

**LEHMAN COLLEGE
OF THE
CITY UNIVERSITY OF NEW YORK**

DEPARTMENT OF COMPUTER SCIENCE

CURRICULUM CHANGE

1. **Type of change:** *Experimental Course*

2.

Department(s)	Computer Science
Career	☒ Undergraduate ☐ Graduate
Academic Level	☒ Regular ☐ Compensatory ☐ Developmental ☐ Remedial
Subject Area	Digital Literacy
Course Prefix & Number	CIS 220
Course Title	Introduction to Cybersecurity
Description	The ubiquity of sensitive personal and financial data transmitted across insecure devices and networks poses a significant risk to our students, and our community businesses. This one-semester course is designed to equip students with the essential knowledge, skills, and the mindset required to protect themselves and their community from common cyberthreats. NOTE: This course is taught as a lecture with lab exercises to reinforce the concepts.
Pre/ Co Requisites	
Credits	3
Hours	4
Liberal Arts	☒ Yes ☐ No
Course Attribute (e.g. Writing Intensive, WAC, etc)	
General Education Component	☒ Not Applicable ☐ Required ☐ English Composition ☐ Mathematics ☐ Science

	_____ Flexible
	_____ World Cultures
	_____ US Experience in its Diversity
	_____ Creative Expression
	_____ Individual and Society
	_____ Scientific World

3. **Rationale:**

The proposed course is presented on the premise that digital literacy is incomplete without a foundational understanding of cybersecurity. Students and graduates today interact with technology in almost every facet of their lives, yet few are systematically educated on the fundamentals of digital self-protection. Particularly, the foundational understanding of risk and the mindset needed to mitigate identified risks.

This course addresses this critical gap by focusing on practical and conceptual knowledge, allowing students to move beyond passive technology consumption to active and informed engagement.

Regular hands-on exercises in class will be used to implement and reinforce the theoretical concepts presented in the course.

Potential for a Cybersecurity Internship based on academic performance.

4. **Learning Outcomes (By the end of the course students will be expected to):**

- Identify common cybersecurity threats and vulnerabilities in personal and business contexts.
- Apply best practices for safeguarding personal information and digital assets.
- Evaluate the ethical and legal implications of cybersecurity decisions.
- Demonstrate practical skills in threat recognition, secure authentication, and incident response.

5. **Date of Departmental Approval:** 9/17/2025