

قسم هندسة تكنولوجيا الامن السيبراني

الرؤية:

تتمثل رؤيا قسم هندسة تكنولوجيا الامن السيبراني في كلية اليرموك الجامعة برغد المجتمع بمهندسين تقنيين في مجال هندسة امن المعلومات والشبكات عامة وفي هندسة تكنولوجيا الامن السيبراني خاصة ذات مستوى عالي من الكفاءة والتقاني والمسؤولية الاخلاقية

الرسالة:

ان مهمة قسم هندسة تكنولوجيا الامن السيبراني في كلية اليرموك الجامعة هي:
• خدمة طلابنا من خلال تعليمهم; كيفية التعامل مع المشاكل وايجاد الحلول المناسبة، الربط بين النظري والعملي، ومهارات القيادة والعمل الجماعي، وقيمة الالتزام والسلوك الأخلاقي، واحترام الآخرين.
• تقديم خريجين مهندسين تقنيين ذات مستوى اكايمي عالي ومهارات عملية واسعة في مجال التخصص.
• المساهمة في تقدم قطاع تكنولوجيا المعلومات والاتصالات من خلال تخريج مهندسين متخصصين في مجال أمن الحاسوب وشبكتها و برمجة أنظمتها وحماية المعلومات الإلكترونية فيها والدفاع عنها.
• تقديم تكنولوجيا ابداعية لمنفعة المجتمع محليا وعالميا في مجال التخصص.
• التعاون مع الهيئات المدنية والعسكرية والأمنية لتسويق مهارات حقل التخصص.

أهداف القسم:

نظرًا للتقدم العلمي والتكنولوجي السريع في مجال امن المعلومات والشبكات يعمل قسم هندسة تكنولوجيا الامن السيبراني
من أجل تحقيق أهداف استراتيجية واضحة تساعده على تحقيق مكانة بارزة داخل المجتمعات الأكاديمية وهي تتضح في التالي:

1. المحافظة على جودة المناهج الدراسية وتحسينها من خلال:
• ادخال المواد الدراسية المحدثة علميا ودوليا في دراسة تخصص هندسة تكنولوجيا الامن السيبراني ومواكبة للتطور العلمي السريع من خلال الاتصال المباشر مع صناع القرار لهندسة الامن السيبراني في كافة انحاء العالم والاتصال المباشر بالكليات والمعاهد المتخصصة بتكنولوجيا الامن السيبراني.
• التقييم والتطوير المستمر للمناهج الدراسية.
• ربط مشاريع الطلاب والأبحاث باحتياجات المجتمع.
• توسيع ادراك الطلاب من خلال التعاون مع المؤسسات الحكومية والتي تختص في التدريب وحفظ الامن.

2. استحداث المختبرات العلمية و تزويدها بأحدث الاجهزة والمعدات التقنية بحقل الاختصاص وإدارتها عن طريق مجموعة من الفنيين المهرة.
3. المحافظة على التطور الفني لأعضاء هيئة التدريس من خلال:
 - تشجيع المشاركة الفعالة في المؤتمرات والورش العلمية والتدريبية سواء على الصعيد المحلي او الدولي.
 - تشجيع مبادرات و انجازات هيئة التدريس.
 - تشجيع العمل الاستشاري وتوفير الخدمات على المستوى المهني في كافة الاختصاصات الهندسية. 4. الانتاج المعرفي من خلال:
 - القيام بالأبحاث النظرية والتطبيقية المتميزة.
 - تشجيع النشر العلمي وتحفيز العمل الجماعي للمجموعات البحثية في مختلف التخصصات.
 - السعي لزيادة مصادر التمويل البحثي من خلال النشر في المجالات الهندسية العالمية.
5. تشجيع الكادر التدريسي والطلبة على تطوير البحوث والمشاريع في مجال الامن السيبراني والقرصنة الاخلاقية.

الفرص الوظيفية للخريجين:

يعمل خريجوا القسم في عدد كبير من المجالات الاكاديمية والامنية والعسكرية والمدنية والاتصالات في البلد وخارجه ومنها على سبيل المثال:

- مهندس امن تكنولوجيا المعلومات.
- رئيس قسم امن المعلومات.
- مستشار الأمن الإلكتروني.
- مدير الحوادث والتهديدات.
- محلل امن البيانات ومخاطرها.
- مطور برامج، مدير مشروع تقنية المعلومات.
- استشاري أنظمة حاسوبية.
- أخصائي الجرائم الإلكترونية.
- محقق أدلة جنائية حاسوبية أو رقمية.
- باحث في هندسة الشبكات وامن المعلومات.

1. **Mission & Vision Statement**

Vision Statement

Our Vision is to provide the community with technical, highly skilled engineers in the field of cybersecurity with a high level of efficiency, dedication, and ethical responsibility to be the vanguard of digital defense.

Mission Statement

Our mission is to Prepare a generation of technical engineers capable of protecting our organization's digital assets and information. This is achieved by employing cutting-edge technology, rigorous strategies, and a culture of continuous improvement. We educate and empower to foster a cyber-aware culture that reduces risk and ensures the success of our institutions.

2. **Program Specification**

Program code:	CSTE	ECTS	240
Duration:	4 levels, 8 Semesters	Method of Attendance:	Full Time

The Cybersecurity Technology Engineering Department program specification provides a comprehensive framework for the department's operation, goals, and objectives. The department offers a Bachelor of Engineering in Cybersecurity Technology Engineering, consisting of core courses in cybersecurity principles, network security, cryptography, and ethical hacking, and elective courses in specialized areas besides some foundation basic and supportive area courses.

