STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

American Public University System
American Military University | American Public University

ISSC483

Course Summary

Course : ISSC421 **Title :** Computer and Network Security
Length of Course : 8 **Faculty :**
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description:

The Internet's explosive growth and the availability of a myriad of devices that connect each of us with one another using a various mobile network technologies empowering us to great capabilities, has given rise to questioning if any limitations do exist. The manners by which we use our devices for the purposes we desire to accomplish, may also disarm us with what is still unknown to us. Concerning ethical issues, cyber governance, and cyber and privacy policies are eminent to keeping order for a chaotic realm of cyber communications. In this course you will explore some of these policies, the ethical approach and our moral duties in cyber obligations.

Course Scope:

This course exposes students to the concerns about moral behavior in the digital realm. Some of the common mitigations, standards, policies and guidelines are also discussed, and material provides an opportunity for the students to get engaged, think of mitigating techniques, discuss ways of preventing cybercrime, interact with one another and observe the effects of unethical behavior in the cyber world.

Objectives

CO-1:Expose the student to a broad range of ethical dilemmas and issues that are found online. Ensure that the students are able to understand the need for ethical judgement, alternate courses of action, and apply various moral principles to the mobile and wireless communication.

CO-2:Examine ethical dilemmas as they relate to the physical and digital realms. Highlight analogies, differences, and challenges that are posed by the ethical issues in the cyber versus physical realms.

CO-3:Deconstruct the processes used to deal with the ethical issues and enable the student to discern the unethical behaviors online. Students should be able to describe the moral principles that play out in various online situations.

CO-4:Demonstrate major philosophical and social questions as they pertain to the digital realm. Enable the student to deconstruct scenarios and articulate the problem from a moral perspective to find a possible resolution.

CO-5:Expose students to conflicting ethical dilemmas in the realm of digital communications. Apply historical and conceptual logic for the deconfliction of perspective and closure.

CO-6:Assess efficacy of ethical theories from the physical domain and apply to the digital transformation. Apply ethics to the emerging technologies and issues.

CO-7:Discuss various legal and regulatory implications of ethics online and unethical digital behavior. Explore how these regulations relate to the discussed ethical frameworks.

Outline

Week 1:

Learning Outcomes

- LO-1: Learn about various cyber-ethics and how they apply to cyber technologies.
- LO-2: Examine various ethical approaches and discuss the value and shortcomings of each.
- LO-3: Explore perspectives for identifying and resolving cyber related ethical issues.

Required Readings
Assignments

- Discussion Week 1

- Term Paper Topic Selection

Recommended Optional Reading

1. Kalu, C. O., C.L.N., Chidi-Kalu, E., Okidi, I. A. A., C.L.N., & Usiedo, B. A., C.L.N. (2020). Issues on Information Systems, ICTs, Cyber-Crimes, Cyber Security, Cyber Ethics, and National Security in Nigeria: Librarians' Research. *Library Philosophy and Practice,* , 1-19. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fissues-on-information-systems-icts-cyber-crimes%2Fdocview%2F2446728289%2Fse-2
2. Mahmoud, A. N., & Nachouki, M. (2021). Evaluating Students' Cyber Ethics Awareness in a Gender-Segregated Environment Under the Impact of COVID-19 Pandemic. *TEM Journal, 10*(3), 1248-1256. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fevaluating-students-cyber-ethics-awareness-gender%2Fdocview%2F2704013794%2Fse-2
3. States, Stanley. *Security And Emergency Planning For Water And Wastewater Utilities*, American Water Works Association, 2009. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/apus/detail.action?docID=3116692.
4. Dua, Sumeet, and Xian Du. *Data Mining and Machine Learning in Cybersecurity*, Auerbach Publishers, Incorporated, 2011. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/apus/detail.action?docID=5896270.
5. Mian, Q. Z. (2019). Cyber Ethics – Cyber Citizen. *Defence Journal, 23*(5), 21. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fcyber-ethics-citizen%2Fdocview%2F2333755245%2Fse-2%3Faccountid%3D8289
6. C. Grady, S. Rajtmajer and L. Dennis, "When Smart Systems Fail: The Ethics of Cyber–Physical Critical Infrastructure Risk," in IEEE Transactions on Technology and Society, vol. 2, no. 1, pp. 6-14, March 2021, doi: 10.1109/TTS.2021.3058605.
7. *Cybersecurity : Public Sector Threats and Responses*, edited by Kim J. Andreasson, Taylor &

Francis Group, 2011. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/apus/detail.action?docID=826942.

