Learning Outcomes Matrix for Cybersecurity Program

No.	Learning Outcome	Knowledge (K)	Skills (S)	Attitudes (A)	Analytical Thinking (AT)	Critical Thinking (CT)	Professional Practices (PP)
PLO 1	Understand core cybersecurity concepts and frameworks	K1: Basic concepts of cybersecurity, principles, and frameworks	S1: Ability to identify and describe cybersecurity models and protocols	A1: Professional attitude towards cybersecurity principles	AT1: Ability to analyze and explain cybersecurity frameworks	CT1: Evaluate various cybersecurity models	PP1: Commitment to ethical and professional standards in cybersecurity
PLO 2	Analyze and assess cybersecurity threats and vulnerabilities	K2: Knowledge of cybersecurity threats, risks, and vulnerabilities	S2: Ability to perform risk assessments and identify vulnerabilities in systems	A2: Attitude towards proactive threat assessment and mitigation	AT2: Analyze data to detect potential threats	CT2: Critically evaluate risk management strategies	PP2: Application of ethical practices when assessing vulnerabilities
PLO 3	Design and implement secure network systems	K3: Understanding of network design principles and security protocols	S3: Ability to design secure networks with encryption and access controls	A3: Responsibility for ensuring security in network design	AT3: Analyze network architectures for vulnerabilities	CT3: Critically evaluate security solutions for network designs	PP3: Adherence to best practices in network security implementation
PLO 4	Use cybersecurity tools for risk management and threat detection	K4: Knowledge of cybersecurity tools for threat detection and risk analysis	S4: Proficiency in using cybersecurity tools like firewalls,	A4: Willingness to keep up with evolving tools and technologies	AT4: Ability to integrate cybersecurity tools for comprehensive security	CT4: Analyze the effectiveness of cybersecurity tools	PP4: Ensure compliance with industry standards while using cybersecurity tools

No.	Learning Outcome	Knowledge (K)	Skills (S)	Attitudes (A)	Analytical Thinking (AT)	Critical Thinking (CT)	Professional Practices (PP)
			intrusion detection systems				
PLO 5	Understand the legal, ethical, and regulatory aspects of cybersecurity	K5: Knowledge of cybersecurity laws, regulations, and ethical standards	S5: Ability to interpret and apply legal and ethical cybersecurity requirements	A5: Ethical responsibility in cybersecurity practices	AT5: Analyze the implications of legal and regulatory decisions in cybersecurity	CT5: Critically assess compliance requirements in real-world scenarios	PP5: Commitment to upholding legal and ethical standards in cybersecurity
PLO 6	Develop and integrate security policies and incident response strategies	K6: Knowledge of security policies and incident response frameworks	S6: Ability to develop and implement security policies and incident response strategies	A6: Awareness of the importance of incident response and continuous security improvements	AT6: Evaluate and improve existing security policies	CT6: Critically assess the effectiveness of incident response strategies	PP6: Ensure that policies comply with industry best practices and standards
PLO 7	Lead teams and collaborate effectively in a cybersecurity environment	K7: Understanding of leadership and teamwork dynamics in cybersecurity	S7: Ability to lead and collaborate within cybersecurity teams	A7: Professional behavior in team settings	AT7: Ability to delegate tasks and make decisions in team environments	CT7: Critically assess team performance and project outcomes	PP7: Commitment to leadership and fostering collaborative environments
PLO 8	Evaluate and apply emerging cybersecurity technologies	K8: Knowledge of emerging technologies in cybersecurity (AI,	S8: Ability to apply new technologies to solve cybersecurity challenges	A8: Openness to adopting innovative technologies	AT8: Analyze emerging technologies' impact on cybersecurity	CT8: Evaluate the potential risks and benefits of new technologies	PP8: Implementation of new technologies in compliance with

No.	Learning Outcome	Knowledge (K)	Skills (S)	Attitudes (A)	Analytical Thinking (AT)	Critical Thinking (CT)	Professional Practices (PP)
		machine learning, blockchain)					professional standards

Key:

- **Knowledge (K)**: Level of knowledge acquired by the student in each learning outcome.
- **Skills (S)**: Practical skills students develop through the learning process.
- **Attitudes (A)**: Behavioral and professional attitudes students are expected to demonstrate.
- **Analytical Thinking (AT)**: The ability to analyze complex problems and data.
- **Critical Thinking (CT)**: Evaluating arguments and solutions to cybersecurity issues.
- **Professional Practices (PP)**: Ethical behavior and adherence to professional standards in the field of cybersecurity.