جامعة الأمير مساعد بن عبدالرحمن
Prince Musaid Bin Abdulrahman University
2011-1432

Student Handbook

Master in Cyber Security

Information Technology Department

College of Computing and Informatics

Prince Musaid Bin Abdulrahman University

Handbook Contents

Handbook contents 2
About the program 3
Program's mission and goals 4
Reasons for creating the program 5
Program learning outcomes 6
Teaching and learning strategies to achieve program learning outcomes 7
Program admission requirements 8
Admission procedures 9
Required documents for admission 10
Duration of study in the program 11
Tuition fees 11
Student rights and support 12
Program facilities and equipment 14
Program educational and research partnerships 16
Career opportunities for graduates of the program 17
Program's graduate attributes 18
Study plan structure 19
Program courses 20
Program courses description 21

About the program

Cybersecurity has become a critical need in the 21st century as users, enterprises and governments increasingly rely upon networked applications for assessing information and making critical business decisions. There is a significant shortage of Cybersecurity skills and expertise throughout the world. This program is designed to provide postgraduate students with a working knowledge of important security standards, techniques to exploit the current systems and networks, and technical depth in terms of expertise in the design of secure systems and their application to real-world problems in different industry sectors.

Program’s mission and goals

Mission:

Providing high-quality and flexible educational, scientific and research environment in the field of Cybersecurity to supply the labor market with qualified cybersecurity experts capable of performing professional services and producing innovative scientific research that contributes to the development of a knowledge society, meeting international requirements, solving community problems and facing future challenges in Cybersecurity.

Goals:

The program aims to provide learners with the knowledge and skills necessary to have the ability to:

1. Provide experts in the field of cybersecurity to perform innovative research in cybersecurity and help achieving the kingdom long term plan of having experts in the field of cybersecurity.
2. Empower students with soft skills and values to effectively communicate and collaborate with others professionally, ethically, legally and serve society's requirements.
3. Ensure the knowledge and skills of students are in line with state-of-the-art cybersecurity techniques.

Reasons for creating the program

The importance and reasons for creating the Master of Cybersecurity program:

1. Keeping pace with the needs of the labor market and the Kingdom's 2030 vision.
2. The need for qualified professionals with the necessary knowledge and skills in the field of Cybersecurity.
3. The need for qualified specialists in the field of combating electronic information crimes.
4. Specialists need to assess and analyze local and international breaches that may occur to information systems.
5. The need for specialists with the ability to know the various vulnerabilities of computer networks and the methods used to penetrate network security and provide comprehensive solutions to reduce these breaches.

Program learning outcomes

On successful completion of the program, students will have:

1. Explain in detail various cyber security models, their capabilities, structure, strengths and weaknesses; and the risks associated with transferring and storing information assets in global organizations.
2. Critically demonstrate state-of-the-art solutions to protect information assets from internal and external threats, risks and intrusions.
3. Analyze various strengths and weaknesses of IT networks and their vulnerabilities to both internal and external threats and intrusions.
4. Develop and evaluate the best cyber security practices and solutions for protecting the Internet and information networks from internal attacks, external cyber-attacks, and intrusions.
5. Demonstrate the application of effective teamwork, oral and written communication, and research skills.
6. Provide advanced solutions to ethical and legal issues related to use of Cybersecurity in local and global environments.

Teaching and learning strategies to achieve program learning outcomes

The Master of Cybersecurity program use several effective teaching strategies to achieve its mission, goals and learning outcomes. The most used teaching strategies are:

1. Group teaching (F2F Lectures)
2. Virtual sessions
3. Class discussions
4. Lab sessions
5. Active learning (group-work case studies and projects)
6. Interactive lectures
7. Individual capstone projects.
8. Presentations
9. Writing research papers

In addition, the Deanship of Admission and Student Affairs provides extracurricular activities for All Prince Musaid Bin Abdulrahman University students according to a plan seeking to achieve the PMAU educational goals. In addition, the Master of Cybersecurity students can:

