POLYTECHNIC INSTITUTE

OU-Tulsa Schusterman Center
4502 East 41st Street
Tulsa, OK 74135
Phone: (918) 660-3456

Administrative Officer

- Teri K. Reed, PH.D., MBA, F.ASEE
  Director of the OU Polytechnic Institute, Professor and George Kaiser Family Foundation Chair

Administrative Staff

- Tarah Hayes, Executive Assistant

Student Services and Advising Staff

- Lauren Deerdoff, Recruiting and Admissions Counselor
- Tally Begaye, Admissions Communications Coordinator

General Information

First announced in 2022, the OU Polytechnic Institute (OUPI) represents a significant advancement for the Tulsa community and region, aiming to address the growing demand in northeast Oklahoma for highly skilled workers in essential STEM fields. This initiative underscores the region's commitment to becoming a leading center for technological growth and employment opportunities.

Developed in collaboration with industry leaders, the school's curriculum is specifically designed to rapidly establish northeast Oklahoma as a technological hub, fostering economic growth and job creation. By offering cutting-edge programs, OUPI equips graduates with the skills to revolutionize Oklahoma's industries.

This degree completion program requires 60 credit hours of 3000-4000 level classes and is structured to be completed within two years, culminating in a Bachelor of Science degree from the University of Oklahoma. Graduates will be positioned to excel in diverse career opportunities available both locally and globally. Through a combination of hands-on learning, interdisciplinary projects, internships, and industry-sponsored senior design projects, students will gain invaluable real-world experience, preparing them to lead Oklahoma into a new era of technological advancement and economic growth.

The Polytechnic Institute embodies learning by doing, providing a practical education in today's digital landscape. The program incorporates a strategic breadth of study coupled with integrated content designed to provide mastery in essential work ready skills including terminal proficiency, collaboration (comprehensive project portfolio), and demonstrable project management and delivery. Additionally, the curriculum is designed to build a student's professional network with other students, faculty as well as local and national employers. It's about fueling innovation through technology and preparing students in Tulsa to propel Oklahoma forward. This approach not only enriches the educational experience but also prepares students to meet the challenges of the future, driving innovation and leadership in the tech sector.

OUPI focuses on high-demand, advanced and applied technology-based education and prepares graduates to transform industries in Oklahoma. From curriculum to on-site training, programs at OUPI will help meet the changing academic and workforce needs of the Tulsa region largely thanks to our close working relationship with industry partners. All classes are in person, hands-on, and in Tulsa.

Programs Offered

- Cybersecurity, B.S.

Programs and Facilities

Computing

The OU Network consists of a high-speed backbone with connections to faculty, staff, laboratory, and classroom computers. Wireless technology extends the network to cover the Polytechnic building, outside areas, laboratories, and classrooms. For more detailed information, visit the https://www.ou.edu/tulsa/it

Support Infrastructure:

The Information Technology department and OUPI have partnered to provide a comprehensive computer support infrastructure. This includes wireless coverage, repair services, network file storage, and classrooms equipped with additional power and network capabilities.

Wireless:

All OUPI buildings have wireless coverage throughout. To connect, choose the network called "WIFI@OU". Registration of your device with your 4+4 is required to access this network. Campus guests can receive temporary, limited access by connecting to the "OUGuest" network.

Repair Services:

IT provides student support for all computing needs. To locate the nearest IT Service Center, visit needhelp.ou.edu. The IT Service Centers are Dell and Apple certified warranty repair centers and provide support for these and other brands of computers. This service is free of charge, excluding any parts.

The OU IT Service Team is unable to provide hardware or software support for machines purchased outside of the U.S.

Network Storage:

200 MB of network storage space is provided for students to store homework, projects, or other files. This space is automatically mapped as H:\ in the cybersecurity computer labs. For assistance connecting to the H:\ drive from home or wirelessly, contact the IT Service Desk at

325-HELP or visit the OU-Tulsa Computer Lab at 1C65 or log on to http://support.ou.edu.

