SYLLABUS

DATE OF LAST REVIEW:	7/2019
CIP CODE:	24.0101
SEMESTER:	Departmental Syllabus
COURSE TITLE:	Legal Issues in Cybersecurity
COURSE NUMBER:	CIST0255
CREDIT HOURS:	3
INSTRUCTOR:	Departmental Syllabus
OFFICE LOCATION:	Departmental Syllabus
OFFICE HOURS:	Departmental Syllabus
TELEPHONE:	Departmental Syllabus
EMAIL:	Departmental Syllabus *KCKCC-issued email accounts are the official means for electronically communicating with our students.*
PREREQUISITES:	CIST0125 Network security.
REQUIRED TEXT AND MATERIALS:	Please check with the KCKCC bookstore, http://www.kckccbookstore.com for the required text for your particular class.

COURSE DESCRIPTION: This course provides students with knowledge of legal and policy related issues to Cybersecurity. It includes topics like the government and the private sector legal authorities and obligations of protecting computer systems and networks, legal, political economy and technology perspectives of Cybersecurity, federal laws, executive orders, regulations, and cyber intrusions related cases, and Cybersecurity international law and politics. The course also explains legislative and technology issues in Cybersecurity area and provides students with chances to discuss this dynamic area issues at the intersection of law, technology, and policy.

METHOD OF INSTRUCTION: A variety of instructional methods may be used depending on content area. These include but are not limited to: lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, and panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE:

I. Legal and policy of technologies that protect intellectual property & sensitive information.
II. Role of technical standards to supplement legal and regulatory requirements.
III. Data breaches and organizational strategies to address such risks.
IV. Information security and usability.
V. Information security and privacy.
VI. Challenges associated with information security law and policy.
VII. Security policy via the examination of current research issues and problems.
VIII. Real-world security policy challenges.

EXPECTED LEARNER OUTCOMES:

A. Upon completion of the course the student will be able to understand the legal and policy issues surrounding technologies protection.
B. Upon completion of the course the student will be able to understand the role of technical standards to supplement legal and regulatory requirements.
C. Upon completion of the course the student will be able to analyze data breaches and organizational strategies to address it.
D. Upon completion of the course the student will be able to understand information security and usability.
E. Upon completion of the course the student will be able to understand information security and privacy.
F. Upon completion of the course the student will be able to understand the challenges associated with information security law and policy.
G. Upon completion of the course the student will be able to understand security policy via the examination of current research issues and problems.
H. Upon completion of the course the student will be able to understand real-world security policy challenges.

COURSE COMPETENCIES:

Upon completion of the course, the student will be able to understand the legal and policy issues surrounding technologies protection.

1. The student shall be able to understand legal and policy of technologies that protect intellectual property
2. The student shall be able to understand legal and policy of technologies that protect sensitive information.

3. The student shall be able to understand legal and policy of technologies that protect organizational information assets.

Upon completion of the course, the student will be able to understand the role of technical standards to supplement legal and regulatory requirements.

4. The student shall be able to explain the role of technical standards to supplement legal requirements.
5. The student shall be able to explain the role of technical standards to supplement regulatory requirements.

Upon completion of the course, the student will be able to analyze data breaches and organizational strategies to address it.

6. The student shall be able to analyze data breaches.
7. The student shall be able to design and implement organizational strategies to address the risk of data breaches.

Upon completion of the course, the student will be able to understand information security and usability.

8. The student shall be able to explain information security
9. The student shall be able to explain information usability
10. The student shall be able to understand the tensions between information security and usability.

Upon completion of the course, the student will be able to understand information security and privacy.

11. The student shall be able to explain information privacy.
12. The student shall be able to understand the tensions between information security and privacy.

Upon completion of the course, the student will be able to understand the challenges associated with information security law and policy.

13. The student shall be able to explain the challenges associated with information security law and policy.
14. The student shall be able to develop the multidisciplinary skills to analyze, manage, and resolve information security law and policy challenges.

Upon completion of the course the student will be able to understand security policy via the examination of current research issues and problems.

15. The student shall be able to gain a basic grounding for future technical and other research in security policy.
16. The student shall be able to examine security policy current research issues and problems.

Upon completion of the course, the student will be able to understand real-world security policy challenges.

17. The student shall be able to gain experience handling real-world security policy challenges.
18. The student shall be able to analysis software and business artifacts using written and oral communication.

ASSESSMENT OF LEARNER OUTCOMES:

Student progress is evaluated by means that include, but are not limited to, exams, written assignments, and class participation.

SPECIAL NOTES:
This syllabus is subject to change at the discretion of the instructor. Material included is intended to provide an outline of the course and rules that the instructor will adhere to in evaluating the student's progress. However, this syllabus is not intended to be a legal contract. Questions regarding the syllabus are welcome any time.

Kansas City Kansas Community College is committed to an appreciation of diversity with respect for the differences among the diverse groups comprising our students, faculty, and staff that is free of bigotry and discrimination. Kansas City Kansas Community College is committed to providing a multicultural education and environment that reflects and respects diversity and that seeks to increase understanding.

Kansas City Kansas Community College offers equal educational opportunity to all students as well as serving as an equal opportunity employer for all personnel. Various laws, including Title IX of the Educational Amendments of 1972, require the college's policy on non-discrimination be administered without regard to race, color, age, sex, religion, national origin, physical handicap, or veteran status and that such policy be made known.

Kansas City Kansas Community College complies with the Americans with Disabilities Act. If you need accommodations due to a documented disability, please contact the Director of the Academic Resource Center, in Rm. 3354 or call at: 288-7670.