8. Warren, M., Wahlstrom, K., Wigan, M., & Burmeister, O. K. (2020). Preface Ethics in the Cyber Age and exploring emerging themes and relationships between ethics, governance and emerging technologies. *Australasian Journal of Information Systems, 24* https://doi.org/10.3127/ajis.v24i0.2889
9. Ramadhan, A., Dana, I. S., & Arymurthy, A. M. (2011). e-Government Ethics : a Synergy of Computer Ethics, Information Ethics, and Cyber Ethics. *International Journal of Advanced Computer Science and Applications, 2*(8) https://www.proquest.com/docview/2656789652?accountid=8289&parentSessionId=mFnZzTJ3P7UtY9ZsnST1NBcOcRD4rtmDTneOSb8Ec9k%3D&pq origsite=primo
10. Singh, R., & Tiwari, A. K. (2020). A Study on Cyber Ethics Awareness and Social Networking. *Research Journal of Engineering and Technology, 11*(2), 37-40. https://www.proquest.com/docview/2464653041?accountid=8289&parentSessionId=Rxx5f9nlOldi0gY%2BjgkSJLY6TJ2L9I1ibXKTLY8K%2FvE%3D&pc origsite=primo
11. Rajamäki, J., & Hämäläinen, H. (2021). Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES. *Information & Security, 50*(1), 103-116. https://www.proquest.com/docview/2591488644?accountid=8289&parentSessionId=lUNvX%2BoAK3CnBsR%2FEgQCWfmFKHSxS0e1LiauUxQoCeY origsite=primo
12. Omer, Jessica (2021) "Ethics and Cyber Libraries: Challenges Facing the Values and Ethics in LIS," *SLIS Connecting*: Vol. 10: Iss. 1, Article 6. https://aquila.usm.edu/slisconnecting/vol10/iss1/6/
13. Warren, M., & Burmeister, O. (2019). Preface to Research on Applied Ethics (Cybersecurity). *Australasian Journal of Information Systems, 23 https://www.proquest.com/docview/2545734985?accountid=8289&parentSessionId=d7s1V7zvPHz%2BjiXi5i2BV9qwhiCPq9Nfl%2B6R3vi8j5Q%3D& origsite=primo*
14. *Thomas Doty, Esq, LLM (2017). ARTICLE: INFORMATION SECURITY, CONFIDENTIALITY, AND CYBER ETHICS FOR LAW ENTITIES. Northern Kentucky Law Review, 44, 1. https://advance-lexis-com.ezproxy2.apus.edu/api/document?collection=analytical-materials&id=urn:contentItem:67WB-X091-DYRW-V37D-00000-00&context=1516831.*

Recommended Media

Week 2:

Learning Outcomes

- LO-1: Learn basic ethical frameworks and see how they relate to the ethical frameworks that can be found in cybersecurity.
- LO-2: Learn the main frameworks in current discussions on cybersecurity and how they apply to the cyber domain.

Required Readings
Assignments

- Discussion Week 2

Recommended Optional Reading
Recommended Media

Week 3:

Learning Outcomes

- LO-1: Expose the students to the U.S. laws and regulations that govern acceptable internet usage.
- LO-2: Compare U.S. policies on network communications to those of E.U. and other nations.

Required Readings
Assignments

- Discussion Week 3

Recommended Optional Reading
Recommended Media

Week 4:

Learning Outcomes

- LO-1: Expose students to unethical behaviors for a greater good and safety improvement online.
- LO-2: Propose several scenarios such that conflicting values will provide a challenging situation in which compromises must be made to achieve network security.

Required Readings
Assignments

- Discussion Week 4

- Term Paper Outline

Recommended Optional Reading

1. Fry, Erika. 2013. "The 6 Worst Kinds of Computer Hackers." Fortune.com. https://fortune.com/2013/02/26/the-6-worst-kinds-of-computer-hackers/
2. Goodchild, Joan. 2013. "Social Engineering in Penetration Tests: Six Tips for Ethical (and Legal) Use." Computer Security Online. April 23 www.csonline.com/article/2133330/social- engineering
3. Hu, Qing, Zhang, Chenghong, and Xu, Zhengchaun. 2012. "Moral Beliefs, Self-Control and Sports: Effective Antidotes to the Youth Computer Hacking Epidemic." 45th Hawaii International Conference on System Sciences http://ieeexplore.ieee.org/document/6149196/
4. Karakasiliotis, Athanasios, Furnell, Steven, and Papadaki, Maria. 2007. "User Security Awareness of Social Engineering and Phishing," Advances in Network and Communication Engineering, 4: 191–198.
5. Levy, Stephen. 1984. Hackers: Heroes of the Computer Revolution. New York: Penguin Group.