Undergraduate Study

Admissions

Admission to the University of Oklahoma (Norman Campus) and subsequently a degree granting college is based upon the admission requirements that are in effect for the semester that a student initiates enrollment at OU. For information on current admission requirements, contact the Office of Admissions & Recruitment, University of Oklahoma, Jacobson Hall, 550 Parrington Oval, Room L-1, Norman, OK 73019-4076 or visit their homepage.

Admission to an undergraduate program within the OU Polytechnic Institute is based upon the program requirements in effect at the time of a student's initial enrollment in any institution (including OU) in the Oklahoma State System of Higher Education. As a completion program, the degrees offered at the OUPI are considered completion degrees in that only the junior (3000) and senior (4000) level courses are offered at the OUPI located at OU-Tulsa. The first two years can be completed either at OU Norman or can be obtained at another institution (see Transfer Students below).

All students seeking admission to a program within the OU Polytechnic Institute must fulfill the following minimum requirements:

1. Completed admission to the University of Oklahoma;
2. At least 24 semester hours of earned college credit;
3. Completion of any curricular deficiencies that may exist in English, Math and/or Science;
4. A declared major in the OUPI; and
5. Obtain at least the minimum combined and OU retention grade point average required for graduation from the program the student has declared. All undergraduate programs in the OUPI may require additional admission requirements beyond those listed above. Refer to the respective area for information regarding additional program admission requirements.

Transfer Students

An undergraduate students transferring from an institution within the Oklahoma State System of Higher Education must fulfill the transfer admission requirements of the University of Oklahoma Office of Admissions & Recruitment. For more information, visit their website.

A student requesting transfer into a program of the OU Polytechnic Institute from another institution will be considered for admission once they have completed at least 24 semester hours of earned college credit with an overall GPA of 2.5. Such an applicant, in addition to satisfying all admission requirements of the University and the college, must be approved by the division director for that particular major.

A student requesting to transfer into a program of the OU Polytechnic Institute from another institution outside of the Oklahoma State System of Higher Education will follow the most recent curriculum requirements for the major the student declares.

Transfer Credit

The following credit hour regulations are specific to transfer students:

- All professional courses not taken at the University of Oklahoma are subject to evaluation for equivalency by the appropriate division of the college prior for the approval of these courses as transfer credit.
- Work accepted from other institutions is subject to validation by the satisfactory completion of at least 30 hours of credit in residence.
- College credit for work experience is permitted only under the supervised conditions of the Preceptor Program of the college or approved internship/field experience courses.

Change of Major Requests

Students interested in pursuing a change of major within OUPI, or who are pursuing a major in another college on either the OU-Norman or OU-Tulsa campus but wish to switch to an OUPI program must meet with an academic advisor in OUPI to change majors. The advisor will assess the student's GPA and completed courses. If the student lacks necessary preparation to begin coursework in the major, the student might be advised to remain in their current major until they are adequately prepared for the course curriculum. In accordance with State Regents' requirements, students are assigned to the degree program year that was current at the time they entered the Oklahoma State System of Higher Education.

College Regulations

Laptop Requirement

Students with a major in the OU Polytechnic Institute will be required to have a laptop computer. Laptop technologies are used to enhance the learning experience, and using a computer will become second nature to all of our students. See Laptop Policy page (PDF) for recommendations for the specifications needed, as well as other pertinent information.

Probation and Advancement

In accordance with the approved retention policy of the Oklahoma State Regents for Higher Education a student must maintain a combined retention minimum grade point average of at least 2.00 (C) in order to be in good academic standing at the University of Oklahoma. A student who fails to maintain the required grade point averages for their program will be notified and required to sign an "Enrollment Contract" each semester their retention grade point average is below the minimum required for graduation. A student on enrollment contract may be denied further enrollment in the college if they fail to fulfill the terms of the enrollment contract during any semester they are on academic notice.

Graduation Policies

The following requirements must be met in order to graduate with a bachelor's degree from the OU Polytechnic Institute:

- Student must have an OU retention and combined retention grade point average of 2.00 or higher.
- Student must have successfully completed a minimum of 120 semester hours inclusive of general education, major course work, and electives. Hours vary depending on degree.
- Student must earn a "C" or better in each course in her/his major.
- Student must complete a minimum of 40 hours of general education approved coursework as outlined by the college and the university.
- Student must complete at least one general education approved course at the upper-division level (3000 – 4000), outside the student's major. Students should take advantage of the "Attribute Type" tool at one.ou.edu or utilize search options at classnav.ou.edu when enrolling in general education course requirements.
- Students must complete a minimum of 40 hours of upper division (3000-4000 level) course work.