1. Participate in Coding workshops/competitions.
2. Join Clubs

Program admission requirements

- Accepted Bachelor's majors: Computer Science, Computer Engineering, Information Systems, Software Engineering, and Information Technology.
- Bachelor's degree (regular or blended education) from a MOE-recognized university. If the certificate is obtained from abroad, it must be accredited according to the equivalency program provided by the Ministry of Education (MOE).
- Have a cumulative GPA in the bachelor’s degree should not be less than Good (2.00 out of 4.00 or 3.00 out of 5.00).
- Submit the result of one of the approved English language tests, either (IELTS-Academic) where (Indicator OR General Training) is not accepted and should be with a score of no less than 5 or (STEP) with a score of no less than 76 Or (TOEFL_IBT) with a score of no less than 45. The period for obtaining the result of the language tests, either (IELTS-Academic) or (STEP) should not exceed 3 years. As for (TOEFL), the result should not exceed 2 years. The validity period of the approved English language tests (3 years for IELTS Academic & STEP) and (2 Years for TOEFL) is excluded for the students who have obtained a bachelor’s degree from universities in countries where the native language is English, and the universities are recognized by the Ministry of Education. You need to submit only one test.
- Submit two scientific recommendations from your professors who thought you in your previous degree.
- If you are an employee, you need to submit a letter from your employer stating that you are permitted to study.
- Graduate assessment tests such as GMAT or GRE are not required, but they can be attached as support for acceptance when preference is given to applicants.
- Applicants should hold Saudi nationality, OR his/her mother is Saudi, OR has an official scholarship to study Master at PMAU.
- Applicants holding non-IT degrees can apply for admission after passing the Pre-Cyber-Security program which is one year in length (27 credits). However, the applicant has to have a bachelor degree in a scientific OR management field, or IT college graduate.
- Applicants who are initially have been accepted, are required to pay the full amount of first semester tuition to get final admission.

Admission procedures

1. Students must submit an admission application via the Admission Portal within the allocated timeframe.
2. A preliminary screening process is carried out by the Deanship of Graduate Studies based on the data provided in the application.
3. Selection criteria will be implemented by the colleges to select from applicants.
4. The Deanship of Graduate Studies will ensure that applicants meet the terms, conditions, and selection criteria.
5. The Deanship of Graduate Studies will upload an initial admission notice on the Admission Portal.
6. Applicants' documents confirmation is carried out at the University branches.
7. Students must pay first-semester tuition fees via the Admission Portal.
8. The Deanship of Graduate Studies will upload the final or conditional admission notice on the Admission Portal.

Required documents for admission

- The documents are submitted electronically through the document upload portal on the **admission site**, and the required documents are:
- A certified copy of the bachelor's degree (Required).
- A certified copy of the academic transcript record (Required).
- A certified copy of the accreditation decision from the Ministry of Higher Education in the event of obtaining the bachelor's degree from a university outside the Kingdom.
- A copy of the civil status card for Saudi students or valid Iqama for non-Saudi (Required).
- A copy of a valid residency permit for non-Saudi students who have official scholarship.
- A copy of the mother's national identity, for non-Saudi students with Saudi mothers.
- Original IELTS (Academic Only) or STEP result (Required).
- Submit two scientific recommendations from your professors who thought you in your previous degree (Academic recommendations only) (Required).
- If you are an employee, you need to submit a letter from your employer stating that you are permitted to study (The letter must clearly state permission to study) (Required).
- Other required documents per program:

    - The classification of the Saudi Commission for (Health care Administration program).
    - Work experience (Only for applicants to the Executive Master of Business Administration, Master of Healthcare Quality and Patient Safety).
    - Professional recommendation letter (Only for applicants to the Executive Master of Business Administration).

<u>It should be noted that:</u>

- If any of the required documents are missing, the application will not be accepted.
- Make sure that the uploaded documents are correct, the Deanship of Graduate Studies has the right to request your original documents for verification, and in case my information and document were inaccurate OR not available, then Prince Musaid Bin Abdulrahman University has the right to cancel your admission without refunding any paid fees and you take full responsibility for that.

- You are required to submit only one English test result.
- The period for obtaining the test result does not exceed two years and is excluded from the requirement. The validity period of the test is (two years) is excluded for the students who have obtained a bachelor's degree from universities in countries where the mother language is English and the universities are recognized by the Ministry of Education. You need to submit only one test.
- For IELTS submitters, make sure the test is Academic, and be advised that "Indicator OR General Training" are not accepted.

Duration of study in the program

- Four semesters, 36 credit hours (12 subjects).

Tuition fees

- Tuition fees for each accredited unit of study.
- Newly admitted students (initial admission) are required to pay the full semester tuition fees to obtain a final admission.
- The fees below don't include value added tax.
- Summer courses tuition fees: an increase of 50% of the fees for each credit hour.