Recommended Media

Week 5:

Learning Outcomes

- LO-1: Explore the world of surveillance and monitoring in the current digital and interconnected world.
- LO-2: Expose students to the various surveillance techniques and discuss the ethics of data gathering methods.
- LO-3: Instigate thoughts and discussions on private company surveillance, ethics and laws associated with the surveillance techniques.

Required Readings
Assignments

- Discussion Week 5

- Assignment 5

Recommended Optional Reading

1. Westacott, Emrys. 2017. “Does Surveillance Make Us Morally Better?” Philosophy Now 79: 6–9. https://philosophynow.org/issues/79/Does_Surveillance_Make_Us_Morally_Better
2. US Legal Dictionary. No Date. “Complicity” (definition). Available online at: https://definitions.uslegal.com/c/complicity/
3. Timan, Tjerk, and Albrechtslund, Anders. 2015. “Surveillance, Self and Smartphones: Tracking Practices in the Nightlife.” Science and Engineering Ethics.
4. Regalado, Antonio. 2013. “Cryptographers Have an Ethics Problem. Mathematicians and Computer Scientists are Involved in Enabling Wide Intrusions on Individual Privacy.” MIT Technology Review. September 13. www.technologyreview.com/s/519281/cryptographers-have-an-ethics- problem/
5. Omand, David. 2013. “NSA Leaks: How to Make Surveillance Both Ethical and Effective.” The Guardian. June 11. Available at: https://www.theguardian.com/commentisfree/2013/jun/11/make-surveill ance-ethical-and-effective

Recommended Media

Week 6:

Learning Outcomes

- LO-1: Discuss the ethical issues of warfare in general, and application of ethical values in cyberwarfare.
- LO-2: Expose students to attributing and labeling malicious activity in cyberspace as cyberwarfare.
- LO-3: Explore possible ethical frameworks that relate to cyberwarfare.

Required Readings
Assignments

- Discussion Week 6

Recommended Optional Reading

1. Waxman, Matthew. 2011. “Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4).” Yale Journal of International Law 36(5): 421–458. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=2654&context=faculty_scholarship
2. Vallor, Shannon. 2013. “The Future of Military Virtue: Autonomous Systems and the Moral Deskilling of the Military.” In Karlis Podins, Markus Maybaum, and Jan Stinissen, eds. 2013 5th Interna- tional Conference on Cyber Conflict. Norfolk, VA: NATO Cooperative Cyber Defense Center of Excellence. https://ieeexplore.ieee.org/document/6568393
3. Stewart, Kenneth. 2013. “Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare.” Naval Postgraduate School. https://nps.edu/-/cyber-security-hall-of-famer-dorothy-denning-discusses-the-ethics-of-cyber-warfare
4. Allhoff, F. (2017). Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare. *Journal of Military Ethics*, *16*(1/2), 124–127. https://doi-org.ezproxy2.apus.edu/10.1080/15027570.2017.1352256

Recommended Media

Week 7:

Learning Outcomes

- LO-1: Discuss ownership of digital property and digital property rights.
- LO-2: Expose students to the conflicting ethical issues in the digital privacy and ownership.
- LO-3: Discuss various vantage points for and against digital property ownership and rights.