- Oklahoma State Regents' policy requires each student to complete a minimum of 60 hours at a senior (4-year) institution.
- Student must complete a senior graduation check with an academic counselor in the OU Polytechnic Dean's Office.
- Student must complete an Application for Graduation at one.ou.edu. This application must be on file with the University Records Office in order for the student to officially graduate from the university.

Senior Graduation Check

All OU Polytechnic Institute Seniors should complete a Graduation Check at least#one semester before they plan to graduate. To schedule a Graduation Check, make an appointment with one of the OUPI Academic Counselors.

Courses

CYBS 3113 Operating Systems Fundamentals 3 Credit Hours
Prerequisite: CYBS 3123. This course introduces major concepts and techniques for designing and implementing operating systems, including memory management, process management, information management, and computer security. Principles of performance evaluation. Class projects require the design and implementation of software systems. A UNIX family operating system will be used. (Sp)

CYBS 3123 Introduction to Unix Systems 3 Credit Hours
Prerequisite: C S 2413 and MATH 1914; and C S 2813 or MATH 2513. This course provides an introduction to the UNIX operating system. Topics include files and directories, electronic mail, security, advanced file systems, network utilities, network file sharing, text utilities, shell programming, regular expressions, UNIX internals, UNIX system administration, UNIX variations, and systems programming. Programming assignments involve the UNIX shell script language. (F)

CYBS 3213 Foundations of Cybersecurity 3 Credit Hours
Prerequisite: C S 2413, MATH 1914 and either C S 2813 or MATH 2513. This course introduces cybersecurity, principles, and technologies. It deals with security issues related to systems and software. Topics include cyber threats and vulnerabilities, information security frameworks and policies, cryptography, penetration testing, and in-depth defense. The goal is to develop a foundation for further study in cybersecurity. (F)

CYBS 3223 Applied Statistics for Computing 3 Credit Hours
Prerequisite: MATH 2423, course is not open to freshmen. This course is an introduction to basic statistical concepts and techniques with an emphasis on application to applied computing. Topics include basic properties of probability, a review of descriptive statistics, common discrete and continuous distributions of data, visualization of real data, hypothesis testing, parametric versus nonparametric tests, supervised and unsupervised learning methods, the bias-variance tradeoff, use of statistical packages. (F)

CYBS 3313 Introduction to Cyber Ethics and Law 3 Credit Hours
Prerequisite: Junior Standing. Legal and ethical issues with networked IT, including privacy, surveillance, digital piracy, and military use. First unit introduces ethical frameworks applicable to cybersecurity, sources of applicable law and regulation. Second unit introduces issues relating to cybercrime: intellectual property, user privacy, information assurance, and harmful online content. Third unit introduces issues with IT in government operations. (Sp)

CYBS 3323 Hardware Security 3 Credit Hours
Prerequisite: CYBS 3123 or concurrent enrollment in CYBS 3123. This course focuses on hardware (HW) security and covers security and trust from the HW perspective. It introduces students to HW components, including SoC and PCB, and examines security and trust issues in such HW components. Topics include digital lock, circuit theory, ASICs and FPGAs, HW security threats, malware, and attacks, along with specific countermeasures against HW attacks. (F)

CYBS 3440 Mentored Research Experience 3 Credit Hours
0 to 3 hours. Prerequisites: ENGL 1113 or equivalent, and permission of instructor. May be repeated; maximum credit 12 hours. For the inquisitive student to apply the scholarly processes of the discipline to a research or creative project under the mentorship of a faculty member. Student and instructor should complete an Undergraduate Research & Creative Projects (URCP) Mentoring Agreement and file it the with the URCP office. Not for honors credit. (F, Sp, Su)

