CYBERSECURITY ANALYTICS AND OPERATIONS

Graduate Program Head	Mary Beth Rosson
Program Code	CYMPS
Campus(es)	University Park (M.S.) World Campus (M.P.S.)
Degrees Conferred	Master of Science (M.S.) Master of Professional Studies (M.P.S.)
The Graduate Faculty	View (https://secure.gradsch.psu.edu/gpms/?searchType=fac&prog=CYMPS)

The Master of Science in Cybersecurity Analytics and Operations program is designed to create a deep understanding of cybersecurity analytics and operations, by blending education relating to technology, incident response, strategic planning, and crisis management. The program also aims to prepare the next generation of cybersecurity analysts to better protect digital information from attack through cyberdefense strategies, including incident response, strategic planning, and crisis management. With a foundation in mathematics and computer programming, students will be prepared to recognize, analyze, defend against, and manage risks related to a wide range of threats to online information, data stores, and networks. The program will be delivered in a resident format that takes one to two years. The total credits of the program is 30. A one-year program starts in a Fall semester, and concludes at the end of the following Summer.

The Master of Professional Studies in Cybersecurity Analytics and Operations (MPSCY) is an innovative program that targets professionals and organizational leaders who seek a professional education and training program. The purpose of the professional master's program is to produce professionals and organizational leaders who not only can select and draw upon the necessary foundations within the cybersecurity analytics and operations technology areas, test the applicability of these foundations for addressing a given issue, and apply the resulting solutions, but also can be aware of the multitude of technological trends and environmental factors that organizations must address in the changing global economy. The M.P.S. equips students to: understand and analyze the profound information and technological changes sweeping the world; meet challenges by developing innovative solutions using the foundations of cybersecurity analytics and operations; and have a clear advantage in today's highly competitive and dynamic environment by continuously learning new trends, issues, and innovations.

Admission Requirements

Applicants apply for admission to the program via the Graduate School application for admission (http://gradschool.psu.edu/prospective-students/how-to-apply/). Requirements listed here are in addition to Graduate Council policies listed under GCAC-300 Admissions Policies (http://gradschool.psu.edu/graduate-education-policies/).

Master of Professional Studies (M.P.S.)

Applicants to the M.P.S. program are required to submit three letters of reference, and a one-three page personal statement of relevant experience and goals.

Because the M.P.S. program is multidisciplinary in nature, students from many different disciplines may be accepted for entry into the program. A bachelor's degree in a related area (e.g., engineering and science), while not necessary for admission, is helpful in the successful completion of the degree. It is expected that students will have a basic level of competency in statistics, as well as computer and information technology. Related work experience can be used to demonstrate such competency. A student may be accepted into the program with provisional status (http://gradschool.psu.edu/graduate-education-policies/gcac/gcac-300/provisional-admission/) for no more than one year while work is completed to meet these expectations.

It is expected that the successful applicant will have an overall grade point average of 3.00 (on a 4.00 scale) or higher for his or her undergraduate study and/or graduate-level study. However, accomplishments demonstrated through work experience and recommendation letters from the applicant's academic adviser or employer will also play an important role in making the admission decision. The most qualified applicants will be accepted into the program until all spaces for new students are filled.

Master of Science (M.S.)

Applicants to the M.S. program are required to submit three letters of reference, a current resume (including present position and any publications), 1 to 3 page statement of goals related to pursuing an advanced degree and career in IST and provide a sample of the applicant's writing (e.g. technical paper, etc.).

Because cybersecurity analytics and operations career opportunities exist in many disciplines, students with a wide range of disciplinary backgrounds may be accepted into the program. A bachelor's degree in a related area (e.g., engineering and science), while not necessary for admission, is helpful in the successful completion of the degree. However, it is expected that students will have a basic level of competency in mathematics and programming.

Entrance Requirement regarding Mathematics: Applicants must complete a Calculus course equivalent to Penn State University's MATH 110 or MATH 140.

Entrance Requirement regarding Programming: Applicants must complete two introductory-level programming courses where both courses used the same language. If an applicant believes his/her work experience satisfies the background, he/she should include a recommendation letter from a technical colleague describing the applicant's coding contributions at work. In addition, students who meet all other academic requirements, but need to improve identified gaps in specific programming skills areas, will have access to educational bridge materials to help improve certain knowledge domains

It is expected that the successful applicant will have an overall grade point average of 3.50 (on a 4.00 scale) or higher for his or her undergraduate study and/or graduate-level study. However, accomplishments demonstrated through work experience and recommendation letters from the applicant's academic adviser or employer will also play an important role in the admission decision as well. The most qualified applicants will be accepted into the program until all spaces for new students are filled.

