Football)
37. University Housing (Faculty-Staff)
C1
C2
C3
C4
C5
C6
C7
G1
G2
G3
G4
R1
R2
R3
R4
R5
R6
FSV1
FSV2