CYBS 3743 Cyberforensics Fundamentals 3 Credit Hours
Prerequisite: CYBS 3213. This course introduces students to cyber forensics and cyber-crime scene analysis fundamentals. The various laws and regulations dealing with computer forensic analysis are discussed. Students are introduced to the emerging international standards for cyber forensic analysis and a formal methodology for conducting computer forensic investigations. (Sp)

CYBS 3813 Network Fundamentals 3 Credit Hours
Prerequisite: C S 2413, MATH 1914, and either C S 2813 or MATH 2513. Introduces the fundamentals of computer networks, including network architectures, network topologies, network protocols, layering concepts (for example, ISO/OSI, TCP/IP reference models), wired and wireless network protocols, communication paradigms (point-to-point vs. multicast/broadcast, connectionless vs. connection-oriented), and networking APIs (sockets). Protocols in all layers will be introduced. In this course, socket programming is also introduced. (Sp)

CYBS 3913 Database Fundamentals 3 Credit Hours
Prerequisite: C S 2413, MATH 1914, and either C S 2813 or MATH 2513. Introduction to the concepts behind relational database systems, modeling with Entity-Relationship diagrams and how these are used for data design. SQL to define, manipulate, and test the database, programmatic access, and practical issues. Strong foundation in database security, auditing principles, practices and methodologies. Topics: application security models, security architecture, access controls, auditing, trust management, privacy, threat vectors, and attack methods. (Sp)

CYBS 3990 Independent Study 1-3 Credit Hours
1 to 3 hours. Prerequisite: permission of instructor and junior standing. May be repeated once with change of content. Independent study may be arranged to study a subject not available through regular course offerings. (F, Sp, Su)

CYBS 4103 Engineering Secure Software 3 Credit Hours
Prerequisite: CYBS 3813 and CYBS 3913. This course covers topics at the intersection of security and software engineering. This course introduces software engineering processes and standards for building secure software applications. It discusses secure software life cycle development principles to include security in every phase. It also explores security issues and vulnerabilities in software applications due to a lack of secure software engineering processes. (F)

CYBS 4123 System Administration 3 Credit Hours
(Slashlisted with CYBS 5123) Prerequisite: CYBS 3123. This course provides a comprehensive introduction to system administration. Topics include virtualization, authentication and authorization, directory services, system management, and system security and set up of modern compute and storage clouds, networking systems, file systems, logging and analysis, and networking. Includes topics related to scripting for all administrative functions. Emphasis is placed on enterprise-level systems. No student may earn credit for both 4123 and 5123. (F, Sp)

CYBS 4133 Ethical Hacking and Penetration Testing 3 Credit Hours
(Slashlisted with CYBS 5133) Prerequisite: CYBS 3113. This course covers concepts related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. No student may earn credit for both 4133 and 5133. (F, Sp)

CYBS 4203 Cybersecurity Risk Management and Assessment 3 Credit Hours
(Slashlisted with CYBS 5203) Prerequisite: CYBS 3213. This course develops competency in information security policies and plans, including controls for physical hardware, software, and networks. The course introduces security risk detection strategies, countermeasures, damage assessment, and control. The course introduces the students to performing information system risk analysis and management audits. Tools for analyzing log files of various kinds will also be introduced. No student may earn credit for both 4203 and 5203. (F)

CYBS 4293 Introduction to Cloud Computing and Security 3 Credit Hours
(Slashlisted with CYBS 5293) Prerequisite: CYBS 3113. Course covers the concepts behind cloud computing, including storage and computing. We will also learn about virtualization, software as a service, and deployment models. We will learn about cybersecurity risks on cloud infrastructure and countermeasures using access policies, distributed access control, key management, and others. Covers topics in the cloud computing security guidelines set forth in international standards organizations. No student may earn credit for both 4293 and 5293. (Sp)

CYBS 4323 IoT Security and Privacy 3 Credit Hours
(Slashlisted with CYBS 5323) Prerequisite: CYBS 3323. This course prepares students to securely develop and operate Internet of Things (IoT) devices considering security and privacy. The course covers concepts of IoT architectures with a focus on security and privacy issues. No student may earn credit for both 4323 and 5323. (F, Sp)