Degree Requirements

Master of Professional Studies (M.P.S.)

Requirements listed here are in addition to Graduate Council policies listed under GCAC-700 Professional Degree Policies (http://gradschool.psu.edu/graduate-education-policies/).

The M.P.S. program requires a minimum of 33 credits, 24 of which must be earned at Penn State. A maximum of 9 transfer credits of high-quality graduate work may be applied toward the requirements for the degree, subject to restrictions outlined in GCAC-309 Transfer Credit (http://gradschool.psu.edu/graduate-education-policies/gcac/gcac-300/gcac-309-transfer-credit/). At least 18 credits must be courses at the 500 or 800 level, with at least 6 credits at the 500 level.

The 33 credits are distributed among the following requirements. A student first takes 21 credits of core courses. The student then takes 9 credits of electives. Lastly, the student must complete a master's project guided by the student's adviser and completed while enrolled in IST 594.

Elective Courses

The elective courses for the M.P.S. will be selected from a list maintained by the program office.

Master'S Project

The project requires all students in the M.P.S. to focus on a well-defined issue or problem relevant to the information sciences and technology. The student will submit a project proposal to his/her faculty adviser for approval. Upon completion of the project, the student will share or present the project results at a final presentation as a component of IST 594.

Code	Title	Credits
Required Courses		
INSC 561	Web Security and Privacy	3
IST 451	Network Security	3
IST 456	Information Security Management	3
IST 543	Foundations of Software Security	3
IST 554	Network Management and Security	3
IST 815	Foundations of Information Security and Assurance	3
IST 820	Cybersecurity Analytics	3
Electives		
Select 9 credits of electives from a list of approved electives available from the program office.		9
Culminating Experience		
IST 594	Research Topics (Master's Project)	3
Total Credits		**33**

Master of Science (M.S.)

Requirements listed here are in addition to Graduate Council policies listed under GCAC-600 Research Degree Policies. (http://gradschool.psu.edu/graduate-education-policies/)

The M.S. in Cybersecurity Analytics and Operations requires a minimum of 30 credits at the 400, 500, 600, or 800 level, with at least 18 credits in the 500 or 600 series combined; 27 of the 30 credits must be earned at Penn State. Students will be able to complete the proposed Master's program in one calendar year (including summer) or two academic years. All of the courses listed below are three credit hour courses, unless otherwise noted. Students pursuing the one-year format must complete the non-thesis track (IST 594). In addition, the one-year M.S. track must adhere to the following conditions:

- Students must take at least one credit of research (IST 594) for each of the three semesters (Fall, Spring, and Summer).
- A research adviser must be assigned to students in their first semester, as selection and discussion of the student's research topic must begin as soon as possible.
- Students who need more time to complete the final paper must be allowed to complete the paper, and have it reviewed and approved after the third semester (Summer) has ended. Students are not required to remain in residence while they complete the final paper. However, extensions granted to students in this program must comply with the Graduate Council policy on deferred grades (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-400/gcac-401-grading-system/).

These 30 credits are distributed among the following requirements:

Code	Title	Credits
Required Courses		
IST 543	Foundations of Software Security	3
IST 554	Network Management and Security	3
IST 815	Foundations of Information Security and Assurance	3
IST 820	Cybersecurity Analytics	3
INSC 561	Web Security and Privacy	3
Electives		
Choose 9-12 Credits from the following:		9-12
IST 451	Network Security	
IST 454	Computer and Cyber Forensics	
IST 456	Information Security Management	
IST 504	Foundations of Theories and Methods of Information Sciences and Technology Research	
IST 511	Information Management: Information and Technology	
IST 555	Intelligent Agents and Distributed Decision Making	
IST 557	Data Mining: Techniques and Applications	
IST 558	Data Mining II	
IST 564	Crisis, Disaster and Risk Management	
IST 816	Web Fundamentals	
IST 841	Search Engines & Information Retrieval	
IST 868	Topics in Visual Analytics for Security Intelligence	
Culminating Experience		
IST 594	Research Topics (Scholarly Paper)	6
or IST 600	Thesis Research	
Total Credits		**30**

Students can choose to complete a thesis or a scholarly paper as the culminating experience for the degree. Students who choose to complete a thesis must complete at least 6 credits in thesis research (IST 600 or IST 610). The thesis must be accepted by the advisers and/or committee members, the head of the graduate program, and the Graduate School, and the student must pass a thesis defense. Students in the non-thesis track must write a satisfactory scholarly paper while enrolled in IST 594 and complete at least 18 credits at the 500 level.