Program	Tuition Fees per one credit	Total program credits	Total Tuition*
Master of Science in Cyber Security	2,250 Saudi riyals	36	81,000 Saudi riyals

* **Total tuition** = (36) Number of credits * (2,250) Riyal per credit = 81,000 Saudi Riyals

Student rights and support

The program, through department and college, provides students with assistance, information, referral and support on a range of academic and personal matters which include:

- Faculty members are required to post their contact information as well as office hours on Blackboard.
- All faculty have physical and virtual office hours each week. Students can contact them via email, video conference, messages, or phone. Faculty are also available throughout the week and respond to students.
- Students of the Master of Cyber Security program have the right to use the health care provided in the health facilities of Prince Musaid Bin Abdulrahman University.
- Students of the Master of Cyber Security program take advantage of the available credit services and facilities such as electronic university books, sports facilities, basements, car parking.
- The on-line Da'am system is available to solve any technical issues students face during lectures and exams.
- The periodic meeting for male and female students is held on a fixed basis at the beginning of each semester, where all students can send direct inquiries and raise inquiries to the Dean of the College of Computing and Informatics.
- Different activities and services were implemented at the Prince Musaid Bin Abdulrahman University and Information Technology department levels to support students during their study journey. For example, the Prince Musaid Bin Abdulrahman University has efficient Student care center portal contains all necessary units the student needs, such as the social counseling unit, Mental Health Support Unit, The academic advising unit, The career counseling and career support unit, The scholarship and aid unit, Talent and Creativity Unit, and the Disabilities Support Unit. This Student care center portal can be reached via https://seu.edu.sa/aasa/en/student-care-center/
- The university seeks to guarantee students' rights and seeks to educate them about their rights and responsibilities. Therefore, the university established two committees to protect students' rights

Sub-Committee for the Protection of Student Rights:

- It considers all educational and administrative grievances and complaints of students, except for administrative matters outside the framework of the college.

Main Committee for Student Rights Protection:

- It considers all students 'grievances and complaints filed against the administrative authorities at the university and grievances coming from the sub-committees.

Special support

- In collaboration with Students Affairs Office, the requirements for special need applicants are provided. Such as elevators between classes' floors, cars' parking and toilets' seats. In addition, the Prince Musaid Bin Abdulrahman University has efficient student care center portal contains all necessary units the student needs, such as the social counseling unit, Mental Health Support Unit, The academic advising unit, The career counseling and career support unit, The scholarship and aid unit, Talent and Creativity Unit, and the Disabilities Support Unit. This student care center portal can be reached via https://seu.edu.sa/aasa/en/student-care-center/

- Moreover, students with special needs are provided with dedicated programs designed to serve them on an individual basis. In addition, there is a specialized psychological and social counseling unit to provide help when needed (Email: pscu@seu.edu.sa).

- Talented and outstanding students receive financial incentives and rewards. The College of Computing and Informatics is challenging talented students through different completions. This contribution aims to spread the spirit of competition among students and motivate them to excel and be creative. The college regularly holds a competition to select the best graduation projects at the level of all university branches and is evaluated by a group of faculty members, as the competition includes educational and applied fields for undergraduate students and Masters. The college also encourages and supports students to participate in local and international conferences and competitions, such as cybersecurity conferences and competitions, programming competitions, and artificial intelligence.

Program facilities and equipment

Different campuses provide modern classrooms with electronic gadgets required for the smooth execution of class hours. The students also avail the opportunities to interact with faculty during visiting hours who are required to be in their allocated office spaces, which are also furnished with all facilities needed for a blended learning environment, including needed hardware and software.

- IT equipment's include:

    1. State of the art computing machines and laptops for faculty members.
    2. 24 hours uninterrupted high-speed Internet provision at all the campuses.
    3. Provision of Prince Musaid Bin Abdulrahman University portal accounts to all the students and faculty members.
    4. Blackboard system as a teaching platform with accounts for all teachers and students to manage their academic activities and conduct virtual sessions.
    5. Attendance, grading, E-mail, and other relevant software.
    6. Access to Saudi Digital Library for all students and faculty alike.

- Blackboard includes full course contents for faculties and students enrolled for any particular course. This includes all needed references.

- Online books are available from WileyPlus, with which the University has a contract.

- The College of Computing and Informatics college also offers hard copies of textbooks to faculty members.

In addition, the Prince Musaid Bin Abdulrahman University has a collection development policy where the librarians communicate with stakeholders to identify strengths and weaknesses to best align the collection with current research and curricular needs. The librarian makes final purchasing decisions with input from the administration, faculty, and students.