CYBS 4333 Incidence Response Management 3 Credit Hours
(Slashlisted with CYBS 5333) Prerequisite: CYBS 3123. This course provides a comprehensive treatment of cyber incidents and how to manage them, including understanding attacker motivation, attack methods, and the anatomy of the attacks. Additionally, topics related to incidence readiness, remote triage tools, memory analysis, malware analysis, disk forensics, network intrusion detection tools, and others will be discussed. No student may earn credit for both 4333 and 5333. (F, Sp)

CYBS 4473 Network Security 3 Credit Hours
(Slashlisted with CYBS 5473) Prerequisite: CYBS 3113. The course deals with understanding all aspects of cybersecurity that involve the network. Topics will include network transport-level security, wireless network security, electronic mail security, IP security, firewalls, VPNs, Secure HTTP, person-in-the-middle attack scenarios, and SSL/TLS and SSH (SP). Learn about various tools for analyzing network data at various levels of the TCP/IP stack and operating security operations centers. No student may earn credit for both 4473 and 5473. (F)

CYBS 4583 Machine Learning for Cybersecurity 3 Credit Hours
Prerequisite: CYBS 3213 and CYBS 3223. Various machine learning concepts, deep learning, time-series analysis, data mining, and other machine-learning concepts. Tools and libraries to analyze data sets, build predictive models, and evaluate the fit of the models. Common learning algorithms, including dimensionality reduction, classification, principal-component analysis, k-NN, k-means clustering, gradient descent, regression, logistic regression, regularization, multiclass data, algorithms, boosting and decision trees. Applies concepts to problems. (F, Sp)

CYBS 4883 Cryptography Fundamentals 3 Credit Hours
Prerequisite: CYBS 3213. This course introduces cryptography and its related tools. Specifically, in this course, cryptographic algorithms, protocols, and techniques will be introduced. The course will also introduce students to public key encryption, key exchange protocols, digital signatures, hashing-based encryption, and Data Encryption Standards. This course will also introduce cryptographic implementation in software and web application programming. (F)

CYBS 4953 Operating and Maintaining Cyber Ranges 3 Credit Hours
Prerequisite: CYBS 4473. Students will learn to use and build a cyber range for various assessments of threats and exploits. They will learn to build configurations for different business operations and the formation of red and blue team exercises. Students will have real-world experiences in handling situations without the real-world risk associated with practicing on live production equipment and systems. (Sp)

CYBS 4963 Cybersecurity Capstone 3 Credit Hours
Prerequisite: CYBS 4103 and Senior Standing. Provides the students with an experience to exhibit their knowledge and skills in all areas of cybersecurity. Students will work in small groups to identify and scope a cybersecurity problem and/or challenges. Required to write a proposal about their project and asked to create a work plan to develop solution to solve the problem/challenge. Create a final report and presentation. (Sp)

CYBS 4990 Independent Study 1-3 Credit Hours
1 to 3 hours. Prerequisite: permission of instructor and senior standing. May be repeated once with change of content. Contracted independent study for topic not currently offered in regularly scheduled courses. (F, Sp, Su)

CYBS 5113 Introduction to Cybersecurity Leadership 3 Credit Hours
Prerequisite: Graduate standing. This course provides an in-depth exploration of insider threats within organizations and the strategies for managing and mitigating these risks. Students will learn about the motivations behind insider threats, detection methods, prevention techniques, and deterrence mechanisms. (F, Sp, Su)

CYBS 5123 System Administration 3 Credit Hours
(Slashlisted with CYBS 4123) Prerequisite: Graduate Standing. This course provides a comprehensive introduction to system administration. Topics include virtualization, authentication and authorization, directory services, system management, and system security and set up of modern compute and storage clouds, networking systems, file systems, logging and analysis, and networking. Includes topics related to scripting for all administrative functions. Emphasis is placed on enterprise-level systems. No student may earn credit for both 4123 and 5123. (F, Sp)

CYBS 5133 Ethical Hacking and Penetration Testing 3 Credit Hours
(Slashlisted with CYBS 4133) Prerequisite: Graduate Standing. This course covers concepts related to ethical hacking and penetration testing methods to assess, exploit, and report security vulnerabilities on systems and their resources. The course will emphasize the ethical application of penetration testing methods and hacking tools. No student may earn credit for both 4133 and 5133. (F, Sp)