Research and projects will focus on areas that include but are not limited to network security, information assurance, secure software development, threat intelligence, and digital forensics. The department will focus on collaborating with industry partners to facilitate internships, co-op programs, and guest lectures for students. Industry partnerships also support research projects, providing real-world relevance to the department's activities.

The department emphasizes the importance of ethical conduct in cybersecurity education and research. Students and faculty must adhere to a strict code of ethics, including respect for privacy, confidentiality, and responsible disclosure. The department regularly assesses its programs and curriculum to ensure alignment with industry standards and emerging trends. Feedback from students, alumni, and industry partners is used to enhance program quality continually.

The program specification for the Cybersecurity Technology Engineering Department serves as a guiding document to maintain high standards of education, research, and ethical practice in cybersecurity. It is subject to periodic review and updates to reflect the evolving nature of cybersecurity technology and industry demands.

The Cybersecurity Technology Engineering program is designed to provide students with the skills to improve themselves by preparing them for a career in the digital sector. The curriculum consists of an integrated set of courses that builds a solid theoretical foundation for the students. Once the foundation is established, the program develops domain-specific skills in the field of cybersecurity. Graduates from the Cybersecurity Technology Engineering Department are equipped with a strong foundation in cybersecurity principles, technologies, and practices. They are well-prepared to pursue various career paths in the field of cybersecurity. Cybersecurity Engineers/Analysts play a crucial role in safeguarding an organization's digital assets, data, and information systems from cyber threats. They utilize their knowledge and skills to proactively identify vulnerabilities, implement security measures, and respond to security incidents.

3. Program Goal

For undergraduate students pursuing a degree in Cybersecurity Technology Engineering, the following generic competencies are typically expected upon graduation:

Technical Knowledge:

- Proficiency in various operating systems (e.g., Windows, Linux, macOS).

- Understanding of networking concepts and protocols.
- Knowledge of programming languages (e.g., Python, C++, Java).
- Familiarity with encryption and cryptography techniques.
- Experience with cybersecurity tools and software (e.g., IDS/IPS, firewalls, antivirus).
- Awareness of emerging cybersecurity threats and trends.

Cybersecurity Fundamentals:

- Understanding cybersecurity principles and best practices.
- Knowledge of risk management and threat assessment methodologies.
- Ability to conduct vulnerability assessments and penetration testing.

Security Policy and Compliance:

- Familiarity with cybersecurity regulations and compliance standards (e.g., GDPR, HIPAA, NIST).
- Ability to develop and enforce security policies and procedures.

Incident Response and Recovery:

- Proficiency in incident detection and response procedures.
- Experience in managing and mitigating security incidents and breaches.
- Knowledge of digital forensics techniques.

Security Architecture and Design:

- Ability to design secure network and system architectures.
- Knowledge of secure coding practices.
- Understanding of cloud security principles.

Security Tools and Technologies:

- Proficiency in using security tools like SIEM (Security Information and Event Management) systems.
- Experience with intrusion detection/prevention systems (IDS/IPS).
- Knowledge of threat intelligence platforms.

Cybersecurity Awareness and Training:

- Ability to educate and train employees on cybersecurity best practices.
- Developing and conducting security awareness programs.

Problem-solving and Analytical Skills:

- Strong analytical thinking and problem-solving abilities.
- Capacity to assess and respond to security incidents and vulnerabilities.

Continuous Learning:

- Commitment to staying up to date with the latest cybersecurity threats and technologies.
- Pursuit of certifications such as CISSP, CISM, CEH, or others as relevant to the role.

These competencies provide a solid foundation for undergraduate students in cybersecurity technology engineering. The specific curriculum and emphasis on these competencies may vary from one institution to another. Still, these skills and knowledge areas are generally considered essential for a successful career in cybersecurity.

4. **Student Learning Outcomes**

The Department of Cybersecurity Technology Engineering requires professionals to possess generic competencies and the technical skills and knowledge needed to perform their roles effectively. Below are some of the generic competencies needed from the Department students:

- ❖ **Problem-solving:** The ability to effectively identify and resolve complex security issues, vulnerabilities, and incidents.
- ❖ **Critical Thinking:** The capacity to analyze information, assess risks, and make informed decisions regarding cybersecurity strategies and solutions.
- ❖ **Adaptability:** Cybersecurity is a rapidly evolving field, so being open to learning new technologies and adapting to emerging threats is crucial.
- ❖ **Communication Skills:** Effective communication is vital for conveying security concerns to non-technical stakeholders, writing security policies, and collaborating with team members.
- ❖ **Teamwork:** Working collaboratively with other cybersecurity professionals, IT staff, and various departments to ensure a cohesive security posture.
- ❖ **Ethical Awareness:** Understanding the ethical considerations and responsibilities of handling sensitive data and conducting security testing.
- ❖ **Compliance Knowledge:** Awareness of relevant cybersecurity regulations, standards, and best practices ensures the organization complies with legal requirements.

- ❖ **Risk Management:** The ability to assess, prioritize, and manage cybersecurity risks to effectively protect the organization's assets.
- ❖ **Continuous Learning:** Stay updated on the latest cybersecurity trends, threats, and technologies through ongoing education and training.
- ❖ **Project Management:** Basic project management skills to effectively plan, execute, and oversee cybersecurity projects.

In conclusion, Cybersecurity Technology Engineering Department professionals must possess technical and generic competencies to excel in their roles. Analytical thinking, continuous learning, adaptability, creativity, teamwork, communication skills, project management, time management, leadership, and customer service are among the essential generic competencies required. These competencies help to enhance competence and promote good performance in the department of computer engineering techniques.