The Prince Musaid Bin Abdulrahman University librarian brings new resources to the attention of different stakeholders for consideration, coordinates trials to electronic resources, negotiates site licenses and user agreements, maintains current subscription lists as well as works with select consortia/ Prince Musaid Bin Abdulrahman University to share resources.

The following selection criteria are considered when evaluating resources:

1. Facilitation of online teaching and learning.
2. Provision of relevance to the existing collection's strengths and weaknesses.
3. Restrictions on the number of users, simultaneous users, or access points.
4. Delivery to users in a timely and convenient manner.

5. Affordability, or comparative cost including the cost of acquisition, licensing, maintenance, service, and potential preservation.
6. Availability of technical support and acceptable licensing requirements.

In addition, the Prince Musaid Bin Abdulrahman University has a subscription to the Saudi Digital Library to provide E-books and other publications for all its employees and students, where each Prince Musaid Bin Abdulrahman University's employee or student can access Saudi Digital Library and directly download scientific references. The Saudi Digital Library can be accessed via the available icon on the Prince Musaid Bin Abdulrahman University's homepage or directly from their website.

It is mandatory for all classes to be held in professionally designed classrooms during the face-to-face hour. Each class is equipped with an electronic podium with the facility to record lecture and sound control apart from other features. Each classroom is connected to the Internet. Multimedia support is available in every classroom. In addition, each classroom is equipped with general amenities like air-conditioning, sufficient lighting, and proper sitting arrangements. All classrooms are regularly monitored to ensure that none of the assets is in bad or disorderly shape.

Program educational and research partnerships

The Prince Musaid Bin Abdulrahman University collaborated with the Colorado State University to develop the Master of Cybersecurity program and teach the program course. The Colorado State University is one of long-distance international accredited degree universities and is the first statutorily defined 100% online public university in the United States.

The Prince Musaid Bin Abdulrahman University is continuing the partnership collaboration with Colorado State University to deliver e-learning content to the students of the Master of Cybersecurity program. Each course is delivered to the Master of Cybersecurity program students by two faculty members: one from the Prince Musaid Bin Abdulrahman University and one from the Colorado State University.

Career opportunities for graduates of the program

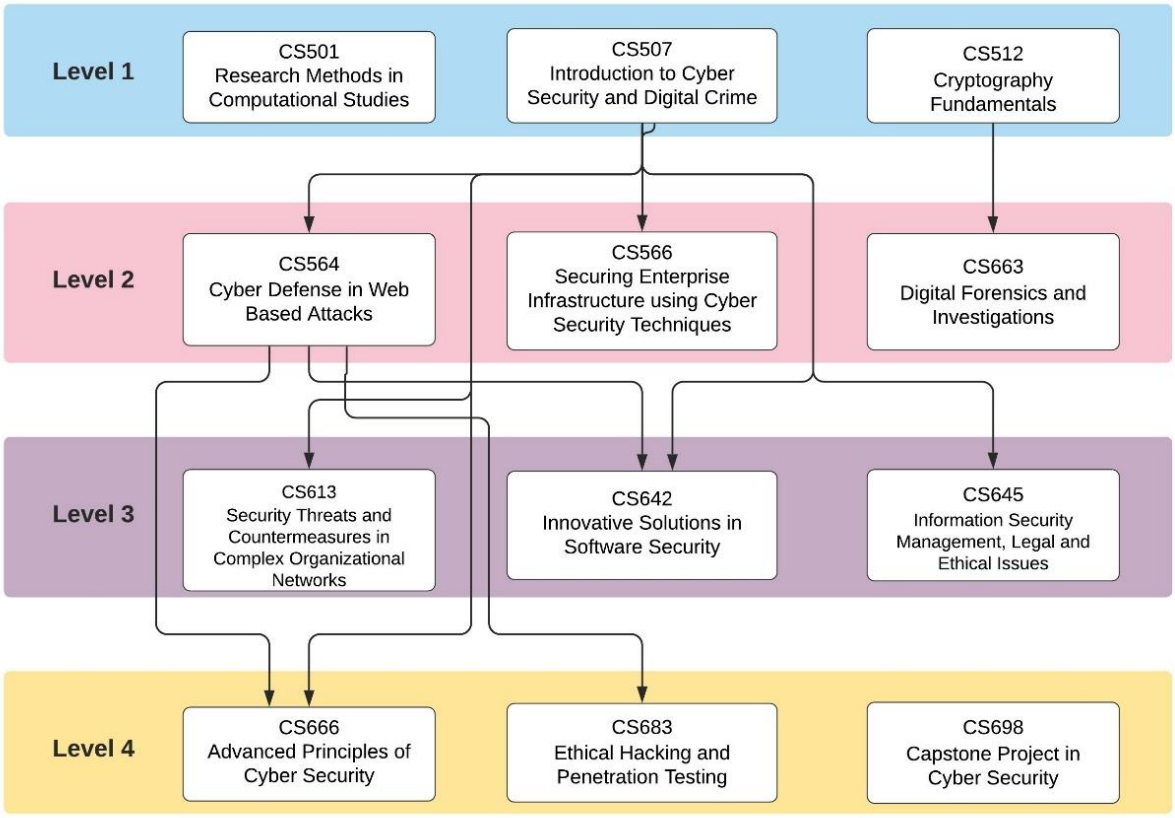
At the end of the program, students will be prepared for the following professions and occupations:

1. Project Manager.
2. Information Security Analyst.
3. Cyber Security Manager.
4. Cyber Security Analyst.
5. Information Security Manager.
6. Information Technology Manager.
7. Network Security Manager.
8. Network Security Analyst.
9. Educational and academic field occupations in general and higher education institutions.

Program’s graduate attributes

1. Preparation of trained cybersecurity professionals to meet high international standards by academic programs.
2. Use the knowledge to prevent cyberattacks and cybercrimes against data, systems and equipment threats.
3. Recognize security problems and violations and find fast solutions by implementing various strategies, creating security plans, and tracking network activities.
4. To use the skills and experience acquired in enterprise to help economic development.
5. Capable of improving personal skills considering change and development, self-development and continuing education.
6. Commitment to professional ethics.
7. Creative and critical thinking.
8. Effective communication orally and in written forms.
9. Effective teamwork collaboration.
10. Commitment to professional ethics.
11. Lifelong learning and continuing education.

Study plan structure



Program courses

Level	Course Code	Course Title	Required or Elective	Pre-Requisite Courses	Credit Hours
Level 1	CS501	Research Methods in Computational Studies	Required	-	3
	CS507	Introduction to Cyber Security and Digital Crime	Required	-	3
	CS512	Cryptography Fundamentals	Required	-	3
Level 2	CS564	Cyber Defense in Web Based Attacks	Required	CS507	3/ Lab
	CS566	Securing Enterprise Infrastructure using Cyber Security Techniques	Required	CS507	3/ Lab
	CS663	Digital Forensics and Investigations	Required	CS507	3/ Lab
Level 3	CS613	Security Threats and Countermeasures in Complex Organizational Networks	Required	CS507	3/ Lab
	CS642	Innovative Solutions in Software Security	Required	CS507 & CS564	3/ Lab
	CS645	Information Security Management, Legal and Ethical Issues	Required	CS507	3
Level 4	CS666	Advanced Principles of Cyber Security	Required	CS507 & CS564	3/ Lab
	CS683	Ethical Hacking and Penetration Testing	Required	CS564	3/ Lab
	CS698	Capstone Project in Cyber Security	Required	Department Approval	3

Program courses description

COURSE NAME: **Research Methods in Computational Studies**

COURSE CODE: **CS501**

COURSE DESCRIPTION: This course provides an overview of the important concepts of research design, data collection, statistical and interpretative analysis, and final report presentation. The focus of this course is not on mastery of statistics but on the ability to use research in Computational Studies. Students will prepare a preliminary research design for projects in their subject matter areas and how to accurately collect, analyze and report data.

Students will focus on the steps needed to design an individual research project or thesis. The course provides real world active learning assignments that seek to integrate the knowledge and skills gained through undergraduate course work. The course focuses on scientific writing, and oral, written, and graphical presentation of data and research results.

COURSE NAME: **Introduction to Cyber Security and Digital Crime**

COURSE CODE: **CS507**

COURSE DESCRIPTION: This course provides an introduction to cyber security and digital crime. Students will learn about cyber security threats, dangers, and risks that organizations face and will develop the ability to analyze potential vulnerabilities that can have an adverse impact on digital assets.