CYBS 5203 Cybersecurity Risk Management and Assessment 3 Credit Hours
(Slashlisted with CYBS 4203) Prerequisite: Graduate Standing. This course develops competency in information security policies and plans, including controls for physical hardware, software, and networks. The course introduces security risk detection strategies, countermeasures, damage assessment, and control. The course introduces the students to performing information system risk analysis and management audits. Tools for analyzing log files of various kinds will also be introduced. No student may earn credit for both 4203 and 5203. (F)

CYBS 5213 Behavioral Cybersecurity 3 Credit Hours
Prerequisite: Graduate standing. This course explores the interdisciplinary field of behavioral cybersecurity, emphasizing the role of human personality in cybersecurity practices. It aims to address the growing challenges posed by the digital age. Course will examine the application of psychological methods, profiling techniques, and the use of game theory in understanding human behavior. (F, Sp, Su)

CYBS 5233 Cybersecurity Ethics, Policy, and Law 3 Credit Hours
Prerequisite: Graduate standing. This course explores the intersection of ethics, policy, and law within the realm of cybersecurity. Students will engage with case studies, legal frameworks, and ethical dilemmas to critically analyze and navigate the complex landscape of digital security. The goal is to develop a foundation for applying ethical considerations in any organizational structure. (F, Sp, Su)

CYBS 5243 Threat Hunting and Incident Response 3 Credit Hours
Prerequisite: Graduate standing. This course provides an in-depth exploration of threat hunting and incident response in cybersecurity. It moves beyond traditional defensive measures to actively seek out and mitigate novel cyber threats. Students will learn how to plan, execute, and recover from hunts, customize frameworks for specific use cases, and respond to incidents, including ransomware attacks. (F, Sp, Su)

CYBS 5253 Cybercrime and Cybersecurity 3 Credit Hours
Prerequisite: Graduate standing. This course delves into the intricacies of cybersecurity and cybercrime, offering a comprehensive overview of the challenges and strategies associated with protecting digital assets. Students will explore various threats, risk management approaches, and the critical roles of people, processes, and technology in cybersecurity. (F)

CYBS 5293 Introduction to Cloud Computing and Security 3 Credit Hours
(Slashlisted with CYBS 4293) Prerequisite: Graduate Standing. Course covers the concepts behind cloud computing, including storage and computing. We will also learn about virtualization, software as a service, and deployment models. We will learn about cybersecurity risks on cloud infrastructure and countermeasures using access policies, distributed access control, key management, and others. Covers topics in the cloud computing security guidelines set forth in international standards organizations. No student may earn credit for both 4293 and 5293. (Sp)

CYBS 5303 Insider Threat and Risk Management 3 Credit Hours
Prerequisite: Graduate standing. This course provides an in-depth exploration of insider threats within organizations and the strategies for managing and mitigating these risks. Students will learn about the motivations behind insider threats, detection methods, prevention techniques, and deterrence mechanisms. (F, Sp, Su)

CYBS 5323 IoT Security and Privacy 3 Credit Hours
(Slashlisted with CYBS 4323) Prerequisite: Graduate Standing. This course prepares students to securely develop and operate Internet of Things (IoT) devices considering security and privacy. The course covers concepts of IoT architectures with a focus on security and privacy issues. No student may earn credit for both 4323 and 5323. (F, Sp)

CYBS 5333 Incidence Response Management 3 Credit Hours
(Slashlisted with CYBS 4333) Prerequisite: Graduate Standing. This course provides a comprehensive treatment of cyber incidents and how to manage them, including understanding attacker motivation, attack methods, and the anatomy of the attacks. Additionally, topics related to incidence readiness, remote triage tools, memory analysis, malware analysis, disk forensics, network intrusion detection tools, and others will be discussed. No student may earn credit for both 4333 and 5333. (F, Sp)

CYBS 5383 Trust in Artificial Intelligence 3 Credit Hours
Prerequisite: Graduate standing. This course explores the intersection of artificial intelligence (AI), management, and trust, delving into how these elements influence each other in modern organizations. It covers various aspects of trust in AI, including organizational, psychological, technological, and ethical dimensions. The course also examines the role of trust in human-machine interaction, AI's impact on innovation, and reducing costs. (F, Sp, Su)

