Learning Outcomes of the College of Computer Science and Information Technology

(Artificial Intelligence and Cybersecurity)

The learning outcomes in the College of Computer Science and Information Technology aim to define the advanced knowledge, technical skills, and professional competencies that students acquire after completing their academic programs in modern specialized departments. This aims to prepare innovative and technically qualified graduates to bridge the digital gap in the labor market and contribute effectively to digital transformation and the protection of society's infrastructure.

1. Learning Outcomes for the Department of Artificial Intelligence (AI)

Graduates of the Artificial Intelligence department are expected to achieve a set of learning outcomes, most notably:

- **Foundational Knowledge:** Acquiring a deep understanding of AI mathematics, algorithms, and advanced data structures.
- **Developing Smart Models:** Proficiency in building and training Machine Learning (ML) and Deep Learning (DL) models using languages such as Python.
- **Natural Language Processing and Computer Vision:** The ability to develop software systems capable of understanding human languages and analyzing images and visual patterns.
- **Complex Problem Solving:** Designing innovative solutions for problems that require human-like simulated thinking and data-driven decision-making.
- **Handling Big Data:** Possessing technical skills to manage and analyze Big Data sets to extract patterns and predictions.
- **Ethics and Responsibility:** Commitment to ethical standards in developing AI technologies and ensuring the absence of bias in algorithms.

2. Learning Outcomes for the Department of Cybersecurity

Graduates of the Cybersecurity department are expected to achieve a set of scientific and professional competencies, including:

- **Network and System Protection:** Acquiring skills to design and secure networks and software systems against breaches and cyber threats.
- **Incident Response:** The ability to detect vulnerabilities, analyze attacks, and develop proactive plans for response and digital disaster recovery.
- **Cryptography and Data Security:** Mastering advanced encryption algorithms and protocols for protecting data privacy and securing its exchange.
- **Digital Forensics:** Acquiring skills in digital investigation and collecting evidence from compromised devices in compliance with legal and technical standards.
- **Penetration Testing:** Developing "Ethical Hacking" skills to evaluate the strength of organizational defense systems and identify weaknesses.
- **Compliance and Legislation:** Familiarity with international and local laws governing cyberspace and security governance standards.

Common Skills (Graduate Competencies)

In addition to the specific specializations, both departments work to enhance general skills, including:

- **Teamwork:** The ability to work effectively within multidisciplinary technical teams.
- **Technical Communication:** The skill of explaining and simplifying complex concepts for non-specialists, both orally and in writing.
- **Continuous Learning:** Developing the ability to keep pace with rapid updates in global technologies and software.

Dean's approval