Required Readings
Assignments

- Discussion Week 7

Recommended Optional Reading

1. Akman, Ibrahim, and Mishra, Alok. 2009. “Ethical Behavior Issues in Software Use: An Analysis of Public and Private Sectors.” Computers in Human Behavior 25(6): 1251–1257. https://www.sciencedirect.com/science/article/abs/pii/S0747563209001204
2. Bohannon, Mark. 2011. “US Administration’s ‘Technology Neutrality’ Announcement Welcome News.” Opensource.com. January 10. https://opensource.com/government/11/1/us-administrations-technology-neutrality-announcement-welcome-news
3. Chien, S. (2014). Cultural Constructions of Plagiarism in Student Writing: Teachers' Perceptions and Responses. *Research in the Teaching of English, 49*(2), 120-140. http://ezproxy.apus.edu/login?qurl=https%3A%2F%2Fwww.proquest.com%2Fscholarly-journals%2Fcultural-constructions-plagiarism-student-writing%2Fdocview%2F1628065126%2Fse-2%3Faccountid%3D8289
4. Himma, K. (2013). The legitimacy of protecting intellectual property rights: The irrelevance of two conceptions of an information commons. *Journal of Information, Communication & Ethics in Society, 11*(4), 210-232. https://doi.org/10.1108/JICES-10-2013-0041
5. Mancic, Z. (2010). Cyberpiracy and morality: Some utilitarian and deontological challenges. *Filozofija i društvo (Zbornik radova)*, *21*(3), 103–117. https://doi.org/10.2298/FID1003103M
6. Calzarossa, M. C., De Lotto, I., & Rogerson, S. (2010). Ethics and information systems -- Guest editors' introduction. *Information Systems Frontiers, 12*(4), 357-359. https://doi.org/10.1007/s10796-009-9198-4

Recommended Media

Week 8:

Learning Outcomes

- LO-1: Expose students to established and adopted Cyber Professional Codes of Ethics.
- LO-2: Discuss some of the current issues in cyber security in light of everything that students learned over the duration of the course.

Required Readings
Assignments

- Discussion Week8

- Project Paper Due

Recommended Optional Reading

1. Electronic Frontier Foundation. No Date. “About EFF.” www.eff.org/about
2. Busby, J.S. and Coeckelbergh, Mark. 2003. “The Social Ascription of Obligations to Engineers.” Science and Engineering Ethics9(3): 363–376.
3. Halaweh, Mohamed. 2013. “Emerging Technology: What Is It?” Journal of Technology Management and Innovation 8(3): 108–115.
4. Levy, Yair, Ramim, Michelle, and Hackney, Raymond. 2013. “Assessing Ethical Severity of e-Learning Systems Security Attacks.” The Journal of Computer Information Systems 53(3): 75–84.
5. Swierstra, Tsjalling. 2015. “Identifying the Normative Challenges Posed by Technology’s ‘Soft’ Impacts.” Nordic Journal of Applied Ethics 9(1): 5–20.

Recommended Media

Evaluation

Forum discussions: 40%

Each week, a discussion question is provided and posts should reflect assimilation of the readings. Students are required to provide a substantive initial post by Thursday at 11:55 pm ET and respond to 2 or more classmates by Sunday 11:55 pm ET. Forum posts are graded on timeliness, relevance, knowledge of the weekly readings, and the quality of original ideas.

Assignment: 40%

There are threee assginments that walk the student towards the Final CAPSTONE project. Three assignments have equal weight totdaling to 40% of the final grade.

Final assignment: 20%

A 15-20 page essay. Specific instructions found in the Assignments tab of the classroom. The six-page essay assignment is actually two questions answered in 3 to 4 pages each and each addresses the issue in CO.

Grading:

Name	Grade %
Discussions	40.00%
Welcome Discussion	4.44%
Week 1: Values and Value Conflicts in Cybersecurity	4.44%
Week 2: Ethical Frameworks	4.44%
Week 3: Cybersecurity Laws Regulations and Government Agencies	4.44%
Week 4: Is All Malicious Activity Unethical?	4.44%
Week 5: The Ethics of Surveillance	4.44%
Week 6: Conflicts in Cyberspace	4.44%
Week 7: Property Rights in the Digital Realm	4.44%
Week 8: Cyber Ethics for Cyber Professionals	4.44%
Assignments	40.00%
Capstone Project Selection	13.33%
Tem Paper Outline	13.33%
Week #5 Assignment - Resolve an Ethical Dilemma	13.33%
FInal Project	20.00%
Final Capstone Project & Presentation	20.00%

Materials

Book Title: The Ethics of Cybersecurity - eBook available online, link provided inside the classroom eReserve

Author: Christen, Gordijn, Loi

Publication Info: Springer Lib

Course Guidelines

Citation and Reference Style

- Attention Please: Students will follow the APA Format as the sole citation and reference style used in written work submitted as part of coursework to the University. Assignments completed in a narrative essay or composition format must follow the citation style cited in the APA Format.