COURSE NAME: **Cryptography Fundamentals**

COURSE CODE: **CS512**

COURSE DESCRIPTION: This course provides students with a thorough review of cryptography and cryptographic techniques as they apply to the area of cyber and computer security. Students will learn about various cryptography techniques along with their advantages and disadvantages. Additionally, discussion will be provided on the various systems that are used to provide secure and encrypted end-to-end communications to include: pre-shared keys, hashing algorithms, certificates, public-key/private key infrastructures and shared secret keys.

COURSE NAME: **Cyber Defense in Web Based Attacks**

COURSE CODE: **CS564**

COURSE DESCRIPTION: This course focuses on external cyber security threats including information networks and the World Wide Web. There will be a detailed view into search engines and current trends of integrating social media outlets into the enterprise as a mean of achieving strategic objectives.

COURSE NAME: **Securing Enterprise Infrastructure using Cyber Security Techniques**

COURSE CODE: **CS566**

COURSE DESCRIPTION: This course gives the students the knowledge and hands on experience of protecting infrastructure services. It covers fundamentals and advanced topics in theoretical and practical infrastructure security. It explains mechanisms and policies. The course also covers types of malware and threats, and techniques used to defend against such threats. Students will have the opportunity to investigate recent research papers and existing technologies relevant to the course topics.

COURSE NAME: **Digital Forensics and Investigations**

COURSE CODE: **CS663**

COURSE DESCRIPTION: This course provides students with insight to cyber security professional intrusion detection methods, cyber security tools, and preventative measures to cyber security risks. Students will learn how to respond to cyber breaches including the recovery, preservation, analysis of digital crime scene evidence, and proper incident response to cyber criminals.

COURSE NAME: **Security Threats and Countermeasures in Complex Organizational Networks**

COURSE CODE: **CS613**

COURSE DESCRIPTION: The course details different network infrastructure security threats, attacks and countermeasures at different organizational network layers including perimeter security defenses, firewalls, virtual private networks, intrusion detection systems, wireless security, mobile network and network security auditing tools.

The following topics will be covered: Network security protocols, Network threats and attacks, Malware, and Defense mechanisms and countermeasures.

COURSE NAME: **Innovative Solutions in Software Security**

COURSE CODE: **CS642**

COURSE DESCRIPTION: This course discusses how to construct secure innovative programs. The course explores secure software development through the use of secure coding, program analysis, and advanced testing. The course details secure programming techniques to defend against source code software vulnerabilities such as overwriting, buffer overflow and code injection. Overview is given for secure web application development against web attacks such as SQL injection, Cross-Site Scripting (XSS), secure session management, and secure authentication.

COURSE NAME: **Information Security Management, Legal and Ethical Issues**

COURSE CODE: **CS645**

COURSE DESCRIPTION: This course examines security governance and policies and how law, ethics, and technology intersect in organizations that rely on information technology. Students will gain an understanding and insight into issues arising from privacy, secrecy, access control, and policy management and enforcement, as well as other legal, and ethical dilemmas prevalent in today's organizations. Special module(s) will be dedicated to study Saudi Laws related to information management and security.

COURSE NAME: **Advanced Principles of Cyber Security**

COURSE CODE: **CS666**

COURSE DESCRIPTION: This course provides students with an overview of cyber security access control to protect resources against unauthorized viewing, tampering, or destruction to ensure privacy, confidentiality, and prevention of unauthorized disclosure. Access Control, Authentication, and Public Key Infrastructure define the components of access control, provide a business framework for implementation, and discuss legal requirements that impact access control programs. The course looks at the risks, threats, and vulnerabilities prevalent in information systems and IT infrastructures and how to handle them.

COURSE NAME: **Ethical Hacking and Penetration Testing:**

COURSE CODE: **CS683**

COURSE DESCRIPTION: This course provides students with the experience needed to secure information systems against attacks such as viruses, worms, as well as other system weaknesses that pose significant danger to organizational data. Students learn ethical hacking and penetration testing to uncover common techniques used by cyber criminals to exploit system vulnerabilities.

COURSE NAME: **Capstone Project in Cyber Security**

COURSE CODE: **CS698**

COURSE DESCRIPTION: In the capstone project students explore the literature, conduct research and develop solutions to help analyze organizations security needs related to continuously evolving security challenges. Students will analyze organizational objectives and propose solution(s) and implementation plan(s). The proposed solution must address strategies to overcome challenges of cyber security related projects such as assessing risks, reduction of fund, and keeping the support of executive management. Students will utilize skills gained throughout the program to demonstrate the ability to design a cyber security project from conception to publishing/deployment.