Minor

A graduate minor is available in any approved graduate major or dual-title program. The default requirements for a graduate minor are stated in Graduate Council policies listed under GCAC-600 Research Degree Policies (http://gradschool.psu.edu/graduate-education-policies/) and GCAC-700 Professional Degree Policies (http://gradschool.psu.edu/graduate-education-policies/), depending on the type of degree the student is pursuing:

- GCAC-611 Minor - Research Doctorate (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-600/gcac-611-minor-research-doctorate/)
- GCAC-641 Minor - Research Master's (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-600/gcac-641-minor-research-masters/)
- GCAC-709 Minor - Professional Doctorate (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-700/gcac-709-professional-doctoral-minor/)
- GCAC-741 Minor - Professional Master's (https://gradschool.psu.edu/graduate-education-policies/gcac/gcac-700/gcac-741-masters-minor-professional/)

Student Aid

Refer to the Tuition & Funding (http://gradschool.psu.edu/graduate-funding/) section of The Graduate School's website. Students in this program are not eligible for graduate assistantships.

World Campus students in graduate degree programs may be eligible for financial aid. Refer to the Tuition and Financial Aid section (http://www.worldcampus.psu.edu/tuition-and-financial-aid/) of the World Campus website for more information.

Courses

Graduate courses carry numbers from 500 to 699 and 800 to 899. Advanced undergraduate courses numbered between 400 and 499 may be used to meet some graduate degree requirements when taken by graduate students. Courses below the 400 level may not. A graduate student may register for or audit these courses in order to make up deficiencies or to fill in gaps in previous education but not to meet requirements for an advanced degree.

Information Sciences and Technology (IST) Course List (https://bulletins.psu.edu/university-course-descriptions/graduate/ist/)

Learning Outcomes

Master of Professional Studies (M.P.S.)

1. [KNOW] Recognize, understand, identify and assess potential threats, vulnerabilities, and consequences in a context from local to global environments.
2. [APPLY/CREATE] Integrate the use of disciplinary methods, techniques, and knowledge to solve practical, real-world problems.
3. [COMMUNICATE] Present scientific evidence and best practice to inform and improve practical, real-world decisions.
4. [THINK] Search, evaluate, and synthesize literature to integrate cyber security principles into disciplines and professional fields.
5. [PROFESSIONAL PRACTICE] Make use of ethical standards and principles of integrity as a foundation in decision-making.

Master of Science (M.S.)

1. [KNOW] Demonstrate appropriate breadth and depth of interdisciplinary knowledge and comprehension of the major issues in cybersecurity analytics and operations.
2. [APPLY/CREATE] Use interdisciplinary knowledge and methods of cybersecurity analytics and operations to plan and conduct a research thesis or scholarly paper.
3. [COMMUNICATE] Communicate the major issues of cybersecurity analytics and operations effectively.
4. [THINK] Demonstrate analytical and critical thinking within cybersecurity analytics and operations, including across discipline.
5. [PROFESSIONAL PRACTICE] Know and conduct themselves in accordance with the highest ethical standards, values, and, where these are defined, the best practices of cybersecurity analytics and operations (as expressed in SARI training modules).

Contact

Campus	University Park
Graduate Program Head	Mary Beth Rosson
Program Contact	Christina Marie Fitzgerald cml195@psu.edu (814) 863-9461
Program Website	View (https://ist.psu.edu/prospective/graduate/)
Campus	World Campus
Graduate Program Head	Mary Beth Rosson
Director of Graduate Studies (DGS) or Professor-in-Charge (PIC)	Edward J Glantz
Program Contact	Christina Marie Fitzgerald College of Information Sciences and Technology E397 Westgate Building University Park PA 16802 cml195@psu.edu (814) 863-9461
Program Website	View (https://www.worldcampus.psu.edu/degrees-and-certificates/penn-state-online-cybersecurity-analytics-and-operations-masters-degree/overview/)