Tutoring

- Tutor.com offers online homework help and learning resources by connecting students to certified tutors for one-on-one help. AMU and APU students are eligible for 10 free hours* of tutoring provided by APUS. Tutors are available 24/7 unless otherwise noted. Tutor.com also has a SkillCenter Resource Library offering educational resources, worksheets, videos, websites and career help. Accessing these resources does not count against tutoring hours and is also available 24/7. Please visit the APUS Library and search for 'Tutor' to create an account.

Late Assignments

- Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. The due date for each assignment is listed under each Assignment.
- Generally speaking, late work may result in a deduction up to 15% of the grade for each day late, not to exceed 5 days.
- As a working adult I know your time is limited and often out of your control. Faculty may be more flexible if they know ahead of time of any potential late assignments.

Turn It In

- Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. This is automatically processed through the Assignments area of the course.

Academic Dishonesty

- Academic Dishonesty incorporates more than plagiarism, which is using the work of others without citation. Academic dishonesty includes any use of content purchased or retrieved from web services such as CourseHero.com. Additionally, allowing your work to be placed on such web services is academic dishonesty, as it is enabling the dishonesty of others. The copy and pasting of content from any web page, without citation as a direct quote, is academic dishonesty. When in doubt, do not copy/paste, and always cite.

Submission Guidelines

- Some assignments may have very specific requirements for formatting (such as font, margins, etc) and submission file type (such as .docx, .pdf, etc) See the assignment instructions for details. In general, standard file types such as those associated with Microsoft Office are preferred, unless otherwise specified.

Disclaimer Statement

- Course content may vary from the outline to meet the needs of this particular group.

Communicating on the Forum

- Forums are the heart of the interaction in this course. The more engaged and lively the exchanges, the more interesting and fun the course will be. Only substantive comments will receive credit. Although there is a final posting time after which the instructor will grade comments, it is not sufficient to wait until the last day to contribute your comments/questions on the forum. The purpose of the forums is to actively participate in an on-going discussion about the assigned content.
- “Substantive” means comments that contribute something new and hopefully important to the discussion. Thus a message that simply says “I agree” is not substantive. A substantive comment contributes a new idea or perspective, a good follow-up question to a point made, offers a response to a question, provides an example or illustration of a key point, points out an inconsistency in an argument, etc.
- As a class, if we run into conflicting view points, we must respect each individual's own opinion. Hateful and hurtful comments towards other individuals, students, groups, peoples, and/or societies will not be tolerated.

Communications

Student Communication

To reach the instructor, please communicate through the MyClassroom email function accessible from the Classlist of the Course Tools menu, where the instructor and students email addresses are listed, or via the Office 365 tool on the Course homepage.

- In emails to instructors, it’s important to note the specific course in which you are enrolled. The name of the course is at the top center of all pages.
- Students and instructors communicate in Discussion posts and other learning activities.
- All interactions should follow APUS guidelines, as noted in the Student Handbook, and maintain a professional, courteous tone.
- Students should review writing for spelling and grammar.
- Tips on Using the Office 365 Email Tool

Instructor Communication

The instructor will post announcements on communications preferences involving email and Instant Messaging and any changes in the class schedule or activities.

- Instructors will periodically post information on the expectations of students and will provide feedback on assignments, Discussion posts, quizzes, and exams.
- Instructors will generally acknowledge student communications within 24 hours and respond within 48 hours, except in unusual circumstances (e.g., illness).
- The APUS standard for grading of all assessments (assignments, Discussions, quizzes, exams) is five days or fewer from the due date.
- Final course grades are submitted by faculty no later than seven days after the end date of the course or the end of the extension period.

University Policies

Consult the Student Handbook for processes and policies at APUS. Notable policies:

- Drop/Withdrawal Policy
- Extension Requests
- Academic Probation

- Appeals
- Academic Dishonesty / Plagiarism
- Disability Accommodations
- Student Deadlines
- Video Conference Policy

Mission

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.

Minimum Technology Requirements

- Please consult the catalog for the minimum hardware and software required for undergraduate and graduate courses.
- Although students are encouraged to use the Pulse mobile app with any course, please note that not all course work can be completed via a mobile device.

Disclaimers

- Please note that course content – and, thus, the syllabus – may change between when a student registers for a course and when the course starts.
- Course content may vary from the syllabus' schedule to meet the needs of a particular group.