Part 2

Department Master Syllabus
Camden County College
Blackwood, New Jersey

Course Number:	**Course Title:**
CIS-115	Cyberspace Ethics and Security

Department/Program: Computer Information Systems

Date of Review: Click here to select a month. Click here to select a year.

(This Department Master Syllabus has been examined by the program/department faculty members and it is decided that no revision is necessary at this time.)

Date of Revision: New Course, May 2020

(This Department Master Syllabus has been examined by the program/department faculty members and it is decided a change requiring a revision is necessary at this time.)

N.B. A change to the course materials alone (textbooks and/or supplementary materials) may not constitute a revision. Any other change to the items listed below on this form is considered a revision and requires approval by the department/program faculty at a department/program meeting and by the division at a Chairs and Coordinator meeting.

Credits:2

Contact Hours	**Lecture:** 2	**Lab:** 0	**Other:** 0

Prerequisites: none

Co-requisites: none

Course Description: This two-credit course provides an up-to-date investigation of the internet's influence on our society and our lives. As the internet use expands and new information technologies are developed worldwide, unprecedented social and moral issues continue to emerge. Students will address problems of censorship, intellectual property, information privacy, and cybersecurity, and discuss potential resolutions that may be reached through technology, law, or a combination of the two. Case studies addressing major corporate data breaches, fair use and the Crypto Wars, and the political impact of regulation and "fake news," among other recent controversies, establishes the global context. As recommended by the Association of Computing Machinery (ACM), this course serves to guide computing professionals' ethical conduct and includes anyone using computing technology "in an impactful way".

Student Learning Outcomes (SLOs)

Course specific student learning outcomes
Upon completion of this course the student will be able to:

- Understand the laws and regulations related to cyberethics as assessed by quizzes, homework and projects.
- Apply the ACM/IEEE Professional Code of Ethics and principles underlying them to computing situations as assessed by quizzes, homework and projects.
- Protect privacy rights in cyberspace as assessed by quizzes, homework and projects.
- Preserve free speech and censorship in cyberspace as assessed by quizzes, projects, and homework
- Safeguard Intellectual Property in cyberspace as assessed by quizzes, projects, and homework
- Secure the Digital Infrastructure as assessed by quizzes, homework and projects.

As assessed by:
quizzes, projects, and homework

General Education Student Learning Outcomes

If this course has applied for General Education Elective Status the general education student learning outcomes listed below must exactly match those the sponsor has identified on the General Education Request form.
General Education SLOs:
NA
As assessed by:
NA

Program Learning Outcomes

List all course level student learning outcomes that interconnect to a particular program learning outcome.
Foster public awareness and understanding of computing, related technologies, and the need for ethical behavior in the use of them personally, locally, nationally, and globally.

Describe the assessment of the interconnected program learning outcome(s).
To be determined by department/program faculty

Course Outline:

I. The Internet and Ethical Values
   A. Cyberethics and Code
   B. Iron Cage or Gateway to Utopia?
   C. Ethical Values and the Digital Frontier
   D. Postscript on Moral Theory
   E. Floridi's Macroethics
   F. Normative Principles

II. Information and Power: Regulating and Governing Networked Technologies
   A. The Early History of the Internet
   B. The Internet's Architecture
   C. Net Neutrality
   D. The World Wide Web
   E. Gatekeepers and Search Engines
   F. Social Networking
   G. Internet Governance
   H. Contested Sovereignty in Cyberspace
   I. Internet Monopolies

III. Free Speech and Censorship in Cyberspace
   A. Speech and Internet Architecture
   B. Pornography in Cyberspace
   C. Hate Speech
   D. Online Threats
   E. Anonymous Speech
   F. Government Censorship and the Fate of Political Speech

IV. Intellectual Property in Cyberspace
   A. Background on Intellectual Property
   B. Issues for the Internet and Networking Technologies
   C. Digital Books and E-Books

V. Privacy Rights in the Age of Surveillance
   A. A Definition and Theory of Privacy
   B. Personal Information on the Internet
   C. Consumer Privacy on the Internet
   D. The United States and the European Union: Divergent Paths to Privacy Protection
   E. A Prescription for Privacy?
   F. Privacy in the Workplace

VI. Securing the Digital Infrastructure
- A. Vulnerabilities of Networked Technologies
- B. Cybercrime
- C. Antipiracy Architectures
- D. Trespass, Hackers, and Hacktivism
- E. Security Measures in Cyberspace
- F. CyberSecurity as a Moral Obligation
- G. The Encryption Controversy: A Public Policy Perspective
- H. New Encryption Disputes and Challenges
- I. Encryption Code, Privacy, and Free Speech

Course Activities:

The classroom activities will include formal and informal lectures and discussion sessions. During lectures, new material, assigned readings and case studies will be examined. Students are encouraged to contribute to the discussion and to ask questions about the material.

Course Materials:

Textbook(s): tba

Supplemental Materials: tba

Software Licenses: N/A

Computers: yes

Course Assessment Plan

How often and by what means will the effectiveness of this course as part of the curriculum be assessed?

To be determined by department/program faculty