CYBS 5443 Cyber Threat and Intelligence 3 Credit Hours
Prerequisite: Graduate standing. This course explores the dynamic and complex nature of cyber threats and the role of intelligence in addressing them. It covers the spectrum of threat intelligence, from tactical to strategic levels, and delves into the methodologies and technologies used to gather, analyze, and apply intelligence to enhance cybersecurity. (F, Sp, Su)

CYBS 5453 Cybersecurity in a Cloud Environment 3 Credit Hours
Prerequisite: Graduate standing. This course provides an in-depth look into the multifaceted aspects of cybersecurity within cloud computing environments. Covering fundamental concepts, architecture, software security, risk issues, and life cycle concerns, students will learn how to secure cloud services and infrastructure effectively. (F, Sp, Su)

CYBS 5473 Network Security 3 Credit Hours
(Slashlisted with CYBS 4473) Prerequisite: Graduate Standing. The course deals with understanding all aspects of cybersecurity that involve the network. Topics will include network transport-level security, wireless network security, electronic mail security, IP security, firewalls, VPNs, Secure HTTP, person-in-the-middle attack scenarios, and SSL/TLS and SSH (SP). Learn about various tools for analyzing network data at various levels of the TCP/IP stack and operating security operations centers. No student may earn credit for both 4473 and 5473. (F)

CYBS 5903 Master's Practicum 3 Credit Hours
Prerequisite: Graduate Standing. The course provides the students with a culminating experience to exhibit their knowledge and skills in all areas of cybersecurity. Students will collaboratively work in small groups to identify and scope a current cybersecurity problem and/or challenge. Students will be required to write a proposal, create a work plan, draft a final report and make a presentation. (Sp)

CYBS 5963 Strategic Planning in Cybersecurity Practicum 3 Credit Hours

Prerequisite: Graduate standing. This capstone course delves into the strategic planning and leadership aspects of cybersecurity. Students will explore the relationship between the business environment and organizational goals, risk management, and protecting information assets. The course will provide tools to build a cybersecurity strategic plan, develop IT security policies, and lead teams in the execution of these plans. (Irreg.)

CYBS 5980 Research for Master's Thesis 2-9 Credit Hours

2 to 9 hours. Prerequisite: Graduate Standing and Instructor Permission. Directed research culminating in the completion of the master's thesis. Variable enrollment, permission of instructor required, two to nine hours; maximum credit required for degree, six hours. (F, Sp)

Faculty

The faculty at OUPI bring a rich blend of industry and academic research experience in communications, automotive, heavy equipment control systems, biotech, law enforcement, first-responder and defense electronics, fintech, and high-end computing. Research interests of the faculty stretch across many applications and industries in cybersecurity, software development and integration, artificial intelligence, and digital manufacturing.

Last Name	First/Middle Name	Middle init.	OU Service start	Title(s), date(s) appointed	Degrees Earned, Schools, Dates Completed
Beattie	Matthew	J	2023	Adjunct of Artificial Intelligence	PhD, University of Oklahoma, 2022
Butt	Ahmed	Ashraf	2024	Assistant Professor of Artificial Intelligence	PhD, Purdue University 2023
Freeze	Christopher		2023	Assistant Professor of Cybersecurity	PhD, University of Oklahoma 2023
Hassell	John		2023	Associate Professor of Software Development & Integration	PhD, University of Oklahoma 2005
Jung	Sungbo		2024	Assistant Professor of Cybersecurity	PhD, University of Louisville 2024
MacDonald	Gregory	G.	2024	Associate Professor of Artificial Intelligence	PhD, University of Oklahoma 2012
Reed	Teri	K	2023	Professor and Director of OUPI	PhD, Arizona State University 1999
Riaz	Muhammad	Sajid	2024	Assistant Professor of Software Development & Integration	PhD, University of Oklahoma 2024
Roller	Chad	B	2024	Assistant Professor of Software Development & Integration	PhD, Rice University 2005